Politique d'horodatage

Politique d'horodatage conforme RGS et ETSI et non certifiée

POLITIQUE D'HORODATAGE CONFORME RGS ET ETSI ET NON CERTIFIE

Version du document :	1.5	**Nombre total de pages :**	35
Statut du document :	☐ Projet	☒ Version finale	
Rédacteur du document :	Emmanuel Montacutelli	DocuSign France	

Liste de diffusion :	☒ Externe	☒ Interne DocuSign France
	Public	

Historique du document :				
Date	Version	Rédacteur	Commentaires	Vérifié par
08/06/2011	0.1	EM	Création du document	
23/06/2011	0.2	EM	Intégration commentaires	
30/01/2012	0.3	EM	Intégration gestion du saut de seconde	
10/02/2012	0.4	EM	Intégration gestion du saut de seconde et gestion des clés d'UH	
26/02/2012	0.5	EM	Correction coquille	
14/05/2012	0.6	EM	Correction de coquille	
05/11/2013	1.0	DV	Passage en version finale et mise à jour de la charte graphique	
08/07/2014	1.1	EM	Suppression d'un service d'AH	JYF
30/12/2015	1.2	EM	Intégration des retours suite à l'audit LSTI 2015	
23/01/2016	1.3	EM	Modification suite au rachat de TDT par DocuSign	
20/03/2017	1.4	EM	Intégration de la norme EN 319 421.	
03/06/2019	1.5	EM	Update PMA contact and certificate information.	

SOMMAIRE

1 INTRODUCTION

1.1 Présentation générale

DocuSign France se positionne en tant que Prestataire de Services d'Horodatage Electronique (ci-après « PSHE »), basé en France, et délivre des Contremarques de Temps dans le cadre de ses besoins internes et des besoins de ses clients. Le présent document constitue les Politiques d'Horodatage de DocuSign France (ci-après « PH ») pour le Service d'horodatage de DocuSign France dénommé « DocuSign France Timestamping ».

Le Service d'horodatage consiste principalement à :

- Générer et signer des contremarques de temps avec une précision de 1 seconde par rapport au temps UTC ;
- Publier les informations de validité des certificats d'Unité d'Horodatage.

En tant que PSHE, DocuSign France déploie plusieurs Autorité d'Horodatage (ci-après « AH »). Le présent document donne les exigences de sécurité pour l'ensemble des AH de DocuSign France. Les différences entre ces AH portent essentiellement sur :

- L'Autorité de Certification (AC) qui émet le certificat pour l'AH ;
- Les algorithmes utilisés ;
- La durée de vie des Contremarques de temps ;
- La qualification de l'AH.

Dès qu'une distinction est à faire au sein d'un paragraphe, alors elle est faite à partir des OID définis dans le présent document. Ce document inclut plusieurs OIDs (qualifié et non qualifié) du PSHE DocuSign France qui sont mises en œuvre par différentes AH de DocuSign France.

Dans le cadre de ce document, un Client est une entité légale qui soumet ou fait soumettre par une Application utilisatrice des Demandes de contremarques de temps pour ses besoins propres.

Une Contremarque de temps permet d'attester de la réalité, à une date et une heure donnée, de l'existence d'une Empreinte Numérique (ou « hash ») qui est soumise au Service d'horodatage de DocuSign France. Les contremarques de temps sont délivrées et signées électroniquement par une AH à l'aide d'Unité(s) d'Horodatage (ci-après « UH »). Ces PH n'imposent 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.

L'objectif de ce document est de définir les engagements qu'DocuSign France, en tant que PSHE pour l'ensemble de ces UH, respecte dans la délivrance et la gestion de contremarques de temps, ainsi que les obligations des autres participants.

Le présent document est complété dans sa partie mise en œuvre par une Déclaration des Pratiques d'Horodatage non publique (DPH) et un contrat de service conclu entre DocuSign France et le client ayant souscrit au Service (Contrat).

