YOUSIGN - POLITIQUE D'HORODATAGE

Version 1.0.2 au 17/09/2018

Historique

Version	Date	Rédigé par	Mise à jour
1.0	31/03/2017	Antoine Louiset	Création du document
1.0.1	20/04/2017	Antoine Louiset	Ajout de la chaine de certification complète au §2.4 Durée maximale sans synchronisation ramenée à 6h au §5.1.2 et §5.1.3 Précisions sur les évolutions de la PH au §8.9 Précision de la politique ETSI respectée au §1.2 Restauration des clés des UH sous contrôle de deux personnes au §5.2.7
1.0.2	17/09/2018	Antoine Louiset	La durée de vie du certificat est de 3 ans.

Etat du document – Classification	**Référence**
Validation – C1 Public	Réf. OID PH : 1.2.250.1.302.2.1.1.0

Table des matières

1 Introduction

1.1 Présentation générale

Le service d'Horodatage de Yousign peut être utilisé par ses clients :

- inclus dans l'offre de signature électronique Yousign, pour fournir des dates fiables, donnant ainsi une bonne assurance sur la qualité des dates associées aux actes de signature,
- directement, en tant que service à part entière.

L'objectif de ce document est de définir les engagements pris par Yousign, en tant qu'AH, pour la délivrance et la gestion de contremarques de temps, de décrire les procédures techniques et organisationnelles mises en œuvre pour le respect de ces engagements, et enfin de définir les obligations des autres participants. En particulier, cette politique décrit les moyens mis en œuvre pour atteindre les objectifs de sécurité du service d'horodatage, comme ceux de création des contremarques de temps et de maintien de l'exactitude des horloges.

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.

Le respect de cette politique permet, après audit de conformité selon les processus établis dans le règlement eIDAS (cf. [EIDAS] et [ETSI_TSP]), la qualification du service d'horodatage de Yousign par l'organe de contrôle national.

Les clauses principales de ce document sont synthétisées dans les Conditions Générales d'Utilisation du service d'horodatage (CGU), que les clients et utilisateurs doivent s'engager à respecter.

La structure de la présente Politique d'Horodatage est basée sur les documents issus de l'ETSI (cf. [ETSI_TIMESTAMP]) et du RGS v2 de l'ANSSI.

1.2 Identification du document

La présente Politique d'Horodatage (PH) est dénommée « Politique d'Horodatage Yousign ». Elle peut être identifiée par son numéro d'identifiant d'objet OID : 1.2.250.1.302.2.1.1.0

Cette politique d'horodatage est conforme à la politique d'horodatage décrite dans le document [ETSI_TIMESTAMP] et identifiée par l'OID BTSP 0.4.0.2023.1.1

1.3 Gestion de la politique

L'entité en charge de l'administration et de la gestion de la politique d'horodatage (PH) est l'AH. L'AH est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PH.

Des précisions sont données sur le processus d'amendement de la PH au §8.9.

1.4 Point de contact

Toute demande relative à la présente Politique d'Horodatage est à adresser à :

Gestion de l'AH Yousign
Yousign SAS
8 allée Henri Pigis
14000 CAEN
contact@yousign.fr

1.5 Généralités

1.5.1 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. La contremarque de temps est demandée directement à l'AH.

Autorité de Certification (AC) – Entité qui délivre et est responsable des Certificats électroniques signés en son nom, conformément à sa Politique de Certification.

Autorité d'Horodatage (AH) – Entité en charge de l'émission et de la gestion des contremarques de temps conformément à une Politique d'Horodatage.

Client – Un client est une entité ayant contractualisé avec Yousign pour pouvoir demander des contremarques de temps. Dans cette PH, un client est un abonné.

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 [TF.460-5].

Horodatage - Service qui associe de manière sûre un événement et une heure afin d'établir de manière fiable l'heure à laquelle cet événement s'est réalisé.

Jeton d'horodatage – Voir Contremarque de temps.

Liste de Certificats Révoqués (LCR) – Liste de certificats ayant fait l'objet d'une révocation avant la fin de leur période de validité.

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 les exigences de sécurité satisfaites. Une PH identifie également les obligations et exigences portant sur les autres intervenants, notamment les Abonnés et les Utilisateurs de contremarques de temps. La PH identifie aussi les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AH applique dans le cadre de la fourniture de ses services d'horodatage pour respecter les exigences qui lui incombe.

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

Système d'horodatage – Ensemble des Unités d'horodatage et des composants d'administration et de supervision utilisés pour fournir le 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 [TF.536-1]).

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.

1.5.2 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
BTSP	Best practices Time-Stamp Policy
CGU	Conditions Générales d'Utilisation du service d'horodatage
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de Gestion de Clés
LCR	Liste des Certificats Révoqués
OID	Object Identifier
PH	Politique d'Horodatage
PSHE	Prestataire de Services d'Horodatage Electronique
UH	Unité d'Horodatage
UTC	Coordinated Universal Time
IETF	Internet Engineering Task Force

2 Dispositions générales

2.1 Obligations de l'Autorité d'Horodatage

L'AH génère et signe les contremarques de temps conformément à la présente PH et aux CGU associées.

L'AH garantit la conformité pour tout acteur intervenant dans la gestion des contremarques de temps par rapport aux exigences et aux procédures prescrites dans cette PH.

L'AH remplit tous ses engagements tels que stipulés dans ses Conditions Générales d'Utilisation.

L'AH met à la disposition des abonnés et utilisateurs l'ensemble des informations nécessaires à la vérification des contremarques de temps.

L'AH respecte les conditions de disponibilité du service d'horodatage convenues contractuellement avec les abonnés.

L'AH maintient une information sur la compromission de la bi-clé des UH.

2.2 Obligations de l'Abonné

Au-delà des exigences spécifiques incluses dans les conditions générales d'utilisation du service d'horodatage, et que doit respecter l'abonné, il est recommandé que ce dernier, au moment de l'obtention d'une contremarque de temps, vérifie que le certificat de l'Unité d'Horodatage ne soit pas révoqué.

2.3 Obligations de l'Utilisateur de contremarques de temps

Pour faire confiance à une contremarque de temps, l'utilisateur devra :

a) 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.

b) tenir compte des limitations sur l'utilisation de la contremarque de temps indiquées dans la PH et dans les conditions générales d'utilisation.

2.4 Obligations pour les AC fournissant les certificats des UHs

Les certificats doivent être délivrés par l'AC « YOUSIGN SAS - SIGN2 CA » selon la Politique de Certification 1.2.250.1.302.1.9.1.0. En particulier, l'AC est responsable de la publication des certificats et des informations de révocation permettant de vérifier le certificat des unités d'horodatage.

