Politique et Pratiques

du service

Goodflag eIDAS qualified timestamp 2

Version 1.1

Date d’entrée en vigueur : 25/09/2026

Tous droits réservés

9 Av Maréchal Leclerc - 10120 ST ANDRE LES VERGERS - FRANCE
Tél. : +33 (0)3 25 43 90 78 – www.goodflag.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 4
1.1 Présentation générale 4
1.2 Définitions 4
1.3 Acronymes 6
1.4 Gestion du document 6
1.4.1 Identification du service 6
1.4.2 Identification du document 6
1.4.3 Déclaration de conformité 7
1.4.4 Entité gérant la PH – Point de contact 7
1.4.5 Amendement du document 7
1.4.6 Procédure d'approbation 8
1.4.7 Publication et consultation 8
1.5 Principe du service d'horodatage qualifié 8
1.6 Documents associés 9
1.6.1 Documents normatifs 9
1.6.2 Conditions Générales d'Utilisation 12
1.6.3 Politique Générale des Services de Confiance 12
1.6.4 Politique de Certification 12
2 Politique d'horodatage 12
3 Déclaration des Pratiques d'Horodatage 12
4 Conditions Générales d'Utilisation du service d'horodatage 13
5 Parties prenantes et obligations 14
5.1 Obligations de l'AH 14
5.2 Obligations pour l'AC fournissant les certificats des UH 15
5.3 Obligations de l'Abonné 15
5.4 Obligations de l'Utilisateur 16
6 Responsabilités concernant la mise à disposition des informations devant être publiées 16
6.1 Entités chargées de la mise à disposition des informations 16
6.2 Informations devant être publiées 16
6.3 Délais et fréquences de publication 16
6.4 Contrôle d'accès aux informations publiées 16
7 Gestion des risques 16
8 Exigences opérationnelles 17
8.1 Organisation interne 17
8.1.1 Fiabilité 17
8.1.2 Rôles de confiance 17
8.2 Ressources humaines 17
8.3 Gestion des actifs 17
8.4 Contrôle d'accès 17
8.5 Cryptographie 17
8.5.1 Génération de clé des UH 17
8.5.2 Certification des clés des UH 17
8.5.3 Protection des clés privées des UH 18
8.5.4 Destruction des clés des UH 18
8.5.5 Exigences de sauvegarde des clés des UH 18
8.6 Horodatage 19
8.6.1 Gestion des requêtes d'horodatage 19

8.6.2 Synchronisation de l'horloge 20
8.7 Sécurité physique et environnementale 21
8.8 Sécurité opérationnelle 21
8.9 Sécurité réseau 21
8.10 Gestion des incidents 21
8.11 Procédure de constitution des données d'audit 22
8.12 Archivage des données 23
8.13 Continuité d'activité 23
8.14 Fin de vie 23
8.15 Conformité 24
9 Exigences de sécurité techniques 24
9.1 Exactitude temps 24
9.2 Algorithmes obligatoires 24
9.3 Durée de validité des certificats de clé publique des UH 24
9.4 Durée d'utilisation des clés privées des UH 24
9.5 Renouvellement des bi-clés des UH 25
10 Profil des certificats et Jetons d'horodatage 25
10.1 Format du certificat des UH émis par l'AC ST 25
10.2 Format des Jetons d'horodatage 26
11 Audit de conformité et autres évaluations 27
12 Autres problématiques métiers et légales 27
12.1 Tarifs 27
12.1.1 Tarifs pour la fourniture de jetons d'horodatage 27
12.1.2 Tarifs pour accéder aux Certificats 27
12.1.3 Tarifs pour accéder aux informations d'état et de révocation des Certificats 27
12.1.4 Tarifs pour d'autres services 27
12.1.5 Politique de remboursement 27
12.2 Responsabilité financière 28
12.2.1 Couverture par les assurances 28
12.2.2 Autres ressources 28
12.2.3 Couvertures et garantie concernant les entités utilisatrices 28
12.2.4 Confidentialité des données professionnelles 28
12.3 Protection des données personnelles 28
12.4 Droits sur la propriété intellectuelle et industrielle 28
12.5 Interprétations contractuelles et garanties 28
12.6 Limite de garantie 28
12.7 Limite de responsabilité 28
12.8 Indemnités 29
12.9 Durée et fin anticipée de validité de la PH/DPH 29
12.10 Notification individuelles et communications entre les participants 29
12.11 Amendements 29
12.12 Dispositions concernant la résolution de conflits 29
12.13 Juridictions compétentes 29
12.14 Conformité aux législations et réglementations 29
12.15 Dispositions diverses 29
12.16 Autres dispositions 29