Les changements majeurs au sein de l'AH qualifiée sont notifiés à l'ANSSI.

L'OID « 1.3.6.1.4.1.22234.2.6.5.8 » identifie la PH qui permet aux AH qui la mette en œuvre d'être qualifiées conformes aux exigences pour le service horodatage telles que prévues par l'ANSSI et la norme ETSI EN 319 421.

Le présente PH et la DPH associée sont élaborées sur la base des documents suivants :

- [RGS PH] : « Référentiel Général de Sécurité, version 2.0, Annexe A5, Politique d'Horodatage Type, Version 3.0 du 27 février 2014 » ;

- [Errata Annexe 3] : « Référentiel Général de Sécurité, version 2.0, Errata de l'annexe A3, Politique de Certification Type, Version 1.0 du 19 octobre 2016 » ;
- [CRYPTO] : « Référentiel Général de Sécurité, version 2.0, Annexe B1, Mécanismes cryptographiques, Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version 2.03 du 21 février 2014, (Annule et remplace la version 1.20 du 26 janvier 2010) ».
- [EN 319 421] : "ETSI EN 319 421 V1.1.1 (2016-03), Electronic Signatures and Infrastructures (ESI), Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".
- [EN 319 422] : "ETSI EN 319 422 V1.1.1 (2016-03), Electronic Signatures and Infrastructures (ESI), Time-stamping protocol and time-stamp token profiles".

1.2 Identification du document

1.2.1 OID de la PH sans labels (RGS ou ETSI)

Cette PH particulière est identifiée par un numéro d'identifiant d'objet (OID) dont la valeur est : 1.3.6.1.4.1.22234.2.6.5.1.1, 1.3.6.1.4.1.22234.2.6.5.4, 1.3.6.1.4.1.22234.2.6.5.5 (horodatage de staging), 1.3.6.1.4.1.22234.2.6.5.6 (horodatage de démo) et 1.3.6.1.4.1.22234.2.6.5.7 (horodatage de production de niveau avancé non certifié ETSI).

Le numéro d'OID de cette PH est indiqué à titre de gestion documentaire et pour utilisation dans les contremarques de temps qui sont générés par les UH pour l'AH.

1.2.2 OID de la PH CDS avec labels RGS et ETSI

Cette PH particulière est identifiée par un numéro d'identifiant d'objet (OID) dont la valeur est : 1.3.6.1.4.1.22234.2.6.5.8. Cette PH est conforme avec les règles identifiées par « ETSI time-stamping identifier, 0.4.0.2023.1.1 (EN 319 421).

L'OID n'est plus certifié ETSI à partir de juillet 2017 : 1.3.6.1.4.1.22234.2.6.5.3.

Le numéro d'OID de cette PH est indiqué à titre de gestion documentaire et pour utilisation dans les contremarques de temps qui sont générés par les UH pour l'AH.

1.3 Gestion de la PH et de la DPH

1.3.1 DocuSign France Policy Management Authority (PMA)

La PMA est DocuSign France.

La PMA est responsable des AC dont elle garantit la cohérence et la gestion du référentiel de sécurité, ainsi que sa mise en application. Le référentiel de sécurité des AH est composé de la présente PH, de la DPH associée, des Conditions Générales de service (qui inclue le TDS requis par l'ETSI) et des procédures mises en œuvre par les composantes de l'UH. La PMA valide le référentiel de sécurité. Elle autorise et valide la création et l'utilisation des composantes des différentes AH. Elle suit les audits et/ou contrôle de conformités effectuées sur les composantes de l'UH, décide des actions à mener et veille à leur mise en application.

1.3.2 Elaboration de la PH et de la DPH

Les PH et les DPH associées sont rédigées et approuvées par la Policy Management Authority (PMA) de DocuSign France.

Toute demande de renseignements est à adresser à DocuSign France selon les modalités du § 1.3.6 ci-après. La PMA a entre autres la responsabilité de veiller à la conformité des DPH avec les présentes PH. La PMA veille également à la complétude du Contrat au regard du service d'horodatage de DocuSign France.

