Politique d'Horodatage
Déclaration des pratiques d'horodatage

V 1.3

OID : 1.3.6.1.4.1.58753.1.1.1.1

Niveau de confidentialité : public

Datasure

Le présent document décrit la politique de l'Autorité d'Horodatage (AH) Datasure. Le présent document contient également la déclaration des pratiques publiques de l'AH. Les pratiques confidentielles sont décrites dans un document annexe, la version confidentielle de la déclaration des pratiques.

L'historique du document est dans le tableau suivant :

Numéro de version	Commentaire
1.0	Version initiale du document
1.1	Modification de la charte graphique du document, de la dénomination sociale (Certisure Certification -> Datasure) et corrections orthographiques mineures
1.2	Correction de la durée d'utilisation de la clé privée
1.3	Mise à jour pour ouverture du service à d'autres abonnés que Datasure.

1 Introduction

Datasure est un Prestataire de Services de Confiance qualifié par l'ANSSI proposant un service d'horodatage électronique qualifié selon le Règlement 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 (dit « eIDAS »).

La présente politique vise à être conforme aux référentiels suivants :

- Référentiels ETSI EN 319 401 et ETSI EN 319 421,
- Référentiels de qualification des services de confiance de l'ANSSI.

Cette conformité permet de viser la reconnaissance du service par l'ANSSI comme service d'horodatage électronique qualifié au sens du Règlement eIDAS.

Le présent document spécifie l'ensemble des engagements pris par l'AH Datasure et spécifie l'ensemble des politiques et pratiques appropriées à la fourniture du service.
Le présent document reprend le plan de la politique d'horodatage type du RGSv2 de l'ANSSI.

1.1 Identification du document

Le présent document est la Politique d'Horodatage / Déclaration des pratiques d'Horodatage (PH/DPH) de l'autorité d'horodatage Datasure.

Elle est identifiée par un numéro d'identifiant unique (OID) : 1.3.6.1.4.1.58753.1.1.1.1

Cette identifiant est composé de la façon suivante :

Racine Datasure	Type de service de confiance	Identifiant du service	Document	Version
1.3.6.1.4.1.58753	1 pour horodatage	1	1 pour PH	1

Cet identifiant est également inclus dans les conditions générales d'Utilisation à destination des utilisateurs (voir §2.6).

1.2 Publication du document

Le présent document est publié sur une page accessible à l'URL suivante :
https://tsa.datasure.net

Le site de publication comporte également :

- Les Conditions Générales d'Utilisation à destination des utilisateurs (voir §2.6) ;
- Les certificats des unités d'horodatage ;
- Les éventuelles certifications de conformité obtenues.

Il est à noter que les informations confidentielles de la DPH ne sont pas publiées.
Le document ne peut être publié qu'après approbation du document par le comité de Direction de Datasure (voir §1.3).
Le document est également communiqué aux employés et à une liste de tiers définie dans la DPH confidentielle.
L'accès en écriture au site de publication est réservé aux personnes habilitées avec une authentification à deux facteurs.

1.3 Gestion de la PH/DPH

L'entité en charge du présent document, de la DPH confidentielle associée et de l'ensemble du corpus documentaire est le comité de Direction de Datasure. Il est responsable de l'approbation, du suivi et des modifications éventuelles de la présente PH/DPH ainsi que des différents documents du corpus documentaire.
La Direction de Datasure a l'entière responsabilité de l'approbation de la PH/DPH et est responsable de la mise en œuvre et du suivi des pratiques.
La nouvelle PH/DPH est publiée sans délai après l'approbation (voir §1.2).

La PH/DPH est revue annuellement et lors de chaque changement majeur. Cette revue de la PH/DPH et des pratiques mises en œuvre est faite sous la responsabilité de la Direction de Datasure.

1.4 Point de contact

Toute demande relative au service est à adresser au point de contact fourni à l'adresse suivante :

Datasure
Autorité d'Horodatage
8 rue Alfred Maurel
34120 PÉZENAS

Datasure peut également être contacté au travers du formulaire de contact disponible sur son site internet : https://www.datasure.net

2 Dispositions générales

2.1 Obligations de l'Autorité d'Horodatage

L'AH vise à respecter l'ensemble des obligations décrites :

- Dans la norme ETSI EN 319 421 ;
- Dans la Politique d'horodatage type du RGSv2 ;
- Dans la procédure de qualification de l'ANSSI applicable aux prestataires de service d'horodatage.

L'AH a les obligations suivantes :

- Générer des jetons d'horodatage conforme à la présente PH/DPH ;
- S'assurer que l'ensemble des acteurs et sous-traitants intervenant dans l'AH respecte la présente PH/DPH, les exigences et dispositions de la DPH confidentielle et les différentes procédures associées ;
- Garantir que l'ensemble des pratiques sont conformes à la présente PH/DPH ;
- Respecter l'ensemble des exigences complémentaires inscrites dans les Conditions générales d'utilisation du service (CGU) ;
- Mettre à disposition des abonnés et utilisateurs l'ensemble des informations nécessaires à la vérification des contremarques de temps.

2.2 Obligations de l'abonné

Un abonné est une personne morale ou personne physique ayant besoin de faire horodater des données par l'Autorité d'horodatage Datasure et qui a accepté les conditions d'utilisation de ce service. L'abonné peut être :

- Une organisation : il comprend plusieurs utilisateurs finaux ou un utilisateur final. Certaines obligations s'appliquant à l'organisation s'appliquent également aux

utilisateurs finaux. L'organisation sera tenue responsable si les obligations ne sont pas correctement respectées par les utilisateurs finaux et, par conséquent, une telle organisation doit informer de manière appropriée ses utilisateurs finaux.

- Un utilisateur final : l'utilisateur final est directement responsable si les obligations ne sont pas correctement respectées.

L'abonné a le devoir d'émettre une requête utilisant un algorithme de hash supporté par l'AH (SHA256, SHA384 ou SHA512).
Il est recommandé que l'abonné, au moment de l'obtention d'un jeton d'horodatage vérifie que le certificat de l'unité d'horodatage n'est pas révoqué.
L'abonné doit respecter ses engagements énoncés dans les CGU et les CGV.

