CONSEIL SUPÉRIEUR DU NOTARIAT

Déclaration des Pratiques d'Horodatage du Notariat

Version	Date	Description	Auteurs	Approbateur
1.0	02/03/2018	Correction suite à l'audit eIDAS	REAL.NOT	Membres du Bureau du CSN
1.1	16/05/2019	Prise en compte du RGPD et changement REAL.NOT en ADSN	REAL.NOT	Membres du Bureau du CSN
1.2	29/09/2020	§1.6 : mise à jour de la version des HSM : (Système :X146, Module de sécurité :V147) §6.2.1 – Correction sens de la phrase pour ecrire : « Les demandes de contremarques et les contremarques émises sont archivées. » §6.2.4 : mise à jour du nom du prestataire IDNomic (ATOS) §6.2.4 : précision : L'Autorité d'Horodatage garantit que si une dérive de l'horloge supérieure à la limite fixée apparait, **elle sera détectée au travers d'un mécanisme de vérification qu'elle a développé spécifiquement**. §6.2.6 : Mise à jour des noms des sites	ADSN	Membres du Bureau du CSN
1.3	21/01/2021	Correction des écarts de l'audit eIDAS de janvier 2021, ajout de la colonne "Approbateur"	ADSN	Membres du Bureau du CSN
1.4	25/01/2021	rise en compte des remarques de l'audit à blanc eIDAS de juillet 2020 o Modification du paragraphe 6.5.1.4	ADSN	Membres du Bureau du CSN
1.5	18/10/2022	Mise à jour des références documentaires Modification du délai de récupération des archives	ADSN	Membres du Bureau du CSN
1.6	12/03/2024	Mise à jour des tailles des clés et charte CSN. Anonymisation du tableau	ADSN	Membres du Bureau du CSN
1.7	11/02/2025	Précision apportée sur la liste des algorithmes de hash acceptés (paragraphe 6.4.7) Précision apportée sur la durée d'utilisation des clés privés (paragraphe 6.4.10)	ADSN	Membre du bureau du CSN

Etat du document	Classification
Publié	Public
OID du document	
1.2.250.1.78.2.1.3.5.4.6.1.2	

Ce document est la propriété exclusive du **CSN**.
Son usage est réservé à l'ensemble des personnes habilitées selon leur niveau de confidentialité.
Sa reproduction est régie par le Code de la propriété intellectuelle qui ne l'autorise qu'à l'usage privé du copiste.

60 Bd de La Tour-Maubourg - 75007 Paris
Tél. : 01 44 90 30 00 - notaires.fr

SOMMAIRE

1 INTRODUCTION

1.1 Présentation générale

Le Conseil Supérieur du Notariat (**CSN**) se positionne en tant qu'Autorité d'Horodatage (ci-après « AH ») et délivre des contremarques de temps pour les besoins des applications de dématérialisation du notariat, les projets Télé@ctes et MICEN notamment.

La solution d'Horodatage est mise en œuvre par **l'ADSN**, qui se positionne comme Prestataire de Service d'Horodatage Electronique (PSHE) pour le **CSN**.

Le présent document constitue la déclaration des pratiques d'horodatage du Notariat (ci-après « DPH ») présentant la mise en œuvre des exigences prises par **l'ADSN** dans le cadre de la Politique d'Horodatage (ci-après « PH ») correspondante.

Dans le cadre de la présente DPH, les utilisateurs du service d'horodatage sont soit :

- **les porteurs d'une clé REAL**, contenant un certificat de signature émis par l'AC REAL. Dans ce cas, l'utilisateur peut être un collaborateur ou un Notaire d'un office, un collaborateur ou un Notaire d'une chambre départementale ou d'un conseil régional, un collaborateur ou un Notaire du **CSN** ou d'un organisme rattaché. Il s'agit dans tous les cas d'une personne physique, agissant dans le cadre de ses activités professionnelles qui souhaite faire des demandes de contremarques de temps. La demande d'horodatage est liée à la demande de signature d'un document et nécessite donc que l'utilisateur possède une clé REAL ;
- **Les applications de dématérialisation, et composants de l'infrastructure de confiance du notariat,** qui demandent des contremarques de temps à l'occasion d'une demande de validation de signature électronique, d'une demande de rafraichissement d'un acte authentique, ou pour d'autres usages nécessitant l'officialisation de l'heure et de la date de traitement.

La présente DPH expose les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la PH, en particulier les processus qu'une Unité d'Horodatage (ci-après « UH ») emploiera pour la création des contremarques de temps et le maintien de l'exactitude de ses horloges. L'AH du **CSN** peut mettre en œuvre plusieurs UH pour supporter son service d'horodatage.

L'Autorité d'Horodatage se conforme aux normes [EN_319401] et [EN_319421] et met en œuvre des profils de jetons d'horodatage conformes à [EN_319422].

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 :

- [PSCO_QUALIF]
- [PSCO_HORO]

1.2 Gestion du document

1.2.1 Identification du document

La présente DPH est identifiée, au sein du référentiel documentaire de l'infrastructure de confiance **l'ADSN**, par un numéro d'identification unique, l'OID : 1.2.250.1.78.2.1.3.5.4.6.1.2.

D'autres éléments, plus explicites, (nom, numéro de version, date de mise à jour) permettent également de l'identifier.

1.2.2 Publication du document

Avant toute publication officielle, la Déclaration des Pratiques d'Horodatage est validée par le Comité d'Approbation.

La présente Déclaration des Pratiques d'Horodatage est publiée sur l'URL : https://www.preuve-electronique.org/DPH_1.2.250.1.78.2.1.3.5.4.6.1.2.pdf

L'ensemble des informations associées notamment les versions antérieures de ces documents, est également publié sur le site www.preuve-electronique.org.

1.2.3 Procédures d'approbation de la conformité de la DPH

1.2.3.1 Composition du comité d'approbation

Le Comité d'Approbation est composé du bureau du **CSN**. Ce dernier approuve la conformité de la DPH à la PH.

1.2.3.2 Déroulement

Les sujets concernant l'autorité d'horodatage sont mis à l'ordre du jour du comité mensuel tenu entre le **CSN** et **l'ADSN**.

En cas de situation d'urgence, des comités restreints extraordinaires peuvent être organisés.

1.2.3.3 Suivi des actions

Le compte rendu du comité mensuel établit la liste des actions liées au service d'horodatage. Lors du comité suivant un point d'avancement est établi sur les actions qui étaient à traiter.

1.2.3.4 Points à mettre à l'ordre du jour d'un comité de pilotage

Le comité de pilotage a pour objectif de gérer et de décider les grandes phases applicables à l'AH. Cela concerne notamment et de manière non exhaustive les actions suivantes :

- Approbation d'une nouvelle DPH ou de nouvelles CGU ;
- Organisation d'une nouvelle cérémonie des clés pour initialiser une nouvelle unité d'horodatage ;
- Gestion des porteurs de secret ;
- Définition de nouveaux gabarits de jetons d'horodatage ;
- Modification de paramètres de sécurité :
    - Changement ou mise à jour des HSM ;
    - Modification de la taille des clés privées des unités d'horodatage ;
    - Modification des algorithmes de signature utilisés ;
- Analyse de remontée d'événement de tentative ou de compromission de clés privées (ce point nécessite l'organisation d'un comité de pilotage extraordinaire) ;
- Analyse de remontée d'événements sur des incidents de sécurité (le cas échéant si l'incident nécessite une remontée vers le comité de pilotage) ;
- Analyse de remontée d'événements de sécurité liés à la synchronisation du temps dans le service d'horodatage (ce point nécessite l'organisation d'un comité de pilotage extraordinaire) ;
- Demande de réalisation de tests de vulnérabilités et de pénétration sur les composants de l'AH ;
- Suivi du plan de correction des vulnérabilités identifiées au cours des différents tests ;

- Révocation / renouvellement d'un certificat d'une unité d'horodatage ;
- Etude d'un rapport d'audit interne ;
- Suivi de la capacité de l'AH ;
- Modification d'aspects contractuels avec les opérateurs techniques ;
- Points divers.

1.2.4 Processus de mise à jour

1.2.4.1 Circonstances rendant une mise à jour nécessaire

La conformité de la DPH à la PH est réexaminée au minimum tous les deux ans.

La mise à jour peut être due :

- A des améliorations ou des modifications profondes du service d'horodatage ;
- A des évolutions du site d'hébergement du service d'horodatage ;
- A des résultats de tests de vulnérabilité ou de pénétration ;
- A des résultats de l'audit interne, dénotant une non-conformité ;
- A des résultats de l'audit de qualification externe.

1.2.4.2 Prise en compte des mises à jour

Les différentes mises à jour à prendre en compte dans la DPH sont établies dans un compte rendu du comité d'approbation de l'AH. La mise en œuvre des modifications suit un cycle projet, prenant en compte :

- La mise à jour documentaire correspondante ;
- La mise à jour du plan d'audit interne ;
- Les évolutions d'architectures techniques éventuelles ;
- Le passage en phase de recette de ces évolutions ;
- La bascule en production du nouveau système.

Dans certains cas, sur décision du comité d'approbation, un audit interne peut être déclenché pour s'assurer que les nouvelles évolutions ne remettent pas en cause les exigences prises par l'AH dans sa PH. Dans le cas contraire, l'auditeur externe ayant délivré la certification devra en être informé.

1.2.4.3 Information des acteurs

Un procès-verbal de mise en production sera délivré au comité d'approbation pour attester de la mise en œuvre des nouvelles fonctionnalités.

La nouvelle DPH est mise en ligne sur le site www.preuve-electronique.org.

1.2.5 Entrée en vigueur de la nouvelle version et période de validité

Le passage en production des évolutions rend valide la nouvelle version de la DPH. Les versions précédentes restent archivées par le responsable de l'AH.

1.2.6 Cohérence de la documentation

L'ensemble des documents applicables dans le cadre de l'AH est référencé dans le document annexe [ref_doc].