La chaîne de certification complète des certificats des unités d'horodatage est la suivante :

- AC Racine : « YOUSIGN SAS - ROOT2 CA »
  - AC Émettrice : « YOUSIGN SAS - SIGN2 CA »
    - Certificat d'unité d'horodatage

2.5 Déclarations des pratiques d'horodatage

L'AH garantit qu'elle possède la fiabilité nécessaire pour fournir le service d'horodatage. En particulier :

a) L'AH a effectué une analyse de risques afin de déterminer les contrôles de sécurité nécessaires et les procédures opérationnelles.

b) L'AH dispose de procédures internes utilisées pour adresser toutes les exigences identifiées dans cette PH.

c) La PH identifie les obligations de toutes les organisations externes participant à la fourniture du service d'horodatage, y compris la politique applicable et les pratiques. Cela inclut l'AC fournissant les certificats aux UH.

d) L'AH met à la disposition des abonnés et des utilisateurs de contremarques de temps les éléments publics de ses procédures opérationnelles dans sa PH, et, s'il y a lieu, toute autre documentation appropriée, tel que nécessaire pour évaluer la conformité à la PH.

e) L'AH dispose d'une organisation adéquate pour la vérification de concordance entre les procédures opérationnelles exposées dans la PH et les engagements pris dans la PH.

f) Le responsable opérationnel de l'AH garantit que les pratiques sont correctement mises en œuvre.

g) L'AH définit une procédure de contrôle périodique de la conformité des pratiques, y compris les responsabilités, à la politique d'horodatage.

h) L'AH doit informer au préalable les abonnés pour tout changement qu'elle a l'intention de faire dans sa politique d'horodatage et, après l'approbation, immédiatement mettre à la disposition des abonnés et des utilisateurs de contremarques de temps la PH.

i) Si l'AH a été évaluée pour être en conformité avec la présente PH et si une modification envisagée à l'initiative de l'AH pouvait entraîner une non-conformité avec ladite PH, alors l'AH soumettra cette modification à l'organisme évaluateur indépendant pour avis.

2.6 Conditions Générales d'Utilisation

L'AH définit des CGU qui reprennent les grands principes décrits dans la présente PH. Ces CGU comprennent une section inspirée du modèle défini dans l'annexe B du document [ETSI_TIMESTAMP].

Les CGU du service d'horodatage sont mises à disposition des abonnés et utilisateurs des contremarques de temps (cf. §2.7).

2.7 Publication des informations

2.7.1 Responsable de la publication

L'AH est responsable de la publication des informations requises.

2.7.2 Informations publiées et localisation

Les informations mises à disposition des abonnés et utilisateurs des contremarques de temps sont les suivantes :

- Le présent document, constituant à la fois la Politique d' Horodatage et la déclaration de pratiques du service ;
- Les Conditions Générales d'Utilisation ;
- Les certificats des Unités d'Horodatage et leur chaîne de certification.

Toutes ces informations sont publiées sur l'URL suivante :

https://yousign.fr/fr/public/document

2.7.3 Délais de publication

Les informations sont publiées dès leur approbation par l'AH, avant l'ouverture du service ou de l'évolution impliquant la modification des informations publiées. De cette sorte, les informations publiées sont toujours à jour par rapport au service disponible.

3 Exigences opérationnelles

3.1 Synchronisation de l'horloge

L'AH garantit que son horloge est synchronisée avec le temps UTC selon l'exactitude déclarée de une seconde. La synchronisation utilise des serveurs de temps synchronisés sur plusieurs sources de référence.

En particulier :

a) Le calibrage de chaque horloge d'UH est maintenu de telle manière que les horloges ne puissent pas normalement dériver en dehors de l'exactitude déclarée.

b) Les horloges des unités d'horodatage sont protégées contre les menaces relatives à leur environnement qui pourraient aboutir à une désynchronisation avec le temps UTC en dehors de l'exactitude déclarée.

c) L'AH s'assure que tout non-respect de l'exactitude déclarée par son horloge interne sera détecté.

d) Si l'horloge d'une UH est détectée comme étant en dehors de l'exactitude annoncée, ou que les serveurs de temps ne sont plus disponibles, alors les contremarques de temps ne seront plus générées.

e) L'AH garantit que la synchronisation de l'horloge est maintenue lorsqu'un saut de seconde est programmé comme notifié par l'organisme approprié. Le changement pour tenir compte du saut de seconde est effectué durant la dernière minute du jour où le saut de seconde est programmé. Un enregistrement du temps exact (à la seconde près) de l'instant de ce changement est effectué.

Les mesures de sécurité techniques mises en place pour le respect de ces exigences sont décrites au §5.1.

3.2 Requête et réponse du service d'horodatage

L'AH Yousign fournit une contremarque de temps en réponse à une requête contenant l'empreinte de la donnée à horodater.

La fourniture d'une contremarque de temps en réponse à une demande n'excède pas quelques secondes[1], ceci afin de ne pas nuire ni dégrader l'ergonomie de l'application appelante.

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

Les précisions concernant le protocole et le format des requêtes du service d'horodatage sont fournies au §6.2.

3.3 Contenu d'une contremarque de temps

Les contremarques de temps sont générées dans un environnement sûr et contiennent les informations suivantes :

- L'identifiant de l'UH fourni à travers le DN du certificat de l'unité d'horodatage ;
- L'identifiant (OID) de la politique d'horodatage appliquée ;
- Un identifiant unique de la contremarque ;
- Un temps, celui du moment de génération de la contremarque, synchronisé avec le temps UTC avec une précision d'une seconde ;
- L'empreinte et l'algorithme d'empreinte de la donnée horodatée.

La contremarque de temps est signée par l'UH avec sa clé privée, réservée à cet usage.

Les précisions concernant le format des contremarques de temps sont données au §6.3.

3.4 Vérification des contremarques de temps

L'AH garantit que les utilisateurs de contremarques de temps ont accès à l'information utilisable pour vérifier la signature numérique des contremarques de temps. En particulier :

a) Les certificats des UH sont disponibles, joints à la contremarque de temps sur demande et toujours disponibles sur l'espace de publication de l'AH (cf. §2.7) ;

b) La chaîne de certification complète est disponible sur l'espace de publication de l'AH (cf. §2.7) ;

[1] Ce temps de réponse est le délai écoulé entre la réception de la requête et la signature de la contremarque de temps résultante.

c) Les informations sur le statut de révocation des certificats sont disponibles en activant les URL disponibles dans les certificats des Unités d'Horodatage (extensions Authority Information Access et cRLDistributionPoint, voir au §6.1).