1.3.3 Délai de préavis

DocuSign France informera les Clients du Service en respectant un préavis de trente (30) jours calendaires avant de procéder à tout changement des présentes PH susceptible de produire un effet majeur sur lesdits Clients.

DocuSign France informera les Clients du Service en respectant un préavis de quinze (15) jours calendaires avant de procéder à tout changement des présentes PH susceptible de produire un effet mineur sur lesdits Clients.

DocuSign France peut modifier les présentes PH sans préavis lorsque, selon l'évaluation du responsable des PH, ces modifications n'ont aucun impact sur eux. Toutefois il informera le Client de la nature de la modification.

1.3.4 Forme de diffusion des avis

Dans les cas de modification soumise à préavis, DocuSign France avise les Clients des modifications apportées aux présentes PH, par tous moyens à sa convenance dont notamment le site Internet de DocuSign France et la messagerie électronique ou son Extranet support, en fonction de la portée des modifications.

1.3.5 Modifications nécessitant l'adoption d'une nouvelle politique

Si un changement apporté aux présentes PH a, selon l'évaluation du responsable des PH, un impact majeur sur un nombre important de Clients, le responsable des PH peut, à sa discrétion, instituer une nouvelle PH avec un nouvel identificateur d'objet (OID).

1.3.6 Point de contact

Toute demande relative aux présentes PH doit être adressée à :

- DocuSign France ;
- Mr. Thibault de Valroger ;
- Contact : Director, Business Development ;
- DocuSign France – 9-15 rue Maurice Mallet - 92131 Issy-les-Moulineaux Cedex – France ;
- Email: DSFCompliance-Risk-Safety@docusign.com.

Toute demande de consultation des DPH de DocuSign France devra faire l'objet d'une demande motivée. Cette demande est instruite en tenant compte des éléments de motivation de la demande et la transmission éventuelle aura lieu conformément aux règles de protection de l'information appliquées par DocuSign France.

1.4 Qu'est-ce que l'horodatage ?

L'horodatage permet d'attester qu'une donnée électronique existe à une date et une heure donnée. Les date et heure sont garanties par une AH qui applique une des PH décrite dans ce document.

En pratique, le Client qui souhaite disposer d'une Contremarque de temps, choisit l'AH qui met en œuvre la PH (OID spécifique) dont les caractéristiques sur les contremarques lui conviennent.

Le Client élabore une demande de contremarque de temps qui contient une empreinte numérique de la donnée électronique qu'il souhaite faire horodater.

Ensuite, le Client transmet la demande de contremarque de temps à l'UH de l'AH. L'AH appose une signature électronique, par l'intermédiaire d'une UH synchronisée par rapport au temps UTC, sur l'empreinte qui lui a été fournie et retourne cette empreinte au Client demandeur.

La signature générée par l'UH lie de manière sûre l'empreinte numérique, et non la donnée électronique elle-même, à la date et l'heure de génération de la contremarque de temps avec une précision de 1 seconde par rapport au temps UTC. Cette signature est vérifiable pendant une période qui débute dès la génération de la contremarque de temps et dont la durée est fixée par l'AH dans les présentes PH.

L'AH tient à disposition des Vérificateurs de Contremarques de temps les informations nécessaires à la vérification de la validité des Contremarques de temps, parmi celles-ci les informations relatives aux états de validité des certificats d'horodatage (chaîne de certification, LCR, …).

Les demandeurs de contremarques de temps qui établissent des demandes de contremarques de temps sont authentifiés par l'AH.

Chaque UH signe les Contremarques de temps pour le compte de l'AH à l'aide d'une clé privée dont la clé publique correspondante a été certifiée au préalable par l'autorité de certification (AC) dénommé ACH choisie en fonction de l'OID de la PH utilisé. Les UH disposent donc de certificats d'UH qui permettent de les identifier.