1.3 Principe du service d'horodatage du notariat

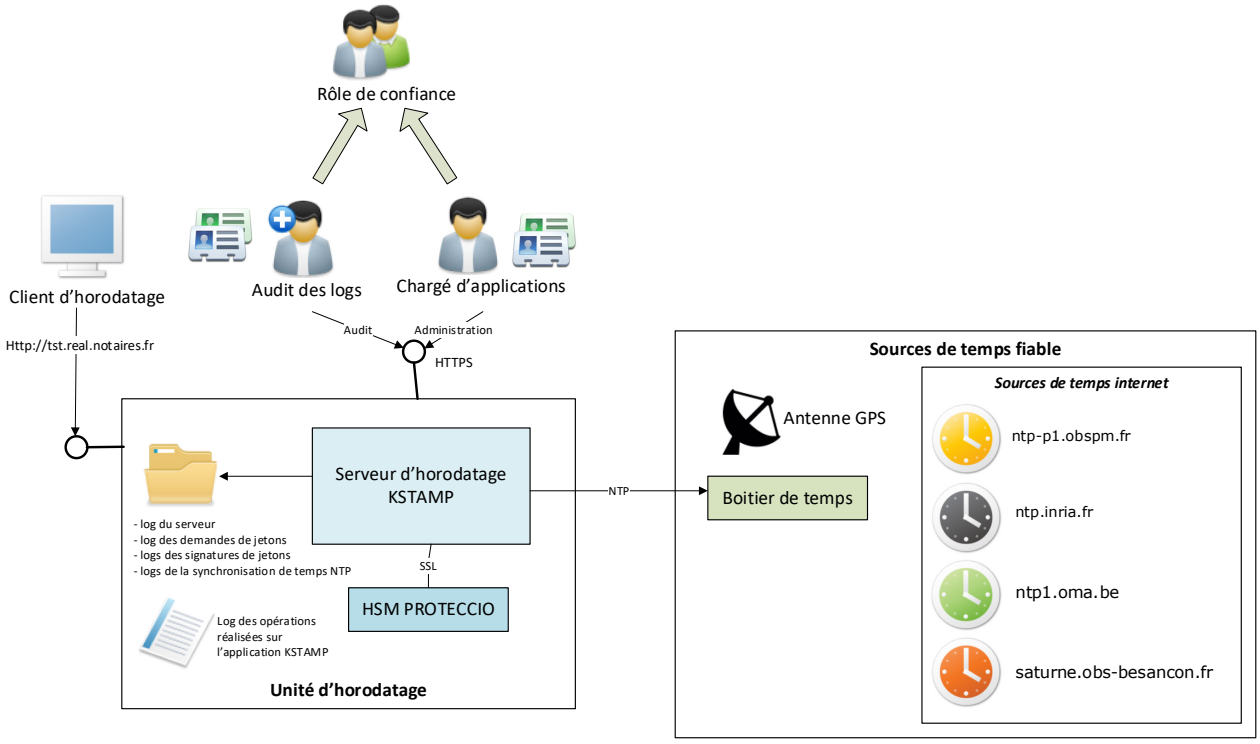
Une contremarque de temps permet d'attester de la réalité, à une date et une heure donnée, de l'existence d'une empreinte numérique (ou « hash ») qui est soumise au service d'horodatage. Les contremarques de temps sont délivrées et signées électroniquement par l'AH à l'aide d'Unité(s) d'Horodatage (ci-après « UH »).

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) fournis par des serveurs de temps autonomes, sous la maîtrise de l'**ADSN** ;
- l'identifiant du certificat de l'UH qui a généré la contremarque de temps ;
- l'identifiant du notariat 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.

Les certificats installés sur les unités d'horodatage du service d'horodatage du notariat sont émis par l'AC REALTS, dont la Politique de Certification est consultable à l'adresse suivante : www.preuve-electronique.org ([ref_PH]).

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 égale à 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 est détaillée au chapitre 6.2.4.
Le schéma ci-dessous décrit les différents composants intervenants dans le service d'horodatage du Notariat ainsi que les interactions possibles entre chaque composant.



1.4 Etablissement de la confiance dans le service d'horodatage du notariat

La garantie apportée par l'autorité d'horodatage s'appuie sur des éléments techniques (décrits précédemment) et des règles de gestion qui sont présentées dans la politique d'horodatage ([ref_PH]).

La PH est élaborée sur la base des documents issus de l'ETSI ([EN_319421]). La DPH reprend la même structure.

1.5 Entités intervenant dans le service d'horodatage

Les acteurs intervenant dans le service d'horodatage sont de deux ordres :

- Les acteurs qui participent à l'AH Notaires ;
- Les acteurs qui participent à l'AC REALTS.

Certains acteurs peuvent être opérationnels dans les deux cadres. La liste des acteurs est décrite dans le document annexe [ref_role].

1.6 Autres aspects

Les unités d'horodatage sont des serveurs virtuels ([ref_kstamp]) intégrant les applications d'horodatage fournies par Atos.
Les modules cryptographiques stockant les clés privées d'horodatages sont des Bull Proteccio. Ces modules sont qualifiés par l'ANSSI au niveau renforcé.

En sus de ces boîtiers d'horodatage, **l'ADSN** met en œuvre des serveurs de temps autonomes ([ref_temps]) dont les modèles sont les suivants : **Meinberg LANTIME/M300-MQ/GPS.**

2 GÉNÉRALITÉS

2.1 Définitions

Abonné - Entité ayant besoin de faire horodater des données par une Autorité d'horodatage et qui a accepté les conditions d'utilisation de ses services.

Autorité de Certification (AC) - Désigne une entité qui a en charge l'application d'au moins une politique de certification. L'AC fournit des prestations de gestion des certificats aux utilisateurs de contremarques de temps. Dans le cadre de l'horodatage l'AC délivre les certificats électroniques aux UH mises en œuvre par l'AH et qui sont rattachées à cette dernière. Cette AC gère aussi les listes de certificats révoqués pour les certificats d'UH.

Autorité d'horodatage (AH) - Au sein d'un PSHE, une Autorité d'Horodatage a en charge, au nom et sous la responsabilité de ce PSHE, l'application d'au moins une politique d'horodatage en s'appuyant sur une ou plusieurs Unités d'Horodatage. Il désigne l'AH chargée de l'application de la politique d'horodatage, répondant aux exigences de la présente PH, au sein du PSHE souhaitant faire qualifier la famille de contremarques de temps correspondante.

Calcul d'empreinte numérique - Désigne le processus algorithmique qui consiste à obtenir une empreinte numérique à partir d'une donnée électronique.

Certification d'un prestataire de services - Le règlement européen n°910/2014 permet à un PSCO d'être contrôlé sur ses pratiques de manière à être certifié pour les services qu'il fournit.

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.

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

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

Demande de contremarque de temps - Désigne la requête qui est soumise par un client à l'AH pour l'émission d'une contremarque de temps. Cette requête contient au minimum l'empreinte numérique à horodater.

Empreinte numérique (ou *Hash*) - Désigne le résultat, d'une fonction de hachage à sens unique, c'est-à-dire d'une fonction calculant une empreinte d'un message de telle sorte qu'une modification même infime du message entraîne la modification de l'empreinte et permet donc de détecter que le message a été modifié.

Jeton d'horodatage - Voir contremarque de temps.

Liste de certificats révoqués (LCR) - Désigne la liste signée électroniquement par l'AC et qui contient l'ensemble des identifiants des certificats d'UH qui ont été révoqués avant leur date d'échéance.

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

Politique de Certification (PC) - Désigne l'ensemble des règles et engagements énoncées et publiées par l'AC décrivant les caractéristiques générales des services de certification et des certificats d'UH qu'elle délivre.

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

Précision - Désigne la différence maximale autorisée entre la date et l'heure UTC fournie par la source de temps externe et la date et heure de la source interne de l'UH qu'il utilise pour générer les contremarques de temps

Prestataire de services de confiance (PSCO) – Le règlement européen n°910/2014 dit « règlement eIDAS » introduit et définit les prestataires de service de confiance (PSCO). Un prestataire de services de confiance est défini comme toute personne ou entité offrant des services tendant à la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique.

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

Produit de sécurité - Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Référencement - Opération réalisée par l'ANSSI qui atteste que l'offre d'horodatage du PSCO est utilisable avec tous les systèmes d'information qui requièrent ce type d'offre. Une offre référencée peut être utilisée dans toutes les applications d'échanges dématérialisés requérant un service d'horodatage. Pour les utilisateurs, le référencement permet de connaître quelles offres d'horodatage ils peuvent utiliser pour quels échanges dématérialisés.

Ressource cryptographique - Désigne le produit de sécurité comportant une ressource cryptographique matérielle et qui est dédié à la mise en œuvre des fonctions d'horodatage de l'UH, notamment la génération, la conservation et la mise en œuvre de la clé privée de signature de l'UH ainsi que la génération des contremarques de temps.

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

Source de temps - Désigne la composante qui fournit une date et une heure (temps). On distingue deux sortes de sources de temps :

- La source de temps externe : Source extérieure au système d'information, qui fournit un temps UTC reconnu comme sûr (antenne GPS, onde radio, serveur NTP, ...) ;
- La source de temps interne : Source interne au système d'horodatage, qui fournit un temps (Cf. date et heure UH) sur la base d'éléments uniquement internes au système d'information.

Synchronisation - Désigne l'opération qui consiste pour une UH à comparer la date et l'heure issue de sa source de temps interne à la date et l'heure fournie par une ou des source(s) de temps externes. Cette comparaison sert à garantir dans le temps que sa source de temps interne délivre une date et une heure avec un écart maximal correspondant à la précision de l'heure l'AH par rapport au temps UTC.

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

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

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

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

Usager - Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques avec des autorités administratives.

Nota - Un agent d'une autorité administrative qui procède à des échanges électroniques avec une autre autorité administrative est, pour cette dernière, un usager.

Utilisateur de contremarque de temps – Entité (personne ou système) qui fait confiance à une contremarque de temps émise sous une politique d'horodatage donnée par une autorité d'horodatage donnée.

Utilisateur final - Abonné ou utilisateur de contremarques de temps.

Vérification d'une contremarque de temps - Désigne l'action de l'utilisateur de contremarque de temps qui consiste à vérifier que la contremarque est valide

2.2 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
CGU	Conditions Générales d'utilisation du service d'horodatage
CSN	Conseil Supérieur du Notariat
DPC	Déclaration des Pratiques de Certification
DPH	Déclaration des Pratiques d'Horodatage
ETSI	European Telecommunications Standards Institute
LCR	Liste des Certificats Révoqués
IGC	Infrastructure de Gestion de Clés
OID	Object Identifier
OSC	Opérateur de Service de Certification
OSH	Opérateur de Service d'Horodatage
PC	Politique de Certification
PH	Politique d'Horodatage
PP	Profil de Protection
PSHE	Prestataire de Services d'Horodatage
UH	Unité d'Horodatage
UTC	Coordinated Universal Time

3 POLITIQUE D'HORODATAGE

La PH applicable est référencée sous [ref_PH].

Les caractéristiques principales de cette politique sont les suivantes :

- la protection des clés et de l'horloge doit respecter les exigences spécifiées au chapitre 9 de la PH ;
- la sauvegarde et l'import des clés privées des unités d'horodatage sont interdits ;
- l'AC générant les certificats de clé publique pour les unités d'horodatage doit gérer le service de révocation pour chaque certificat publié ;
- Les certificats installés sur les UH sont émis par l'AC REALTS opérée par **l'ADSN**.

4 DÉCLARATION DES PRATIQUES D’HORODATAGE

Il s’agit du présent document.

5 CONDITIONS GÉNÉRALES D'UTILISATION

Compte tenu de la complexité de lecture d'une PH pour des utilisateurs non-spécialistes du domaine, l'AH définie également des conditions générales d'utilisation correspondant aux *« TSA Disclosure Statement » (TDS)* définis dans l'annexe B de [EN_319421].

Ces 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 et la 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.
- 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 ponts 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 www.preuve-electronique.org et sont référencées sous [ref_cgu].

