CONSEIL SUPÉRIEUR DU NOTARIAT

Politique d'Horodatage du Notariat

Version	Date	Description	Auteurs	Approbateur
1.1	16/05/2019	Prise en compte RGPD et changement REAL.NOT en ADSN	REAL.NOT	Membre du bureau du CSN
1.2	29/09/2020	§1.2.2 – Précision « plage de service » §6.2.1 – Correction sens de la phrase pour ecrire : « Les demandes de contremarques et les contremarques émises sont archivées. » §6.5.1.7 – Précision dans le tableau des durées de conservation	ADSN	Membre du bureau du CSN
1.3	21/01/2021	§1.3 Correction des écarts de l'audit eIDAS de janvier 2021. Rajout de la déclaration de conformité au niveau ETSI NCP+ de l'AC REALTS. Ajout de la colonne "Approbateur"	ADSN	Membre du bureau du CSN
1.4	25/01/2021	Prise en compte des remarques de l'audit à blanc eIDAS de juillet 2020 o Modification du paragraphe 6.5.1.4	ADSN	Membre du bureau du CSN
1.5	18/10/2022	Mise à jour et corrections mineures Modification du délai de récupération d'archive	ADSN	Membre du bureau du CSN
1.6	12/03/2024	Mise à jour des tailles des clés et charte CSN. Anonymisation du tableau.	ADSN	Membre 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	PUBLIQUE
OID du document	
1.2.250.1.78.2.1.3.5.4.6.1.1	
Cette politique est conforme à la politique de l'ETSI dont l'OID est le suivant :	
0.4.0.2023.1.1	

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 politique d'horodatage du **Notariat** (ci-après « PH ») présentant ce service d'horodatage.

Dans le cadre de la présente PH, 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.

L'objectif de ce document est de définir les engagements que le CSN, en tant qu'AH, respecte dans la délivrance et la gestion de contremarques de temps, ainsi que les obligations des autres participants.

Le présent document est complété, dans sa partie mise en œuvre, par une Déclaration des Pratiques d'Horodatage (DPH) et des Conditions Générales d'utilisation du service d'horodatage (CGU).

Une 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 (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.

Cette PH n'impose pas d'exigences sur le lien entre l'empreinte numérique à horodater et le contenu de la donnée électronique qui en est à l'origine. Cette vérification est à la charge de l'utilisateur du 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 « Politique d'Horodatage du Notariat » est identifiée, au sein du référentiel documentaire de l'infrastructure de confiance de l'**ADSN**, par un numéro d'identification unique, l'OID : 1.2.250.1.78.2.1.3.5.4.6.1.1.

Les contremarques de temps respectant la présente politique, la référenceront en utilisant ce numéro d'identification unique « OID » (cf. chapitre 6.2.5).

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 Politique d'Horodatage est validée par le Comité d'Approbation

La présente Politique d'Horodatage est publiée sur l'URL : http://www.preuve-electronique.org/PH_1.2.250.1.78.2.1.3.5.4.6.1.1.pdf

L'ensemble des informations associées notamment les versions antérieures de ces documents, sont également publiées sur le site www.preuve-electronique.org. La plage de service de ce site est 24h/24 et 7j/7.

1.2.3 Procédures d'approbation de la conformité de la DPH

L'approbation de la conformité de la DPH à la Politique d'horodatage est prononcée par le CSN, au vu des audits effectués.

1.2.4 Processus de mise à jour

1.2.4.1 Circonstances rendant une mise à jour nécessaire

La mise à jour de la Politique d'Horodatage est un processus impliquant tous les acteurs et faisant l'objet d'une démarche rigoureuse. Il est enclenché essentiellement pour procéder à des modifications importantes, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique ou combler des lacunes.

La Politique d'Horodatage est réexaminée à minima tous les deux ans.

1.2.4.2 Prise en compte des mises à jour

Toutes les remarques, ou souhaits d'évolution, sur la présente politique sont à adresser par courriel à l'adresse suivante :

exploitation.carte.real@notaires.fr

Ces remarques et souhaits d'évolution sont examinés par le bureau du CSN, qui engage si nécessaire le processus de mise à jour de la présente Politique d'Horodatage.

1.2.4.3 Information des acteurs

Lorsqu'une mise à jour a été planifiée, les informations relatives à cette évolution sont mises en ligne sur les lieux de publication (cf. 1.2.2).

Indépendamment de ce mode de communication, les acteurs peuvent à tout moment se renseigner auprès du Comité d'Approbation pour obtenir plus d'informations, en envoyant un mail à exploitation.carte.real@notaires.fr.

La publication d'une nouvelle version de la Politique d'Horodatage consiste à archiver la version précédente et mettre en ligne dans le répertoire prévu à cet effet, les éléments suivants :

- Document au format PDF ;
- OID du document ;

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

Lorsqu'une nouvelle version de la Politique d'Horodatage est mise en ligne, tous les utilisateurs des infrastructures notariales, et tous les représentants de ses principaux partenaires, sont informés par l'intermédiaire d'au moins un des canaux de communication habituels de la profession (message sur le portail intranet, courriers aux partenaires, presse interne de la profession notamment).

La nouvelle version de la Politique d'Horodatage entre en vigueur avant la génération d'une contremarque de temps portant l'OID de la Politique d'Horodatage concernée.

1.2.6 Cohérence de la documentation

Cette Politique d'Horodatage décrit le contexte de production de contremarques de temps et, de fait, ne constitue qu'une brique du référentiel documentaire de l'**ADSN**.

Le bureau du CSN s'assure de la cohérence de ce référentiel documentaire et de l'adéquation de la présente Politique d'Horodatage avec les autres documents, plus particulièrement les politiques de signature et de certification.

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.