La société Datasure est également un abonné du service au sens strict du terme au travers de ses services Datasure. Le service peut ainsi bénéficier aux clients de Datasure au travers de ses services à valeur ajoutée. L'abonné Datasure doit respecter ses engagements énoncés dans les CGU qui sont *de facto*, un document interne de Datasure, prenant la forme d'une convention de service interne.

2.3 Obligations de l'utilisateur

L'utilisateur du jeton d'horodatage (incluant les utilisateurs finaux, mais aussi les clients ou toute personne souhaitant vérifier la preuve d'antériorité des services Datasure) devra vérifier le jeton en :

- Comparant le haché des données horodatées avec le haché présent dans le jeton d'horodatage ;
- Vérifiant la signature du jeton à l'aide du certificat de l'unité d'horodatage ;
- Vérifiant la validité du certificat d'horodatage. Cette vérification est réalisée en s'appuyant sur la chaîne de certification et la liste de certificats révoqués (LCR) émis par l'autorité de certification.

Ces vérifications peuvent être réalisées de façon automatique par des outils standards du marché tels qu'Acrobat Reader™ ou les bibliothèques Open-Source SD-DSS (fournies par la Commission européenne) et OpenSSL.

2.4 Obligations de l'AC fournissant les certificats des unités d'horodatage

Les certificats des UH sont émis par une AC qualifiée au sens du Règlement eIDAS. Cette AC doit respecter les obligations décrites dans sa propre PC/DPC ainsi que les exigences de la procédure de qualification de l'ANSSI. Cette AC est sélectionnée par Datasure parmi la liste des AC qualifiées par l'ANSSI[1]. Elle doit également être certifiée vis-à-vis de la norme ETSI EN 319411-1.

2.5 Déclaration des pratiques d'horodatage

Le présent document contient la version publique de la déclaration des pratiques d'horodatage. Les pratiques jugées confidentielles sont précisées dans une déclaration des pratiques confidentielles associées au présent document et référant l'ensemble des pratiques et procédures de l'AH. L'AH garantit qu'elle possède la fiabilité nécessaire pour fournir des services d'horodatage. En particulier :

a. L'AH a fait une évaluation de risques pour évaluer les actifs et les menaces pour ces actifs afin de déterminer les contrôles de sécurité nécessaires et les procédures opérationnelles (voir 4.2.6.1) ;
b. L'AH dispose, comme mentionné plus haut, d'une déclaration des pratiques (dont la partie non-confidentielle est incluse dans le présent document) ainsi que des procédures documentées. Cette DPH et ces procédures visent à adresser toutes les exigences de la politique d'horodatage ;
c. La déclaration des pratiques d'horodatage identifie les obligations de toutes les organisations externes participant à la fourniture des services d'horodatage, y compris la politique applicable et les pratiques. Cela inclut l'AC fournissant les certificats aux unités d'horodatage ;
d. L'Autorité d'horodatage met à la disposition des abonnés et utilisateurs de jetons d'horodatage, les éléments publics de sa déclaration des pratiques d'horodatage au travers du présent document et à travers des conditions d'utilisation publiées sur son site (voir 1.2).

[1] Datasure s'offre la possibilité d'opérer sa propre AC racine dédiée à l'horodatage pour le renouvellement futur de ces UH. Cette AC racine sera alors opérée conformément aux exigences de l'ANSSI et de l'ETSI.

e. L’AH dispose d’une organisation adéquate permettant l’approbation de la présente PH/DPH ainsi que de la DPH confidentielle, ainsi que l’approbation de la concordance entre les deux documents ;
f. Le responsable de l’AH garantit que les pratiques sont correctement mises en œuvre ;
g. L’AH définit une procédure de contrôle périodique (audit interne) de la conformité des pratiques, y compris les responsabilités, à la déclaration des pratiques d’horodatage.
h. L’AH informe au préalable les abonnés pour tout changement qu'elle a l'intention de faire dans la partie publique de sa déclaration des pratiques d'horodatage et, après l'approbation comme dans (e) ci-dessus, immédiatement mettre à la disposition des abonnés et des utilisateurs de jeton d’horodatage la partie publique révisée de la déclaration des pratiques d’horodatage comme exigé sous (d) ci-dessus. Aussi, afin de respecter l’esprit de la norme, Datasure notifiera les abonnés des services Datasure qui utilisent l’horodatage. Cela peut prendre la forme d’une notification par email à l’ensemble des abonnés.
i. L’AH ayant été évaluée pour être en conformité avec la présente PH/DPH, si une modification envisagée à l'initiative de l’AH pouvait entraîner une non-conformité avec ladite PH/DPH ou avec la version confidentielle DPH, alors l’AH soumettra cette modification à l'organisme évaluateur indépendant pour avis.

2.6 Conditions générales d’Utilisation

L'AH publie également, en complément de la présente PH, des Conditions Générales d'Utilisation (CGU) à destination des abonnés et utilisateurs de jetons d’horodatage correspondant aux "*TSA Disclosure Statement*" de la norme ETSI 319 401.

Les conditions générales d’utilisation sont publiées sur le site de publication de Datasure (voir §1.2) et contiennent les conditions générales d’abonnement.
Elles sont fournies au format PDF et en Français.

Des conditions générales d’abonnement entre l’AH et la société Datasure sont signées pour acceptation par l’abonné (la Direction de Datasure, responsable du service Datasure) au travers d’une convention de service.
Elles sont fournies au format PDF et en Français.

2.7 Conformité avec les exigences légales

L'AH garantit la conformité avec les exigences légales. En particulier :

- Des mesures techniques appropriées et organisationnelles sont prises pour assurer un niveau adéquat de protection des données à caractère personnel, conformément au RGPD ;
- Les informations fournies au service Datasure ne sont pas divulguées, sauf dans le cas :
    - D'un accord express du propriétaire des données ;
    - D'une décision judiciaire ;
    - D'une exigence légale.
- Les pratiques de l'AH sont non-discriminatoires. Chaque fois que cela est possible, Datasure met en œuvre tous les moyens nécessaires pour rendre accessible son service aux personnes en situation de handicap. En particulier, les recommandations sur l'accessibilité sont prises en compte.

3 Exigences opérationnelles

3.1 Gestion des requêtes de contremarques de temps

L'AH Datasure fournit un jeton d'horodatage à la requête de l'abonné, contenant les données à horodater. La fourniture d'une contremarque de temps est quasi immédiate et se fait de façon synchrone.
La contremarque de temps générée est conservée par l'AH.