Copyright Goodflag 2026

1 Introduction

1.1 Présentation générale

Au début de l'année 2025, la société Lex Persona a adopté le nom commercial Goodflag. En revanche, toutes les références techniques et organisationnelles, telles que les gabarits des Certificats, les Certificats d'AC, l'organe de gouvernance de l'AC, etc., conservent le nom Lex Persona et sont toujours en vigueur.

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 qualifiés, 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_319_421]) et l'AH met en œuvre des jetons respectant les profils décrits dans [ETSI_319_422].

En sus et dans le cadre de la qualification eIDAS de son service d'horodatage en France, l'AH se conforme également aux exigences prévues par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) dans les référentiels suivants :

- [ANSSI_PSCO] ;
- [ANSSI_HOR].

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 définit également des Conditions Générales d'Utilisation (CGU) correspondant au « TSA Disclosure Statement » défini dans l'annexe B de [ETSI_319_421]. Ces CGU sont mises à la disposition des Abonnés et des Utilisateurs (cf. 6.2).

1.2 Définitions

Abonné : Entité légale, ayant contracté avec Lex Persona / Goodflag 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.

Empreinte : Résultat d'une fonction cryptographique non réversible appliquée sur une donnée qui fournit une représentation de taille fixe et limitée de cette donnée.

Jeton d'horodatage : Donnée signée qui lie l'empreinte 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.460-6 [TF.460-6].

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 proposés par Lex Persona à ses clients.

Lex Persona Trust Service Provider Board (LPTSP Board) : Comité de direction du LPTSP.

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) : Échelle de temps réalisée par le laboratoire « k » et maintenue en accord étroit avec le temps UTC, avec pour objectif d'atteindre ±100 ns. La liste des laboratoires disposant d'une réalisation UTC(k) reconnue figure au chapitre 1 de la Circulaire T diffusée par le BIPM [BIPM_T].

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.

Copyright Goodflag 2026

1.3 Acronymes

Acronyme	Description
AC	Autorité de Certification
AC ST	Autorité de Certification de l'AC « Sunnystamp Timestamping »
AH	Autorité d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
BTSP	Best practices Time-Stamp Policy
CGU	Conditions Générales d'Utilisation
DN	Distinguished Name
DPH	Déclaration des Pratiques d'Horodatage
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
LCR	Liste des Certificats Révoqués
LPTSP	Lex Persona Trust Service Provider
OCSP	Online Certificate Status Protocole
OID	Object Identifier
PC	Politique de Certification
PGSC	Politique Générale des Services de Confiance
PH	Politique d'Horodatage
QCP	Qualified Certificate Profile
UC	Utilisateur de Certificat
UH	Unité d'Horodatage
UTC	Coordinated Universal Time

1.4 Gestion du document

1.4.1 Identification du service

Le service d'horodatage « Goodflag eIDAS qualified timestamp 2 » est identifié par l'identifiant d'objet (OID) 1.3.6.1.4.1.22542.100.2.2.

1.4.2 Identification du document

La présente politique d'horodatage de « Goodflag eIDAS qualified timestamp 2 » est identifiée par l'identifiant d'objet (OID) **1.3.6.1.4.1.22542.100.2.2.1.**

La présente PH est conforme à la politique BTSP de l'ETSI, identifiée par l'OID 0.4.0.2023.1.1 [ETSI_319_421].

Les valeurs d'OID peuvent être amenées à évoluer ou à être complétées dans le cadre de l'évolution de l'offre de services, sous le contrôle du Lex Persona Trust Service Provider Board (LPTSP Board).

Toute modification majeure de la politique d'horodatage fait l'objet d'une mise à jour du présent document, du dernier indice de son OID et d'une publication dans le dépôt d'informations officielles de Lex Persona. L'OID de la présente politique permet aux Clients, aux auditeurs, aux

Copyright Goodflag 2026

autorités de supervision et aux parties tierces de se référer précisément au corpus de règles qui encadre le service.

