

## Politique d'Horodatage du Notariat

| Version | Date       | Description                                      | Auteurs       | Société    |
|---------|------------|--|---------------|------------|
| 1.0     | 06/04/09   | Rédaction  | Y. THOMASSIER | APPLI.NOT  |
| 2.0     | 31/08/11   | Mise en conformité RGS                           | P. PELLEGRIN  | APPLI.NOT  |
| 2.1     | 21/03/2012 | Relecture  | Y.THOMASSIER  | APPLI.NOT  |
| 2.2     | 22/05/2012 | Modification                                     | P.PELLEGRIN   | APPLI.NOT  |
| 2.3     | 23/08/2012 | Modification                                     | Y.THOMASSIER  | APPLI .NOT |
| 2.4     | 14/03/2013 | Modification                                     | Y.THOMASSIER  | APPLI.NOT  |
| 2.5     | 06/06/2013 | Modification                                     | Y.THOMASSIER  | REAL.NOT   |
| 2.6     | 16/03/2014 | Révision annuelle                                | Y.THOMASSIER  | REAL.NOT   |
| 2.7     | 30/01/2015 | Révision annuelle                                | Y.THOMASSIER  | REAL.NOT   |
| 2.8     | 16/03/2015 | Mise en conformité RGSv2                         | Y.THOMASSIER  | REAL.NOT   |
| 2.9     | 30/06/2015 | Mise à jour suite à l'audit interne              | P. PELLEGRIN  | REAL.NOT   |
| 2.10    | 13/05/2016 | Mise à jour pour la transition RGS V2 vers eIDAS | Y. THOMASSIER | REAL.NOT   |
| 2.20    | 09/08/2016 | Prise en compte des remarques LSTI               | P.PELLEGRIN   | REAL.NOT   |

| Etat du document             | Classification |
|------------------------------|----------------|
| Validé                       | PUBLIQUE       |
| OID du document              |                |
| 1.2.250.1.78.1.1.3.1.4.6.1.6 |                |

Ce document est la propriété exclusive de REAL.NOT.  
Son usage est réservé à l'ensemble des personnes habilitées selon leur niveau de confidentialité.  
Sa reproduction est régie par le Code de la propriété intellectuelle qui ne l'autorise qu'à l'usage privé du copiste.