3.2 Fichier d'audit

Afin d'assurer la traçabilité de son service, l'AH Datasure enregistre et conserve des traces dans des fichiers d'audit.

En particulier, sont conservées :

- L'ensemble des traces des demandes reçues par le service et des réponses retournées ;
- L'ensemble des traces pertinentes relatives à l'administration du service d'horodatage ;

- L’ensemble des traces pertinentes relatives au fonctionnement du service d’horodatage ;
- L’ensemble des traces pertinentes concernant les événements liés au cycle de vie des clés d’UH et au cycle de vie des certificats associés ;
- L’ensemble des traces pertinentes concernant la synchronisation des horloges et serveurs de temps utilisés par l’UH, y compris la perte de synchronisation ou le recalibrage/la resynchronisation des horloges.

Des mesures de sécurité (au niveau physique, réseau et système) sont mises en place afin d’assurer l’intégrité, la disponibilité et la confidentialité des traces. Il doit être particulièrement difficile, voire impossible, d’altérer ou détruire les traces d’événements. La DPH confidentielle décrit les moyens mis en œuvre.
La durée de conservation des journaux du service est conservée pendant une période minimale de 7 ans, conformément aux exigences de l’ANSSI. Cette durée de 7 ans est applicable même après arrêt d’activité de l’AH.
Tous les événements sont datés. Les horloges utilisées pour dater les événements doivent être synchronisées avec UTC au moins une fois par jour.

3.3 Gestion de la durée de vie de la clé privée

L’AH Datasure garantit que la clé privée ne sera pas utilisée au-delà de la date de validité du certificat. Cela est obtenu par la mise en place de mesures techniques et organisationnelles. En particulier :

- La clé privée d’UH est renouvelée par anticipation avant la fin de la période d’utilisation de la clé précédente ;
- La clé privée d’UH est détruite en fin de période d’utilisation (voir 5.6 et 5.10).

3.4 Synchronisation de l'horloge

Conformément aux exigences eIDAS, l’AH Datasure garantit une synchronisation de ces horloges horodatage avec UTC avec la précision définie en §5.1. Cette précision est obtenue par la mise en œuvre de serveurs de temps synchronisés. Ces derniers sont synchronisés sur *a minima* une source de temps référencée UTC(k).
Le mécanisme de synchronisation est confidentiel et fait partie du corpus documentaire de l’AH. Ce mécanisme garantit les points suivants :

- Le calibrage de chaque horloge d'unité d'horodatage est maintenu de telle manière que les horloges ne puissent pas normalement dériver à l'extérieur de l'exactitude déclarée ;
- Les horloges des unités d'horodatage doivent être protégées contre les menaces relatives à leur environnement qui pourraient aboutir à une désynchronisation avec le temps UTC en dehors de l'exactitude déclarée[2] ;
- L'Autorité d'horodatage garantit que, si son horloge interne ne respecte plus l'exactitude déclarée, alors l'anomalie est automatiquement détectée[3] ;
- Si l'horloge d'une unité d'horodatage est détectée comme étant en dehors de l'exactitude annoncée, les contremarques de temps ne sont plus générées ;
- L'Autorité d'horodatage garantit que la synchronisation de l'horloge est maintenue lorsqu'un saut de seconde est programmé. Le changement tient compte du fait que le saut de seconde est effectué durant la dernière minute du jour où le saut de seconde est programmé. Un enregistrement du temps exact (selon l'exactitude déclarée) de l'instant de ce changement est effectué.

3.5 Exigences du contenu d'une contremarque de temps

L'AH garantit que les jetons d'horodatage sont générés en toute sécurité et incluent le temps correct. Le jeton d'horodatage inclut également le certificat d'unité d'horodatage. Ce certificat indique les informations suivantes :

L'identifiant du pays dans lequel l'Autorité d'horodatage est établie	Cette information est fournie dans le champ C du certificat.
L'identifiant de l'Autorité d'horodatage	Cette information est fournie par les champs O et OI du certificat.
L'identification de l'unité d'horodatage	Cette information est fournie par le champ CN du certificat.

Le jeton d'horodatage contient également l'OID de la présente PH/DPH (voir 1.1).
Chacun des jetons d'horodatage contient :

- Un identifiant unique ;

[2] Les menaces identifiées sont décrites dans l'analyse de risques. Les menaces étudiées prennent en compte : les modifications par du personnel non autorisé, les ondes radio et les chocs électriques.

[3] En cas de désynchronisation entraînant la production d'horodatages erronés, l'information sur de tels événements est publiée à destination des utilisateurs sur le site de publication (voir §1.2).

- La date inscrite dans le jeton d'horodatage est reliée à un temps fourni par un laboratoire UTC(k) grâce au mécanisme de synchronisation décrit en §3.4. Le temps est synchronisé avec UTC avec la précision décrite en §3.4 ;
- La valeur de hachage et l'identifiant d'algorithme de hachage ;
- La signature produite par la clé privée de l'unité d'horodatage (voir §3.1).

Les jetons sont conformes aux exigences du chapitre §6.

3.6 Compromission de l'AH

L'Autorité d'horodatage garantit, dans le cas d'événements qui affectent la sécurité des services d'horodatage (incluant la compromission de la clé privée de signature d'une unité d'horodatage ou la perte détectée de calibrage qui pourrait affecter des jetons d'horodatage émis) qu'une information appropriée est mise à la disposition des abonnés et utilisateurs de contremarques de temps. Cette notification se fera au travers d'une publication (voir §1.2). Concernant les utilisateurs de jetons d'horodatage de l'abonné Datasure, , la notion de notification sera non applicable. Cependant, dans le respect de l'esprit de la norme, le service Datasure identifiera les clients impactés et les notifiera.

Les dispositions suivantes sont prises en compte en cas de compromission :

- Le plan de secours (PCA/PRA) de l'Autorité d'horodatage traite le cas de la compromission réelle ou suspectée de la clé privée de signature d'une unité d'horodatage ou la perte de calibrage de l'horloge d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises.
- Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises, l'Autorité d'horodatage met à la disposition de tous les utilisateurs de contremarques de temps une description de la compromission qui est survenue. Cette notification se fait via une publication sur le site référencé en §1.2 ;
- Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises, l'Autorité d'horodatage prendra les mesures nécessaires pour que les contremarques de temps de cette unité ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation. Ces dispositions prennent la forme d'une suspension de l'activité de l'unité d'horodatage et en cas de compromission avérée, de son décommissionnement.