1.4.3 Déclaration de conformité

Le service d'horodatage Goodflag eIDAS qualified timestamp 2 est un service de confiance d'horodatage qui s'appuie notamment :

- Sur le service « Sunnystamp Timestamping CA » de délivrance des certificats des UH, conforme à la norme [ETSI_319_411-2] au niveau QCP-l, incluant les exigences NCP+ de [ETSI_319_411-1]

1.4.4 Entité gérant la PH – Point de contact

LEX PERSONA
9 AVENUE MARECHAL LECLERC
10120 ST-ANDRE-LES-VERGERS
FRANCE
Courriel : pki@sunnystamp.com
Téléphone : +33 (0)3 25 43 90 78

1.4.5 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.

1.4.5.1 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.

1.4.5.2 Circonstances selon lesquelles l'OID doit être changé

L'OID du Service (cf. 1.4.1), porté dans le champ policy des Jetons d'horodatage, demeure inchangé pendant toute la durée de vie du Service ; toute révision de la présente PH fait évoluer le dernier indice de l'OID du document (cf. 1.4.2), la version opposable à un Jeton étant celle en vigueur à la date de son genTime. Seule une évolution des engagements opposables du Service

Copyright Goodflag 2026

justifierait un changement de l'OID, afin que les Abonnés et les Utilisateurs puissent clairement identifier les exigences applicables aux Jetons d'horodatage.

1.4.6 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.

1.4.7 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.

L'ensemble des informations associées notamment les versions antérieures de ces documents, les certificats des UH sont également publiées sur le site https://tsa2.sunnystamp.com/repository.
La plage de service de ce site est 24h/24 et 7j/7.

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 Principe du service d'horodatage qualifié

Une contremarque de temps permet d'attester de la réalité, à une date et une heure donnée, de l'existence d'une empreinte numérique (ou « hash ») qui est soumise au service d'horodatage.

Les contremarques de temps sont délivrées et signées électroniquement par l'AH à l'aide d'Unité(s) d'Horodatage.

La garantie de cette association est fournie au moyen d'une contremarque de temps qui est une structure signée qui contient en particulier :

- La valeur de hachage et l'algorithme de hachage de la donnée qui a été horodatée ;
- La date et le temps universel (UTC) ;
- L'identifiant du certificat de l'UH qui a généré la contremarque de temps ;
- L'identifiant de Lex Persona en tant qu'AH (inclus dans le certificat d'horodatage) ;

- L'identifiant de l'Autorité de Certification ayant signé les clés privées installées sur les unités d'horodatage.

Dans le cadre de cette PH, la date et le temps de chaque contremarque de temps sont synchronisés avec le temps UTC avec une précision de 1 seconde. La présente PH applique un format de contremarque de temps standard défini par le [RFC 3161]. La gestion de la synchronisation de l'horloge du service d'horodatage garantit la maîtrise d'une dérive du temps inférieure à 1 seconde.

1.6 Documents associés

1.6.1 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://cyber.gouv.fr/reglementation/reglementation-identite-confiance-numerique/securite-echanges-voie-electronique/reglement-eidas/la-liste-nationale-de-confiance/
[BIPM_T]	Circulaire T du Bureau International des Poids et Mesures, qui identifie notamment les laboratoires disposant d'une réalisation UTC(k) reconnue. https://www.bipm.org/
[ETSI_119_312]	ETSI TS 119 312 V2.1.1 (2026-06) Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites. https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/02.01.01_60/ts_119312v020101p.pdf
[ETSI_119_615]	ETSI TS 119 615 V1.4.1 (2026-05) Electronic Signatures and Infrastructures (ESI); Trusted lists; Procedures for using and interpreting European Union Member States national trusted lists. https://www.etsi.org/deliver/etsi_ts/119600_119699/119615/01.04.01_60/ts_119615v010401p.pdf

Copyright Goodflag 2026

[ETSI_319_102] ETSI EN 319 102-1 V1.4.1 (2024-06) 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_319199/31910201/01.04.01_60/en_31910201v010401p.pdf

[ETSI_319_401] ETSI EN 319 401 V3.2.1 (2026-01) Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
https://www.etsi.org/deliver/etsi_en/319400_319499/31940103.02.01_60/en_319401v030201p.pdf

[ETSI_319_411-1] ETSI EN 319 411-1 V1.5.1 (2025-04) Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates. Part 1: General requirements.
https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.05.01_60/en_31941101v010501p.pdf