## SOMMAIRE

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>INTRODUCTION</b>  | <b>4</b>  |
| 1.1      | PRESENTATION GENERALE  | 4         |
| 1.2      | GESTION DU DOCUMENT  | 5         |
| 1.2.1    | Identification du document   | 5         |
| 1.2.2    | Publication du document  | 5         |
| 1.2.3    | Composition du comité d'approbation  | 5         |
| 1.2.4    | Processus de mise à jour   | 5         |
| 1.2.5    | Entrée en vigueur de la nouvelle version et période de validité                                | 6         |
| 1.2.6    | Cohérence de la documentation  | 6         |
| 1.3      | PRINCIPE DU SERVICE D'HORODATAGE DU NOTARIAT   | 6         |
| 1.4      | ETABLISSEMENT DE LA CONFIANCE DANS LE SERVICE D'HORODATAGE DU NOTARIAT                         | 7         |
| 1.5      | ENTITES INTERVENANT DANS LE SERVICE D'HORODATAGE   | 7         |
| 1.6      | AUTRES ASPECTS   | 9         |
| <b>2</b> | <b>GENERALITES</b>   | <b>10</b> |
| 2.1      | DEFINITIONS  | 10        |
| 2.2      | ABREVIATIONS   | 13        |
| <b>3</b> | <b>POLITIQUE D'HORODATAGE</b>  | <b>14</b> |
| <b>4</b> | <b>DECLARATION DES PRATIQUES D'HORODATAGE</b>  | <b>15</b> |
| <b>5</b> | <b>CONDITIONS GENERALES D'UTILISATION</b>  | <b>16</b> |
| <b>6</b> | <b>EXIGENCES RESPECTEES PAR L'AUTORITE D'HORODATAGE</b>  | <b>17</b> |
| 6.1      | DISPOSITIONS GÉNÉRALES   | 17        |
| 6.1.1    | Obligation de l'Autorité d'Horodatage  | 17        |
| 6.1.2    | Obligation de l'abonné   | 17        |
| 6.1.3    | Obligation de l'Utilisateur de Contremarque de Temps   | 17        |
| 6.1.4    | Obligations des Autorités de Certification fournissant des certificats aux Unités d'Horodatage | 17        |
| 6.1.5    | Déclaration des Pratiques d'Horodatage   | 18        |
| 6.1.6    | Conditions Générales d'Utilisation   | 18        |
| 6.1.7    | Conformité avec les exigences légales  | 19        |
| 6.2      | EXIGENCES OPERATIONNELLES  | 19        |
| 6.2.1    | Gestion des requêtes   | 19        |
| 6.2.2    | Fichiers d'audit   | 20        |
| 6.2.3    | Gestion de la durée de vie de la clé privée  | 20        |
| 6.2.4    | Synchronisation de l'horloge   | 21        |
| 6.2.5    | Contenu d'une Contremarque de Temps  | 22        |
| 6.2.6    | Compromission de l'Autorité d'Horodatage   | 23        |
| 6.2.7    | Fin d'activité   | 24        |
| 6.3      | EXIGENCES PHYSIQUES, ENVIRONNEMENTALES, PROCEDURALES ET ORGANISATIONNELLE                      | 25        |
| 6.3.1    | Exigences physiques et environnementales   | 25        |
| 6.3.2    | Exigences procédurales   | 26        |
| 6.3.3    | Exigences organisationnelles   | 28        |
| 6.4      | EXIGENCES DE SECURITE TECHNIQUES   | 30        |
| 6.4.1    | Exactitude du temps  | 30        |
| 6.4.2    | Génération des clés  | 31        |
| 6.4.3    | Certification des clés de l'UH   | 31        |
| 6.4.4    | Protection des clés privées des UH   | 31        |
| 6.4.5    | Exigences de sauvegarde des clés des UH  | 31        |
| 6.4.6    | Destruction des clés des UH  | 31        |
| 6.4.7    | Algorithmes obligatoires   | 32        |
| 6.4.8    | Vérification des contremarques de temps  | 32        |
| 6.4.9    | Durée de vie des clés publiques des UH   | 32        |
| 6.4.10   | Durée d'utilisation des clés privées des UH  | 32        |

|           |   |           |
|-----------|---|-----------|
| <b>7</b>  | <b>DOCUMENTS CITES EN REFERENCE</b>   | <b>33</b> |
| 7.1.1     | <i>Réglementations</i>  | 33        |
| 7.1.2     | <i>Documents techniques</i>   | 33        |
| <b>8</b>  | <b>EXIGENCES SUR LES FORMATS DES CONTREMARQUES DE TEMPS, DES CERTIFICATS ET DES LCR ET SUR LES ALGORITHMES CRYPTOGRAPHIQUES</b> | <b>34</b> |
| 8.1       | CONTREMARQUE DE TEMPS   | 34        |
| 8.2       | CERTIFICATS ET LCR  | 34        |
| 8.3       | ALGORITHMES CRYPTOGRAPHIQUES  | 34        |
| <b>9</b>  | <b>EXIGENCES DE SECURITE DU MODULE D'HORODATAGE DES UH</b>  | <b>35</b> |
| 9.1       | EXIGENCES SUR LES OBJECTIFS DE SECURITE   | 35        |
| 9.2       | EXIGENCES COMPLEMENTAIRES   | 35        |
| <b>10</b> | <b>VERIFICATION DES CONTREMARQUES DE TEMPS</b>  | <b>36</b> |
| 10.1      | EMPILEMENT DES CONTREMARQUES DE TEMPS   | 36        |
| 10.2      | GESTION DE LA REVOCATION PAR L'AC REALTS  | 36        |
| <b>11</b> | <b>PRECISION DE LA SYNCHRONISATION DE L'HORLOGE</b>   | <b>37</b> |
| <b>12</b> | <b>PROTOCOLE D'HORODATAGE</b>   | <b>38</b> |
| 12.1      | CONFORMITE RFC 3161   | 38        |
| 12.2      | CONFORMITE ETSI TS 101861   | 38        |
| <b>13</b> | <b>COMPATIBILITE AVEC [ETSI_PH]</b>   | <b>39</b> |
| <b>14</b> | <b>GABARIT DE CERTIFICAT D'UNE UH</b>   | <b>40</b> |

## 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 **REAL.NOT**, 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 rafraîchissement 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 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 est qualifiée RGSv2 pour le profil « Horodatage ».