6 EXIGENCES RESPECTÉES PAR L'AUTORITÉ D'HORODATAGE

6.1 Dispositions générales

6.1.1 Obligation de l'Autorité d'Horodatage

Vis-à-vis de la présente déclaration, l'Autorité d'Horodatage :

- Génère et signe les contremarques de temps conformément à la PH ;
- Respecte et se conforme aux exigences et procédures définies dans la PH et dans les Conditions Générales d'Utilisation applicables ;
- Garantie que la mise en œuvre des exigences exprimées dans la PH est faite conformément à ce qui est décrit dans la présente DPH ;
- Met à disposition de ses utilisateurs l'ensemble des informations nécessaires permettant de vérifier les contremarques de temps qu'elle aura émises. Cette vérification est faite :
    - Pour les demandes initiées par les personnes physiques à travers l'outil de signature électronique intégré aux logiciels métiers du notariat ;
    - Pour les demandes initiées par les applications de dématérialisation du notariat à travers ces mêmes applications (le serveur de validation notamment), à l'occasion de la réception de la contremarque.

6.1.2 Obligation de l'abonné

Les logiciels métiers sont en capacité de vérifier la validité des contremarques de temps délivrées par l'AH.

De manière générale, la vérification de la contremarque de temps est traitée par l'application utilisée par l'abonné. Néanmoins, l'AH met à disposition des abonnés les éléments nécessaires à cette vérification.

Ces éléments sont publiés sur le site www.preuve-electronique.org et contiennent notamment :

- Les certificats de la chaîne de certification ayant émis le certificat de l'unité d'horodatage ;
- La LCR en cours de validité.

Un service ocsp est également mis en œuvre pour vérifier le statut des certificats (ocsp.preuve-electronique.org).

6.1.3 Obligation de l'Utilisateur de Contremarque de Temps

Les utilisateurs de contremarques de temps peuvent :

- vérifier que la contremarque de temps a été correctement signée et que le certificat de l'UH est valide à l'instant de la vérification ;
- s'assurer que les contremarques de temps sont obtenues auprès des UH mises en place par **l'ADSN** ;
- s'assurer que les demandes de contremarques de temps sont faites exclusivement pour l'usage des applications de dématérialisation des Notaires.

Les utilisateurs de contremarque de temps doivent prendre en compte les limitations d'usages du service d'horodatage.

Ces vérifications sont réalisées par les logiciels métiers qui exploitent le logiciel de signature mis en place par la profession sur tous les postes informatiques qui le

nécessitent. Le logiciel de signature exploite des politiques ou profils de signature, développées par **l'ADSN**, qui instrumentent notamment la vérification du jeton d'horodatage et qui répondent ainsi aux exigences susmentionnées.

6.1.4 Obligations des Autorités de Certification fournissant des certificats aux Unités d'Horodatage

L'Autorité de Certification AC REALTS délivrant des certificats aux unités d'horodatage fournit un service de révocation. Les engagements de l'AC REALTS sont consultables à travers sa Politique de Certification (https://www.preuve-electronique.org) et référencée sous [ref_PC_realts].

L'AC REALTS est conforme aux exigences prévues par [EN319411].

l'ADSN met à disposition les informations de gestion des certificats, dont le statut de révocation des certificats. Les points de distribution des CRL (HTTP et LDAP) et du service OCSP sont précisés dans la Politique de Certification de l'AC REALTS, consultable sur le site https://www.preuve-electronique.org.

6.1.5 Déclaration des Pratiques d'Horodatage

L'autorité d'Horodatage garantit via les mesures suivantes qu'elle possède la fiabilité nécessaire pour fournir des services d'horodatage :

- L'AH a rédigé une analyse des risques de son service d'horodatage ([ref_analyse_risque]) ;
- L'AH adresse l'ensemble des exigences décrites dans la PH ([ref_PH]) ;
- La DPH décrit toutes les exigences que doivent respecter les éventuelles tierces parties dans le cadre du service d'horodatage (voir paragraphes 6.1.2, 6.1.3 et 6.1.4) ;
- L'AH met à disposition, sur le site www.preuve-electronique.org, des abonnés et des applications utilisatrices les données nécessaires à la validation des contremarques de temps, soit :
    - Les certificats des unités d'horodatage émis par l'AC REALTS ;
    - Les CRL de l'AC REALTS ;
    - Le certificat de l'AC REALTS ;
    - Toutes les versions des politiques d'horodatage.

- L'AC REALTS met à disposition un service OCSP à l'URL ocsp.preuve-electronique.org.
- L'AH organise un audit interne pour attester que la DPH est conforme à la PH
- L'audit organisé par l'AH prend en compte le contrôle des mesures techniques, non techniques et organisationnelles ;
- L'AH garantit qu'elle mettra à jour la PH en cas de changements majeures des pratiques d'horodatage de son service (voir paragraphe 1.2.4) ;
- L'AH garantit 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 (voir paragraphe 1.2.4).

6.1.6 Conditions Générales d'Utilisation

L'AH définit des Conditions Générales d'Utilisation de l'Horodatage (CGU) qui reprennent les grands principes décrits dans la présente PH. Ces CGU sont basées sur le modèle défini dans l'annexe B de [EN_319421]. Les CGU applicables sont référencées dans le document [ref_cgu]. L'AH définit des CGU conformes au paragraphe 5.

6.1.7 Conformité avec les exigences légales

Toutes les informations de ce paragraphe sont décrites dans [ref_PH]

6.2 Exigences opérationnelles

6.2.1 Gestion des requêtes

Les demandes de contremarques de temps sont exécutées par les UH de l'AH selon le protocole défini par la [RFC_3161]. Le profil de la contremarque de temps est conforme à [EN_319422].

Les utilisateurs « personnes physiques » utilisent leurs applications métiers pour faire une demande d'horodatage. Opérationnellement, cette demande d'horodatage est pilotée par le logiciel de signature du notaire, et elle consiste à effectuer une connexion en mode HTTP vers le serveur d'horodatage (voir [ref_kstamp]. Cette opération est généralement réalisée à l'issue d'une opération de signature électronique. L'identifiant de la PH a utilisée sur le serveur d'horodatage est indiqué dans la requête.

Les « serveurs d'applications ou serveurs de l'infrastructure de confiance » se connectent directement au service d'horodatage. Ces demandes sont généralement liées à des demandes de validation de signature électronique, à la création d'archives pérennes sur le long terme.

Dans les deux cas, les utilisateurs du service d'horodatage produisent un condensat (hash) des données qu'ils souhaitent horodater, et le transmettent au système d'horodatage sans authentification.

L'AH génère la contremarque de temps à partir du condensat des données qui lui est transmis par les utilisateurs (empreinte de la donnée à horodater) et la lui retourne. La durée de création de la contremarque de temps n'excède pas quelques secondes suite à la réception d'une requête d'horodatage.

Les demandes de contremarques et les contremarques émises sont archivées.

6.2.2 Fichiers d'audit

Les journaux système du service d'horodatage sont conservés sur le serveur d'horodatage et envoyés vers le serveur de traces du SIEM opéré par **l'ADSN**.

Les serveurs KSTAMP, dont les spécifications sont décrites dans [ref_kstamp] permettent :

- De protéger en confidentialité les traces ;
- De tracer et de conserver tous les événements d'administration des serveurs d'horodatage. Ces éléments sont contenus en base de données et sont extraits régulièrement pour être archivés ;
- D'horodater les traces. Chaque événement contient la date et l'heure d'apparition de cet événement ;

La gestion et le contenu des traces sont décrits dans le document [ref_trace].

L'AH met en œuvre une sauvegarde des éléments visant à conserver la traçabilité suffisante en cas d'enquêtes légales, notamment :

- Les éléments sauvegardés sont les suivants :
  - Le fichier de traces des appels au serveur Apache de KSTAMP
  - Le fichier de traces des appels applicatifs du serveur KSTAMP contenant notamment :
    - Le numéro de série du jeton généré
    - Le hash de la donnée horodatée
    - L'heure positionnée dans le jeton
  - Le contenu de la base de données listant :

        - Les compteurs de jetons émis
        - Les actions d'administration réalisées sur le boîtier
    - Les requêtes et les réponses d'horodatage
    - Les traces des synchronisations NTP dans le fichier /var/log/message du boîtier KSTAMP
- Tous les événements liés à la gestion du cycle de vie des clés d'horodatage sont tracés (création, renouvellement, destruction, installation sur une UH) lors d'une cérémonie des clés décrites dans le document [ref_kc]. Le document de cérémonie des clés sont écrits à chaque fois que cela est nécessaire ;
- Tous les événements liés à la gestion du cycle de vie des certificats d'horodatage sont tracés (création, renouvellement, destruction, installation sur une UH) lors d'une cérémonie des clés décrites dans le document [ref_kc]. Le document de cérémonie des clés sont écrits à chaque fois que cela est nécessaire ;
- Tous les événements liés à la gestion des serveurs de temps sont tracés (initialisation, dépassement de la dérive maximale, dépassement de la précision autorisée, synchronisation, saut de seconde). Ces éléments sont tracés dans les fichiers journaux du service NTP. La description des éléments tracés par les serveurs de temps est établie dans le document [ref_temps] ;

6.2.3 Gestion de la durée de vie de la clé privée

Les clés privées des UH sont générées par les HSM des serveurs d'horodatage. Les clés publiques correspondantes sont certifiées par l'AC REALTS qui respecte les différentes clauses de sa PC et de sa DPC (voir [ref_pc_realts] et [ref_dpc_realts]).

Ces clés privées sont exclusivement utilisées pour des certificats d'horodatage dans le cadre du service d'horodatage du Notariat.

La solution KSTAMP permet de :

- Créer un espace client en définissant la fonction de hachage à utiliser ainsi que le système cryptographique à utiliser pour la signature ;
- Générer une bi-clé sur l'espace client créé précédemment et récupérer la CSR correspondante ;
- Créer un « Document Signer » (DS) dans cet espace avec le certificat signé par la PKI externe.

Cela permet d'associer la clé privée à un seul DS. Ce dernier peut être modifié, rendu inactif, supprimé…

L'ensemble « Espace client » et DS correspond à la notion de « contexte d'horodatage » définie dans le Profil de Protection « Horodatage ».

Les clés sont utilisées exclusivement dans un contexte d'horodatage KSTAMP sur le serveur d'horodatage et n'ont pas d'existence en dehors de ce contexte conformément aux spécifications du serveur d'horodatage KSTAMP (voir [ref_kstamp]).

Le contexte établit par le serveur KSTAMP intègre notamment :

- Les informations de certificats à utiliser par le boîtier ;
- La clé privée associée ;
- Les algorithmes cryptographiques à utiliser pour signer les jetons ;
- La durée de vie du contexte, basé sur la durée de vie du certificat ;
- L'OID de la PH.

A la fin du contexte d'horodatage, la clé privée devient inutilisable. Un nouveau contexte KSTAMP doit être mis en œuvre sur la base d'une nouvelle clé privée.

L'Autorité d'horodatage garantit que les clés de signature des UH ne sont pas employées au-delà de la fin de leur cycle de vie :

a) Des procédures sont en place pour s'assurer 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) A la fin du contexte d'horodatage, la clé privée est systématiquement détruite. Un nouveau contexte doit être mis en œuvre sur la base d'une nouvelle clé privée.

Les clés privées ne sont pas exportables.