[ETSI_319_411-2] ETSI EN 319 411-2 V2.6.1 (2025-06)
Policy and security requirements for Trust Service Providers issuing certificates.
Part 2: Requirements for trust service providers issuing EU qualified certificates
https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.06.01_60/en_31941102v020601p.pdf

[ETSI_319_412-1] ETSI EN 319 412-1 V1.6.1 (2025-06) Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
https://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.06.01_60/en_31941201v010601p.pdf

[ETSI_319_412-3] ETSI EN 319 412-3 V1.4.1 (2026-07) Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
https://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.04.01_60/en_31941203v010401p.pdf

[ETSI_319_412-5] ETSI EN 319 412-5 V2.6.1 (2026-05) Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
https://www.etsi.org/deliver/etsi_en/319400_319499/31941205/02.06.01_60/en_31941205v020601p.pdf

Copyright Goodflag 2026

[ETSI_319_421] ETSI EN 319 421 V1.3.1 (2025-07) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.03.01_60/en_319421v010301p.pdf

[ETSI_319_422] 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 (UE) N° 910/2014 du Parlement Européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, tel que modifié par la Directive (UE) 2022/2555 et par le Règlement (UE) 2024/1183.

[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

[TF.460-6] Recommandation ITU-R TF.460-6 (2002) – Standard-frequency and time-signal emissions.

Copyright Goodflag 2026

1.6.2 Conditions Générales d'Utilisation

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

1.6.3 Politique Générale des Services de Confiance

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

1.6.4 Politique de Certification

[PC_ST] Politique de Certification de l'AC « Sunnystamp Timestamping CA » délivrant les certificats des UH au niveau QCP-l de [ETSI_319_411-2].
https://pki2.sunnystamp.com/repository

2 Politique d'horodatage

Pour cette politique, la date et le temps de chaque contremarque de temps doivent être synchronisés avec le temps UTC avec une exactitude de 1 seconde.

La présente PH impose un format de contremarque de temps spécifique, qui doit répondre aux exigences du chapitre 10 ci-dessous.

Cette politique impose l'usage d'un protocole d'horodatage spécifique pour demander et obtenir une contremarque de temps auprès d'une AH définie dans la [RFC_3161] et profilée dans le document [ETSI_319_422].

Les caractéristiques principales de cette politique sont les suivantes :

- La protection des clés et de l'horloge doit respecter les exigences spécifiées au chapitre 8.5.3 ci-dessous ;
- La clé privée d'une UH n'est ni séquestrée ni archivée ;
- L'AC générant les certificats de clé publique pour les unités d'horodatage doit gérer le service de révocation pour chaque certificat publié.

3 Déclaration des Pratiques d'Horodatage

La déclaration des pratiques d'horodatage expose les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la politique d'horodatage, en particulier les processus que l'AH emploie pour la création des contremarques de temps et le maintien de l'exactitude de ses horloges.

La déclaration des pratiques d'horodatage est une description détaillée des pratiques opérationnelles de l'AH mises en œuvre pour la délivrance des contremarques de temps et la gestion des services d'horodatage.

La déclaration des pratiques d'horodatage définit comment l'Autorité d'horodatage se conforme aux exigences physiques, environnementales, procédurales, organisationnelles et techniques identifiées dans la présente politique d'horodatage.

Le présent document constitue la Politique d'Horodatage et la Déclaration des Pratiques d'Horodatage (PH/DPH) de l'AH.

Les procédures internes propres à la Déclaration des Pratiques d'Horodatage (DPH) sont confidentielles et ne sont pas exposées dans ce document.

4 Conditions Générales d'Utilisation du service d'horodatage

Les conditions générales d'utilisation ne sont pas destinées à remplacer la politique d'horodatage mais sont destinées à des abonnés et à des utilisateurs de contremarques de temps non-techniciens afin qu'ils puissent facilement comprendre l'information essentielle dont ils doivent avoir connaissance.

Les conditions générales d'utilisation peuvent aider une Autorité d'horodatage à démontrer comment elle répond aux exigences réglementaires, en particulier celles liées à la protection du consommateur.