## 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 REAL.NOT, par un numéro d'identification unique, l'OID : 1.2.250.1.78.1.1.3.1.4.6.1.6

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'Approbatation

La présente Politique d'Horodatage est publiée sur l'URL : [www.preuve-electronique.org/PH\\_1.2.250.1.78.1.1.3.1.4.6.1.6.pdf](http://www.preuve-electronique.org/PH_1.2.250.1.78.1.1.3.1.4.6.1.6.pdf)

L'ensemble des informations associées notamment les versions antérieures de ces documents, sont également publiées sur le site [www.preuve-electronique.org](http://www.preuve-electronique.org).

### 1.2.3 Composition du comité d'approbation

Le Comité d'Approbation est composé du bureau du CSN. Ce dernier approuve la Politique d'Horodatage.

### 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 **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](mailto:exploitation.carte.real@notaires.fr)

Ces remarques et souhaits d'évolution sont examinés par le Comité d'Approbation, 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.1.3).

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](mailto: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 ;
- Date et heure exacte d'entrée en vigueur.

Le document archivé porte, en filigrane sur ses pages, la mention « Document obsolète ».

### **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 de la nature, de la date et de l'heure du changement, 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 après sa mise en ligne et reste valide jusqu'à l'entrée en vigueur d'une nouvelle version.

### **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 **REAL.NOT**.

Le Comité d'Approbation 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 (ci-après « UH »).

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

- la valeur de hachage et l'algorithme de hachage de la donnée qui a été horodatée ;
- la date et le temps universel (UTC) ;
- l'identifiant du certificat de l'UH qui a généré la contremarque de temps ;
- l'identifiant du notariat en tant qu'AH (inclus dans le certificat d'horodatage) ;
- l'identifiant de l'Autorité de Certification ayant signé les clés privées installées sur les unités d'horodatage.

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

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 l'ETSI TS 102 023 ([ETSI\_PH]) et de la Politique d'Horodatage Type (RGS – Politique d'Horodatage Type) définie par le Référentiel Général de Sécurité (RGS) version 2.

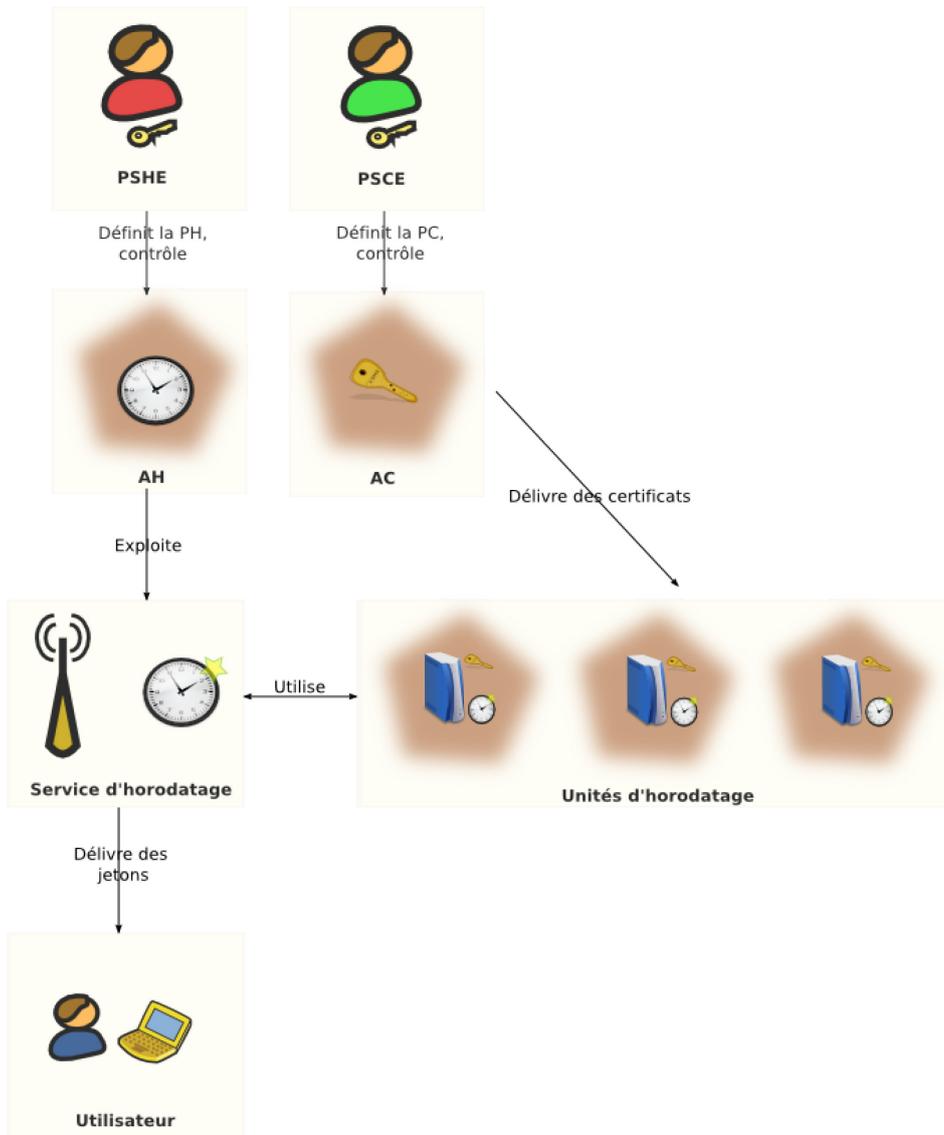
## **1.5 Entités intervenant dans le service d'horodatage**