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

- la valeur de hachage et l'algorithme de hachage de la donnée qui a été horodatée ;
- la date et le temps universel (UTC) ;
- l'identifiant du certificat de l'UH qui a généré la contremarque de temps ;
- l'identifiant 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 [PC REALTS] est consultable à l'adresse suivante : www.preuve-electronique.org, et qui est conforme aux exigences ETSI de niveau NCP+ (0.0.2042.1.2).

Dans le cadre de cette PH, la date et le temps de chaque contremarque de temps sont synchronisés avec le temps UTC avec une précision de 1 seconde. La présente PH applique un format de contremarque de temps standard défini par le [RFC 3161]. La gestion de la synchronisation de l'horloge du service d'horodatage est détaillée au chapitre 6.2.4.

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 présente politique d'horodatage. La politique d'horodatage présente aux utilisateurs les engagements que prend l'autorité d'horodatage, notamment ceux pris en matière de sécurité, et décrit de façon macroscopique les moyens mis en œuvre pour tenir ces engagements. Elle revêt une grande importance car elle incarne le niveau de confiance atteint par le service d'horodatage. Elle traduit la reconnaissance formelle de l'importance accordée par l'autorité d'horodatage à la sécurité du service. Les exigences pour les services d'horodatage décrits dans ce document incluent des exigences portant, à la fois sur la gestion de l'horodatage et sur le fonctionnement des unités d'horodatage qui publient les contremarques de temps. L'Autorité d'horodatage, telle qu'identifiée dans la contremarque de temps, a la responsabilité d'assurer que ces exigences sont remplies.

La présente PH est élaborée sur la base des documents issus de [EN_319401], de [EN_319421] et de [EN_319422].

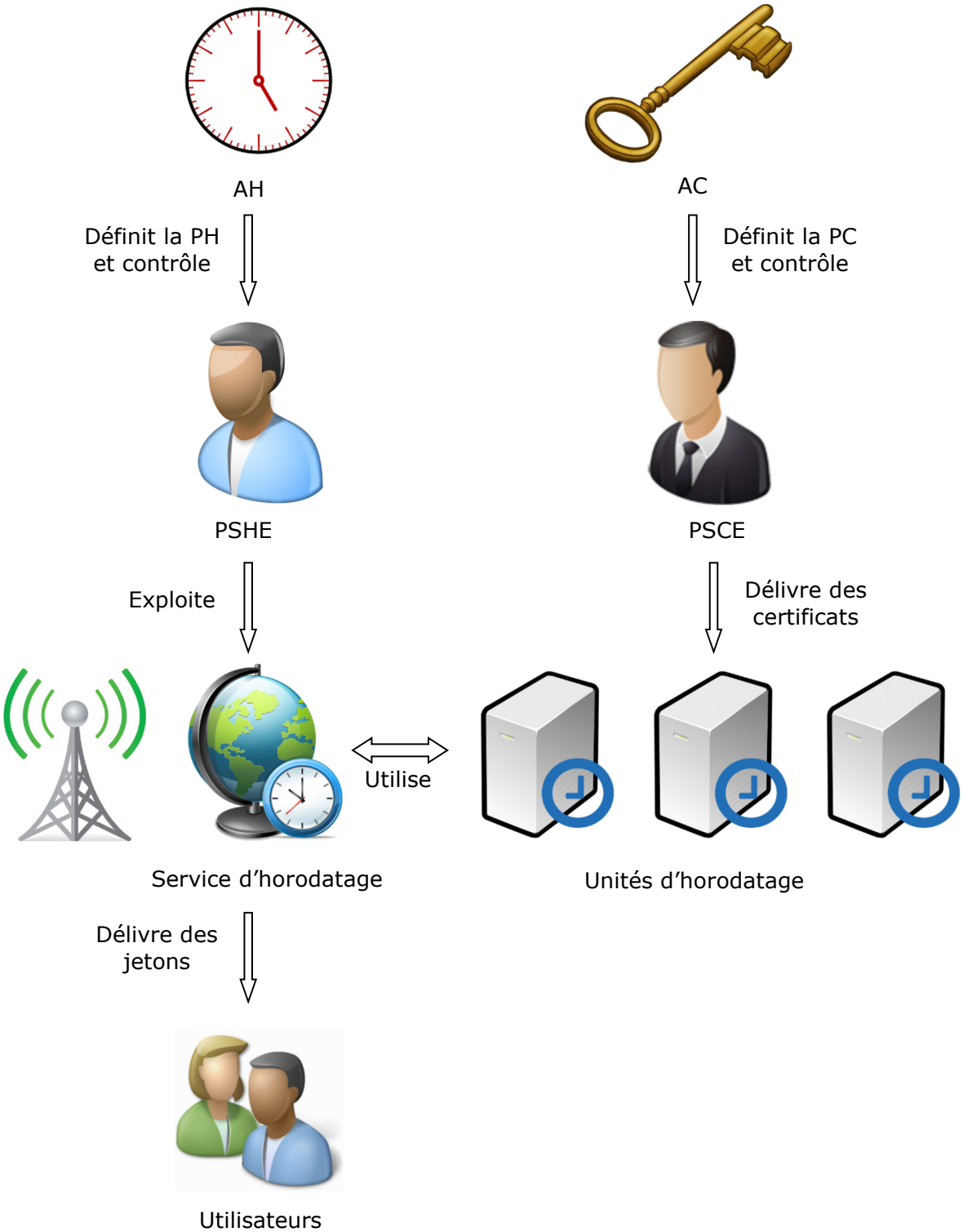
1.5 Entités intervenant dans le service d'horodatage

Le CSN est le responsable de l'Autorité d'Horodatage qui est exploitée et maintenue en condition opérationnelle par l'**ADSN**.