L'Autorité d'horodatage publie également dans des Conditions Générales d'Utilisation du service d'horodatage les parties suivantes :

- Le cadre d'application des CGU et le contexte global des engagements de l'AH via la PH/DPH ;
- Les coordonnées de l'AH ;
- Les types et le cadre d'utilisation des contremarques de temps en précisant notamment :
  - La précision de la date des contremarques de temps par rapport à l'échelle de temps UTC ;
  - Les algorithmes de hachage autorisés pour constituer l'objet horodaté ;
  - La durée minimum pendant laquelle il est possible de vérifier les contremarques de temps, à compter de leur date de génération ;
- Les limites de confiance, notamment :
  - Les engagements sur la précision des jetons ;
  - Les durées de conservation des traces ;
- Les obligations des abonnés ;
- Les obligations des utilisateurs de contremarque de temps pour permettre la vérification des jetons, notamment :
  - Les informations permettant de vérifier la contremarque de temps ;
  - Les modes opératoires envisageables pour vérifier les jetons ;

Copyright Goodflag 2026

- Les limitations de responsabilité et les garanties de l'AH ;
- La PH et la DPH appliquée ;
- Les règles appliquées en matière de protection des informations confidentielles ;
- Les règles appliquées en termes d'assurance de l'AH ;
- Les lois applicables et les règles de règlement des litiges ;
- Les points de publication des documents de l'AH, les niveaux de certifications et les audits obtenus par l'AH.

L'Autorité d'horodatage définit ses propres conditions générales d'utilisation et les rend disponibles aux abonnés et aux utilisateurs de contremarques de temps sous une forme lisible, compréhensible et pérenne.

Elles peuvent être téléchargées sur le site indiqué au chapitre 1.4.7.

5 Parties prenantes et obligations

5.1 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 émis, selon les modalités indiquées dans la présente PH (cf. 6.2) ;
- 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 des [PC_ST] des AC émettrices de ces certificats ;
- Authentifier les demandes de Jetons d'horodatage soumises par les Abonnés à l'AH ;

Copyright Goodflag 2026

- Garantir qu'elle mettra à jour la PH en cas de changements majeurs des pratiques d'horodatage de son service ;
- Assurer la communication auprès de l'ANSSI, notamment dans le cas d'incidents de sécurité critiques ;
- 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.

5.2 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 selon [ETSI_319_411-2] au niveau QCP-l, incluant les exigences NCP+ de [ETSI_319_411-1].

Cette AC décrit les exigences qu'elle respecte dans [PC_ST] et 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 de sa Politique de Certification [PC_ST] ;
- 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.

5.3 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.

Copyright Goodflag 2026

5.4 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. 8.6.1.2) et de tenir compte des limitations, indiquées dans la présente PH et dans les CGU, sur l'utilisation des Jetons d'horodatage.

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

6.1 Entités chargées de la mise à disposition des informations

Voir chapitre 2 de la [PGSC].

6.2 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 ;
- Les éléments publics archivés, notamment les anciennes versions des PH/DPH et les anciens certificats des UH.

6.3 Délais et fréquences de publication

Voir chapitre 2 de la [PGSC].

6.4 Contrôle d'accès aux informations publiées

Voir chapitre 2 de la [PGSC].

7 Gestion des risques

Voir chapitre 3 de la [PGSC].

L'analyse des risques intègre notamment dans les menaces celles qui peuvent atteindre la gestion de l'horloge interne du service d'horodatage, les impacts d'une non-détection d'une anomalie sur l'horloge interne.

Les résultats de l'analyse de risques font apparaître les modalités de sécurisation des systèmes liés à l'horodatage.

8 Exigences opérationnelles

8.1 Organisation interne

8.1.1 Fiabilité

Voir chapitre 7.2 de la [PGSC].

8.1.2 Rôles de confiance

Voir chapitre 4.2 de la [PGSC].

8.2 Ressources humaines

Voir chapitre 4.3 de la [PGSC].

8.3 Gestion des actifs

Voir chapitre 4.1 de la [PGSC].

Les actifs liés au service d'horodatage sont considérés comme des actifs sensibles, cela comprend notamment les composants support à l'application d'horodatage, aux composants cryptographiques assurant la sécurité des clés privées des UH, les composants en support de la synchronisation du temps délivré par le service d'horodatage dans ses jetons.

8.4 Contrôle d'accès

Voir chapitre 5.2 de la [PGSC].