Le CSN est le responsable de l'Autorité d'Horodatage qui est exploitée et maintenue en condition opérationnelle par REAL.NOT.

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 le RGS, 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. Cette AC est qualifiée RGSv2 pour le profil « Certificats de services applicatifs » au niveau \*.

La représentation schématique est alors la suivante :



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

| CSN  |   | REAL.not  |  | Utilisateurs                      |                                 |
|--|---|-----------|--|-----------------------------------|---------------------------------|
| Fonctions  | Rôles                                       | Fonctions | Rôles  | Fonctions                         | Rôles                           |
| AH<br>Notaires                                   | Définit la PH                               | PSHE      | Utilise les UH à travers le service d'horodatage | Personnes physiques (porteurs)    | Demande des jetons d'horodatage |
|  | Contrôle l'application de la PH par le PSHE |           | Exploite le service d'horodatage                 | Applications de dématérialisation |                                 |
| Délivre des jetons d'horodatage aux utilisateurs |   |           |  |                                   |                                 |
| AC REALTS  | Définit la PC                               | PSCE      | Signe des demandes de certificats                |                                   |                                 |

|  |  |  |                                       |  |  |
|--|--|--|---------------------------------------|--|--|
|  |  |  | pour les UH                           |  |  |
|  | Contrôle<br>l'application<br>de la PC par<br>le PSCE |  | Exploite les<br>services de<br>la PKI |  |  |

\* 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. Opérationnellement, la demande d'horodatage est réalisée par une connexion HTTP ou RCP non authentifiée au serveur d'horodatage

### **1.6 Autres aspects**

Les unités d'horodatage utilisent des boîtiers cryptographiques matériels pour générer et stocker les clés privées des certificats électroniques.

## 2 GÉNÉRALITÉS

### 2.1 Définitions

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

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

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

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

**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)** - L'ordonnance 2005-1516 introduit et définit les prestataires de service de confiance (PSCO). Un prestataire de services de confiance est défini comme toute personne 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.

**Qualification d'un produit de sécurité** - Acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les fonctions de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le RGS. La procédure de qualification des produits de sécurité est décrite dans le Décret RGS. Le RGS précise les trois processus de qualification :

- qualification de niveau élémentaire,
- qualification de niveau standard,

- qualification de niveau renforcé.

**Qualification d'un prestataire de services d'horodatage** - Le Décret RGS décrit la procédure de qualification des PSCO. Un PSHE étant un PSCO particulier, la qualification d'un PSHE est un acte par lequel un organisme de qualification atteste de la conformité de tout ou partie de l'offre d'horodatage d'un PSHE à la PH Type (RGS).