- En cas d'un événement majeur dans le fonctionnement de l'Autorité d'horodatage ou d'une perte de calibrage, qui pourrait affecter des contremarques de temps émises, chaque fois que cela sera possible, l'Autorité d'horodatage mettra à la disposition des utilisateurs de contremarques de temps toute information pouvant être utilisée pour identifier les contremarques de temps qui pourraient avoir été affectées, à moins que cela ne contrevienne à la vie privée des abonnés ou à la sécurité du Service d'horodatage.
- L'AH préviendra directement et sans délai l'ANSSI (voir §4.2.3).

3.7 Fin d'activité de l'AH

En cas de cessation d'activité de son AH, Datasure doit s'assurer que l'impact sur les utilisateurs soit réduit au maximum et doit assurer la maintenance continue des informations nécessaires pour vérifier la justesse des contremarques de temps.
À ce titre, Datasure a mis en œuvre un plan d'arrêt d'activité (PAA) adressant l'ensemble des actions à exécuter :

- L'AH Datasure notifiera l'ANSSI de son plan d'arrêt d'activité ;
- L'AH Datasure rendra disponible sur son site internet (voir §1.2) l'information concernant son arrêt d'activité ;
- L'Autorité d'horodatage abrogera les autorisations données aux sous-traitants d'agir pour son compte dans l'exécution de n'importe quelles fonctions touchant au processus de génération des jetons d'horodatage ;
- Le Groupe Certisure maintiendra les obligations de maintien des fichiers d'audit et des archives nécessaires pour démontrer son fonctionnement correct durant une période raisonnable. En cas d'arrêt total de l'activité, Datasure transférera à un organisme fiable ses éléments pour la même durée de conservation cible ;
- Le Groupe Certisure maintiendra ou transférera à un organisme fiable ses obligations de rendre disponible aux utilisateurs de contremarques de temps pendant une période raisonnable ses clés publiques ainsi que ses certificats ;
- L'AH Datasure détruira de façon définitive les clés privées de telle façon que celles-ci ne puissent être recouvrées ;
- L'ensemble des certificats d'unité d'horodatage seront révoqués.

Le plan d'arrêt d'activité est tenu à jour. Il est revu annuellement et lors de tout changement majeur.

En cas d'arrêt d'activité de son AH, le service Datasure utiliserait d'autres services d'horodatages qualifiés en lieu et place de ses propres unités d'horodatage, afin d'assurer la continuité du service Datasure.

Datasure prend les mesures nécessaires pour couvrir les dépenses pour accomplir ses exigences minimales dans le cas où l'Autorité d'horodatage tomberait en faillite ou pour d'autres raisons où Datasure serait incapable de couvrir les dépenses par lui-même.

4 Exigences physiques et environnementales, procédurales et organisationnelles

4.1 Exigences physiques et environnementales

L'Autorité d'horodatage doit garantir que l'accès physique aux services critiques est contrôlé et que les risques physiques d'atteinte à ses actifs sont réduits au minimum. En particulier :

- L'accès physique aux équipements concernés par les services d'horodatage est limité aux individus autorisés ;
- Des contrôles sont mis en œuvre pour éviter la perte, des dégâts ou la compromission d'actifs et l'interruption des activités et ;
- Des contrôles sont mis en œuvre pour éviter la compromission ou le vol d'informations ou d'équipements informatiques.

Les composants critiques pour l'opération sécurisée du service de confiance sont localisés dans un environnement de sécurité muni d'une protection physique contre les intrusions et de mécanismes d'alarme.

Des contrôles d'accès sont appliqués aux modules d'horodatage pour remplir les exigences de sécurité des modules d'horodatage. Les contraintes sur l'environnement d'exploitation, identifiées dans la documentation liée à la certification du module (Profil de Protection, cible de sécurité), sont remplies.

Les contrôles suivants complémentaires sont appliqués à la gestion du service d'horodatage :

- Le système d'horodatage fonctionne dans un environnement qui protège physiquement les services de la compromission. Des moyens sont mis en œuvre pour se protéger d'un accès non autorisé aux systèmes ou aux données ;
- La protection physique est réalisée par la création d'un périmètre de sécurité dédié clairement défini (c'est-à-dire des barrières physiques) autour des unités d'horodatage ; tout environnement partagé avec d'autres organisations est exclu de ce périmètre.
- Le service d'horodatage doit également être séparé logiquement des autres services afin d'être protégé des compromissions et des accès non autorisés.

Toute entrée dans la zone de sécurité physique est soumise à des moyens de surveillance. Cette surveillance est réalisée en toute indépendance. Toute personne non autorisée est obligatoirement accompagnée par une personne autorisée dans la zone sécurisée. Toutes entrées et sorties sont tracées.

Des contrôles de sécurité physique et environnementale sont mis en œuvre pour protéger l'environnement qui abrite les ressources du système, les ressources du système elles-mêmes et les équipements utilisés pour remplir leur fonction ; la politique de sécurité physique et environnementale de l'Autorité d'horodatage pour les systèmes concernés par la gestion de l'horodatage concerne au minimum le contrôle d'accès physique, la protection vis-à-vis des catastrophes naturelles, les facteurs de sécurité liés au feu, la défaillance des services de base (par exemple le secteur, les télécommunications), l'écroulement de la structure, des fuites de plomberie, la protection contre le vol, la casse et la pénétration et, le rétablissement de la sécurité après un désastre.

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

4.2 Exigences procédurales

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

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

- Un rapport d'incident et des procédures de réponse aux incidents doivent être 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 ;
- Des procédures sont établies et mises en œuvre pour tous les rôles de confiance et administratifs qui impactent la fourniture des services d'horodatage.

4.2.1 Manipulation et sécurité des supports

L'AH assure un niveau approprié de protection des biens et des supports de ces biens, y compris les biens dématérialisés.

4.2.1.1 Considérations générales

Tous les supports sont traités de manière sécurisée conformément aux exigences de la classification de l'information. Les supports contenant des données sensibles doivent être retirés de manière sécurisée quand ils ne sont plus utiles.
En particulier, l'AH s'assure en particulier que les données sensibles sont protégées en cas de réutilisation d'enregistrement (par exemple, des fichiers effacés) ou de supports pouvant être accessibles à des utilisateurs non autorisés.