4 Mesures de sécurité non techniques

4.1 Mesures de sécurité physique et environnementale

L'AH garantit que l'accès physique aux services critiques est contrôlé et que les risques physiques et environnementaux d'atteinte à ses actifs sont réduits au minimum.

Des mesures de sécurité sont mises en place sur les sites d'hébergement de l'infrastructure du système d'horodatage, afin de protéger l'environnement et les composantes elles-mêmes. Ces mesures sont les suivantes :

a) Contrôle d'accès physique :

L'accès physique aux équipements du service d'horodatage est limité aux seuls individus autorisés. Si nécessaire, une personne non-autorisée peut accéder à certaines installations si elle est accompagnée de façon permanente par une personne habilitée.

Les sites, accessibles 24H/24H, 7j/7j, sont sous la surveillance permanente d'une équipe de sécurité. Les accès sur les sites sont sécurisés et strictement règlementés. Une double vérification de l'identité et de l'autorisation d'accès de chaque intervenant sur le site est effectuée à l'accueil, puis au poste de sécurité.

Un système d'accès par badge individuel complète ce dispositif en limitant l'accès aux zones autorisées et en permettant une traçabilité des personnes sur le site. Trois check points sont installés entre l'entrée du site et l'espace client.

De plus, la sûreté des locaux est assurée par un système CCTV doublé de caméras infrarouges en extérieur. Un nombre important de caméras filment et enregistrent numériquement les locaux et l'extérieur des bâtiments. Une batterie de moniteurs de contrôle enregistrent et conservent les données filmées sur une période allant jusqu'à 6 mois.

b) Protection vis à vis des catastrophes naturelles :

Les datacenters sont situés sur des sites non exposées à des risques naturels ou environnementaux majeurs. L'analyse de risque propre à ces sites prend en compte la situation géographique et propose les mesures de sécurité adaptées au contexte.

Les mesures mises en œuvre assurent la protection contre un écroulement du bâtiment.

c) Prévention et protection incendie :

La protection contre les incendies repose sur un ensemble de moyens :

- Un système de sécurité incendie de catégorie A
- Un système d'extinction par Azote
- Application des règles R7/R13/R4
- Maintenance de la norme NFS 940
- Formation régulière des équipes
- Moyens d'accueil et d'intervention pompiers
- Murs stables au feu 2 heures et portes coupe-feu 1 heure

d) Protection contre la défaillance d'alimentation électrique :

Les sites bénéficient de deux alimentions provenant de deux sous stations EDF différentes et cheminant par deux arrivées privatives distinctes. En cas de disparition d'une alimentation, le basculement sur le deuxième câble toujours sous tension est effectif au bout de 5 secondes.
Toute l'installation électrique est assurée de base en N+1 minimum.
Le site dispose de trois groupes électrogènes permettant une autonomie effective de cinq jours à pleine charge. En cas d'absence totale de tension sur les deux câbles EDF, les groupes électrogènes prennent le relais automatiquement en 20 secondes.

e) Protection contre la défaillance de connexions réseau :

Les sites disposent de deux arrivées réseau distinctes par des fournisseurs d'accès différents. Les équipements du site garantissent de façon transparente aux ressources hébergées un accès continu au réseau.

f) Climatisation :

Les salles sont climatisées par trois groupes froid, redondées en N+1, avec une configuration en allées chaudes et froides garantissant une température optimale de fonctionnement (maximum 30/35°Cdans les allées chaudes).
La norme d'hygrométrie admise est de 50% avec + ou – 10% d'écart.

g) Protection contre les dégâts des eaux et les fuites de plomberie :

- Détection de l'eau dans les faux planchers
- Architecture de drainage (pompes de drainage et relevage dans les galeries en sous-sol)

h) Protection contre le vol, la casse et la pénétration :

Des contrôles sont mis en œuvre sur site pour empêcher des équipements, de l'information, des médias et du logiciel touchant aux services d'horodatage d'être enlevés du site sans autorisation.

i) Rétablissement de la sécurité après un désastre :

Les sites disposent de plans de continuité et de reprise d'activité à même de garantir une disponibilité de 99,99%.

Des contrôles spécifiques d'accès physique sont appliqués aux modules cryptographiques des unités d'horodatage pour remplir les contraintes sur l'environnement d'exploitation de ces matériels (fournies dans sa cible de sécurité et son certificat de qualification). En particulier, ces matériels sont placés dans des baies fermées et accessibles uniquement au personnel Yousign autorisé.

4.2 Mesures de sécurité procédurales

4.2.1 Sécurité des systèmes

L'Autorité d'horodatage garantit que les composants du système d'Horodatage sont sûrs et correctement opérés, avec un risque minimal d'échec. En particulier :

L'intégrité des composants du système d'horodatage et l'information sont protégés contre les virus, les logiciels malveillants et non autorisés

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 soient réduits au minimum.

Les supports employés dans les systèmes d'horodatage sont manipulés de manière sécuritaire pour les protéger des dégâts, du vol, de l'accès non autorisé et de l'obsolescence.

4.2.2 Manipulation et sécurité des supports

Tous les supports doivent être traités de manière sécuritaire conformément aux exigences de la classification de l'information. Les supports contenant des données sensibles doivent être retirés de manière sécuritaire quand ils ne sont plus utiles.

4.2.3 Planification de système

Les charges doivent être contrôlées et des projections de charge dans le futur doivent être effectuées pour garantir que les puissances de traitement et de stockage adéquates seront disponibles.

4.2.4 Rapport d'incident et réponse

L'Autorité d'Horodatage agira d'une façon opportune et coordonnée pour répondre rapidement aux incidents et limiter l'impact des infractions à la sécurité. Tous les incidents seront rapportés aussitôt que possible après l'incident.

4.2.5 Procédures de fonctionnement et responsabilités

Des procédures sont établies et mises en œuvre pour tous les rôles de confiance et administratifs qui impactent la fourniture des services d'horodatage

Les opérations de sécurité sont séparées des autres opérations. Elles incluent :

- 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 de sécurité sur les composantes du service d'horodatage sont réalisées par du personnel de confiance.

4.2.6 Déploiement et Maintenance

L'AH emploie des produits et systèmes de confiance.