**Référencement** - Opération réalisée par l'Administration qui atteste que l'offre d'horodatage du PSCE 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  $\pm 100$  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](http://www.bipm.org)).*

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

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

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

**Utilisateur final** - Abonné ou utilisateur de contremarques de temps.

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

## **2.2 Abréviations**

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

|           |   |
|-----------|---|
| AC        | Autorité de Certification                                   |
| AH        | Autorité d'horodatage                                       |
| ANSSI     | Agence Nationale de la Sécurité des Systèmes d'Information  |
| CGU       | Conditions Générales d'utilisation du service d'horodatage  |
| CSN       | Conseil Supérieur du Notariat                               |
| Delta-LRC | Liste de Révocation des Certificats partielle               |
| SGMAP     | Secrétariat Général à la Modernisation de l'Action Publique |
| 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                        |
| RGS       | Référentiel Général de Sécurité                             |
| 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 ETSI TS 101 861 V1.4.1.

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.

Contrairement à la politique d'horodatage, la DPH n'est pas publiée.

Cependant, l'Autorité d'horodatage publie dans la présente PH les parties suivantes :

- Le cadre d'application de la DPH ;
- Les coordonnées de l'AH ;
- La PH appliquée ;
- 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 ;
- La précision de la date des contremarques de temps par rapport à l'échelle de temps UTC ;
- Les obligations des abonnés ;
- Les obligations des utilisateurs de contremarque de temps ;
- Les informations permettant de vérifier la contremarque de temps ;
- Les limitations de responsabilité.

Ces informations publiques sont intégrées aux conditions générales d'utilisation (cf. chapitre suivant).

## **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 correspondant aux « *TSA Disclosure Statement* » (*TDS*) définis dans l'annexe B de l'ETSI 102023.

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 spécifie dans ses conditions générales d'utilisation les identifiants des politiques d'horodatage supportés.

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](http://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.

#### 6.1.3 Obligation de l'Utilisateur de Contremarque de Temps

Les utilisateurs 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 **REAL.NOT** ;
- s'assurer que les demandes de contremarques de temps sont faites exclusivement pour l'usage des applications de dématérialisation des Notaires.

#### 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 (<http://www.preuve-electronique.org>).

**REAL.NOT** 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, pour le profil « Certificats de services applicatifs », est qualifiée au sens du RGSv2 pour le niveau \*.

### **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](http://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 ;
  - Les CRL de l'AC REALTS ;
  - Le certificat de l'AC REALTS ;
  - Toutes les versions des politiques d'horodatage avec leur date de validité.
- 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'organisme qui lui a délivré les différentes qualifications, RGSv2 notamment.

### **6.1.6 Conditions Générales d'Utilisation**

L'AH définit des CGU qui reprennent les grands principes décrits dans la présente PH. Ces CGU sont basées sur le modèle défini dans l'annexe B de l'ETSI 102023. L'AH décrit dans ces CGU les informations suivantes :

- Les obligations de l'abonné ;
- Les obligations des utilisateurs de contremarques de temps ;
- Une information sur le point de contact du service d'horodatage ;
- Une référence et une description de la PH appliquée ;
- Au moins un algorithme de hachage ;
- La période de temps minimum durant laquelle les contremarques de temps seront vérifiables par l'utilisateur de contremarques de temps et l'abonné. Ce temps ne tient pas compte des éventuelles procédures de révocation du certificat d'une unité d'horodatage ;
- L'exactitude du temps fourni dans les contremarques de temps par rapport au temps UTC ;
- L'ensemble des limitations du service d'horodatage, notamment le périmètre applicatif pour lequel les contremarques de temps sont fournies ;
- Les informations nécessaires pour vérifier les contremarques de temps ;
- La période de conservation des données d'audit ;
- Le système légal applicable ;
- Les limitations de responsabilité de l'AH ;
- Les procédures pour les plaintes et le règlement des litiges ;
- L'ensemble de la chaîne de certification de l'AC REALTS et les points de publications des CRL ;
- Le pays dans lequel l'AH est installée.

## 6.1.7 Conformité avec les exigences légales

### 6.1.7.1 Droit applicable

Le présent document est régi par la loi française.

### 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 REAL.NOT

Sur le plan de la propriété intellectuelle, les produits mis en œuvre par **REAL.NOT** 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

En conformité avec les dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le traitement automatisé des données nominatives, réalisé à partir des plates-formes **REAL.NOT** a fait l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés [CNIL].