L'Autorité d'Horodatage utilise dans son service d'horodatage des boîtiers de temps qui assurent un niveau de performance conforme aux exigences exprimées dans [EN_319421], notamment au niveau de la gestion de la dérive et de la précision de temps fournies dans les contremarques de temps.

Le CSN est également le responsable de l'AC REALTS qui émet les certificats nécessaires aux unités d'horodatage du service d'horodatage du notariat.

La représentation schématique est alors la suivante :


AH
AC
Définit la PH et contrôle
Définit la PC et contrôle
PSHE
PSCE
Exploite
Délivre des certificats
Utilise
Service d'horodatage
Unités d'horodatage
Délivre des jetons
Utilisateurs

Les rôles et fonctions assumées par les différents acteurs sont les suivants :

<table>
<tr><th colspan="2">CSN</th><th colspan="2">ADSN</th><th colspan="2">Utilisateurs</th></tr>
<tr><th>Fonctions</th><th>Rôles</th><th>Fonctions</th><th>Rôles</th><th>Fonctions</th><th>Rôles</th></tr>
<tr><td rowspan="3">AH
Notaires</td><td>Définit la PH</td><td rowspan="4">PSHE</td><td>Utilise les UH à travers le service d'horodatage</td><td>Personnes physiques (porteurs)</td><td rowspan="3">Demande des jetons d'horodatage</td></tr>
<tr><td rowspan="2">Contrôle l'application de la PH par le PSHE</td><td>Exploite le service d'horodatage</td><td rowspan="2">Applications de dématérialisation</td></tr>
<tr><td>Délivre des jetons d'horodatage aux utilisateurs</td></tr>
<tr><td rowspan="2">AC REALTS</td><td>Définit la PC</td><td>Signe des demandes de certificats pour les UH</td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>Contrôle l'application de la PC par le PSCE</td><td rowspan="2">PSCE</td><td>Exploite les services de l'IGC</td></tr>
</table>

* Dans le contexte du Notariat, l'utilisateur « personne physique » est un porteur détenteur d'une clé REAL. La demande d'horodatage est dépendante du processus de demande de signature d'un document. Ce processus nécessite que le porteur saisisse le code PIN de sa clé REAL.

1.6 Autres aspects

Les unités d'horodatage utilisent des boîtiers cryptographiques matériels pour générer et stocker les clés privées des certificats électroniques de signature de contremarques de temps. Ces boîtiers sont qualifiés au niveau renforcé par l'ANSSI.

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. Le service d'horodatage n'est utilisé que dans le cadre des applications de dématérialisation du notariat fournies par l'ADSN. Dans le cas de cette présente PH, l'abonné est donc l'ADSN.

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
ADSN	Association pour le Développement du Service Notarial
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
Delta-LRC	Liste de Révocation des Certificats partielle
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

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

La présente PH impose un format de contremarque de temps spécifique, qui doit répondre aux exigences du chapitre 8 ci-dessous.

Cette politique impose l'usage d'un protocole d'horodatage spécifique pour demander et obtenir une contremarque de temps auprès d'une AH définie dans le RFC3161 et profilée dans le document [EN_319422].

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 ci-dessous ;
- la sauvegarde et l'import des clés privées 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.

4 DÉCLARATION DES PRATIQUES D’HORODATAGE

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

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

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

La politique d'horodatage est ainsi un document moins spécifique que la déclaration des pratiques d'horodatage.

La déclaration des pratiques d'horodatage est toujours approuvée par le CSN.

Comme la PH, la DPH est publiée sur le site de publication identifié au paragraphe 1.2.2.

5 CONDITIONS GÉNÉRALES D'UTILISATION

Compte tenu de la complexité de lecture d'une PH pour des utilisateurs non-spécialistes du domaine, l'AH définit également des conditions générales d'utilisation [CGU] 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'Autorités 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.

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 Politique, 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 présente PH et dans les Conditions Générales d'Utilisation applicables ;
- Garantie que la mise en œuvre des exigences exprimées dans le présent document est faite conformément à ce qui est décrit dans sa Déclaration des Pratiques d'Horodatage ;
- 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.
Les abonnés de contremarques de temps doivent :

- 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 abonnés de contremarque de temps doivent adhérer aux CGU prévues par l'AH et notamment accepter les limitations d'usages du service d'horodatage.

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.

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).

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) sont précisés dans la Politique de Certification de l'AC REALTS, consultable sur le site http://www.preuve-electronique.org.

L'AC REALTS met également en œuvre un service OCSP exposé sur Internet à l'adresse suivante : ocsp.preuve-electronique.org.

6.1.5 Déclaration des Pratiques d'Horodatage

L'AH a défini un document de Déclaration des Pratiques d'Horodatage décrivant la mise en œuvre des exigences prises dans la présente PH. Ce document interne, garantit que l'AH possède la fiabilité nécessaire pour fournir les services d'horodatage, notamment :

- L'AH a rédigé une analyse des risques de son service d'horodatage ;
- L'AH adresse l'ensemble des exigences décrites dans la présente PH ;
- La DPH décrit toutes les exigences que doivent respecter les éventuelles tierces parties dans le cadre du service d'horodatage

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 de signature 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, déclaration de pratiques et conditions générales d'utilisation 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.

L'AH garantit que tout changement majeur dans ses pratiques d'horodatage fera l'objet d'une notification auprès de l'organe de contrôle ayant délivré la qualification eIDAS du service d'horodatage.

6.1.6 Conditions Générales d'Utilisation

L'AH définit des CGU conformes au paragraphe 5.

6.1.7 Conformité avec les exigences légales

6.1.7.1 Droit applicable

Le présent document est régi par la règlementation européenne.

6.1.7.2 Règlement des différends

Toutes contestations et litiges survenant dans l'interprétation et la mise en œuvre du présent document seront soumis à la juridiction des tribunaux compétents de la cour d'appel de Paris.