6.2.4 Synchronisation de l'horloge

Le serveur KSTAMP est synchronisé directement en NTP sur les trois serveurs de temps autonomes Meinberg LANTIME M300. Ces serveurs de temps sont directement reliés :

- à une source de temps GPS.
- Aux sources NTP suivantes :
  - ntp.inria.fr : serveur primaire basé en France.
  - ntp-p1.obspm.fr : serveur primaire basé en France. Ce serveur, situé à l'observatoire de Paris, est un serveur dit UTC(k). Il est donc référencé[i] par le Bureau International Poids et Mesures (BIPM).
  - saturne.obs-besancon.fr: serveur primaire basé à Besançon
  - ntp1.oma.be : serveur primaire du Royal Observatory of Belgium, est également un serveur dit UTC(k).

Le serveur KSTAMP sélectionne ensuite la source de temps la plus stable et la plus fiable parmi le pool des sources reconnues sûres par le boîtier, selon le protocole NTP. Un traitement spécifique développé par l'ADSN permet l'arrêt de la délivrance de jeton d'horodatage en cas de dérive de temps supérieure aux exigences définies [ref_AlgoSynchroTemps].

ATOS assure la maintenance logicielle et matérielle du serveur d'horodatage dont le calibrage de l'horloge, les sauts d'horloge programmés, les synchronisations.

La société KAIROS assure la maintenance logicielle et matérielle du boîtier de temps autonome. Il s'agit du distributeur et du mainteneur officiel des produits Meinberg en France.

l'ADSN assure la supervision de la solution d'horodatage.

Les clauses de maintenance sont définies dans le contrat entre **l'ADSN** et ses prestataires.

En cas de panne, l'éditeur de la solution KSTAMP :

- Assiste le personnel de **l'ADSN** à distance ;
- Se déplace sur site s'il ne peut faire autrement.

L'Autorité d'Horodatage garantit que si une dérive de l'horloge supérieure à la limite fixée apparait, elle sera détectée au travers d'un mécanisme de vérification qu'elle a développé spécifiquement.

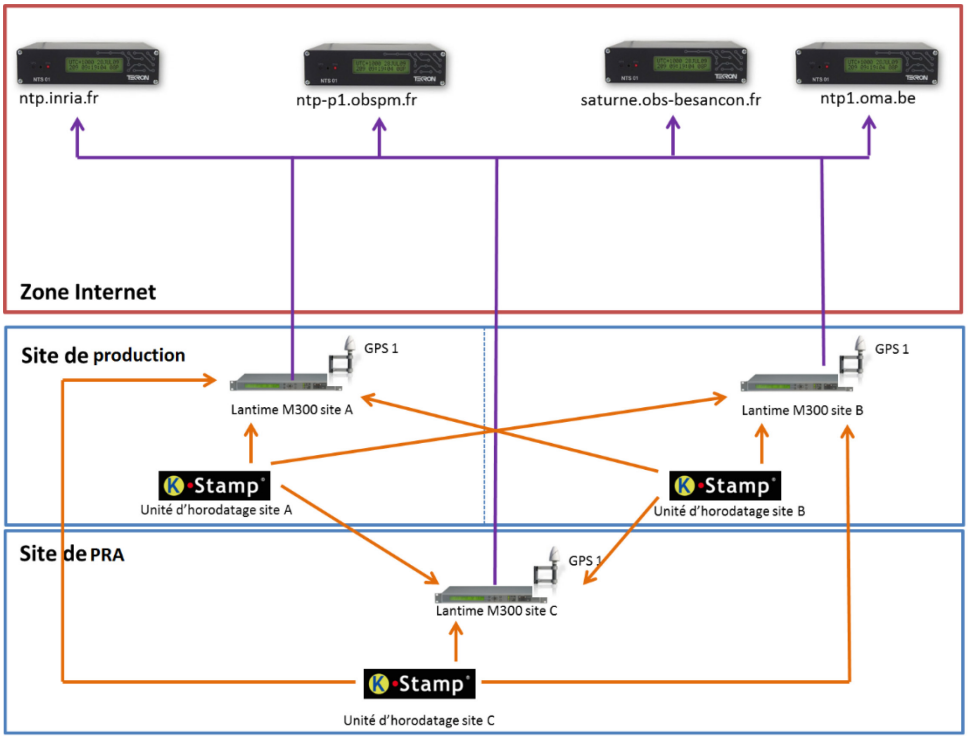
L'Autorité d'Horodatage garantie la calibration des horloges en cas de saut de seconde.

En tout état de cause, les unités d'horodatage sont automatiquement interrompues dans les cas suivants :

- Le calibrage de l'horloge n'est plus respecté ;

- L'horloge est désynchronisée ;
- Le saut de seconde n'a pas été respecté.

L'architecture de la synchronisation de l'horloge mis en œuvre par **l'ADSN** est alors la suivante :



6.2.5 Contenu d'une Contremarque de Temps

Structure	Valeur
TimeStampToken	
ContentInfo	Id-smime-ct-TSTInfo
SignedData	
Version	03
DigestAlgorithms	Sha512
EncapContentInfo	
Version	01
Policy	*OID de la politique*
MessageImprint	
hashAlgorithm	Sha256 ou sha512
hashedMessage	Condensat envoyé par l'application appelante
SerialNumber	N° de série du jeton
Gentime	Date de génération du jeton
Accuracy	Précision égale à la seconde
Nonce	Valeur du nonce positionné par l'application appelante
Extension	0.4.0.19422.1.1 positionné uniquement si demandé par la requête de demande de jeton d'horodatage
Certificates	

Structure	Valeur
Certificat	Certificat de l'UH
Certificat	REALTS 20XX
Certificat	Notaires de France 2033
SignerInfos	
Version	01
SignerIdentifier	
Issuer	DN du certificat de l'AC signataire du certificat de l'UH
SerialNumber	N° de série du certificat de l'UH
DigestAlgorithm	Sha512
SignedAttributes	
contentType	id-smime-ct-TSTInfo
signingTime	Date de signature du jeton
messageDigest	Condensat du jeton
id-smime-aa-signingCertificate	OID : 1.2.840.113549.1.9.16.2.47
	Algorithme de condensat du certificat de l'UH : SHA512
	Condensat du certificat de l'UH
SignatureAlgorithmIdentifier	sha512WithRSAEncryption
SignatureValue	Valeur de la signature du jeton

6.2.6 Reprise suite à compromission et sinistre

L'Autorité d'horodatage garantit dans le cas d'événements qui affectent la sécurité des services d'horodatage, incluant la compromission de la clé privée de signature d'une unité d'horodatage ou la perte détectée de calibrage qui pourrait affecter des contremarques de temps émises, qu'une information appropriée est mise à la disposition des abonnés et des utilisateurs de contremarques de temps. En particulier :

a) Le plan de secours de l'Autorité d'horodatage traite le cas de la compromission réelle ou suspectée de la clé privée de signature d'une unité d'horodatage ou la perte de calibrage de l'horloge d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises.

b) Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises, l'Autorité d'horodatage mettra à la disposition de tous les abonnés et utilisateurs de contremarques de temps une description de la compromission qui est survenue.

c) Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises, l'Autorité d'horodatage prendra les mesures nécessaires pour que les contremarques de temps de cette unité ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.

d) En cas d'un évènement majeur dans le fonctionnement de l'Autorité d'horodatage ou d'une une perte de calibrage, qui pourrait affecter des contremarques de temps émises, chaque fois que cela sera possible, l'Autorité d'horodatage mettra à la disposition de tous ses abonnés et des 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.

e) En cas d'information d'une compromission impactant le service d'horodatage, l'AH et l'OSH déclenchent une cellule de crise afin de déterminer les actions à mener pour rétablir le service au plus tôt. Par mesure de précaution, l'AH :

   a. Demande à l'OSH l'arrêt immédiat des services de dématérialisation exploitant la clé REAL ;

   b. Demande à l'OSH de diffuser immédiatement l'information à l'ensemble des parties concernées

   c. L'AH prévient directement et sans délai le point de contact de l'ANSSI http://www.ssi.gouv.fr en suivant la procédure de remontée et de traitement des incidents et des compromissions

Des procédures et des moyens de remontée et de traitement des incidents sont mis en œuvre : sensibilisation, formation des personnels, et analyse des différents journaux d'événements, procédure de gestion des incidents. Cf. Procédure [ref_incidents].

La procédure de gestion des incidents précise les différentes phases de constatation de l'incident, l'information de personnes compétentes, la traçabilité, la qualification, la mise en œuvre de la procédure d'escalade, la résolution et la phase de clôture de l'incident.

6.2.6.1 Procédure de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Un plan de continuité / reprise d'activité est mis en place [ref_pra] permettant de répondre aux exigences de disponibilité des différentes composantes de l'AH.

Ce plan est testé une fois par an.

6.2.6.2 Compromission des clés privées de l'Autorité d'Horodatage

La gestion de la compromission d'une clé privée de l'AH est décrite dans [ref_dpc_realts] au paragraphe 5.7.3.

6.2.6.3 Compromission de la synchronisation du service d'horodatage

La gestion de la compromission de la synchronisation du service d'horodatage est décrite dans [ref_compromission].

6.2.6.4 Autres cas de compromission

Les cas de compromission des éléments secrets des autres composantes sont traités dans le plan de continuité d'activité.

Les éléments ci-après traitent de la compromission d'un algorithme ou d'un paramètre associé, tels que l'algorithme de condensat utilisé dans les certificats ou la longueur de la clé des certificats.

L'AH et plus particulièrement l'OSH se tiennent continuellement informés des cas de compromission des éléments susmentionnés, par le biais d'organismes comme l'ANSSI.

En cas d'information d'une compromission impactant les certificats des UH, l'AH et l'OSH déclenche une cellule de crise afin de déterminer les actions à mener pour rétablir le

service au plus tôt. Les actions à prendre sont alors décrites dans le compte rendu de cette cellule de crise et font l'objet d'une mise en œuvre par l'OSH dans les délais courts.

Par mesure de précaution, l'AH demande à l'OSH :

- l'arrêt immédiat des services d'horodatage ;
- de diffuser immédiatement l'information sur le site www.preuve-electronique.org.
- L'AH prévient directement et sans délai le point de contact de l'ANSSI http://www.ssi.gouv.fr

6.2.6.5 Procédures de reprise en cas de compromission

La continuité d'activité du service d'horodatage est assurée par la mise en œuvre sur 2 sites géographiquement distants des composants. Le détail des éléments mis en œuvre est décrit dans [ref_bascule].

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 REALTS ayant servi à générer les certificats des UH ;

En cas de compromission de la clé privée de l'AC REALTS, la procédure mise en place est détaillée dans [ref_compromission].

Concernant les autres cas de compromission, dans le cadre du plan de continuité d'activité, **l'ADSN** dispose de deux salles serveurs hébergées sur 2 sites différents à Marseille (MRS1 et MRS2, site de productions), et d'une salle serveur en région parisienne (héberge l'environnement de PCA).

Les trois salles disposent des mêmes équipements et des mêmes logiciels pour faire fonctionner le service d'horodatage. Notamment chaque salle possède ses propres Unités d'Horodatage, chacune ayant des clés privées différentes, émises par l'AC REALTS.

En cas de compromission de l'Autorité d'Horodatage et plus particulièrement des clés privées des Unités d'Horodatage, les équipes de **l'ADSN** exploitant le service d'Horodatage déclenchent une bascule vers la salle B ou C ; les clés privées des UH des salles B et C n'étant elles pas compromises.