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

4.3 Mesures de sécurité vis-à-vis du personnel

L'AH garantit que le personnel et les pratiques d'embauche améliorent et concourent à la fiabilité des opérations de l'AH. En particulier :

a) L'Autorité d'Horodatage emploie un personnel qui possède l'expertise, l'expérience et les qualifications nécessaires pour les services offerts, tels que l'exige la fonction.
b) Les rôles de sécurité et les responsabilités, comme spécifié dans la politique de sécurité de l'AH, sont documentés dans des descriptions de poste. Les rôles de confiance, sur lesquels la sécurité du fonctionnement de l'AH repose, sont clairement identifiés.
c) Des descriptions de fonctions sont définies pour le personnel de l'AH (aussi bien provisoire que permanent) du point de vue de la séparation des responsabilités et du principe du privilège minimum, selon la sensibilité de la fonction sur la base des responsabilités et des niveaux d'accès, et indiquent le type d'enquête à effectuer sur le passé, le type de formation appropriée et les particularités de la fonction.
d) Le personnel met en œuvre des procédures administratives et de gestion ainsi que des processus en accord avec les procédures de gestion de sécurité de l'information de l'AH

Les contrôles complémentaires suivants sont appliqués à la gestion de l'horodatage :

e) le personnel de gestion employé possède :
    - la connaissance de la technologie de l'horodatage et ;
    - la connaissance de technologie de la signature numérique et ;
    - la connaissance des mécanismes pour le calibrage ou la synchronisation des horloges des unités d'horodatage avec le temps UTC et ;
    - pour le personnel avec des responsabilités de sécurité, une bonne connaissance des procédures de sécurité, et ;
    - l'expérience avec la sécurité de l'information et l'évaluation des risques.
f) Tout le personnel de l'AH dans des rôles de confiance est libre de conflit d'intérêt qui pourrait porter préjudice à l'impartialité des opérations de l'AH.
g) Les rôles de confiance incluent les rôles qui impliquent les responsabilités suivantes :
    - les officiers chargés de la sécurité : responsabilité complète d'administrer la mise en œuvre des pratiques de sécurité ;
    - les administrateurs système : autorisés à installer, configurer et maintenir les unités d'horodatage de l'AH pour la gestion de l'horodatage ;

- les opérateurs système : responsables pour faire fonctionner les unités d'horodatage de l'AH de manière quotidienne et autorisés pour effectuer les opérations de sauvegarde et des secours ;
- les auditeurs de système : autorisés à consulter les archives et les fichiers d'audit des unités d'horodatage.

h) Le personnel de l'AH est formellement nommé aux rôles de confiance par la direction responsable de la sécurité.

i) L'AH s'interdit de nommer aux rôles de confiance ou de gestion toute personne connue pour avoir une condamnation pour un crime sérieux ou une autre infraction qui affecte son adéquation avec la position. Le personnel n'a pas accès aux fonctions de confiance avant que les contrôles nécessaires ne soient achevés

4.4 Constitution des données d'audit

L'AH enregistre les informations appropriées concernant le fonctionnement du service d'horodatage, en particulier :

a) Les enregistrements d'audit relatifs à l'administration des services d'horodatage :

- gestion des opérateurs d'administration
- connexion / déconnexion des opérateurs d'administration (même en cas d'échec)
- configuration technique ou métier (définition d'une politique d'horodatage)

b) Les enregistrements d'audit relatifs au fonctionnement du service d'horodatage :

- démarrage et arrêt des services
- traitement d'une demande de jeton
- défaillance / indisponibilité du service

c) Les enregistrements d'audit concernant les événements touchant au cycle de vie des clés et certificats d'UH :

- génération de clés
- demande de certificat
- génération du certificat
- import du certificat
- désinstallation d'un certificat
- destruction de la clé privée

d) Les enregistrements d'audit concernant les événements touchant à une synchronisation de l'horloge des UH, y compris les événements touchant à la détection de perte de synchronisation :

- déclaration des sources de temps
- pertes d'accès à une source de temps
- détection de perte de synchronisation
- resynchronisation de l'horloge
- saut de seconde

Chacun de ces événements comprend au minimum les données suivantes :

- Type de l'événement
- Auteur (personne physique, système)
- Date et heure
- Résultat de l'évènement (échec ou réussite)

L'intégrité, la protection contre la suppression et la confidentialité des enregistrements d'audit sont assurés par une gestion d'accès physique, système et réseau appropriée.

Les traces techniques sont conservées sans purge sur les équipements du système d'horodatage. Une procédure de sauvegarde quotidienne permet d'exporter ces traces, protégées en intégrité (calcul d'empreinte) et confidentialité (chiffrement), vers des systèmes de conservation sur le long terme. Les journaux du service d'horodatage sont conservés pendant 7 ans au minimum après l'expiration du certificat d'horodatage actif.

4.5 Continuité d'activité

Au-delà de la continuité d'activité assurée au niveau de l'hébergement, l'AH met en place son propre plan de continuité d'activité concernant les données et les secrets du système.

Les composantes du système d'horodatage disposent d'une sauvegarde hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un évènement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.). Les fonctions de sauvegarde et de restauration seront effectuées par des administrateurs autorisés conformément aux mesures de sécurité procédurales.

Les sauvegardes hors sites sont réalisées dans un environnement sécurisé en accès physique et logique, et sécurisé contre les risques d'incendie et d'inondation.

4.6 Gestion des incidents

L'AH 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 UH 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) l'AH traite le cas de la compromission réelle ou suspectée de la clé privée de signature d'une UH ou la perte de calibrage de l'horloge d'une UH, qui pourrait affecter des contremarques de temps émises dans le cadre d'un plan de secours

b) Dans le cas d'une compromission, réelle ou suspectée, l'AH mettra à la disposition de tous les abonnés et utilisateurs de contremarques de temps une description de la compromission qui est survenue.

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

d) Dans le cas d'une perte de connexion prolongés avec les serveurs de temps, l'AH prendra les mesures nécessaires pour que les contremarques de temps de cette UH ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.

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

f) L'AH prévient directement et sans délai le point de contact de l'organe de contrôle national.

4.7 Cessation d'activité de l'AH

Des procédures de fin d'activité définies par l'AH garantissent 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 assurent en particulier la maintenance continue des informations nécessaires pour vérifier la justesse de contremarques de temps. En particulier :

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

   - l'AH rendra disponible à tous ses abonnés et utilisateurs de contremarques de temps l'information concernant sa fin d'activité ;

   - l'AH abrogera les autorisations données aux sous-traitants d'agir pour son compte dans l'exécution de n'importe quelles fonctions touchant au processus de génération des contremarques de temps ;

   - l'AH transférera à un organisme fiable ses obligations de maintien des fichiers d'audit et des archives nécessaires pour démontrer son fonctionnement correct durant une période raisonnable ;

   - l'AH maintiendra ou transférera à un organisme fiable ses obligations de rendre disponibles aux utilisateurs de contremarques de temps pendant une période raisonnable ses clés publiques ainsi que ses certificats;

   - les clés privées des UH seront détruites de telle façon que les clés privées ne puissent pas être recouvrées.

b) L'AH prend les mesures nécessaires pour couvrir les dépenses pour accomplir ces exigences minimales dans le cas où l'AH tomberait en faillite ou pour d'autres raisons serait incapable de couvrir les dépenses par elle-même.

c) L'AH prévient directement et sans délai le point de contact de l'organe de contrôle national.