6.1.7.3 Propriété intellectuelle des infrastructures ADSN

Sur le plan de la propriété intellectuelle, les produits mis en œuvre par l'**ADSN** dans le service d'horodatage appartiennent aux éditeurs de ces produits.

Les utilisateurs de ces services ne disposent d'aucun droit de propriété intellectuelle sur ces différents éléments. Toute utilisation ou reproduction, totale ou partielle, de ces éléments et/ou des informations qu'ils contiennent, par quelque procédé que ce soit, est strictement interdite et constitue une contrefaçon sanctionnée par le Code de la propriété intellectuelle, sauf accord préalable et écrit du Conseil Supérieur du Notariat.

6.1.7.4 Données nominatives

Le CSN ou un tiers désigné par lui assure la confidentialité de toutes données nominatives et éventuellement de certains événements conformément à ce qui est stipulé dans la présente PH. Le CSN s'engage à demander le respect de cette confidentialité auprès de toute entité intervenant pour lui ainsi qu'auprès de ses salariés.
Le CSN s'engage à prendre et à maintenir les mesures nécessaires pour assurer la sécurité et la confidentialité de toutes données à caractère personnel et ce, conformément aux dispositions du Règlement (UE) 2016/679 du 27 avril 2016 [RGPD].
L'exécution et la gestion des Conditions Générales supposent la mise en œuvre d'un traitement de données à caractère personnel auquel l'utilisateur consent et dont le CSN est le responsable. Conformément à la réglementation applicable en la matière, l'utilisateur est informé que la communication de ses données est obligatoire et nécessaire pour l'utilisation du servie d'horodatage.
En vertu du Règlement (UE) 2016/679 du 27 avril 2016, le titulaire peut accéder aux données le concernant auprès :

- du Responsable de traitement, le Conseil Supérieur du Notariat, Autorité de certification, 60 boulevard de La Tour-Maubourg, 75007 PARIS – Tel : +33 1 44 90 30 00, - mail : autorite-certification@notaires.fr
- ou du délégué à la protection des données du CSN, cil-csn@notaires.fr - 95 avenue des logissons, 13107 VENELLES Cedex.

Le cas échéant, le titulaire peut également demander la rectification ou l'effacement des données le concernant, obtenir la limitation du traitement de ces données ou s'y opposer pour motif légitime, hormis les cas où la réglementation ne permet pas l'exercice de ces droits.
Si le titulaire estime, après avoir contacté le Responsable de traitement ou le délégué à la protection des données, que ses droits ne sont pas respectés ou que le traitement n'est pas conforme aux règles sur la protection des données, il peut adresser une réclamation en ligne ou par voie postale auprès d'une autorité de contrôle.

6.2 Exigences opérationnelles

6.2.1 Gestion des requêtes

Les demandes de contremarques de temps sont exécutées par les UH de l'AH NOTAIRES 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. Cette opération est généralement réalisée à l'issue d'une opération de signature électronique.

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

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

- Tous les éléments sauvegardés sont référencés ;
- Les événements sauvegardés sont protégés en intégrité et en confidentialité ;
- Tous les événements d'administration des serveurs d'horodatage sont tracés et conservés ;
- L'instant précis des événements est tracé ;
- Les événements d'audit sont conservés en sureté de manière à éviter les effacements et la perte de ces données ;
- Tous les événements liés à la gestion du cycle de vie des clés d'horodatage sont tracés (création, renouvellement, destruction, installation sur une UH) ;
- Tous les événements liés à la gestion du cycle de vie des certificats d'horodatage sont tracés (création, renouvellement, destruction, installation sur une UH) ;
- 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) ;
- Les requêtes et les réponses sont conservées.

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.

Ces clés privées sont exclusivement utilisées pour des certificats d'horodatage dans le cadre du service d'horodatage du NOTARIAT. Les clés sont utilisées dans un contexte d'horodatage sur le serveur d'horodatage et n'ont pas d'existence en dehors de ce contexte.

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 d'horodatage est synchronisé avec trois serveurs de temps autonomes, eux-même synchronisés sur :

- Un signal GPS ;
- 4 sources de temps NTP :
  - ntp.inria.fr
  - ntp-p1.obspm.fr
  - saturne.obs-besancon.fr
  - ntp1.oma.be

La moyenne des informations obtenues détermine l'heure exacte.

L'éditeur de la solution d'horodatage assure la maintenance logicielle du serveur d'horodatage dont le calibrage de l'horloge, les sauts d'horloge programmés, les synchronisations. L'**ADSN** assure la supervision de la solution d'horodatage.

Les clauses de maintenance sont définies dans le contrat entre l'**ADSN** et l'éditeur du serveur d'horodatage.

En cas de panne, l'éditeur :

- 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.

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.

6.2.5 Contenu d'une Contremarque de Temps

Les contremarques incluent une date et une heure d'UH avec une précision donnée au regard du temps UTC.

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

Les contremarques de temps émises par l'AH respectent, de base, les exigences correspondantes du [RFC_3161], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	**Description ou valeur**	**Elément contenant**	
		Certificat	Jeton
Version	1		X
Policy	OID de la PH		X
Pays de l'AH	FR	X	
AC Id	Identifiant de l'AC	X	
AH Id	Identifiant de l'AH	X	
UH Id	Identifiant de l'UH	X	
messageDigest	Condensat (hash) des données à horodater		X
serialNumber	Identifiant unique de la contremarque de temps		X
GenTime	Heure de génération de la contremarque de temps calculée par rapport à une source UTC(k)		X
accuracy	Contient la précision fournie par l'UH, égale à 1 seconde		X
nonce	Identique à celui présenté lors de la demande de génération si celui-ci est présent dans cette dernière		X
certReq	Le certificat de l'UH		X
reqPolicy	Spécifie la politique d'horodatage utilisée		X

La contremarque de temps est signée par l'UH à l'aide du certificat délivré par l'AC REALTS. Ce certificat et la clé privée correspondante sont utilisés exclusivement pour cet usage.