Les événements redoutés déclenchant une bascule des activités du service d'horodatage vers le site de secours sont définis dans les documents d'exploitation maintenus par **l'ADSN** [ref_bia].

Les salles B et C peuvent fonctionner de manière autonome le temps nécessaire au rétablissement de la salle A.

La procédure, maintenue par **l'ADSN**, de mise en service sur le site B du service d'horodatage permet de s'assurer de :

- L'émission de contremarques de temps valides ;
- La validité et de la non révocation du certificat de l'UH du site de secours.

Le détail des actions enclenchées par cette bascule ainsi que les délais de remise en activité des services sont précisés dans les documents d'exploitation maintenus par **l'ADSN**. Ce fonctionnement permet à l'AH de garantir un service d'horodatage avec un haut niveau de disponibilité.

Plus généralement, les incidents liés au service d'horodatage sont traités selon la procédure de gestion des incidents en vigueur chez **l'ADSN** [ref_incidents].

En tout état de cause, **l'ADSN** réalisera un audit suite à la compromission et :

- Mettra à disposition des abonnés et des utilisateurs de contremarque de temps une description de la compromission ou de la perte de synchronisation détectée sur le site internet www.preuve-electronique.org, en précisant notamment la date de début de la compromission ;
- Coupera l'unité d'horodatage suspectée de compromission ;
- Basculera sur l'ensemble des flux sur le second boîtier KSTAMP sur le site de secours ;
- Demandera la révocation du certificat de l'unité d'horodatage et du certificat de l'AC REALTS qui a émis le certificat de l'UH ;
- Mettra à disposition quand cela est possible les éléments permettant d'identifier les contremarques de temps émises qui pourraient être compromises ou suspectées de compromission, notamment les numéros de série des jetons présumés compromis ainsi que le numéro de série du certificat de l'UH concerné ;
- Préviendra le point de contact identifié sur le site de l'ANSSI http://www.ssi.gouv.fr ;

6.2.6.6 Capacités de continuité d'activité suite à un sinistre

Les procédures de reprise en cas de compromission sont définies dans le document [ref_compromission].

6.2.7 Fin d'activité

L'Autorité d'horodatage garantie que les dérangements potentiels aux abonnés et aux utilisateurs de contremarques de temps seront réduits au minimum suite à la cessation d'activité du service d'horodatage et assurera en particulier la maintenance continue des informations nécessaires pour vérifier la justesse de contremarques de temps. En particulier :

a) Avant que l'Autorité d'horodatage ne termine ses services d'horodatage les procédures suivantes seront exécutées au minimum :

- l'Autorité d'horodatage rendra disponible à tous ses abonnés et aux utilisateurs de contremarques de temps l'information concernant sa fin d'activité sur le site internet www.preuve-electronique.org, en précisant notamment la date de fin d'activité ;
- l'Autorité d'horodatage abrogera les autorisations données aux sous-traitants d'agir pour son compte dans l'exécution de n'importe quelles fonctions touchant au processus de génération des contremarques de temps ;
- l'Autorité d'horodatage 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'organisme tiers sera sélectionné le cas échéant et **l'ADSN** s'assurera à ce stade du niveau de sécurité du service proposé par ce tiers ;
- l'Autorité d'horodatage maintiendra ou transférera à un organisme fiable ses obligations de rendre disponible aux utilisateurs de contremarques de temps pendant une période raisonnable ses clés publiques ainsi que ses certificats ;

- les clés privées des unités d'horodatage seront détruites de telle façon que les clés privées ne puissent pas être recouvrées. L'AH demandera la révocation de l'ensemble des certificats installés sur les serveurs KSTAMP
- l'Autorité d'horodatage fera établir un PV d'arrêt d'activité par un huissier pour constater l'arrêt réel ;

b) L'Autorité d'horodatage prend les mesures nécessaires pour couvrir les dépenses pour accomplir ces exigences minimales dans le cas où l'Autorité d'horodatage

tomberait en faillite ou pour d'autres raisons serait incapable de couvrir les dépenses par elle-même.

c) L'Autorité d'horodatage prendra des dispositions pour la fin du service. Cela inclura:
- un avis aux abonnés et aux utilisateurs de contremarques de temps ;
- un transfert des obligations de l'Autorité d'horodatage à d'autres organismes.

d) Préviendra le point de contact identifié sur le site de l'ANSSI http://www.ssi.gouv.fr ;

Le choix de l'organisme qui récupèrera les données d'audit sera défini dans le cadre du plan de fin d'activité mis en œuvre par l'AH. En tout état de cause, **l'ADSN** s'engage à maintenir les informations présentes sur le site www.preuve-electronique.org qu'il a publié pendant son activité d'OSH pour le compte du CSN.

L'AH provisionne les coûts nécessaires et suffisants pour maintenir le site de publication www.preuve-electronique.org.

6.3 Exigences physiques, environnementales, procédurales et organisationnelle

6.3.1 Exigences physiques et environnementales

6.3.1.1 Situation géographique et construction des sites

La localisation géographique des sites (Marseille et Clichy) ne nécessite pas de mesures particulières face à des risques de type tremblement de terre, explosion, risque volcanique ou crue.

6.3.1.2 Accès physique

Une procédure de gestion des accès physiques est rédigée (cf [ref_accès])
Les accès sont réglementés en fonction du rôle de confiance confié à la personne.

L'accès physique aux fonctions de génération des certificats, gestion des révocations, toutes fonctions opérées par l'OSH, est strictement limité aux seules personnes nominativement autorisées.

L'accès physique aux composantes du service d'horodatage supportant ces fonctions est limité aux seules personnes autorisées par la mise en place d'un périmètre de sécurité physique, permettant la séparation des rôles entre les différents intervenants, et par la mise en place d'un contrôle d'accès électronique par badge ou clé.

La traçabilité des accès est assurée par l'enregistrement des utilisations des badges électroniques.

En dehors des heures ouvrables, des mesures de détection d'intrusion physique sont mises en œuvre.

Des mesures de sécurité physique sont également mises en place pour limiter les accès aux supports sensibles (dossier de cérémonie des clés notamment) en plaçant les documents dans des armoires sécurisées ou locaux fermés.

Les procédures de génération, de renouvellement et de révocation technique d'un certificat sont opérées directement sur les interfaces du serveur d'horodatage KSTAMP.

Les composants d'horodatage sont hébergés dans la baie eIDAS qui bénéficie d'une sécurité renforcée. En ce sens seules des personnes habilitées à pénétrer dans les salles serveurs, à ouvrir la baie eIDAS et ayant le rôle d'opérateurs du serveur KSTAMP peuvent réaliser ces actions. Le nombre de ces personnes est extrêmement restreint et l'habilitation d'une nouvelle personne nécessite la validation du RSSI. Ce rôle de confiance est formalisé dans un courrier signé par le président de **l'ADSN** et le collaborateur en question.

6.3.1.3 Alimentation électrique et climatisation

Des mesures de secours sont mises en œuvre par l'OSH de manière à ce qu'une interruption de service d'alimentation électrique (mise en œuvre de moyens techniques tels que des onduleurs et groupes électrogènes, avec redondance des équipements), ou une défaillance de climatisation (redondance climatiseurs, alarmes de dysfonctionnement), ne portent pas atteinte aux engagements pris par l'AH en matière de disponibilité (gestion des révocations et informations relatives à l'état des certificats en particulier).

6.3.1.4 Exposition aux dégâts des eaux

La définition du périmètre de sécurité prend en considération les risques inhérents aux dégâts des eaux. Des moyens de protection sont mis en œuvre pour parer les risques résiduels (installation sur un plancher en surélévation pour parer une rupture de canalisation par exemple). Cette exigence est prise en considération par l'OSH pour les aspects archivage des enregistrements, relatifs aux documents papiers qui sont stockés dans une salle choisie en conséquence.

6.3.1.5 Structures physiques des bâtiments

Les bâtiments hébergeant l'OSH sont construits en suivant les règles de l'art.

6.3.1.6 Prévention et protection incendie

Les moyens de prévention et de lutte contre l'incendie permettent de respecter les engagements pris par l'AH en matière de disponibilité (gestion des révocations et informations relatives à l'état des certificats en particulier), et de pérennité de l'archivage, en mettant en œuvre de moyen de prévention (sensibilisation et formation du personnel), de détection (détecteur fumée et incendie) et de lutte contre l'incendie (signalisation et disposition d'extincteur dans les lieux sensibles).

6.3.1.7 Conservation des supports

Les moyens de conservation des supports permettent de respecter les engagements pris par l'AC en matière de restitution et de pérennité de l'archivage. Les archives et supports électroniques d'archivage sont placés et conservés en armoires fortes. Cette exigence est prise en considération par l'OSH pour les aspects archivage des enregistrements.

6.3.1.8 Mise hors service des supports

Les supports recensés comme sensibles en termes de confidentialité font l'objet de mesures de destruction lorsqu'ils parviennent en fin de vie (broyage sécurisé pour le papier, effacement des données). Cf. Procédure [ref_proc_destruction].

6.3.1.9 Sauvegarde hors site

L'ADSN possède une infrastructure d'horodatage sur trois sites distants pour permettre une reprise d'activité des services d'horodatage.

Le service d'horodatage garantit que son service est fonctionnel sur un des trois sites à un instant donné mais ne permet pas de reconstruire un service d'horodatage.

La présente DPH ne définit pas de procédure de sauvegarde pour les clés des UH. Les clés privées des UH sont générées sur un HSM et ne sont pas exportables.

Les fichiers d'audits sont stockés sur les serveurs d'horodatage et transmis sur le serveur de log du SMSI. La procédure de centralisation et d'archivage des fichiers sur le SMSI sont décrits dans le document [ref_trace].

Une procédure d'archivage des fichiers de sauvegarde est mise en œuvre par l'**ADSN**.

Le contenu de ces sauvegardes est décrit dans le paragraphe 6.2.2. Cette procédure d'archivage consiste à envoyer les données vers le système d'archivage mutualisé de l'**ADSN** qui permet de garantir la confidentialité et l'intégrité des données mises en archive. Les fichiers d'archives sont signés et horodatés en XADES-T.

6.3.2 Exigences procédurales

6.3.2.1 Analyse des risques

Le service d'horodatage fait partie du périmètre de l'étude de risques menée régulièrement par l'**ADSN**.

Le document référent applicable est le suivant : [ref_analyse_risque].

6.3.2.2 Gestion des supports

Le service d'horodatage se conforme à la politique de sécurité en vigueur à l'**ADSN**.

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. Ces exigences sont décrites dans le document applicable suivant [ref_proc_destruction].

6.3.2.3 Planification de systèmes

Le serveur KSTAMP permet de connaître le nombre de jetons émis par jour. Ce nombre est suivi régulièrement par l'OSH, qui met si besoin à l'ordre du jour des comités de pilotage des problèmes potentiels liés à la capacité du service d'horodatage.