Les supports sont manipulés de façon sécurisée afin de les protéger contre les dommages, le vol, l'accès non autorisé et l'obsolescence.
Des procédures sont mises en place contre l'obsolescence et la détérioration des supports pendant la période de temps requise pour leur utilisation.

4.2.1.2 Considérations spécifiques relatives aux systèmes fiables

L'AH utilise des systèmes fiables pour stocker les données qui lui sont fournies, sous une forme vérifiable de manière que :

- Les données ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée par ces données ;
- Seules des personnes autorisées peuvent introduire et modifier les données conservées ;
- L'authenticité de ces données peut être vérifiée

4.2.1.3 Considérations spécifiques relatives au HSM

L'AH met en place des mesures spécifiques relatives au HSM afin de garantir que :

- Le HSM n'a pas été modifié ou altéré durant son transport ;
- Le HSM n'a pas été modifié ou altéré durant son stockage ;
- L'installation, l'activation, la copie des clés privée des unités d'horodatage, dans le HSM, ne peuvent être réalisées que par des personnels en rôle de confiance, sous contrôle double (dual control) et au sein d'un environnement sécurisé ;
- Les clés sont effacées avant la mise au rebut du matériel de façon qu'il soit quasiment impossible de permettre leur récupération.

4.2.2 Planification de Système

Les charges des différents composants sont contrôlées et des projections de charge dans le futur sont effectuées pour garantir que des puissances de traitement et des stockages adéquats seront disponibles.

4.2.3 Rapport d'incident et réponse

L'ensemble des systèmes font l'objet d'une surveillance (monitoring), en particulier des accès et de l'utilisation/charge des systèmes (voir section précédente). Ces activités de surveillance prennent en compte la sensibilité des données manipulées.
Les événements suivants sont surveillés *a minima* :

- Les démarrages et arrêts des fonctions de création de traces des systèmes ;
- La disponibilité et le niveau d'utilisation des services.

L'Autorité d'horodatage agit d'une façon opportune et coordonnée pour répondre rapidement aux incidents et limiter l'impact des infractions à la sécurité. Tous les incidents doivent être rapportés aussitôt que possible après l'incident en suivant les procédures définies. La gestion des incidents est réalisée par des personnes en rôle de confiance.

En particulier, en cas d'incident de sécurité grave (atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les

données à caractère personnel qui y sont conservées), l'ANSSI sera notifiée de l'incident en suivant la procédure de notification d'incident dédiée, et au plus tard dans les 24 heures après la découverte de l'incident.

Cette notification est réalisée au moyen du formulaire mis en ligne sur le site de l'ANSSI. Les abonnés, utilisateurs et/ou clients du service Datasure impactés seront également notifiés.
En cas d'incident majeur concernant les données personnelles, les personnes physiques impactées seront notifiées chaque fois que cela est possible. La CNIL sera informée dans les 72 heures.

La surveillance des systèmes inclut une revue des traces du système. L'objectif de cette revue est de découvrir des comportements malicieux. Ces revues s'appuient sur des mécanismes automatiques et permettent d'alerter de potentielles failles de sécurité ou d'événements critiques.

Toutes vulnérabilités critiques sont adressées dans une période de 48h après leur découverte. Pour toute vulnérabilité, l'AH doit :

- Créer et mettre en œuvre un plan de mitigation de la vulnérabilité ;
- Documenter sur une base factuelle le choix de ne pas traiter une vulnérabilité.

La réponse à incident doit être mise en œuvre de façon à minimiser les impacts des incidents et dysfonctionnements.

4.2.4 Procédures de fonctionnement et responsabilités

Les opérations de sécurité doivent être séparées des autres opérations. Les opérations de sécurité 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.

4.2.5 Gestion d'Accès au Système

L’AH applique l’ensemble des règles définies dans le guide d’hygiène informatique publié par l’ANSSI, pour le niveau « standard ». Les règles de niveau renforcées sont mises en œuvre chaque fois que cela est possible. La PSSI rappelle l’ensemble de ces règles.

4.2.5.1 Réseau

L’AH protège ses systèmes et réseaux des attaques.
Pour se faire, l’AH a segmenté ses systèmes en réseaux et zones séparées en se basant sur l’analyse de risque. La séparation prend en compte la séparation des systèmes sur les plans à la fois fonctionnels, logiques et physiques.
L’AH applique des niveaux de sécurité et de contrôle similaire pour tous les systèmes localisés au sein d’une même zone.
Les accès et communications entre chaque zone sont contrôlés et limités. Elles sont réduites au minimum nécessaire à l’opération du service.
Ces contrôles - en particulier des pare-feu (firewalls) - sont mis en œuvre pour protéger le réseau interne de l'Autorité d'horodatage des accès non autorisés. Les accès non-autorisés incluent l'accès par des abonnés mais également des tierces personnes au réseau interne.
Les pare-feu (firewalls) sont configurés pour bloquer tous les protocoles et les accès non nécessaires au fonctionnement de l'Autorité d'horodatage.
Les règles réseau font l’objet de revues régulières. La revue est réalisée *a minima* de façon annuelle.

Tous les systèmes critiques sont regroupés au sein des zones les plus sécurisées. Les réseaux opérationnels et les réseaux d’administration sont séparés. Les services d’administration sont dédiés à cet effet et ne peuvent être utilisés pour d’autres besoins.
L’AH s’assure que toute communication entre deux composants de sécurité est obligatoirement établie au travers d’un canal sécurisé. Ce canal est isolé des autres canaux. Cette séparation peut être obtenue par des moyens physiques, logiques ou cryptographiques. Le canal sécurisé permet l’identification de l’origine et du destinataire, ainsi que la protection en intégrité et confidentialité du contenu échangé.

L’AH réalise de façon régulière des scans de vulnérabilité. La régularité cible est trimestrielle. Les éléments de preuve relatifs à la qualité, l’éthique, l’expertise et l’indépendance des personnes réalisant les scans sont conservés afin de démontrer la pertinence des rapports.