Conformément à l'article 32 de la loi n° 78-17 du 6 janvier 1978, les utilisateurs sont informés que les données personnelles qu'ils communiquent pourront être transmises et exploitées par **REAL.NOT** et les différents partenaires intervenant dans les échanges concernés.

Les utilisateurs sont informés qu'ils disposent d'un droit d'accès, de rectification et d'opposition portant sur les données le concernant en écrivant à l'**ADSN**, Service Correspondant à la protection des données, 95 avenue des Logissons 13107 VENELLES [cpd-adsn@notaires.fr](mailto:cpd-adsn@notaires.fr), 0820.845.988.

Les utilisateurs des services **REAL.NOT** sont tenus de respecter les dispositions de la loi relative à l'informatique, aux fichiers et aux libertés, dont la violation est passible de sanctions disciplinaires et pénales.

Ils doivent notamment s'abstenir, s'agissant des informations nominatives auxquelles ils accèdent, de toute collecte, de toute utilisation détournée et, d'une manière générale, de tout acte susceptible de porter atteinte à la vie privée ou à la réputation des personnes.

## 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]. Ce protocole est conforme à [ETSI\_TSP].

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

TCP ou 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 NOTAIRES 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.

L'AH NOTAIRES ne conserve pas la contremarque de temps générée.

### **6.2.2 Fichiers d'audit**

Les journaux du service d'horodatage sont conservés sur le serveur d'horodatage jusqu'à archivage.

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 sûreté 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) ;

### **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 un serveur de temps autonome, lui-même synchronisé sur :

- Un signal GPS ;
- 5 sources de temps NTP :
  - canon.inria.fr
  - ntp0.nl.uu.net
  - ntp-p1.obspm.fr
  - saturne.obs-besancon.fr
  - ntp1.oma.be

En sus du serveur de temps autonome, le serveur d'horodatage est synchronisé directement avec 4 serveurs NTP différents sur Internet. Les serveurs Internet utilisés sont les suivants :

- canon.inria.fr
- ntp0.nl.uu.net
- ntp-p1.obspm.fr
- saturne.obs-besancon.fr

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. **REAL.NOT** assure la supervision de la solution d'horodatage.

Les clauses de maintenance sont définies dans le contrat entre **REAL.NOT** et l'éditeur du serveur d'horodatage.

En cas de panne, l'éditeur :

- Assiste le personnel de **REAL.NOT** 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 apparaît, elle sera détectée.

L'Autorité d'Horodatage garantit 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 NOTAIRES 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   | Élément contenant |       |
|----------------------|---|-------------------|-------|
|                      |   | Certificat        | Jeton |
| <i>version</i>       | 1   |                   | X     |
| <i>Policy</i>        | OID de la PH  |                   | X     |
| <i>Pays de l'AH</i>  | FR  | X                 |       |
| <i>AC Id</i>         | Identifiant de l'AC   | X                 |       |
| <i>AH Id</i>         | Identifiant de l'AH   | X                 |       |
| <i>UH Id</i>         | Identifiant de l'UH   | X                 |       |
| <i>messageDigest</i> | Condensat (hash) des données à horodater  |                   | X     |
| <i>serialNumber</i>  | Identifiant unique de la contremarque de temps  |                   | X     |
| <i>GenTime</i>       | Heure de génération de la contremarque de temps calculée par rapport à une source UTC(k)                |                   | X     |
| <i>accuracy</i>      | absent car égal à 1 seconde   |                   | X     |
| <i>nonce</i>         | Identique à celui présenté lors de la demande de génération si celui-ci est présent dans cette dernière |                   | 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 Compromission de l'Autorité d'Horodatage

La compromission de l'AH peut être due à :

- Vols des serveurs des unités d'horodatage ;
- Vol des clés privées des UH ;
- La compromission de la clé privée de l'AC REALTS ayant servi à générer les certificats des UH ;
- Une atteinte à la sécurité ou d'une perte d'intégrité du service qualifié ;

En cas de compromission de la clé privée de l'AC REALTS, la procédure mise en place est détaillée dans la PC/DPC en vigueur pour cette AC.

Concernant les autres cas de compromission, dans le cadre du plan de continuité d'activité, **REAL.NOT** 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 **REAL.NOT** 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 **REAL.NOT**.