6.3.2.4 Gestion des incidents

Un agent est installé sur les équipements pour relever des anomalies sur la base de mots clés configurés. Pour chaque anomalie détectée, une alerte est remontée dans une interface de supervision suivie par les équipes de « run » qui sont en charge de créer un ticket d'incident affecté aux équipes d'exploitation ou de sécurité pour traitement de l'incident.
Ces processus sont décrits dans la procédure [ref_incidents]

6.3.2.5 Manipulation et sécurité des systèmes

L'AH met en œuvre une politique de classification de l'information sur l'ensemble des éléments du service d'horodatage (voir [ref_classification]).

6.3.2.6 Procédures de fonctionnement et responsabilités

Les opérations de sécurité sur les composantes du service d'horodatage sont réalisées par du personnel de confiance qui est explicitement mis au courant de ses responsabilités et sont séparées du reste des opérations.

Les opérations de sécurité incluent notamment :

- Les procédures opérationnelles et les responsabilités ;
- La planification et la qualification des systèmes sécurisés ;
- La protection vis-à-vis du logiciel malveillant ;
- La maintenance avec support HP (alerte directe chez le fournisseur qui intervient en moins de 2 heures) ;
- La gestion du réseau d'interconnexion du serveur (LAN). Le Réseau REAL® est géré directement par l'ADSN ;
- Le contrôle actif des journaux d'audit, l'analyse des événements et les suites à donner et analyse des traces remontées au niveau du SMSI ;
- Le traitement et la sécurité des médias ;
- L'échange des données et du logiciel.

Les opérations d'exploitation et d'administration sont séparées.

6.3.2.7 Amélioration continue des systèmes d'information

Dans le cadre de la démarche d'amélioration continue, l'**ADSN**:

- réalise des audits,
- fait de la veille technologique,
- maintien à jour les composants du service d'horodatage,
- réalise des analyses de risques,
- déroule des recettes sécurité.

6.3.2.8 Gestion d'accès au système

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

L'accès aux systèmes du service d'horodatage est réservé aux seules personnes formellement habilitées. Les administrateurs sont munis d'un identifiant personnel permettant de tracer nominativement l'ensemble des accès aux systèmes.

Des équipements de filtrage sont positionnés en amont des serveurs d'horodatage pour garantir que seuls les flux nécessaires et suffisants sont autorisés à accéder à ces serveurs. Les équipements d'infrastructure sont positionnés dans une zone sécurisée.

Toutes les traces liées à l'administration des systèmes sont conservées conformément aux exigences exposées dans le paragraphe 6.2.2. Les incidents sur les serveurs d'horodatage font l'objet de remontées d'alertes vers une équipe en charge de les détecter (run) et les analyser (équipe exploitation et équipe sécurité) et de réagir selon des procédures formelles.

L'ensemble des traces est exposé dans le document [ref_trace]. Les traces sont regroupées sous 5 catégories :

- Evènements systèmes des différentes composantes de l'IGC : ces traces sont issues des traces systèmes de chacun des composants serveurs du service d'horodatage.
- Evènements liés à la journalisation du service d'horodatage : KSTAMP embarque une fonction de journalisation des différents événements et pour laquelle une action d'extraction des traces est mise en œuvre annuellement par l'**ADSN.**

- Gestion des administrateurs : les différents comptes administrateurs (profils) sont définis dans des fichiers de paramétrage, et associés à des DN de certificats spécifiques. Les demandes de certificats pour des administrateurs du service d'horodatage font l'objet d'une demande tracée auprès du responsable de l'AH.
- Paramétrage du contexte d'horodatage du serveur d'horodatage : ces traces constituent les données d'audit du serveur KSTAMP et font l'objet d'une extraction annuelle
- Fonctionnement de l'AH : ces éléments de vie du service d'horodatage sont tracés à travers les différents procès-verbaux des cérémonies de clés, des demandes de création et des demandes de destruction.

Les composants de réseau locaux sont mis dans un environnement physiquement sûr. Leurs configurations sont périodiquement vérifiées.

L'ADSN décrit les règles de sécurité à respecter dans les documents suivants :
- [ref_pssi]
- [ref_charte]

6.3.2.9 Déploiement et Maintenance

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

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

6.3.3 Exigences organisationnelles

6.3.3.1 Rôles de confiance

Les rôles de confiance suivant sont définis dans le document [ref_PH]. Les personnes identifiées pour ces rôles sont décrites explicitement dans le document [ref_role].

6.3.3.1.1AH

L'AH est le **CSN**.

6.3.3.1.2Prestataire de Services d'Horodatage Electronique

Le PSHE est **l'ADSN**, et s'organise à partir d'un Comité de Pilotage (revue de processus OSC / OSH) qui se réunit tous les mois.

6.3.3.2 Identification et authentification pour chaque rôle

Les personnes disposant d'un rôle de confiance sont notifiées formellement par un courrier signé par le président de l'**ADSN** ou d'**ADNOV** (filiale de l'ADSN) et le collaborateur en question.

L'authentification technique sur le serveur d'horodatage est définie dans le document [ref_kstamp].

6.3.3.3 Rôles exigeant une séparation des attributions

Les informations décrivant la séparation des attributions sont décrites dans le document [ref_PH].

L'OSH a défini dans le document [ref_role], les attributions associées aux rôles.

6.3.3.4 Mesures de sécurité vis à vis du personnel

6.3.3.4.1 Qualifications, compétences, et habilitations requises

Tout intervenant amené à occuper un rôle identifié comme sensible est soumis à une clause de confidentialité, gérée par l'employeur ou contractualisée dans le cas des mandataires.

L'OSH s'assurent que les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles.

Le personnel d'encadrement de l'OSH possède l'expertise appropriée, et est familier des procédures de sécurité.

Toute personne intervenant dans des rôles de confiance est informée de ses responsabilités (description de poste) et des procédures liées à la sécurité du système et au contrôle du personnel.

L'OSH organise de manière récurrente (au moins 1 fois par an) une session de formation à la sécurité (nouvelles menaces, bonnes pratiques de sécurité) pour les personnes opérants / exploitants l'infrastructure d'horodatage. Le contenu de la session de formation est décrit dans le document [ref_formation].

Un recensement des personnes formées aux applications (PKI, KSTAMP) est tenu à jour et une formation est assurée le cas échéant pour les nouvelles personnes intervenant dans l'infrastructure de confiance (nouveaux chargés d'application par exemple). Ce recensement identifie le niveau d'éducation et le niveau d'expérience des personnes.

6.3.3.4.2 Procédures de vérification des antécédents

Il est demandé aux personnes appelées à occuper un rôle sensible au sein du service d'horodatage de fournir une déclaration sur l'honneur attestant pour la personne :

- De ne pas avoir de conflit d'intérêt dans le poste qu'elle occupe ;
- De ne pas avoir commis de délits relatifs à la cybercriminalité.

6.3.3.4.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement.

Cela concerne essentiellement le personnel de l'**ADSN** opérant sur les composantes du service d'horodatage.

Les personnels participant au service d'horodatage ont notamment des connaissances sur les thèmes suivants :

- Technologie et fonctionnement de l'horodatage ;
- Technologie et principe de la signature électronique ;
- Connaissance des principes de calibration et de synchronisation des horloges de temps ;
- Connaissance et respect des règles de sécurité pour les personnels techniques.

6.3.3.4.4 Exigences en matière de formation continue et fréquences des formations

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux intervenants dans la mesure où cette évolution impacte le mode de travail de ces intervenants.

Les intervenants sont formés à la gestion des incidents et sont au fait de l'organisation de remontée d'incidents (hotline et processus de suivi).

6.3.3.4.5Fréquence et séquence de rotations entre différentes attributions

Sans objet.

6.3.3.4.6Sanctions en cas d'actions non autorisées

Se reporter au règlement intérieur [ref_reglement_interieur].

6.3.3.4.7Exigences vis à vis du personnel des prestataires externes

Les exigences vis-à-vis des prestataires externes sont contractualisées. Il s'agit essentiellement du personnel de surveillance du site de Venelles, de l'hébergeur du site de Clichy, de l'hébergeur des sites de Marseille, du centre de services de télépilotage et des équipes de l'éditeur du serveur d'horodatage qui a en charge le maintien opérationnel du système.

Les types d'engagement sont des contrats relatifs à la réalisation d'une prestation, des engagements de confidentialité et une charte d'utilisation des moyens informatiques.

6.3.3.4.8Documentation fournie au personnel

Les règles de sécurité sont communiquées au personnel lors de la prise de poste, en fonction du rôle affecté à l'intervenant. Les personnes appelées à occuper un rôle opérationnel dans le service d'horodatage disposent des procédures correspondantes.

6.4 Exigences de sécurité techniques

6.4.1 Exactitude du temps

Les horloges des UH sont synchronisées localement sur le serveur d'horodatage.

Ce dernier se synchronise conformément à ce qui est décrit dans le paragraphe 6.2.4.
Le système d'horodatage des Notaires est donc synchronisé avec au moins un serveur UTC(k). Cette synchronisation se fait via NTP. Ceci permet de mettre en évidence que le temps au sein du système d'horodatage est fiable.

La précision du service d'horodatage est égale à 1 seconde.

Les dispositifs de contrôles de la synchronisation sont assurés par :

- le serveur d'horodatage KSTAMP ([ref_kstamp]) ;
- le serveur de temps autonome ([ref_temps]).

6.4.2 Génération des clés

Les clés privées des UH sont des clés de 2048 bits pour les clés générées avant le 01 janvier 2024, et 3072 bits pour les suivantes, générées directement depuis les interfaces du serveur d'horodatage. Ces clés sont générées puis stockées sur le HSM associé au serveur d'horodatage.

La procédure de génération est décrite dans le document [ref_kstamp].

La génération des clés privées des unités d'horodatage est réalisée durant une cérémonie des clés qui fait l'objet d'un procès-verbal, réalisée dans un environnement sécurisé par des personnels de confiance au moins sous double contrôle.

6.4.3 Certification des clés de l'UH

Une fois la clé privée générée par le serveur d'horodatage, une CSR est émise. La procédure de certification de cette clé est une procédure manuelle qui consiste à :

- Copier la CSR sur une clé USB ;
- Déposer la CSR sur le serveur PKI de l'AC REALTS ;
- De sélectionner dans les interfaces de la PKI le profil « REALTS Horodatage » ;
- De procéder à la signature de la clé ;
- De récupérer le certificat ainsi généré et le stocker sur la clé USB ;
- D'installer le certificat sur l'unité d'horodatage depuis les interfaces de KSTAMP.

Ces opérations sont réalisées durant une cérémonie des clés, décrite dans le document [ref_kc]. Le document de cérémonie des clés est établi pour chaque cérémonie. Il se matérialise sous forme d'un script signé par les participants et qui sert de Procès-Verbal.

Les clés sont signées par une AC suivant les recommandations de [EN_319411] et dont la PC est décrite dans le document suivant [ref_pc_realts].

6.4.4 Protection des clés privées des UH

Les clés privées des UH sont stockées dans un HSM Bull Proteccio. Ce module est qualifié par l'ANSSI au niveau renforcé .

6.4.5 Exigences de sauvegarde des clés des UH

La présente PH ne comporte pas de politique de sauvegarde des clés des UH. Les clés des UH ne sont ni exportables ni sauvegardables. En cas de pertes des clés, une nouvelle cérémonie sera organisée pour en générer des nouvelles et établir un nouveau certificat sur le boîtier.