L’AH réalise des tests de pénétration avant la mise en place de l’infrastructure technique et après chaque mise à jour significative de l’infrastructure. Ces tests de pénétration doivent être réalisés annuellement.
De même que pour les scans, les éléments de preuve relatifs à la qualité, l’éthique, l’expertise et l’indépendance des personnes réalisant les tests sont conservées afin de démontrer la pertinence des rapports.

4.2.5.2 Gestion des comptes

L'Autorité d'horodatage garantit une administration efficace des utilisateurs (cela inclut les opérateurs, les administrateurs et les 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. Le principe du moindre privilège est appliqué lors de la configuration des accès.

4.2.5.3 Contrôle d’accès

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 système utilitaires sera limitée et très contrôlée.

4.2.5.4 Identification et authentification du personnel

Le personnel de l'Autorité d'horodatage est correctement identifié et authentifié avant d'utiliser des applications critiques liées à l'horodatage.

4.2.5.5 Responsabilité des personnels

Le personnel de l'Autorité d'horodatage sera tenu responsable de ses activités. Une traçabilité des actions est mise en œuvre.

4.2.5.6 Gestion de l'horodatage

L'Autorité d'horodatage garantit que des composants de réseaux locaux (par exemple les routeurs) sont placés dans un environnement physiquement sûr et que leurs configurations sont périodiquement vérifiées pour la conformité avec les exigences indiquées par l'Autorité d'horodatage.

4.2.5.7 Surveillance

Une surveillance permanente et des équipements d'alarme est mise en œuvre pour permettre à l'Autorité d'horodatage de détecter, d'enregistrer et de réagir rapidement à n'importe quelle tentative non autorisée et/ou irrégulière d'accès à ses ressources.

4.2.6 Déploiement et Maintenance

L'Autorité d'horodatage emploie des produits et systèmes de confiance.

4.2.6.1 Analyse de risque

Une analyse des exigences de sécurité est effectuée au moment de la conception et de l'étape de spécification 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.

L'AH réalise cette analyse de risque afin d'identifier, analyser et évaluer les risques. Les risques techniques, mais également les risques métiers sont pris en compte.
L'AH sélectionne des mesures appropriées de traitement du risque, en s'appuyant sur les résultats de l'analyse de risque. Les mesures de traitement du risque permettent de s'assurer que le niveau de sécurisation est approprié vis-à-vis du niveau de risque.
L'AH détermine l'ensemble des exigences de sécurité et les procédures opérationnelles qui sont nécessaires à la mise en œuvre des mesures retenues. Ces éléments sont documentés dans la PSSI, ainsi que dans la présente PH/DPH, ainsi que dans la version confidentielle de la DPH.

L'analyse de risque est revue et mise à jour de façon régulière. Celle-ci est revue *a minima* annuellement et lors de tout changement majeur (voir § 4.2.6.3), notamment en cas de modification des politiques ou pratiques relatives à la fourniture du service d'horodatage.
L'analyse de risque fait l'objet d'une approbation formelle par le comité de Direction de Datasure qui accepte, au travers de cette approbation, le risque résiduel identifié.
En outre, l'analyse de risque fait l'objet d'une procédure d'homologation. Cette procédure d'homologation est réalisée préalablement à la fourniture du service de confiance qualifié puis révisée au moins tous les deux ans.

4.2.6.2 Politique de sécurité du système d'information

Datasure a défini une politique de sécurité du système d'information (PSSI). La PSSI est approuvée formellement par le comité de Direction de Datasure. La PSSI définit l'approche générale de l'organisation pour sa gestion de la sécurité de l'information.
Tout changement de la PSSI sera notifié aux tiers impactés, si cela s'avère nécessaire. Ces tiers peuvent inclure des abonnés, les utilisateurs, l'organisme d'évaluation ou l'organe de contrôle.

La PSSI est documentée, mise en œuvre et tenue à jour. Pour cela, des mesures de contrôle de sécurité et des procédures opérationnelles sont mises en place. Ces mesures couvrent les sites, les systèmes d'information et les biens impliqués dans la délivrance du service d'horodatage.
La PSSI est communiquée à l'ensemble des employés entrant dans son périmètre.
L'AH Datasure a l'entière responsabilité de la conformité de ses procédures à la PSSI, même dans le cas où de la sous-traitance est mise en œuvre.
En cas de sous-traitance, les responsabilités de chacun sont définies contractuellement. En particulier, le sous-traitant est tenu de mettre en œuvre l'ensemble des règles de sécurité qui lui sont applicables.
Lorsque l'AH a recours à un sous-traitant, elle s'assure que l'interface avec le sous-traitant est sécurisée et qu'elle est utilisée en conformité avec les recommandations du sous-traitant.

La PSSI est revue régulièrement, *a minima* de façon annuelle et à chaque changement majeur dans le système d'information. Cela afin d'assurer la continuité de son application, de sa cohérence et de son efficacité, même en cas de changement significatif.

Tout changement ayant un impact sur le niveau de sécurité doit obligatoirement être validé par le comité de Direction de Datasure.

Les configurations des systèmes mis en œuvre par l'AH Datasure doit régulièrement faire l'objet de vérification afin de s'assurer qu'ils sont en ligne avec la politique de sécurité. L'intervalle maximum entre deux vérifications est documenté dans la version confidentielle de la DPH.

4.2.6.3 Gestion des changements

Des procédures de contrôle de changement doivent être appliquées pour les nouvelles versions, les modifications et les corrections d'anomalies de n'importe quel logiciel opérationnel.
En cas d'intentions de changements dans la présente PH/DPH qui impacterait l'usage du service, le changement sera préalablement notifié :

- Auprès des abonnés et utilisateurs de jetons d'horodatage par une publication sur le site (voir §1.2) ;
- Auprès des clients de Datasure par un message électronique envoyée à leur adresse de contact.

Les changements apportés sont documentés.

En cas de modification importante dans la fourniture de son service de confiance, l'AH Datasure informe l'ANSSI selon les modalités convenues.

Ces modifications importantes comprennent notamment, sans s'y limiter :

- Les changements induits par une modification de la politique de service ou des conditions générales d'utilisation associées ;
- Les changements de sous-traitants ;
- Les modifications des conditions d'hébergement ;
- Les changements de matériels cryptographiques ;
- Les modifications d'architecture technique ;
- Les changements de procédures d'enregistrement et d'identification ;
- Les changements dans la gouvernance de l'AH.