5 Mesures de sécurité techniques

5.1 Gestion de la synchronisation de l'horloge

Chaque unité d'horodatage s'assure que les contremarques de temps sont produites avec une exactitude de temps de 1 seconde par rapport au temps UTC. Pour cela, elle utilise son horloge interne et des sources de temps.

5.1.1 Gestion des sources de temps

Les sources de temps utilisées par chaque unité d'horodatage sont au minimum :

- Le signal GPS reçu par une installation propre à l'AH
- Des serveurs de temps de référence, au minimum :
    - Serveur NTP de l'Observatoire de Paris : ntp.obspm.fr
    - Serveur NTP de l'Université de Caen : ntp.unicaen.fr

Le matériel permettant l'acquisition du signal GPS est maintenu et supervisé par l'infrastructure de l'AH. Ce matériel est lui-même doté d'une horloge interne précise.

5.1.2 Synchronisation des UH

L'horloge interne des unités d'horodatage est synchronisée par le protocole NTP.

Toutes les heures, la dérive de l'horloge de l'unité d'horodatage est contrôlée par rapport aux sources de temps.

Nous considérons que l'horloge est synchronisée lorsque nous sommes synchronisés avec 2 sources de temps distinctes. Cette vérification a lieu toutes les heures. Dans ce cas, nous conservons la synchronisation en place pendant 6 heures. Dans le cas où l'horloge locale est désynchronisée, la génération de jeton d'horodatage est immédiatement arrêtée. Une nouvelle vérification de la synchronisation à lieu 5 secondes plus tard.

5.1.3 Gestion des incidents de synchronisation

Si l'écart mesuré entre l'heure interne d'une unité d'horodatage et l'heure d'une source de temps de référence est supérieur à 1 seconde, cet écart est vérifié avec les autres sources de temps. Si l'écart de 1 seconde est constaté avec au moins deux sources de temps, alors une perte de synchronisation de l'horloge est considérée avérée.

Dans ce cas :

- L'unité d'horodatage stoppe immédiatement la délivrance de contremarques de temps ;
- La perte de synchronisation est journalisée ;
- La perte de synchronisation est remontée par le système de supervision du service ;
- L'unité d'horodatage recommence régulièrement une mesure d'écart afin de reprendre l'émission de contremarques de temps dès que son horloge est revenue à la précision souhaitée.

En cas d'indisponibilité ponctuelle de toutes les sources de temps, l'unité d'horodatage poursuit la délivrance de contremarques pendant 6 heures, délai pendant lequel la dérive de l'horloge est négligeable grâce à la synchronisation NTP sur l'horloge du matériel d'acquisition dont l'horloge interne est particulièrement précise. L'unité d'horodatage poursuit une interrogation régulière des sources de temps. Au-delà de 6 heures, une perte de synchronisation est déclarée, et le traitement décrit ci-dessus est exécuté.

5.1.4 Gestion des sauts de seconde

La gestion des sauts de seconde est entièrement automatisée par le service.

La survenue d'un saut de seconde est une information déclarée par les serveurs NTP, dès la première heure du jour de son occurrence. Lorsqu'une unité d'horodatage prend connaissance de ce saut de seconde, elle se place dans un mode spécifique qui entraine un comportement adéquat lors de la dernière seconde du jour.

Nous utilisons la donnée envoyée par les serveurs NTP afin de gérer un saut de seconde, si le NTP indique que le jour actuel contient un saut de seconde (leapsecond) positive ou négative, la génération de jeton met en pause toutes les demandes le temps que le saut de seconde soit terminée par itération de 500 ms et les jetons sont générés et renvoyés une fois le saut de seconde terminé.

5.1.5 Prise en compte de menaces

L'horloge de l'unité d'horodatage ne peut pas être modifiée, exceptée par un ingénieur système de confiance. Une modification non autorisée de cette horloge serait détectée dès la prochaine comparaison de l'horloge de l'unité avec les sources de temps.

Afin de se protéger contre une falsification des réponses NTP d'une source de temps non authentifiée, l'unité d'horodatage se base toujours au minimum sur deux sources de temps pour évaluer la dérive de sa propre horloge.

5.2 Gestion des bi-clés des unités d'horodatage

5.2.1 Génération de clé

L'AH garantit que les clés cryptographiques des UH sont produites dans des circonstances et un environnement contrôlés, au cours d'une cérémonie de clés faisant l'objet d'un procès-verbal.

Ces clés sont générées et protégées au sein d'un HSM (Hardware Security Module) cryptographiques qualifié et ne sont pas exportées, excepté pour leur sauvegarde. La longueur des clés de l'AH est de 2048 bits avec l'algorithme RSA.

5.2.2 Certification des clés de l'unité d'horodatage

L'AH s'assure que la valeur de la clé publique et l'identifiant de l'algorithme de signature contenus dans la demande de certificat de l'UH sont égaux à ceux générés par l'UH.

Le certificat de l'UH est généré par l'AC «YOUSIGN SAS - SIGN2 CA ».

La demande de certificat envoyée auprès de l'AC contient, en plus des informations exigées dans la PC de l'AC pour la partie enregistrement, au moins les informations suivantes :

- le nom (DN) de l'UH pour laquelle la demande de certificat est faite ;
- la valeur de la clé publique (et l'identifiant de l'algorithme).

L'AH vérifie lors de l'import du certificat de l'UH qu'il est bien émis par l'AC requise et qu'il est conforme au gabarit attendu. L'AH s'assure que l'UH ne peut être opérationnelle qu'une fois ces vérifications effectuées avec succès.

5.2.3 Durée de validité des certificats de clé publique des unités d'horodatage

La durée de validité des certificats des UH ne peut pas excéder :

- la durée de vie cryptographique de la clé privée associée,
- la date de fin de validité du certificat de l'AC émettrice.

Par défaut, cette durée est de 3 ans.

5.2.4 Protection des clés privées des unités d'horodatage

Les clés privées des UH sont stockées dans un moyen cryptographique décrit au §5.3.1.