6.4.6 Destruction des clés des UH

Les interfaces de KSTAMP permettent de procéder à la destruction de la clé privée, intégrant de fait les actions suivantes :

- Suppression de la clé privée dans la configuration du serveur d'horodatage (destruction du contexte d'horodatage) ;
- Destruction réelle de la clé sur le module HSM via son interface d'administration.

6.4.7 Algorithmes obligatoires

L'AH, dans la limite des algorithmes qu'elle reconnaît :

- Accepte des valeurs de hachage générées par des clients et employant les algorithmes de hachage conformes à [TS_119312]. Les algorithmes de calcul d'empreinte numérique acceptés sont SHA-256 et SHA-512;
- Génère des contremarques de temps signées selon les algorithmes et les longueurs de clés conformes à [TS_119312]. Les bi-clés de l'UH sont des bi-clés RSA de 2048 bits pour les clés générées avant le 01 janvier 2024, et 3072 bits pour les suivantes, utilisant l'algorithme SHA-512.

Il est donc de la responsabilité des applications utilisatrices de se conformer à [TS_119312] et de générer des condensats à horodater à l'aide de la fonction SHA-256 ou SHA-512.

6.4.8 Vérification des contremarques de temps

Les contremarques de temps sont vérifiées :

- En local sur le poste du Notaire, lorsque la demande est faite par une application métier. Cette vérification est effectuée par le logiciel de signature, installé sur le poste de l'utilisateur à l'origine de la requête, et intégré au logiciel métier ;

- A travers l'un des serveurs de validation de l'**ADSN** à l'occasion de chaque transaction métier lorsque la demande est faite par une application de dématérialisation notariale.

Les vérifications mises en œuvre sont de manière synthétique :

- Vérification de la postériorité de l'horodatage du jeton par rapport à la date contenue dans la signature électronique ;
- Vérification de l'empreinte du jeton d'horodatage avec l'empreinte fournie par l'application appelante ;
- Vérification de la signature du jeton d'horodatage ;
- Remontée de la chaîne de confiance d'AC du certificat de l'Unité d'Horodatage ;
- Vérification de la validité des certificats de la chaîne de confiance de certificats d'AC à partir des CRL à la date de la vérification ou du service OCSP mis à disposition

Si une application tierce souhaite vérifier la validité d'un jeton délivré par l'AH, il faut alors :

- Vérifier que le gabarit du jeton est bien conforme aux éléments décrits en [ref_gabarit];
- S'assurer que le jeton a été signé par un certificat émis par l'AC REALTS et dont le gabarit du certificat est décrit en [ref_gabarit];
- S'assurer de la chaîne de certification correspondante jusqu'à l'AC racine « Notaires de France » ;
- S'assurer que le certificat d'horodatage utilisé n'était pas révoqué au moment de l'horodatage ;
- Vérifier que le condensat présent dans le jeton représente bien les données à horodater. Cela consiste à calculer de nouveau le condensat des données à horodater avec les paramètres cryptographiques définis dans le jeton et à comparer le résultat du condensat obtenu avec celui présent dans le jeton ;
- S'assurer que le contenu du champ « accuracy » présent dans le jeton est bien égal à 1 seconde.

6.4.9 Durée de vie des clés publiques des UH

La durée de vie des clés publiques des UH est de 3 ans. Cette durée ne pourra être plus longue que :

- La durée de vie cryptographique de l'algorithme utilisé pour la signature ;
- La durée de vie du certificat de l'AC qui l'a émis.

6.4.10 Durée d'utilisation des clés privées des UH

La durée d'utilisation des clés privées des UH est de 1 an maximum à partir de la date d'activation du certificat sur l'UH. La date d'activation du certificat est le début d'utilisation des clés privées.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

6.5.1.1 Identification et authentification

Les systèmes, applications et bases de données identifient et authentifient de façon unique les administrateurs. Toute interaction entre le système et un utilisateur n'est possible qu'après une identification et une authentification soient réussies. Pour chaque interaction, le système établit l'identité de l'entité.

Différents modes d'authentifications sont utilisés selon les applications de la plate-forme OSH : par mot de passe sur les serveurs LANTIME ; l'accès aux interfaces du KSTAMP est contrôlé par certificat.

Chaque certificat est nominatif et les interfaces d'authentification du KSTAMP sont configurées pour n'autoriser que les certificats formellement habilité et émis par l'AC REALTECH.

Les informations d'authentification sont stockées de façon telle qu'elles sont seulement accessibles par des utilisateurs autorisés (personnel de confiance).

6.5.1.2 Contrôle d'accès

Les profils et droits d'accès aux équipements de l'OSH sont définis et documentés, ainsi que les procédures d'enregistrement et de « désenregistrement » des utilisateurs, dans les documents [ref_gestion_droits].

Les accès physiques sont exclusivement réservés aux personnes habilitées ou sous l'accompagnement d'une personne habilitée. Cette règle s'applique sur l'ensemble des sites d'hébergement de l'AH.

La gestion des droits dans le service d'horodatage est basée sur une reconnaissance des DN des certificats des personnes habilitées à accéder aux interfaces.

Les supports utilisés par les intervenants autorisés de l'OSH sont manipulés conformément aux exigences du plan de classification.

6.5.1.3 Administration et exploitation

Un ensemble cohérent de procédures et de documentation sous la responsabilité de l'OSH permettent l'administration et l'exploitation sécurisée de l'AH :

- L'utilisation de programmes utilitaires est restreinte et contrôlée ;
- Les procédures opérationnelles d'administration et exploitation de l'AH sont documentées, suivies et régulièrement mises à jour ;
- Les fichiers de configuration systèmes sont référencés. L'intégrité des fichiers de configuration système est vérifiée de manière automatique (calcul d'empreintes et comparaison par rapport à une base de référence).
- La configuration des équipements réseaux est contrôlée hebdomadairement par le SOC de l'**ADSN**.
- Des mesures de durcissement des composants de l'AH sont mises en œuvre ;
- Les conditions de mise en service (paramétrage initial de sécurité des serveurs) sont documentées ;
- Les conditions de fin de vie (destruction et mise au rebut) des équipements sont documentées afin de garantir la non divulgation des informations sensibles qu'ils peuvent détenir ;
- Les matériels sensibles de l'AH sont maintenus afin de garantir la disponibilité des fonctions et des informations ;
- Les personnels concernés par ces procédures sont désignés, conformément au document [ref_role] ;
- La maintenance des services d'horodatage est prise en compte dans le processus de gestion du changement mis en œuvre au sein de l'**ADSN**.

6.5.1.4 Intégrité des composantes

Des mesures de maîtrise de détection et de prévention sont mises en œuvre sur l'ensemble des composants du PSHE afin de fournir une protection contre les logiciels malveillants, par l'intermédiaire des plateformes Sécurité de l'**ADSN**, fournissant les fonctions de passerelle entre l'Intranet et l'Internet, et disposant de moyen de filtrage de flux (pare-feu) et d'anti-virus.

Les composantes du réseau local (OSH) sont maintenues dans un environnement physiquement sécurisé par l'intermédiaire d'une architecture à base de pare-feux ; des vérifications périodiques de conformité de leur configuration sont effectuées.

Une revue des configurations des composantes du système est réalisée hebdomadairement.

Des tests de pénétrations sont réalisés régulièrement par l'OSH sur l'ensemble du périmètre de l'IGC. Les résultats des tests de pénétration sont accessibles ici [ref_resultats_penetration].

Une veille vulnérabilités quotidienne est mis en place sur le périmètre OSH.
Pour chaque vulnérabilité critique détectée, une analyse est effectuée dans un délai de 48h maximum après détection.
En cas de décision de non application de patch de sécurité ou de correction de la vulnérabilité concernée, les raisons sont documentées.

6.5.1.5 Sécurité des flux

Des mesures de sécurité sont mises en œuvre de manière à garantir l'authentification d'origine, l'intégrité et la confidentialité le cas échéant des données échangées entre entités intervenant dans le processus.

6.5.1.6 Journalisation et audit

Un suivi d'activité est effectué au travers des journaux d'événements. Les événements journalisés sont les événements système et les événements applicatifs, tels que décrit dans le document [ref_trace].

6.5.1.7 Archivage des données

6.5.1.7.1Types de données à archiver

Voir [ref_ph]

6.5.1.7.2Période de conservation des archives

Voir [ref_ph]

6.5.1.7.3Protection des archives

Concernant la protection des archives, elles sont transférées sur un support de stockage à long terme de type WORM. La garantie de confidentialité et de pérennité est alors assurée par le support de conservation.

6.5.1.7.4Procédure de sauvegarde des archives

Le tableau suivant précise la fréquence et le support de sauvegarde par type de données.

Type de données	Fréquence	Support d'archivage
Logiciels	A chaque mise en production	Bibliothèque des supports définitifs
Configurations des logiciels	A chaque mise en production	Bibliothèque des supports définitifs
Journaux système	Tous les jours	Serveur d'archivage
Journaux techniques	Tous les jours	Serveur d'archivage
Journaux de l'application d'horodatage	Tous les jours	Serveur d'archivage
Journaux NTP	Tous les jours	Serveur d'archivage

Evènements fonctionnels	Tous les jours	Base de données KSTAMP
Documentation	A chaque mise à jour	Ariane
Documents papier	A chaque production	Armoire PKI

Les évènements sont journalisés dans la base de données du KSTAMP. Aucun évènement n'est purgé.

Le serveur d'archivage est sauvegardé tous les soirs également.

Les demandes de contremarques et les contremarques émises sont archivées.

6.5.1.7.5Exigences d'horodatage des données

L'horodatage des données des événements journalisés est synchrone en dehors des opérations hors ligne. Pour cela, les composants de l'AH sont synchronisés sur un même serveur synchronisé avec l'heure universelle. La fourniture de l'heure universelle est assurée par un service NTP porté par un serveur d'infrastructure, synchronisé sur les serveurs de temps autonomes. Ce système offre une précision de l'heure à 1 seconde.

6.5.1.7.6Système de collecte des archives

Sans objet.

6.5.1.7.7Procédure de récupération et de vérification des archives

La récupération et la vérification des archives sont effectuées dans un délai conforme à l'utilisation des certificats délivrés. Un délai de 7 jours ouvrés est nécessaire pour récupérer les archives. Toute vérification nécessite une demande de consultation. Cf. [ref_archive].

6.5.1.8 Supervision et contrôle

Une surveillance permanente est mise en place et des systèmes d'alarme installés pour détecter enregistrer et réagir rapidement face à toute tentative non autorisée et ou irrégulière d'accès aux ressources physique (détection d'intrusion physique dans bâtiment de l'OSH à Venelles, Marseille et à Clichy) et logique (passerelles de filtrages de flux) des systèmes informatiques.

La liste des événements journalisés est décrite dans [ref_trace].

6.5.1.9 Sensibilisation

L'usager du service d'horodatage est l'équipe sécurité de l'**ADSN** qui définit et implémente les politiques d'horodatage.

L'OSH s'assure d'avertir et de sensibiliser aux problématiques d'horodatage les équipes métiers de **l'ADSN** utilisatrices au travers de leurs applications.

Les sessions de formation organisées par l'AH contribuent à cette sensibilisation [ref_formation].