Les modifications entraînant des changements dans la liste de confiance publiée par l'ANSSI sont notifiées dans les meilleurs délais.

L’AH adresse à l’ANSSI une synthèse de l’ensemble des modifications apportées à la fourniture de son service, impactant les constats présentés dans le rapport d’évaluation de la conformité, à une fréquence annuelle.

4.2.6.4 Gestion des vulnérabilités

L’AH définit et applique des procédures permettant d’assurer :

- Que les mises à jour de sécurité sont appliquées dans un temps raisonnable après leur mise à disposition ;
- Que les mises à jour de sécurité ne sont appliquées que si elles n’introduisent pas de nouvelles vulnérabilités additionnelles ou des instabilités qui ne seraient pas contrebalancées par les bénéfices de la mise en œuvre.

Les raisons de ne pas appliquer une mise à jour de sécurité doivent être documentées.

4.3 Exigences organisationnelles

L'Autorité d'horodatage garantit que le personnel (interne ou contractuel) et les pratiques d'embauche améliorent et concourt à la fiabilité des opérations de l'Autorité d'horodatage.

4.3.1 Expertise

L'Autorité d'horodatage emploie un personnel qui possède l'expertise, la formation, l'expérience et les qualifications nécessaires pour les services offerts, tels que l'exige la fonction. En particulier, le personnel a réalisé des formations sur la sécurité informatique et la protection des données à caractère personnel avec la spécificité d’un service d’horodatage et les fonctions occupées au sein de ce service.
Le personnel est en nombre suffisant pour assurer le volume de travail nécessaire pour la fourniture du service.
L’expertise des employés est acquise au travers de l’expérience, de formations spécifiques ou d’une combinaison des deux. La formation continue des employés inclut une mise à niveau, a minima annuelle, de la connaissance des nouvelles menaces et pratiques de sécurité.

Le personnel de gestion employé doit posséder :

- 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.

Le personnel d'encadrement possède également, au travers de son expérience ou d'une formation relative au service d'horodatage, une familiarité avec les procédures de sécurité applicable à son personnel. Il doit également être familier des notions relatives aux responsabilités en matière de sécurité et disposer d'une expérience en sécurité de l'information et en analyse de risque suffisante pour être en mesure d'assurer la fonction d'encadrement.

4.3.2 Rôle et responsabilité

Les rôles de sécurité et les responsabilités, comme spécifiées dans la politique de sécurité de l'Autorité d'horodatage, sont documentés dans des descriptions de poste. Les rôles de confiance, sur lesquels la sécurité du fonctionnement de l'Autorité d'horodatage repose, sont clairement identifiés au travers de fiches de poste mises à disposition des personnels.
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 modules d'horodatage de l'Autorité d'horodatage pour la gestion de l'horodatage;
- Les opérateurs système : responsables pour faire fonctionner les modules d'horodatage de l'Autorité d'horodatage de manière quotidienne. 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 modules d'horodatage.

Le personnel de l'Autorité d'horodatage doit être formellement nommé aux rôles de confiance par la direction responsable de la sécurité. La personne nommée en rôle de confiance accepte également formellement son rôle et ses responsabilités.

L'AH met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté de ses personnels.

L'Autorité d'horodatage ne nomme pas 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.
Le contrôle inclut une vérification de l'extrait de casier judiciaire (bulletin n°3).
Datasure peut décider en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions de la personne, de lui retirer ces attributions. Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans)
Des sanctions disciplinaires sont prévues en cas de non-respect des consignes énoncées dans la DPH ou dans la PSSI.

4.3.3 Séparation des rôles

Des descriptions de fonctions sont définies pour le personnel de l'Autorité d'horodatage (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.
À ce titre, les rôles pouvant présenter des conflits d'intérêts ainsi que les aires de responsabilité doivent faire l'objet, chaque fois que cela est possible, d'une séparation des rôles pour réduire les opportunités d'atteinte, volontaire ou non, à l'intégrité du SI ou d'une mauvaise utilisation des biens.

Les fiches de poste doivent indiquer le type d'enquête à effectuer sur le passé, le type de formation appropriée et les particularités de la fonction. Quand cela est nécessaire, ces descriptions de fonctions doivent faire la différence entre les fonctions générales et les fonctions spécifiques à l'Autorité d'horodatage. Ces descriptions de fonctions doivent inclure des exigences d'expérience et de compétences.

4.3.4 Conflit d'intérêts

Tout le personnel de l'Autorité d'horodatage dans des rôles de confiance doit être libre de conflits d'intérêt qui pourrait porter préjudice à l'impartialité des opérations de l'Autorité d'horodatage.

4.3.5 Suivi des procédures

Afin d'assurer le suivi des procédures, Datasure a mis en place un Système de Management de la sécurité de l'information et de la qualité en s'inspirant des pratiques de l'ISO 27001 et de l'ISO 9001.
Le personnel doit effectuer des procédures administratives et de gestion ainsi que des processus en accord avec les procédures de gestion de sécurité de l'information de l'Autorité d'horodatage.

5 Exigences de sécurité techniques

La présente section contient les exigences de sécurité techniques, en particulier relatives à l'exactitude du temps et à la cryptographie. En particulier, des mesures de contrôles appropriées sont mises en place pour toutes clés cryptographiques ou tout dispositif cryptographique tout a long de leur cycle de vie.

5.1 Exactitude temps

Les unités d'horodatage fournissent une exactitude de l'ordre de la seconde.

5.2 Génération de clé

L'Autorité d'horodatage doit garantir que toutes les clés cryptographiques sont produites dans des circonstances contrôlées. Cette génération est réalisée par des personnes en rôle de confiance, et sous contrôle double (dual control), c'est-à-dire que deux personnes en rôle de confiance sont requises pour toute opération de création de clés.
Le personnel autorisé à réaliser cette opération doit être limité à celle requise pour cette opération. La DPH confidentielle précise les moyens mis en place pour limiter cette capacité.

En particulier, la génération des clés de signature des unités d'horodatage est effectuée dans un module cryptographique (HSM)

- Certifié a minima au niveau EAL4 des critères communs ;
- Répondant aux exigences de qualification de l'ANSSI.

Les algorithmes utilisés sont définis en §5.7.