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

La procédure, maintenue par **REAL.NOT**, 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 **REAL.NOT**. Ce fonctionnement permet à l'AH NOTAIRES de garantir un service d'horodatage avec un haut niveau de disponibilité.

Plus généralement, les incidents liés au service d'horodatage sont traités selon la procédure de gestion des incidents en vigueur chez **REAL.NOT**.

En tout état de cause, REAL.NOT 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>.

En cas d'atteinte à la sécurité ou perte d'intégrité du service d'horodatage, l'AH s'engage à avertir sous 24h le point de contact identifié sur le site de l'ANSSI <http://www.ssi.gouv.fr>.

### **6.2.7 Fin d'activité**

En cas de fin d'activité du service d'horodatage, REAL.NOT :

- Rendra disponible à ses abonnés et aux utilisateurs des contremarques de temps l'information de la cessation d'activité ;
- Abrogera l'ensemble des autorisations délivrées à des tiers dans le cadre du service d'horodatage ;
- Transférera à un organisme fiable les informations d'audit ;
- Fournira à un organisme fiable les informations nécessaires à la vérification des contremarques de temps ;
- Détruira les clés privées de toutes les unités d'horodatage de son service d'horodatage.
- Demandra la révocation de l'ensemble des certificats installés sur les unités d'horodatage de son service d'horodatage.

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 NOTAIRES. En tout état de cause, l'AH et REAL.NOT s'engagent à maintenir les informations présentes sur le site [www.preuve-electronique.org](http://www.preuve-electronique.org).

L'AH préviendra dès que possible le SGMAP en utilisant le formulaire de contact prévu à cet effet (<http://references.modernisation.gouv.fr/contact-rgs>) et le point de contact précisé sur le site de l'ANSSI <http://www.ssi.gouv.fr> ([secretariat.anssi@ssi.gouv.fr](mailto:secretariat.anssi@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](http://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 du site (Venelles) 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 **REAL.NOT** de manière à ce qu'une interruption de service ne portent 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 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).

#### **6.3.1.6 Conservation des supports**

Les documents de l'AH NOTAIRES ne nécessitent pas d'archivage. Les documents « projet » afférents au service d'horodatage sont stockés sur un Intranet et bénéficient d'une sauvegarde quotidienne.

#### **6.3.1.7 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 chez **REAL.NOT**.

#### **6.3.1.8 Sauvegarde hors site**

**REAL.NOT** 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, notamment :

- Pour les clés des UH. Les clés privées des UH sont générées sur un HSM et ne sont pas exportables ;
- Pour les événements d'audit. Les fichiers d'audits sont disponibles sur le serveur d'horodatage et peuvent être intégrés dans le processus d'archivage automatisé de 'REAL.NOT.

### **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 **REAL.NOT**.

#### **6.3.2.2 Gestion des supports**

Le service d'horodatage se conforme à la politique de sécurité en vigueur chez **REAL.NOT**.

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 **REAL.NOT**, 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 PKI de **REAL.NOT**, qui relatera un incident de signature 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 **REAL.NOT**.

### **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**

REAL.NOT met en œuvre un processus d'amélioration continue dans le cadre de son service d'horodatage.

### **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 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 réseau 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 **REAL.NOT**, 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 tous les 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 technicien de supervision réseau et système ;
- 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 REAL.NOT.

### **6.3.3.3 Rôles exigeant une séparation des attributions**

La PH de l'AH NOTAIRES garantit la séparation des rôles 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.

### **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.

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 informatiques.

Ces procédures de vérification ne sont pas nécessaires pour les Notaires du fait du caractère assermenté de la profession.

#### **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 **REAL.NOT** 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 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 un serveur de temps autonome, lui-même relié à un signal GPS et des serveurs de temps NTP ;
- Sur 4 serveurs de temps (NTP) différents sur Internet.

La moyenne de temps des 4 serveurs NTP permet d'établir l'heure du service d'horodatage.

Les serveurs de synchronisation NTP sont les suivants :

- canon.inria.fr : serveur primaire basé en France.
- ntp0.nl.uu.net : serveur primaire basé en Hollande

- 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

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 de 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. 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, 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.