8.5 Cryptographie

8.5.1 Génération de clé des UH

L'AH garantit que les clés cryptographiques des UH sont produites dans des circonstances et dans un environnement contrôlé par Lex Persona, 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, dont elles ne sortent que pour l'opération de duplication décrite au chapitre 8.5.5. La longueur des clés des UH est d'au moins 3072 bits avec l'algorithme RSA.

8.5.2 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 1.6.4.

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 unique (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.

8.5.3 Protection des clés privées des UH

Les clés privées des UH sont stockées dans des HSM certifiés CC EAL4+.

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.

8.5.4 Destruction des clés des UH

Les clés privées des UH sont détruites dès la fin de leur durée d'utilisation (cf. 9.4).

8.5.5 Exigences de sauvegarde des clés des UH

Les clés privées des UH ne sont ni séquestrées ni archivées. Elles sont uniquement dupliquées, une seule fois après leur génération, vers un second HSM aux fins de haute disponibilité : l'opération est réalisée dans un environnement sécurisé sous le contrôle d'au moins deux porteurs de secrets, la clé est chiffrée par le HSM avant toute sortie, le fichier de transfert est détruit dès l'import terminé et les deux instances sont associées au même certificat.

Copyright Goodflag 2026

8.6 Horodatage

8.6.1 Gestion des requêtes d'horodatage

8.6.1.1 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 minimum 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 fixée à 1 seconde ;
- Le « nonce » (dans le cas où il a été renseigné dans la requête) ;
- L'extension `esi4-qtstStatement-1` 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.

8.6.1.2 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 5.4).

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'AC qui a délivré le certificat d'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://eidas.ec.europa.eu/efda/tl-browser/#/screen/home) ;
- 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 vérifié par l'application de vérification de signature utilisée conformément à [ETSI_319_102]. 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 restent vérifiables au-delà de la période de validité des certificats des UH émettrices, l'AC maintenant l'information de statut de révocation de ces certificats après leur expiration.

8.6.2 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.

Les mesures de sécurité autour de la synchronisation du temps au sein du service d'horodatage sont détaillées dans le chapitre 9.1

8.7 Sécurité physique et environnementale

Voir chapitre 4 de la [PGSC].

8.8 Sécurité opérationnelle

Voir chapitre 4 de la [PGSC].

L'AH définit en sus les rôles de confiance spécifiques suivants :

- Des administrateurs des boîtiers de temps, en charge d'assurer les opérations d'administration et de maintien en conditions de sécurité de ces boîtiers
- Des administrateurs des équipements cryptographiques hébergeant les clés privées des UH
- Des porteurs de secrets pour l'accès aux opérations sensibles sur le boîtier cryptographique stockant les clés privées des unités d'horodatage. Le regroupement d'un sous-ensemble de ces porteurs est nécessaire pour la réalisation de ces opérations.

8.9 Sécurité réseau

Voir chapitre 5.4 de la [PGSC].

8.10 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

Copyright Goodflag 2026

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. Par mesure de précaution, l'AH :
   a. Déclenche l'arrêt immédiat des services du service d'horodatage ;
   b. Informe l'ensemble des parties concernées ;
   c. Notifie l'ANSSI (https://cyber.gouv.fr) sans délai et au plus tard dans les 24 heures suivant la prise de connaissance de l'événement, conformément à l'article 19.2 de [EIDAS].

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.

La compromission de l'AH peut être due :

- Au vol des serveurs des unités d'horodatage ;
- Au vol des clés privées des UH ;
- A la compromission de la clé privée de l'AC ayant servi à générer les certificats des UH. Dans ce cas, la procédure mise en place est détaillée dans [PC_ST].

8.11 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.

Copyright Goodflag 2026

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

Les traces sont protégées en intégrité et en confidentialité.

8.12 Archivage des données

Voir chapitre 4.5 de la [PGSC].

Les données à archiver sont les suivantes :

- PH/DPH et CGU ;
- Les accords contractuels entre l'AH et les Abonnés ;
- Les Certificats des unités d'horodatage et LCR publiés ;
- Journaux d'événements ;
- Les rapports d'audit.

Ces archives sont conservées pendant toute la durée de vie de l'AH à l'exception des journaux d'événements qui sont conservés pendant 7 ans après l'expiration du Certificat d'UH.

8.13 Continuité d'activité

Voir chapitre 4.6 de la [PGSC].

8.14 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 identifié sur le site https://cyber.gouv.fr ;
- 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.