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.

6.2.6.1 Procédure de remontée et de traitement des incidents et des compromissions

Des procédures et des moyens de remontée et de traitement des incidents (sensibilisation, formation des personnels, et analyse des différents journaux d'événements) sont mis en œuvre.

Un incident majeur – perte, suspicion de compromission, compromission ou vol de clé privée de gestion des certificats par exemple – est immédiatement signalé à l'AH. La publication de révocation du certificat, si elle s'avère nécessaire, est effectuée dans la plus grande urgence par tout moyen nécessaire.

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

Un plan de continuité d'activité est mis en place permettant de répondre aux exigences de disponibilité des différentes composantes du service d'horodatage.

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

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 la PC en vigueur pour cette AC [PC REALTS].

6.2.6.4 Compromission de la synchronisation du service d'horodatage

La synchronisation des horloges internes du service d'horodatage est contrôlée et des mécanismes sont mis en œuvre pour écarter une source de temps qui ne fournirait plus un temps fiable.

En cas de défaillance majeure du système de synchronisation l'UH concernée arrête d'émettre des jetons d'horodatage.

6.2.6.5 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. 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

6.2.6.6 Procédures de reprise en cas de compromission

Dans le cadre du plan de continuité d'activité, **l'ADSN** dispose sur son site principal de deux salles serveurs séparées d'une cinquantaine de mètres l'une de l'autre par des portes coupe-feu, et d'une troisième salle serveur en région parisienne. Les salles serveur principales (salles A et B) hébergent l'environnement de production, la salle C 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 de la salle B et C n'étant elles pas compromises.

Les problèmes d'exploitation 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**.

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 les salles B et C 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 REALTS 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 à l'**ADSN**.

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 détectée ;
- Coupera l'unité d'horodatage suspectée de compromission ;
- 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 ;
- Préviendra le point de contact identifié sur le site de l'ANSSI http://www.ssi.gouv.fr.

6.2.6.7 Capacités de continuité d'activité suite à un sinistre

La capacité de continuité de l'activité suite à un sinistre est précisée dans la [DPH].

Ce Plan prend en compte les mesures mises en œuvre en cas de compromission de la clé de signature des contremarques de temps et en cas de perte de calibration d'une horloge interne du service d'horodatage du Notariat**.**

6.2.7 Fin d'activité

L'Autorité d'horodatage garantit 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 ;
- 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'Autorité d'horodatage maintiendra ou transfèrera 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.

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

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 préviendra dès que possible le point de contact précisé sur le site de l'ANSSI http://www.ssi.gouv.fr de la fin d'activité de son service d'horodatage.

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 tremblements de terre, explosion, risque volcanique ou crue.

6.3.1.2 Accès physique

Une procédure de gestion des accès physiques est rédigée.
Les accès sont réglementés en fonction du rôle de confiance confié à la personne.

L'accès physique aux fonctions d'horodatage (ceci comprend les fonctions de gestion des certificats des Unités d'Horodatage) est strictement limité aux seules personnes nominativement autorisées.

L'accès physique au système 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.

6.3.1.3 Alimentation électrique et climatisation

Des mesures de secours sont mises en œuvre par l'**ADSN** de manière à ce qu'une interruption de service ne porte pas atteinte aux engagements pris par l'AH en matière de disponibilité (signature et délivrance des contremarques de temps)

- alimentation électrique : mise en œuvre de moyens techniques tels que des onduleurs et groupes électrogènes, avec redondance des équipements ;
- défaillance de climatisation : redondance climatiseurs, alarmes de dysfonctionnement.

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).

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 (signature et délivrance des contremarques de temps), et de pérennité de l'archivage, en mettant en œuvre des moyens 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.

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, conformément à la politique de sécurité en vigueur à l'**ADSN**.

6.3.1.9 Sauvegarde hors site

L'ADSN possède une infrastructure d'horodatage sur deux 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 deux sites à un instant donné mais ne permet pas de reconstruire un service d'horodatage.

La présente PH 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.

Concernant les journaux d'événements, les conditions mises en œuvre sont décrites dans le paragraphe 6.5.1.6.

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**.

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

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

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.

6.3.2.3 Planification de systèmes

Les montées en charge sont contrôlées et des projections de charge dans le futur sont effectuées pour garantir que les puissances de traitement nécessaires, les stockages adéquats et les engagements de services sont disponibles et atteints.

6.3.2.4 Gestion des incidents

Un rapport d'incident et des procédures de réponse aux incidents sont employés d'une telle façon que les dégâts liés aux incidents de sécurité et aux défaillances sont réduits au minimum, notamment :

- Tout dysfonctionnement du service d'horodatage est identifié par l'équipe « production » de l'**ADSN**, qui prend les mesures nécessaires à la remise en service de l'UH défaillante, ou à la bascule sur le site de secours ;
- Le support aux utilisateurs est assuré par la cellule de gestion d'exploitation IGC de l'**ADSN**, qui relatera un incident d'horodatage dans l'outil de suivi des incidents ;
- Les incidents liés au service d'horodatage sont traités selon la procédure de gestion des incidents en vigueur chez l'**ADSN**.

6.3.2.5 Manipulation et sécurité des systèmes

L'AH met en œuvre une politique de classification sur l'ensemble des éléments du service d'horodatage.

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 ;
- La gestion du réseau ;
- Le contrôle actif des journaux d'audit, l'analyse des événements et les suites à donner ;
- Le traitement et la sécurité des médias ;
  L'échange des données et du logiciel.