#### **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 Luna PCI. Ce module est certifié FIPS 140-2 niveau 3.

#### **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 aux exigences des autorités compétentes en la matière comme par exemple [DCSSI\_ALGO]. L'algorithme de calcul d'empreinte numérique accepté est SHA-1 au minimum ;
- Génère des contremarques de temps signées selon les algorithmes et les longueurs de clé conformes aux exigences des autorités compétentes en la matière comme par exemple [DCSSI\_ALGO]. La bi-clé de l'UH est au minimum une bi-clé RSA de 2048 bits utilisant l'algorithme SHA-256.

#### 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 **REAL.NOT** à l'occasion de chaque transaction métier lorsque la demande est faite par une application de dématérialisation notariale.

#### 6.4.9 Durée de vie des clés publiques des UH

La durée de vie des clés publiques des UH est de 2 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 de vie des clés privées des UH est de 2 ans.

## 7 DOCUMENTS CITÉS EN RÉFÉRENCE

### 7.1.1 Réglementations

| Renvoi       | Document  |
|--------------|---|
| [CNIL]       | Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004                                  |
| [DécretRGS]  | Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005   |
| [Ordonnance] | Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électronique entre les usagers et les autorités administratives et entre les autorités administratives |

### 7.1.2 Documents techniques

| Renvoi       | Document  |
|--------------|---|
| [DCSSI_ALGO] | Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, ANSSI, Version 1.20 du 26 janvier 2010 Les informations sont consultables sur le site <a href="http://www.ssi.gouv.fr">http://www.ssi.gouv.fr</a> |
| [ETSI_PH]    | ETSI TS 102 023 V1.2.2 (2003-01)<br>Policy requirements for Time-Stamping Authority   |
| [ETSI_TSP]   | ETSI TS 101 861 V1.4.1 (2002-03)<br>Time Stamping Profile   |
| [RFC 3161]   | IETF - Internet X.509 Public Key Infrastructure - Time-Stamp Protocol - 08/2001   |
| [RGS]        | <a href="http://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_Corps_du_texte.pdf">http://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_Corps_du_texte.pdf</a>   |
| [PH_Type]    | <a href="http://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_A5.pdf">http://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_A5.pdf</a>   |
| [RGS_A4]     | <a href="http://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_A4.pdf">http://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_A4.pdf</a>   |

## 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 NOTAIRES ont une structure TimeStampToken conforme au [RFC3161].

Le tableau ci-dessous reprend l'ensemble des champs d'un TimeStampToken tels que définis dans le [RFC3161].

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  |
| <i>Accuracy</i>   | Ce champ n'est pas positionné car la précision du temps délivré dans la contremarque de temps par rapport au temps UTC(k) est d'une seconde. |
| <i>Ordering</i>   | Ce champ n'est pas positionné  |
| <i>Tsa</i>        | Ce champ n'est pas positionné  |
| <i>Extensions</i> | Aucune extension n'est marquée critique  |

Les champs en italique, optionnels vis-à-vis du RGS, ne sont pas contenus dans les contremarques de temps conformes à la présente PH.

### 8.2 Certificats et LCR

Les gabarits des certificats d'UH sont conformes aux exigences des certificats de type « cachet » dont la clé privée associée est utilisée pour signer des jetons d'horodatage décrites dans le document [RGS\_A4].

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-256. Cet algorithme respecte les recommandations en la matière et en vigueur en France.

## 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 ;
- Être 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 ;
- Être 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 ;
- Être 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 qualifié FIPS 140-2 niveau 3.

## **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 signée 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***

L'AC REALTS publie des CRL qui permettent d'attester de l'état du certificat d'une UH.

## **11 PRÉCISION DE LA SYNCHRONISATION DE L'HORLOGE**

La précision de l'horloge est de 1 seconde par rapport au temps UTC(k). Dans ce cadre, la contremarque de temps ne fait pas apparaître 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 réglementations et normes en vigueur ;
- Le passage réussi à des outils de validation de la contremarque de temps.

### **12.2 Conformité ETSI TS 101861**

Le profil des contremarques de temps est conforme à l'[ETSI\_TSP].

## **13 COMPATIBILITÉ AVEC [ETSI\_PH]**

La présente PH est conforme à l'[ETSI\_PH].

## **14 GABARIT DE CERTIFICAT D'UNE UH**

Les certificats des Unités d'Horodatage mises en œuvre par l'Autorité d'Horodatage du Notariat sont disponibles sur le site : <http://www.preuve-electronique.org>.