5.2.5 Durée d'utilisation des clés privées des UH

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

5.2.6 Gestion de la durée de vie de la clé privée

L'AH garantit que les clés privées de signature des UH ne sont pas employées au-delà de la fin de leur cycle de vie. En particulier :

a) Des procédures opérationnelles ou techniques assurent 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) Le Système d'horodatage détruit, de façon sécurisée, la clé privée si la fin de la période d'utilisation de cette clé privée a été atteinte.

5.2.7 Sauvegarde des clés des unités d'horodatage

Les clés privées des UH font l'objet d'une copie de secours (sauvegarde) qui ne peut être restaurée que par les administrateurs de sécurité de l'AH. Au minimum deux porteurs de secrets, désignés pendant la cérémonie des clés initiale, sont requis pour procéder à la restauration d'une clé privée d'UH dans une nouvelle partition du HSM. La sécurité de la sauvegarde est assurée par les mécanismes de sécurité intrinsèques au HSM, assurant un niveau de protection équivalent au stockage interne dans le HSM.

La restauration des clés privées des UH ne peut être réalisée qu'en présence, au minimum, de deux personnes distinctes, parmi les rôles de confiance suivants : responsable légal de l'AH, responsable de l'AH, responsable de l'unité d'horodatage, responsable de sécurité du système d'horodatage.

5.2.8 Destruction des clés des unités d'horodatage

Les clés de signature des UH sont détruites à la fin de leur cycle de vie.

5.3 Cryptographie

5.3.1 Moyens cryptographiques

Les clés privées des UH sont stockées dans un HSM certifié CC EAL4+ et qualifié par l'ANSSI.

5.3.2 Gestion du cycle de vie

Le moyen cryptographique est déployé selon les préconisations d'emploi spécifiées dans sa cible de sécurité et rappelées dans le rapport de qualification du matériel. Ceci garantit en particulier :

- L'intégrité du HSM durant son transport depuis le fournisseur ou le cas échéant entre deux sites d'hébergement utilisés par Yousign ;
- La sécurité physique (cf. §4.1) et logique du matériel pendant son exploitation ;
- La sécurité des opérations d'administration, réalisées lors de cérémonies de clés par des porteurs de secret sous le contrôle de l'AH et du responsable de sécurité.

5.3.3 Gestion des Secrets

Les sites dans lesquels sont conservées les sauvegardes sont protégés contre les risques d'incendies et d'inondation. De plus, les accès physiques et logiques sont protégés et soumis à une gestion des droits et à une authentification forte.

S'il y a utilisation de documents papiers, ou de supports amovibles telles qu'un CD, une clé USB de stockage, un disque dur externe ou une carte à puce, ceux-ci seront conservés dans un coffre-fort.

Des procédures de gestion protègent les supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AH s'engage à conserver les informations qu'ils contiennent.

La mise hors service des différents supports varie en fonction de leur nature. En ce qui concerne les documents papiers, les CD, les clés USB de stockage, les cartes à puce, ils seront broyés en fin de vie (fin d'utilisation ou obsolescence). Les supports de stockage seront vidés, puis détruits à l'aide d'un marteau. Les HSM seront mis hors service en suivant les directives du constructeur.

5.3.4 Algorithmes obligatoires

L'AH accepte de générer des contremarques de temps pour les empreintes calculées avec les algorithmes suivants :

- SHA-256 ;
- SHA-384 ;
- SHA-512.

Les contremarques de temps sont signées selon les algorithmes et les longueurs de clé conformes à l'état de l'art. Actuellement, la bi-clé de l'UH est une bi-clé RSA de 2048 bits et l'algorithme de signature utilise une fonction de hachage SHA-256.

5.3.5 Contrôle d'accès

L'Autorité d'Horodatage garantit que l'accès au système d'horodatage est limité aux individus dûment autorisés. En particulier :

a) Des contrôles (par pares-feux) sont être mis en œuvre pour protéger le réseau interne de l'AH d'accès non autorisés incluant l'accès par des abonnés et des tierces personnes.

   Les pares-feux sont aussi configurés pour bloquer tous les protocoles et les accès non nécessaires au fonctionnement de l'AH.

b) L'AH effectue une administration efficace des utilisateurs (opérateurs, administrateurs et auditeurs), pour maintenir la sécurité du système, y compris la gestion des comptes des utilisateurs, l'audit, et la modification ou le retrait rapide d'accès.
c) l'AH 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.
d) Le personnel de l'AH est dûment identifié et authentifié avant d'utiliser des applications critiques liées à l'horodatage.
e) Le personnel de l'AH sera tenu responsable de ses activités, par exemple en conservant des fichiers d'audit.

Les contrôles complémentaires suivants sont appliqués à la gestion de l'horodatage :

f) L'Autorité d'horodatage garantit que des composants de réseau locaux (par exemple les routeurs) seront mis dans un environnement physiquement sûr et que leurs configurations sont périodiquement vérifiées pour la conformité avec les exigences indiquées par l'AH.
g) Une surveillance permanente et des équipements d'alarme est mise en oeuvre pour permettre à l'AH de détecter, d'enregistrer et de réagir rapidement à n'importe quelle tentative non autorisée et/ou irrégulière d'accès à ses ressources.
h) L'Autorité d'Horodatage garantit que les opérations d'administration système des plateformes sont réalisées exclusivement sur un réseau dédié, depuis un poste d'administration sans accès au réseau extérieur.

5.3.6 Sécurité des plateformes informatiques

L'AH applique la politique de sécurité des systèmes d'information de Yousign sur toute l'infrastructure informatique du service d'horodatage.

Cette politique garantit en particulier :

- Une organisation interne de la sécurité pilotée par un comité de direction de la société ;
- La mise en place de système de contrôle de flux (détection d'intrusion, fermeture des ports non explicitement autorisé) ;
- La mise en place systématique de contrôle d'accès logique dont le niveau de sécurité est adpaté au contexte d'emploi ;
- L'interdiction de la connexion au réseau d'administration de l'entreprise par une connexion sans fil ;
- La traçabilité systématique des accès pour garantir entre autre l'imputabilité des actions ;
- Le déploiement de solutions de sécurité pour lutter contre les virus et autres logiciels malveillants sur les plateformes du service ;
- La gestion des vulnérabilités par analyse journalières des alertes de sécurité communiquées par un CERT avec lequel Yousign a contractualisé ;
- La conduite régulière de tests de vulnérabilité réseau
- La conduite périodique, et au moins annuelle, de tests d'intrusion sur le système d'horodatage.