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

6.3.2.7 Amélioration continue des systèmes d'information

ADSN met en œuvre un processus d'amélioration continue dans le cadre de son service d'horodatage et des processus support.

6.3.2.8 Gestion d'accès au système

L'Autorité d'horodatage garantit que l'accès aux fonctions du système, à l'information et aux applications est limité conformément à la politique de contrôle d'accès et que le système d'horodatage possède les contrôles informatiques de sécurité suffisants pour la séparation des rôles de confiance identifiés dans les pratiques d'horodatage, y compris la séparation des fonctions d'administrateur de sécurité et des fonctions opérationnelles. En particulier, l'utilisation de programmes 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 certificat personnel sur support physique 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 analyser et de réagir selon des procédures formelles.

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

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 :

6.3.3.1.1 AH

L'AH est chargée de la mise en œuvre de la PH, de ses évolutions, et de sa prise en compte par les différentes structures. Elle fait faire les contrôles de conformité, valide les plans d'actions relatifs aux mesures correctives.

6.3.3.1.2 Prestataire de Services d'Horodatage Electronique

Le PSHE est garant de l'application opérationnelle de la PH. Pour le notariat le rôle de PSHE est tenu par l'**ADSN**, et s'organise à partir d'un Comité de Pilotage (revue de processus OSC / OSH).

Le Comité de Pilotage a notamment pour mission de :

- Faire réaliser les analyses de risques sur le périmètre dont il a la charge ;
- Décider de la stratégie de gestion des risques ;
- Valider et suivre les plans d'actions correspondants ;

- Faire réaliser les audits internes sur sa composante, et suivre la mise en place des mesures correctives nécessaires.

Le comité de pilotage se réunit au minimum tous les deux mois pour une revue de processus. Ce comité regroupe :
- L'AH ;
- Le PSHE, assurant également le suivi des mesures de sécurité.

Les rôles de confiance définis et le nombre de personnes disposant de ce rôle de confiance pour le service d'horodatage sont au moins :
- 2 administrateurs de la plateforme d'horodatage : responsabilité de la configuration et du paramétrage des unités d'horodatage ;
- 1 chargé de la sécurité informatique : responsabilité complète d'administrer la mise en œuvre des pratiques de sécurité ;
- 2 techniciens d'exploitation : suivi et maintien en conditions opérationnelles du service d'horodatage ;
- 1 auditeur système : suivi et revue des incidents du service d'horodatage ;
- 1 responsable de sécurité informatique : responsabilité complète de définir et de contrôler la mise en œuvre des pratiques de sécurité ;
- 1 responsable de sécurité physique : responsabilité complète sur les habilitations d'accès et la sécurité physique de la zone d'hébergement du service d'horodatage.

L'AH a également défini des porteurs de secrets pour l'accès aux opérations sensibles sur le boîtier cryptographique stockant les clés privées des unités d'horodatage. Le regroupement d'un sous-ensemble de ces porteurs est nécessaire pour la réalisation de ces opérations.

6.3.3.2 Identification et authentification pour chaque rôle

Des mesures d'identification et d'authentification sont mises en place afin de supporter la mise en œuvre de la politique de contrôle d'accès et la traçabilité des opérations ; la politique de contrôle d'accès limite l'accès aux seules personnes autorisées conformément à leur besoin d'en connaître.

Les rôles attribués concernant les services d'horodatage sont notifiés par courrier aux personnes concernées par le président de l'**ADSN**.

6.3.3.3 Rôles exigeant une séparation des attributions

La PH garantit la séparation des rôles effectuée selon le principe de moindre privilège. La génération d'un nouveau certificat d'UH fait intervenir l'AC REALTS qui bénéficie d'un partage des rôles lié à son statut de Prestataire de Service de Certification Electronique.

Pour la génération d'une nouvelle clé d'UH, la procédure exige la présence :
- 1 administrateur de l'AC REALTS ;
- 1 porteur de secret de l'AC REALTS, différent de l'administrateur.

Le PSHE décrit également les rôles disponibles et les actions associées sur chaque équipement de l'infrastructure d'horodatage.

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.

Le PSHE s'assure que les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles. Notamment les personnels de l'OSH

suivent des formations au moins annuellement sur les menaces informatiques et les pratiques de sécurité du système d'information.

Le personnel d'encadrement du PSHE 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.

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.

6.3.3.4.5 Fréquence et séquence de rotations entre différentes attributions

Sans objet.

6.3.3.4.6 Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont énoncées dans le règlement intérieur.

6.3.3.4.7 Exigences 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 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.

6.3.3.4.8 Documentation 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 sur 3 serveurs de temps autonomes, eux-mêmes reliés à un signal GPS et des serveurs de temps NTP.

La moyenne de temps des 3 serveurs NTP permet d'établir l'heure du service d'horodatage.

Les serveurs de synchronisation NTP utilisés par les serveurs de temps autonomes sont les suivants :

- 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 par le Bureau International Poids et Mesures (BIPM).
- saturne.obs-besancon.fr : serveur primaire basé à Besançon
- ntp1.oma.be : serveur primaire de l'observatoire royal de Belgique

Le système d'horodatage des Notaires est donc synchronisé avec au moins un serveur UTC(k). 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.

6.4.2 Génération des clés

La génération des bi-clés cryptographiques des UH est réalisée à l'aide de ressources cryptographiques matérielles. Les modules utilisés sont qualifiés au niveau renforcé par l'ANSSI et respectent les exigences de [PSCO_HORO].

A aucun moment, lors de cette génération, les clés privées d'UH ne sont exportées de ces ressources. La génération des clés privées des unités d'horodatage est réalisée durant une cérémonie des clés qui fait l'objet d'un procès-verbal. Cette cérémonie est réalisée dans un environnement sécurisé, par des personnels de confiance au moins sous double contrôle.