Lorsqu'une faille de sécurité est observée sur une des composantes de l'OSH, les personnes concernées sont mises au courant de l'impact de cette faille, et un plan d'action est défini pour couvrir cette faille sous un délai raisonnable.

6.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Le PSHE met en œuvre un Système de Management du Système d'Information (SMSI).

6.6 Mesures de sécurité liées au développement des systèmes

Les infrastructures de développement et d'essai sont séparées des infrastructures opérationnelles du service d'horodatage. Deux plateformes sont utilisées : une plateforme de pré-production et une plateforme de production.

Les critères de recette et validation de nouveaux systèmes d'information, de mises à niveau et nouvelles versions sont établis et des essais adéquats du système sont effectués avant sa recette et sa mise en production. Cf. [ref_changement].

Un plan de capacité est établi pour garantir le bon traitement des demandes de contremarques de temps traitées par l'AH REALTS. Cf. [ref_capacite]

6.7 Mesures de sécurité réseau

Les mesures mises en place répondent à l'analyse de risques effectuée sur le système d'information [ref_analyse_risque].

Les communications réseaux véhiculant des informations confidentielles font l'objet de mesures de protection contre l'écoute des informations sur la base du protocole SSL.

Des scans périodiques de détection de vulnérabilités sur les équipements du PSHE accessibles depuis l'Intranet des notaires (Réseau REAL) ou l'Internet sont conduits.

Des passerelles de sécurité sont mises en place afin de protéger la composante locale du système d'information des accès non autorisés depuis l'Intranet des notaires (Réseau REAL) et Internet.

Les accès aux interfaces techniques du KSTAMP se font depuis les salles hébergeant les serveurs ou depuis la salle d'administration à distance de Venelles. Seuls les opérateurs de l'AH ont accès à ces interfaces.

Un ensemble d'équipements de filtrage protègent l'AH en scindant l'infrastructure en plusieurs zones fonctionnelles protégées.

La redondance des accès sur les services du PSHE exposés sur Internet est assurée par la mise en œuvre de deux accès réseaux distincts.

7 DOCUMENTS CITÉS EN RÉFÉRENCE

7.1.1 Réglementations

Renvoi	Document
[eIDAS]	Règlement Européen 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 et abrogeant la directive 1999/93/CE

7.1.2 Documents techniques

Renvoi	Document
[RFC_3161]	IETF - Internet X.509 Public Key Infrastructure - Time-Stamp Protocol - 08/2001
[EN_319401]	General Policy Requirements for Trust Service Providers
[EN_319421]	Policy & security requirements for TSP issuing time-stamps
[EN_319422]	Time-stamping protocol and time-stamp profiles
[TS_119312]	Cryptographic suites
[EN_319401]	General Policy Requirements for Trust Service Providers
[EN_319421]	Policy & security requirements for TSP issuing time-stamps
[EN_319422]	Time-stamping protocol and time-stamp profiles
[PSCO_QUALIF]	Exigences de l'ANSSI applicables pout tout prestataire de service de confiance qualifié (https://www.ssi.gouv.fr/uploads/2017/01/eidas_psc-qualifies_v1.2_anssi.pdf)
[PSCO_HORO]	Exigences de l'ANSSI applicables pour tout prestataire d'horodatage qualifié (https://www.ssi.gouv.fr/uploads/2016/06/eidas_horodatage-qualifie_v1.1_anssi.pdf)
[TS_119312]	Cryptographic suites
[ref_doc]	Plan d'attribution des OID
[ref_gabarit]	Description des certificats et CRL
[ref_PH]	Politique d'horodatage dont l'OID est 1.2.250.1.78.2.1.3.5.4.6.1.1
[ref_role]	Rôles et responsabilités
[ref_actifs]	Inventaire des actifs
[ref_kstamp]	Spécifications techniques des applications d'horodatage d'ATOS (guide installation, guide de configuration…)
[ref_temps]	Manual LANTIME M300 GPS PZF GPS-DCF77 NETWORK TIME SERVER (15/09/2009)
[ref_cgu]	CGU Horodatage 1.2.250.78.1.1.3.1.4.6.1.8
[ref_PC_realts]	PC AC REALTS 1.2.250.1.78.2.1.3.5.1.1
[ref_dpc_realts]	DPC AC REALTS 1.2.250.1.78.2.1.3.5.1.2
[ref_analyse_risque]	Analyse des risques
[ref_kc]	PV de cérémonie des clés pour chaque cérémonie
[ref_proc_destruction]	Procédure Gestion des destructions des données sensibles
[ref_classification]	Maitrise de la documentation
[ref_trace]	Recensement et gestion des traces
[ref_pssi]	PSSI l'**ADSN**
[ref_charte]	Charte Informatique
[ref_reglement_interieur]	Règlement intérieur l'**ADSN**
[ref_compromission]	Procédure de gestion des compromissions et suspicions de compromission des composants d'horodatage

[ref_bascule]	Mode Opératoire de la bascule OSH
[ref_pra]	Plan de reprise d'activité des services de confiance l'**ADSN**
[ref_bia]	Analyse de risques + Gérer la bascule PSCE PSHE
[ref_incidents]	Procédure de gestion des incidents OSH
[ref_formation]	Support des sessions de formation à la sécurité des SI
[ref_gestion_droits]	Procédure Validation des demandes d'accès et Gérer les habilitations
[ref_configuration]	Référentiel des configurations des composants de l'AH
[ref_resultats_penetration]	Résultats des tests de pénétration réalisés sur l'infrastructure d'horodatage
[ref_archive]	Procédure de gestion des archives OSH
[ref_changement]	Procédure de gestion des changements
[ref_capacite]	Plan de capacité de la charge du service d'horodatage
[ref_accès]	Procédure Attribuer un badge d'accès et procédure Gérer les exceptions d'accès
[ref_AlgoSynchroTemps]	Documentation technique NTP Monit

8 EXIGENCES SUR LES FORMATS DES CONTREMARQUES DE TEMPS, DES CERTIFICATS ET DES LCR ET SUR LES ALGORITHMES CRYPTOGRAPHIQUES

8.1 Contremarque de temps

Les contremarques de temps fournies par l'AH ont une structure TimeStampToken conforme au [RFC_3161].

Le tableau ci-dessous reprend l'ensemble des champs d'un TimeStampToken tels que définis dans le [RFC_3161].

Une contremarque de temps conforme à la présente PH respecte, de base, les exigences correspondantes du [RFC_3161], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Exigences
messageImprint	Valeur hachée du message suivant l'algorithme défini dans le paragraphe suivant
Accuracy	Ce champ est positionné et contient une valeur inférieure ou égale à 1 seconde.
Ordering	Ce champ n'est pas positionné
Tsa	Ce champ n'est pas positionné
certReq	Quelle que soit la valeur de la requête, le jeton contient toujours la chaîne de certification associée
Extensions	Aucune extension n'est marquée critique

8.2 Certificats et LCR

Les gabarits des certificats d'UH et des LCR sont conformes aux exigences décrites dans [AC REALTS].

Il est rappelé ici que :

- L'extension « Extended Key Usage » est présente, marquée critique, et ne contient que l'identifiant « id-kp-timeStamping » à l'exclusion de toute autre ;
- Le champ « DN Subject » identifie l'AH suivant les mêmes règles que l'identification des AC et l'identifiant propre à l'UH concernée, au sein de l'AH, est porté dans l'attribut commonName du DN de ce champ (au sein d'une AH, chaque UH a un identifiant unique) ;
- La durée de vie maximale est bornée selon le couple {durée de vie cryptographique de la clé ; fin de validité de la durée de vie de l'AC émettrice}.

8.3 Algorithmes cryptographiques

L'algorithme mis en œuvre pour la génération des certificats et le calcul des hachés dans les contremarques de temps est SHA-512. Cet algorithme respecte les exigences prévues dans [TS_119312].

9 EXIGENCES DE SÉCURITÉ DU MODULE D'HORODATAGE DES UH

9.1 Exigences sur les objectifs de sécurité

Le module d'horodatage, utilisé par l'AH pour générer et mettre en œuvre les clés de signature des UH et pour générer les contremarques de temps, répond aux exigences de sécurité suivantes :

- Garantir que la génération des bi-clés des UH est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- Assurer la confidentialité et l'intégrité des clés privées de signature des UH durant tout leur cycle de vie, et permettre leur destruction sûre en fin de vie ;
- Garantir l'authenticité et l'intégrité des clés publiques lors de leur export hors du module (à fins de certification par une AC) ;
- Lors de son importation dans le module, vérifier la correspondance entre le certificat importé et la clé publique de l'UH contenue dans le module ;
- Etre capable d'identifier et d'authentifier ses utilisateurs ;
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- Etre capable de mener une série de tests, lors des phases d'initialisation, de personnalisation et d'opération, pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Etre capable de détecter les tentatives d'altérations physiques et d'entrer dans un état sûr quand une tentative d'altération est détectée ;
- Permettre de créer une signature numérique, pour signer les contremarques de temps générées par l'UH, qui ne révèle pas les clés privées de l'UH et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- Empêcher toute importation / exportation des clés privée de l'UH ;
- Garantir la synchronisation de son horloge avec le temps UTC suivant la précision définie dans la présente DPH ;
- Fournir des contremarques de temps conformes aux requêtes reçues.

9.2 Exigences complémentaires

Le module cryptographique utilisé pour stocker les clés privées des UH est qualifié au niveau renforcé par l'ANSSI.

10 VÉRIFICATION DES CONTREMARQUES DE TEMPS

10.1 Empilement des contremarques de temps

Les contremarques de temps peuvent être validées durant la durée de vie du certificat de l'UH qui a signé la contremarque.

Pour maintenir la capacité de vérifier une contremarque de temps après la durée de vie du certificat de l'UH qui a signé cette contremarque, les applications utilisatrices peuvent si nécessaire procéder à un réhorodatage de la contremarque de temps initial.

Pour pouvoir réaliser ces opérations d'empilement de contremarques de temps et permettre leur vérification, l'AH archive via l'AC REALTS l'ensemble des CRL valides publiées.

Le processus de vérification consistera alors sur ces bases à vérifier chacune des contremarques de temps empilées.

10.2 Gestion de la révocation par l'AC REALTS

L'AC REALTS publie des CRL qui permettent d'attester de l'état du certificat d'une UH.
L'AC REALTS met à disposition sur Internet un service OCSP.

11 PRÉCISION DE LA SYNCHRONISATION DE L'HORLOGE

La précision de l'horloge est égale à 1 seconde par rapport au temps UTC(k). Cette précision est indiquée dans la contremarque de temps à travers le champ « accuracy ».

12 PROTOCOLE D'HORODATAGE

12.1 Conformité RFC 3161

La validité de la conformité à la [RFC_3161] est obtenue par :

- L'utilisation d'un serveur d'horodatage conforme aux règlementations et normes en vigueur ;
- Le passage réussi à des outils de validation de la contremarque de temps.

12.2 Conformité EN 319422

Le profil des contremarques de temps est conforme à [EN_319422].

13 GABARIT DE CERTIFICAT D'UNE UH

Les certificats des Unités d'Horodatage mises en œuvre par l'AH sont disponibles sur le site https://www.preuve-electronique.org.

[i] https://webtai.bipm.org/database/showlab.html