Les clés cryptographiques ne sont pas importées dans différents modules cryptographiques, sauf à des fins éventuelles de sauvegarde. En tout état de cause, une clé privée ne pourra être associée qu'à un et un seul certificat (voir §5.3). Seule une clé cryptographique peut être active à un instant t.

5.3 Certification des clés de l'unité d'horodatage

Les clés publiques de vérification des unités d'horodatage sont mises à disposition des utilisateurs au travers d'un certificat d'unité d'horodatage rendu public sur le site de publication (voir §1.2).

Pour l'émission des certificats, l'AH fait appel à une AC qualifiée au sens du Règlement eIDAS (§2.4).

L'Autorité d'Horodatage doit s'assurer que la valeur de la clé publique et l'identifiant de l'algorithme de signature contenus dans la demande de certificat de l'Unité d'Horodatage sont égaux à ceux générés par l'Unité d'Horodatage.

L'Autorité d'Horodatage s'assure qu'une demande de certificat d'Unité d'Horodatage auprès d'une Autorité de Certification contient les informations exigées pour un certificat de type cachet et vérifie en particulier :

- La valeur de la clé publique (et l'identifiant de l'algorithme) ;
- La durée d'utilisation souhaitée pour la clé privée.

L'Autorité d'Horodatage vérifie, lors de l'import du certificat de l'Unité d'Horodatage, qu'il provient bien de l'Autorité de Certification auprès de laquelle la demande de certificat a été effectuée. L'AH vérifie également que le certificat a été signé correctement. Cette vérification inclut la vérification de la chaîne complète de certificat jusqu'à l'autorité racine.
L'Autorité d'Horodatage s'assure que l'Unité d'Horodatage ne peut être opérationnelle qu'une fois ces exigences remplies.

5.4 Protection des clés privées des unités d'horodatage

L'Autorité d'horodatage garantit que des clés privées des unités d'horodatage restent confidentielles et conservent leur intégrité. En particulier, les clés de signature des unités d'horodatage sont gardées et utilisées à l'intérieur d'un HSM aux caractéristiques définies en §5.2.

5.5 Exigences de sauvegarde des clés des unités d'horodatage

Les clés privées des unités d'horodatage peuvent faire l'objet de copies de secours, soit dans un module d'horodatage qualifié au niveau renforcé par l'ANSSI, soit hors d'un module d'horodatage, mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du module d'horodatage et, notamment, s'appuyer sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. L'évaluation de la robustesse cryptographique et le choix de l'algorithme s'appuient sur les normes référencées en §5.7.
Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module d'horodatage de telle manière que les clés privées des unités d'horodatage ne soient à aucun moment en clair en dehors du module d'horodatage.

5.6 Destruction des clés des unités d'horodatage

L'Autorité d'horodatage garantit que les clés de signature des unités d'horodatage sont détruites à la fin de leur cycle de vie.

5.7 Algorithmes obligatoires

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

- Supporte des valeurs de hachage générées par des clients et employant les algorithmes de hachage conformes aux exigences de l'ANSSI et des spécifications techniques de l'ETSI. L'AH supporte les algorithmes suivants : SHA256, SHA384, SHA512.
- Génère des contremarques de temps signées selon les algorithmes et les longueurs de clé conformes aux exigences de l'ANSSI et des spécifications techniques de l'ETSI. Les bi- clés des UH ont les caractéristiques suivantes : Algorithme de signature RSA 2048 bits / Algorithme de hachage SHA-256 (256 bits).

Datasure pourra choisir dans les futures versions de sa PH/DPH d'utiliser des algorithmes plus robustes (SHA512 et RSA 4096).

Les choix des algorithmes s'appuient sur les référentiels suivants :

- Norme SOGIS et les recommandations de l'ANSSI.
- ETSI TS 119 312

En cas de conflit, la recommandation de l'ANSSI aura la préférence.

5.8 Vérification des contremarques de temps

L'Autorité d'horodatage doit garantir que les utilisateurs de contremarques de temps ont accès à l'information utilisable pour vérifier la signature numérique des contremarques de temps. En particulier les certificats des unités d'horodatage sont joints à la contremarque de temps, ils sont également publiés sur le site de Datasure (voir §1.2).

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

La durée de validité des certificats des unités d'horodatage ne doit pas être plus longue que :

- La durée de vie cryptographique de la clé privée associée ;
- La fin de validité du certificat d'AC qui l'a émis.

Datasure se fournit auprès d'une AC qualifiée au sens du Règlement eIDAS (voir §2.4), qui, *de facto*, respecte ces exigences en tant qu'AC qualifiée.

5.10 Durée d'utilisation des clés privées des UH

La durée d'utilisation d'une clé privée sera au plus égale à la période de validité du certificat de clé publique correspondant. Toutefois elle sera en pratique réduite afin que la validité des contremarques de temps générées avec cette clé puisse être effectuée durant un laps de temps suffisant. En tout état de cause, la durée d'utilisation de la clé privée ne pourra dépasser 3 ans. Dans la pratique, elle sera renouvelée de façon anticipée afin de garantir un recouvrement entre nouvelles et anciennes UH.

Les clés privées ne peuvent être utilisées au-delà de leur période de validité. En particulier,

- Des mesures techniques et opérationnelles sont mises en œuvre de façon à mettre en place une nouvelle clé avant que la clé courante n'expire ;
- Les clés privées sont alors détruites, ainsi que toutes les copies de sauvegardes, afin que la clé ne puisse être restaurée.

6 Exigences sur les formats des contremarques de temps, des certificats et des LCR et sur les algorithmes cryptographiques

6.1 Contremarque de temps

Les jetons d'horodatage ou contremarques de temps fournis par l'AH Datasure sont conformes à la norme RFC 3161 et la norme ETSI EN 319422.
Ils sont délivrés de façon sécurisée et contiennent une date correcte.
En particulier, la date et l'heure du jeton sont traçables jusqu'à un laboratoire UTC(k) (voir §3.4). La date et l'heure sont synchronisées avec la précision donnée en §5.1.

6.2 Certificats et LCR

Les gabarits des certificats d'UH sont conformes à la PC de l'AC émettrice (voir §7 de la PC Certigna). http://politique.certigna.fr/PCcertignaentityca.pdf
L'OID du profil est 1.2.250.1.177.2.6.1.9.1
Les LCR sont conformes à la PC de l'AC émettrice.