8.15 Conformité

Voir chapitre 6 de la [PGSC].

9 Exigences de sécurité techniques

9.1 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).

9.2 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 3072 bits et l'algorithme de signature des Jetons d'horodatage utilise une fonction de hachage SHA256.

9.3 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 maximum.

9.4 Durée d'utilisation des clés privées des UH

La durée d'utilisation des clés privées des UH est limitée à 2 ans, valeur portée dans l'extension PrivateKeyUsagePeriod du certificat de l'UH, afin de faciliter la vérification des Jetons d'horodatage grâce à une période adéquate de validité du certificat.

9.5 Renouvellement des bi-clés des UH

Les certificats des UH ne font l'objet ni d'un renouvellement ni d'une re-clé : conformément à la [PC_ST], tout nouveau certificat d'UH résulte d'une demande initiale complète portant sur une nouvelle bi-clé.

L'AH met en œuvre les procédures nécessaires pour qu'une nouvelle bi-clé soit générée et certifiée avant l'échéance de la durée d'utilisation de la clé privée en service :

- L'AH surveille l'échéance de la durée d'utilisation de la clé privée de chaque UH en service ;
- Une nouvelle bi-clé est générée dans les conditions décrites au chapitre 8.5.1, puis une demande initiale de certificat est adressée à l'AC dans les conditions décrites au chapitre 8.5.2 ;
- La nouvelle UH est mise en service après les vérifications décrites au chapitre 8.5.2, en recouvrement avec l'UH sortante afin d'assurer la continuité du Service ;
- L'UH sortante cesse d'émettre des Jetons d'horodatage au plus tard à l'échéance de la durée d'utilisation de sa clé privée ;
- L'ensemble des instances de la clé privée sortante est détruit dans les conditions décrites au chapitre 8.5.4.

Le certificat de l'UH sortante n'est pas révoqué : il reste publié et son statut de révocation reste disponible jusqu'à son expiration et au-delà, afin de permettre la vérification des Jetons d'horodatage déjà émis.

10 Profil des certificats et Jetons d'horodatage

10.1 Format du certificat des UH émis par l'AC ST

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 Timestamping CA OI = NTRFR-480622257 OU=0002 480622257 O = LEX PERSONA C = FR
Sujet	CN = **ClientName** TSU**XX** eIDAS qualified timestamp 2 *(où* **ClientName** *est le nom de l'entité et* ***XX*** *est l'identifiant de l'UH allant de 01 à 99)* serialNumber = Identifiant unique généré par l'AC OI = NTRFR-480622257

Copyright Goodflag 2026

	O = LEX PERSONA C = FR
Validité	3 ans maximum
Signature	SHA256withRSA
Clé publique	RSA 3072 bits

Extensions :

Champ	Critique	Valeur
AuthorityInfoAccess	Non	id-ad-caIssuers= https://pki2.sunnystamp.com/certs/sunnystamp-timestamping-ca.cer id-ad-ocsp= http://ocsp2.sunnystamp.com/sunnystamp-timestamping-ca
AuthorityKeyIdentifier	Non	Empreinte SHA1 de la clé publique de l'émetteur
BasicConstraints	Oui	cA=false
CertificatePolicies	Non	OID=0.4.0.194112.1.1 (QCP-l) OID=1.3.6.1.4.1.22542.100.1.1.4.2 URL=https://pki2.sunnystamp.com/repository
CRLDistributionPoints	Non	http://pki2.sunnystamp.com/crls/sunnystamp-timestamping-ca.crl http://pki3.sunnystamp.com/crls/sunnystamp-timestamping-ca.crl
ExtendedKeyUsage	Oui	id-kp-timeStamping
Key Usage	Oui	digitalSignature, nonRepudiation
PrivateKeyUsagePeriod	Non	notAfter = date de génération du certificat + 2 ans (cf. 9.4)
qcStatements	Non	esi4-qcStatement-1 (QcCompliance) esi4-qcStatement-6 (QcType = id-etsi-qct-eseal)
SubjectKeyIdentifier	Non	Empreinte SHA1 de la clé publique du sujet

10.2 Format des Jetons d'horodatage

Les Jetons d'horodatage, conformes à la norme [RFC_3161] et au profil [ETSI_319_422], 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)

Copyright Goodflag 2026

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-qtstStatement-1`

11 Audit de conformité et autres évaluations

Voir chapitre 6 de la [PGSC].