Les modules des clés privées d'UH ont une longueur de 2048 bits pour l'algorithme RSA pour les clés générées avant le 01 janvier 2024, et 3072 bits pour les suivantes.

6.4.3 Certification des clés de l'UH

La certification des clés d'une UH revient à paramétrer le serveur d'horodatage pour qu'il utilise le certificat de signature de l'UH lors d'une demande de contremarque de temps.

La configuration du serveur utilisé dans l'AH garantit le lien entre le demandeur d'une contremarque et les droits dont dispose le serveur d'horodatage pour lui la délivrer.

Les informations suivantes font parties de la demande :

- Le CN qui sera complété par le profil de génération du certificat de la PKI pour aboutir au DN du certificat de l'UH;
- La valeur de la clé publique suivant (module et exposant) ;

La vérification de ces informations lors de l'import du certificat est faite par l'unité d'horodatage en contrôlant ces informations par rapport à celle fournies dans la demande de certificat.

L'import du certificat permet de valider et d'initialiser le contexte d'horodatage et ainsi permettre le démarrage de l'unité d'horodatage.

6.4.4 Protection des clés privées des UH

Les clés privées des UH sont stockées dans un HSM BULL Proteccio. Ce module est certifié Critères Communs EAL4 augmentés et qualifié renforcé par l'ANSSI.

Le HSM ne contient pas l'application d'horodatage mais est connectée de manière directe, unique et sécurisée à l'application d'horodatage et seule cette dernière peut accéder aux clés de signature des UH.

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 pas exportables et ne sont de fait pas sauvegardées.

6.4.6 Destruction des clés des UH

En fin de vie d'une clé privée d'UH, normale ou anticipée (révocation), cette clé est détruite par une opération d'administration du boîtier HSM. Elle n'est pas exportable et n'est pas sauvegardée.

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 éléments nécessaires pour les applications tierces pour vérifier un jeton d'horodatage sont :

- Publiés sur le site de publication indiqué au 1.2.2 (chaîne de certification, Politique de Certification, Politique d'Horodatage, LCR, …) ;
- Contenus dans le jeton qui a été retourné par l'AH (condensat des données horodatées, précision de la contremarque de temps, algorithmes cryptographiques utilisés …) ;

Les modalités de vérifications sont décrites dans la DPH [DPH]

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 doivent identifier et authentifier et 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 doit pouvoir établir l'identité de l'entité.

Les informations d'authentification sont stockées de façon telle qu'elles soient seulement accessibles par des utilisateurs autorisés.

6.5.1.2 Contrôle d'accès

Les profils et droits d'accès aux équipements du PSHE sont définis et documentés, ainsi que les procédures d'enregistrement et de désenregistrement des utilisateurs.

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

L'utilisation de programmes utilitaires est restreinte et contrôlée.

Les procédures opérationnelles d'administration et exploitation du service d'horodatage sont documentées, suivies et régulièrement mises à jour.

Les conditions de mise en service (paramétrage initial de sécurité des serveurs) sont documentées. Les configurations mises en œuvre permettent de renforcer le niveau de sécurité des systèmes en appliquant des mesures de durcissement. Les mesures sont décrites dans la DPH [DPH].

Les conditions de fin de vie (destruction et mise au rebus) des équipements sont documentés afin de garantir la non divulgation des informations sensibles qu'ils peuvent détenir.

L'ensemble des matériels sensibles du service d'horodatage fait l'objet de procédure de maintenance afin de garantir la disponibilité des fonctions et des informations. Les procédures sont documentées.

Les personnels concernés par ces procédures sont désignés formellement.

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.

Les composantes du réseau local (OSH) sont maintenues dans un environnement physiquement sécurisé ; des vérifications périodiques de conformité de leur configuration sont effectuées.

Des tests réguliers de pénétration et de détection de vulnérabilités sont réalisés sur l'ensemble des composantes techniques de l'OSH.

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 possible au travers des journaux d'événements. Tous les événements liés à la sécurité des systèmes sont journalisés. Le détail des événements concernés sont décrits dans la DPH [DPH].

6.5.1.6.1 Type d'événement à enregistrer

Il est nécessaire d'enregistrer les événements suivants :

- Les événements systèmes des différentes composantes du service d'horodatage (démarrage des serveurs, accès réseau, …) que ce soit sur le site actif ou le site de sauvegarde ;
- Les événements techniques des applications composant le service d'horodatage, sur le site actif ou le site de sauvegarde ;
- Les événements fonctionnels des applications composant le service d'horodatage (demande de certificats, validation, révocation, …) sur le site actif ou le site de sauvegarde ;
- Les évènements liés aux clés de signature des unités d'horodatage (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction, ...) ;
- Les événements liés à la synchronisation des horloges internes du service d'horodatage (synchronisation normale, re-calibration, saut de seconde) ;
- La transmission des certificats aux Responsables des certificats d'horodatage et, selon les cas, acceptations / rejets explicites par ces Responsables ;

- La publication et mise à jour des informations liées à l'AH (PH, certificats d'UH, etc.) ;

- Les opérations effectuées.

Ces journaux doivent permettre d'assurer la traçabilité et l'imputabilité des actions effectuées (horodatage, affectation à l'intervenant).

6.5.1.6.2 Fréquence de traitement des journaux d'événements

Les journaux d'événements sont exploités :

- De manière quotidienne dans le cadre de processus automatisé de contrôle ;

- Systématiquement en cas de remontée d'événement anormal ;

- Manuellement durant les revues mensuelles de processus.