6 Profil des certificats et contremarques de temps

6.1 Format du certificat d'horodatage

Les certificats de signature des contremarques de temps respectent le gabarit suivant :

Champ		**Valeur**
version		2 (c'est-à-dire version3)
serialNumber		Nombre aléatoire à longueur fixe.
signature		
- algorithm		SHA256WithRSA
- parameters		RSAParams : NULL
issuer Distinguished Name		CN=YOUSIGN SAS - SIGN2 CA, OU=794513986, O=YOUSIGN SAS, L=CAEN, ST=CALVADOS, C=FR
validity		
- notBefore		Date de création
- notAfter		Date de création + 3 ans
subject Distinguished Name		CN=Unité d'horodatage N Yousign, SERIALNUMBER = <numéro de série basé sur la date> O=YOUSIGN SAS, C=FR, OI= NTRFR:794513986
subjectPublicKeyInfo		
- algorithm - algorithm - parameters		rsaEncryption RSAParams : 05 00
- subjectPublicKey		RSAPublicKey (2048 bits)
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé

Extensions	Criticité	Valeur
- authorityKeyIdentifier	Non	Hash de la clé publique de l'émetteur
- subjectKeyIdentifier	Non	Hash de la clé publique du sujet
- keyUsage	Oui	digitalSignature
- extKeyUsage	Non	id-kp-timestamping
- authorityInformationAccess	Non	accessMethod : id-ad-caIssuers accessLocation : http://crl.yousign.fr/yousignsassign2ca.crt http://crl2.yousign.fr/yousignsassign2ca.crt http://crl3.yousign.fr/yousignsassign2ca.crt accessMethod : id-ad-ocsp accessLocation : http://ocsp.yousign.fr
- privateKeyUsagePeriod		Extension non utilisée
- certificatePolicies	Non	Stratégie du certificat : Identificateur de stratégie = 1.2.250.1.302.1.9.1.0
- basicContraints - cA - pathLenConstraint	Oui	 false None
- cRLDistributionPoints	Non	Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL : http://crl.yousign.fr/crl/yousignsassign2ca.crl URL : http://crl2.yousign.fr/crl/yousignsassign2ca.crl URL : http://crl3.yousign.fr/crl/yousignsassign2ca.crl
- subjectInfoAccess		Extension non utilisée

Tableau 1 : Format du certificat d'horodatage

6.2 Format des requêtes de contremarque

Les requêtes de contremarques de temps doivent être envoyées par les clients en utilisant le protocole http et en respectant le format décrit par la RFC 3161 (dans son paragraphe §2.4.1).

Les requêtes doivent de plus répondre aux restrictions suivantes :

Champ	Commentaires	Valeur attendue
version	Version du format	1
messageImprint - hashAlgorithm - hashedMessage	OID de l'algorithme de hash (empreinte) Hash des données à horodater	Les seuls algorithmes d'empreinte autorisés sont définis au §5.3. La valeur du hash est libre.
reqPolicy	Optionnel : OID de la PH à appliquer	Si ce champ est présent, il doit avoir la valeur 1.2.250.1.302.2.1.1.0

nonce	Optionnel : Donnée anti-rejeu	Absent ou valeur libre
certReq	Optionnel : Demande à l'UH d'inclure son certificat de signature dans la réponse	Absent ou true/false
extensions	Interdites : La requête n'est pas traitée si une extension est présente	Absent

Tableau 2 : Format des requêtes de contremarque

Les requêtes ne sont pas signées par leur émetteur.

6.3 Format des contremarques de temps

Les réponses envoyées par le service d'horodatage respectent le format décrit par la [RFC_3161] (dans son paragraphe §2.4.2) amendée par la [RFC_5816]. Elles sont signées par la clé privée de l'unité d'horodatage qui les produit.

En particulier, les champs significatifs (structure TSTInfo) sont définis comme suit :

Champ	**Commentaires**	**Valeur**
version	Version du format	1
policy	OID de la PH	1.2.250.1.302.2.1.1.0
messageImprint - hashAlgorithm - hashedMessage	OID de l'algorithme de hash (empreinte) hash des données à horodater	Identiques aux valeurs inclues dans la demande (les algorithmes d'empreinte autorisés sont restreints par la politique)
serialNumber	Identifiant unique de la contremarque de temps	Généré par l'UH
genTime	Heure de la contremarque de temps	Heure de l'UH au moment de la génération, donnée avec les millièmes de seconde
accuracy	Précision	1 seconde
nonce	Donnée anti-rejeu uniquement si nonce était présent dans la requête de jeton	Identique à celui présent dans la requête
extensions	Extension supplémentaires optionnelles	Aucune extension supplémentaire

Tableau 3 : Format des contremarques de temps

De plus, l'identifiant du certificat de l'unité d'horodatage est indiqué dans une structure de type **ESSCertIDv2** comme indiqué dans la RFC 5816 (au paragraphe §2.2.1).

Enfin, si et seulement si la requête demande la fourniture du certificat de l'unité d'horodatage par le champ **certReq**, alors ce certificat est fourni dans le champ **certificates** de la structure **SignedData**.

7 Audit de conformité et autres évaluations

7.1 Fréquences et / ou circonstances des évaluations

Un contrôle de conformité est réalisé lors de la mise en service du système et suite à toute modification significative. De plus, un audit sera réalisé au moins tous les ans. Les audits sont réalisés en interne par du personnel de Yousign ou bien sous la forme d'une prestation auprès d'acteurs spécialistes de la sécurité des systèmes d'information et ayant des compétences reconnues dans le domaine de la signature électronique.

Dans le cadre d'obtention de certifications des services d'horodatage, l'audit de certification est réalisé par une société externe dument accréditée.

7.2 Identités / qualifications des évaluateurs

Les contrôleurs sont des employés de la société Yousign. Yousign s'engage à mandater des personnes disposant des compétences en sécurité requises pour auditer et vérifier la conformité du système.

7.3 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante du système (contrôles ponctuels) ou sur l'ensemble de l'architecture du service d'horodatage (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la PH de l'AH ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

Pour ce faire, les auditeurs présenteront pour approbation au Comité de Direction Technique la liste des composantes et procédures qui seront auditées.

7.4 Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AH, un avis parmi les suivants : "réussite", "échec", "à confirmer". Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AH qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation des certificats de la composante, la révocation de l'ensemble des certificats du service, etc. Le choix de la mesure à appliquer est effectué par l'AH et doit respecter ses politiques de sécurité internes.

- En cas de résultat "à confirmer", l'AH remet au responsable de la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.