12 Autres problématiques métiers et légales

12.1 Tarifs

12.1.1 Tarifs pour la fourniture de jetons d'horodatage

L'AH peut appliquer un tarif sur la délivrance de jetons d'horodatage.

12.1.2 Tarifs pour accéder aux Certificats

Les Certificats de la chaîne de confiance incluant le certificat de l'AC et des UH sont mis à disposition des Utilisateurs gratuitement via le site de publication de l'AH et de l'AC.

12.1.3 Tarifs pour accéder aux informations d'état et de révocation des Certificats

L'accès aux informations d'état de révocation des Certificats, délivrés par l'AC à travers les LCR qu'elle publie et les réponses OCSP qu'elle produit, est gratuit.

12.1.4 Tarifs pour d'autres services

Sans objet.

12.1.5 Politique de remboursement

Sans objet.

Copyright Goodflag 2026

12.2 Responsabilité financière

12.2.1 Couverture par les assurances

Voir chapitre 7.2 de la [PGSC].

12.2.2 Autres ressources

Voir chapitre 7.2 de la [PGSC].

12.2.3 Couvertures et garantie concernant les entités utilisatrices

En cas de dommage subi par une entité intervenant dans l'IGC, et sous contrat avec l'AH, du fait d'un manquement par l'AH à ses obligations, l'AH pourra être amenée à dédommager l'entité dans la limite de la responsabilité de l'AH définie dans le contrat établi entre l'AH et l'entité.

12.2.4 Confidentialité des données professionnelles

Voir chapitre 7.3 de la [PGSC].

Ne sont pas considérées comme confidentielles, toutes les informations publiées par l'AH.

12.3 Protection des données personnelles

Voir chapitre 7.4 de la [PGSC].

12.4 Droits sur la propriété intellectuelle et industrielle

Voir chapitre 7.5 de la [PGSC].

12.5 Interprétations contractuelles et garanties

Voir chapitre 7.6 de la [PGSC].

12.6 Limite de garantie

Les limites des garanties offertes par l'AH sont décrites dans l'accord d'utilisation des Jetons.

Ces limites sont applicables dans la limite des lois et règlements en vigueur.

12.7 Limite de responsabilité

L'AH ne pourra être tenue responsable pour tout dommage consécutif à des erreurs, inexactitudes ou omissions entachant les informations contenues dans les jetons, dès lors que ces erreurs, inexactitudes ou omissions résultent du caractère erroné des informations communiquées par l'Abonné.

Enfin, l'AH ne pourra être tenue responsable, dans la limite de la loi française, de perte financière, de perte de données ou de dommage indirect lié à l'utilisation d'un Jeton.

La responsabilité de l'AH sera strictement limitée, quelles que soient les causes, et quels que soient les faits générateurs, et quels que soient les préjudices causés, au montant payé à l'AH

par l'Abonné sur les 3 derniers mois et ce dans le respect et les limites de la loi applicable. Sauf prescription légale contraire, toute action de l'Abonné au titre des présentes devra intervenir au plus tard dans un délai de 3 mois à compter de la survenance du fait générateur fondant l'action.

12.8 Indemnités

Sans objet.

12.9 Durée et fin anticipée de validité de la PH/DPH

Voir chapitre 7.10 de la [PGSC].

La présente PH/DPH reste en application au moins jusqu'à la fin de vie du dernier Jeton émis par l'AH.

En fin de validité de la présente PH/DPH, les intervenants dans le service d'horodatage restent liés par la présente PH/DPH pour tous les Jetons émis lorsqu'elle était en vigueur, sans limitation de durée.

12.10 Notification individuelles et communications entre les participants

Le LPTSP Board publie une nouvelle version de la présente PH/DPH sur le site de publication de l'AH après l'avoir validé.

12.11 Amendements

Voir chapitre 7.12 de la [PGSC].

12.12 Dispositions concernant la résolution de conflits

Voir chapitre 7.13 de la [PGSC].

12.13 Juridictions compétentes

Voir chapitre 7.14 de la [PGSC].

12.14 Conformité aux législations et réglementations

Voir chapitre 7.15 de la [PGSC].

12.15 Dispositions diverses

Voir chapitre 7.16 de la [PGSC].

12.16 Autres dispositions

Voir chapitre 7.17 de la [PGSC].