6.5.1.6.3 Période de conservation des journaux d'événements

La période de conservation des journaux d'événement doit être :

- De un mois pour les événements systèmes ;

- De un an pour les événements techniques ;

- Conforme aux obligations légales pour les événements fonctionnels.

6.5.1.6.4 Protection des journaux d'événements

Les journaux d'événements doivent être accessibles uniquement au personnel autorisé de l'OSH. Ils ne sont pas modifiables de manière non autorisée et des alarmes sont remontées en cas de modification des journaux, ou des paramètres définissant le contenu des journaux.

6.5.1.6.5 Procédure de sauvegarde des journaux d'événements

Les procédures de sauvegarde des journaux sont quotidiennes par delta avec les sauvegardes précédentes, et globales de manière hebdomadaire.

6.5.1.6.6 Système de collecte des journaux d'événements

Les événements enregistrés au sein du service d'horodatage sont centralisés au sein d'un SIEM.

6.5.1.6.7 Notification de l'enregistrement d'un événement au responsable de l'événement

Sans objet

6.5.1.6.8 Evaluation des vulnérabilités

Le contrôle des journaux d'événement système et technique est continu et quotidien afin de permettre une anticipation des vulnérabilités, et des remontées d'alerte en cas de vulnérabilités. Ces contrôles sont réalisés via des processus automatiques qui permettent de détecter des anomalies.

Le SIEM mis en œuvre sur le périmètre du service d'horodatage permet le contrôle manuel des journaux des événements fonctionnels qui est réalisé à la demande en cas de litige, ou pour analyse de comportement du service d'horodatage.

Une revue mensuelle des événements anormaux est réalisée par le comité de pilotage de l'AH à travers une séance de revue de processus.

6.5.1.7 Archivage des données

6.5.1.7.1 Types de données à archiver

Les données à archiver sont les suivantes :

- logiciels exécutables et fichiers de configuration ;
- PH, DPH et CGU ;
- Certificats des unités d'horodatage et LCR publiés ;
- Journaux d'événements.

6.5.1.7.2 Période de conservation des archives

Le tableau suivant présente les périodes de conservation des archives pour chaque type de donnée

Type de données	Période de conservation
Logiciels	Version n – 1
Configurations des logiciels	Version n – 1
LCR & Certificats d'horodatage	23 ans
Evènements système	1 mois
Evènements techniques	1 an
Journaux de l'application d'horodatage (demandes et réponses d'horodatage)	10 ans
Journaux de synchronisation NTP	Sans limite
Evènements fonctionnels	23 ans
Documentation	10 ans
Demandes de génération ou de révocation de certificats	23 ans
Formulaires d'enregistrement des Responsables des Certificats d'Horodatage	23 ans
Procès-Verbaux de génération des clés d'horodatage	23 ans

6.5.1.7.3 Protection des archives

Quel que soit leur support, les archives sont protégées en intégrité, et ne sont accessibles qu'aux personnes autorisées. Ces archives sont lisibles et exploitables sur l'ensemble de leur cycle de vie.

L'OSH met en œuvre les moyens nécessaires pour garantir la conservation des archives sur une période conforme aux exigences légales en matière de fourniture d'éléments de preuves. La durée de conservation et les moyens mis en œuvre sont décrits dans [DPH].

6.5.1.7.4 Procédure de sauvegarde des archives

Les archives sont sauvegardées de manière sécurisée, certaines en double enregistrement. Les moyens mis en œuvre pour réaliser la sauvegarde garantissent que les éléments ne peuvent pas être supprimés ou détruits facilement.

6.5.1.7.5 Exigences d'horodatage des données

L'horodatage des données des événements journalisés est synchrone en dehors des opérations hors ligne. Pour cela, les composants du service d'horodatage sont synchronisés sur un même serveur lui-même synchronisé avec l'heure universelle.

6.5.1.7.6 Système de collecte des archives

Sans objet.

6.5.1.7.7 Procédure de récupération et de vérification des archives

La récupération et la vérification des archives peuvent être effectuées dans un délai conforme à l'utilisation des certificats délivrés. Un délai de 7 jours ouvrés est nécessaire pour récupérer les archives.

6.5.1.8 Supervision et contrôle

Une surveillance permanente est mise en place et des systèmes d'alarme sont installés pour détecter enregistrer et réagir rapidement face à toute tentative non autorisée et ou irrégulière d'accès aux ressources (physique et / ou logique).

L'OSH met en œuvre un système de surveillance des processus d'enregistrement des traces, notamment les arrêts / relances de ces processus.

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.

Lorsqu'une faille de sécurité est observée sur une des composantes de l'OSH, les personnes concernées sont mise 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 de la Qualité (SMQ) et un Système de Management de la Sécurité 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.

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.

Un plan de capacité est établi pour garantir le bon traitement des demandes de contremarques de temps traitées par l'AC REALTS.

6.7 Mesures de sécurité réseau

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

Les communications réseau véhiculant des informations confidentielles font l'objet de mesures de protection contre l'écoute des informations. Les composants réseaux correspondants sont hébergés dans un environnement sûr et des contrôles réguliers des configurations sont opérés régulièrement.

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.

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
[RGPD]	Règlement (UE) 2016/679 du 27 avril 2016
[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
[DPH]	Déclaration des Pratiques d'Horodatage de l'AH REALTS
[CGU]	Conditions Générales d'Utilisation du service d'horodatage
[AnalyseRisques]	Analyse des risques
[PC REALTS]	Politique de Certification de l'AC REALTS
[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)

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 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 certifié Critères Communs EAL4 augmentés et qualifié 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, il convient de 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

Voir [PC_REALTS].

11 PRÉCISION DE LA SYNCHRONISATION DE L'HORLOGE

La précision de l'horloge est inférieure ou 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 boîtier 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 : http://www.preuve-electronique.org.