- En cas de réussite, l'AH confirme au responsable de la composante contrôlée la conformité aux exigences de la PH.

8 Autres problématiques

8.1 Tarifs

8.1.1 Tarifs pour la fourniture de contremarques de temps

Se référer aux conditions contractuelles en vigueur.

8.1.2 Tarifs pour accéder aux informations publiées par l'AH

L'accès aux informations publiées par l'AH est gratuit.

8.1.3 Tarifs pour accéder aux LCR et au répondeur OCSP

L'accès aux LCR et au répondeur OCSP est gratuit.

8.1.4 Politique de remboursement

Se référer aux conditions contractuelles en vigueur.

8.2 Responsabilité financière

8.2.1 Couverture par les assurances

L'AH applique des niveaux de couverture d'assurance raisonnables et a souscrit à cet effet une assurance responsabilité civile au titre de la réalisation de son activité professionnelle.

8.2.2 Couverture et garantie concernant les entités utilisatrices

Sans objet.

8.3 Confidentialité des données professionnelles

8.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- les procédures internes de l'AH,
- les clés privées des unités d'horodatage et des composantes de l'AH,
- les données d'activation associées aux clés privées d'AH et des composantes,
- tous les secrets de l'AH,
- les journaux d'évènements des composantes de l'AH.

8.3.2 Informations hors du périmètre des informations confidentielles

Sans objet.

8.3.3 Responsabilités en termes de protection des informations confidentielles

Yousign applique des procédures de sécurité pour garantir la confidentialité des informations identifiées ci-dessus. Yousign s'engage à respecter la législation et la réglementation en vigueur sur le territoire français.

Les informations fournies par les abonnés à l'AH ne sont pas divulguées, à moins de leur accord, d'une décision judiciaire ou d'une exigence légale.

8.4 Protection des données personnelles

Dans le cadre du service d'horodatage, l'AH ne traite aucune donnée personnelle et n'a donc pas de relations avec la CNIL pour ce service.

Les informations fournies par les abonnés à l'AH ne sont pas divulguées, à moins de leur accord, d'une décision judiciaire ou d'une exigence légale.

8.5 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par Yousign sont protégés par la législation et réglementation en vigueur.

Les utilisateurs ne disposent d'aucun droit de propriété intellectuelle sur les différents éléments mis en œuvre par Yousign pour assurer son service d'horodatage.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages Web, bases de données, textes originaux, ...) est sanctionnée par le Code de la propriété intellectuelle.

8.6 Limite de responsabilité

Yousign ne pourra pas être tenu pour responsable d'une utilisation non autorisée ou non conforme des contremarques de temps.

De plus, dans la mesure des limitations de la loi française, Yousign ne saurait être tenu responsable :

- d'aucune perte financière ;
- d'aucune perte de données ;
- d'aucun dommage indirect lié à l'utilisation d'une contremarque;
- d'aucun autre dommage.

En toute hypothèse, la responsabilité de Yousign sera limitée, tous faits générateurs confondus et pour tous préjudices confondus, au montant payé à Yousign pour l'accès au service d'horodatage et ce, dans le respect et les limites de la loi applicable.

8.7 Indemnités

Sans objet.

8.8 Durée et fin anticipée de validité de la PH

8.8.1 Durée de validité

La PH de l'AH doit rester en application au moins jusqu'à la fin de vie du dernier certificat d'unité d'horodatage émis au titre de cette PH.

8.8.2 Fin anticipée de validité

Cette PH reste en application jusqu'à la publication d'une nouvelle version.

8.8.3 Effets de la fin de validité et clauses restant applicables

Sans objet.

8.9 Amendements à la PH

8.9.1 Procédures d'amendements

L'AH contrôlera que tout projet de modification de sa PH reste conforme aux exigences de la norme [ETSI_TIMESTAMP]. En cas de changement important, l'AH pourra faire appel à une expertise technique externe, si elle le juge nécessaire.

8.9.2 Mécanisme et période d'information sur les amendements

Lors de tout changement important impactant la PH, Yousign informera les abonnées et les utilisateurs au travers d'un communiqué distribué par voie électronique sur son site internet. Si besoin, une communication par courrier électronique ou postal pourra être réalisée.

8.9.3 Circonstances selon lesquelles l'OID doit être changé

L'OID de la PH de l'AH peut être spécifié par un abonné dans les requêtes de contremarques de temps et est systématiquement inscrit dans les contremarques de temps générées par l'AH. Cet OID, via le lien avec la PH qui est publique, permet aux abonnés et aux utilisateurs de connaître les conditions de génération des contremarques de temps et en particulier les exigences de sécurité associées.

Si ces conditions sont modifiées de façon importante (par exemple changement d'algorithme cryptographique, augmentation de la précision du temps contenu dans les contremarques, augmentation significative des exigences de sécurité opérationnelle), alors l'AH fera évoluer l'OID. Ainsi les abonnés et les utilisateurs pourront clairement distinguer quelles contremarques de temps correspondent à quelles conditions de génération et quelles exigences de sécurité associées.

En particulier, l'OID de la PH de l'AH évoluera dès lors qu'un changement majeur intervient dans les exigences de la norme [ETSI_TIMESTAMP] (et qui sera signalé comme tel, notamment par une évolution de l'OID BTSP de cette norme).

8.10 Dispositions concernant la résolution de conflits

Les présentes politiques sont soumises au droit français

En cas de litige entre les parties découlant de l'interprétation, l'application et/ou l'exécution du contrat et à défaut d'accord amiable entre les parties ci-avant, la compétence exclusive est attribuée au tribunal de commerce de Caen.

8.11 Juridictions compétentes

Se rapporter au chapitre 8.10.

8.12 Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PH sont, notamment, ceux de la loi française et du règlement européen eIDAS [EIDAS].

8.13 Transfert d'activités

Les procédures en cas de transfert d'activité peuvent être demandés à l'AH en s'adressant à elle aux coordonnées mentionnées au §1.4.

9 Annexe 1 : Documents cités en référence

9.1 Réglementation

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
[EIDAS]	Règlement Européen n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

Tableau 4 : Documents règlementaires

9.2 Documents techniques

Renvoi	Document
[ETSI_TSP]	ETSI EN 319 401 v2.0.0 : Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI_TIMESTAMP]	ETSI EN 319 421 v1.1.1 : Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[RFC_3161]	IETF - Internet X.509 Public Key Infrastructure - Time-Stamp Protocol -08/2001
[RFC_5816]	IETF - ESSCertIDv2 Update for RFC 3161 – 03/2010

Tableau 5 : Documents techniques