2 GENERALITES

2.1 Définitions

Application utilisatrice : désigne un ensemble d'applications informatiques qui fait appel au Service d'horodatage de l'AH et à DocuSign France en qualité PSHE. Plus particulièrement, ce terme désigne l'ensemble cohérent d'informations et de programmes informatiques ayant pour objet de transmettre des Demandes de contremarque de temps à l'UH. Le Client, ou un Client du Client, a la responsabilité de l'Application utilisatrice.

Autorité de Certification Fille (ou **AC Fille**) : désigne la (ou les) entité(s) hiérarchiquement rattachée(s) à l'AC Racine et certifiée(s) par cette dernière, et qui assure(nt) la gestion du cycle de vie des Certificats d'UH.

Autorité de Certification Racine (ou **AC Racine**) : désigne l'entité de plus haut niveau dans l'Infrastructure à Clé Publiques et qui certifie les Autorités de Certification filles.

Autorité de Certification d'Horodatage (ACH) : désigne une entité qui délivre les Certificats électroniques aux UH mises en œuvre par l'AH et rattachées à cette dernière. Cette ACH gère aussi les listes de certificats révoqués pour les certificats d'UH. L'ACH applique sa Politique de Certification (PC) pour la gestion des certificats d'UH.

Autorité d'Horodatage (AH) : désigne une entité qui a en charge l'application d'au moins une PH en s'appuyant sur une ou plusieurs UH. L'AH délivre des Contremarques de temps avec une précision donnée et à partir de Source de temps choisies.

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

Certificat(s) d'AC : désigne(nt) un fichier électronique émis pour une AC Fille par l'Autorité de certification Racine.

Certificat(s) UH : désigne(nt) une pièce d'identité électronique signée par une Autorité de Certification (ACH) et certifiant du lien entre une identité et la Clé publique de la personne physique titulaire du Certificat.

Certificat d'AC auto signé : désigne un certificat d'AC signé par la clé privée de cette même AC.

Client (ou **Abonné** au sens du RGS) : désigne l'entité ayant contracté avec DocuSign France pour bénéficier du Service d'horodatage de DocuSign France dans le cadre de son activité professionnelle ou personnelle.

Chemin de certification (ou **chaîne de confiance**, ou **chaîne de certification**) **:** désigne l'ensemble d'AC où chaque AC est certifiée par une AC d'échelon supérieur. À titre d'illustration, une AC délivrant des certificats à des UH peut elle-même être certifiée par une AC, dite « AC intermédiaire », qui à son tour peut être certifiée par une autre AC intermédiaire, ainsi de suite jusqu'à l'AC de plus haut niveau, auto signée, dite « AC racine ».

Contremarque de Temps : Donnée signée qui lie une représentation d'une donnée à un temps particulier fournit par une UH, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là. Cette contremarque de temps est signée électroniquement par une Unité d'Horodatage (UH). Une Contremarque de temps permet d'établir la preuve que l'empreinte numérique existe à la date et l'heure qui y figure.

Coordinated Universal Time (UTC) : désigne l'échelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5 [TF.460-5].

Date et heure d'UH (temps particulier) : désigne une date et une heure particulière qui sont créées par l'horloge interne de l'UH. L'horloge interne de cette UH est synchronisée avec des Source(s) de temps externe(s) afin de créer une date et une heure avec une précision donnée au regard du temps UTC. Dans le cadre de la PH, la date et l'heure d'UH de DocuSign France contenue dans les Contremarque de Temps est la date et l'heure légale française, construite à partir de la synchronisation avec plusieurs source de temps UTC(k).

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

Demande de contremarque de temps : désigne la requête qui est soumise par un Client à l'AH pour l'émission d'une contremarque de temps. Cette requête contient l'empreinte numérique de la donnée à horodater.

Données électroniques : désigne un ensemble de données structurées pouvant faire l'objet de traitement informatique par les applications informatiques du Client. Le calcul de l'empreinte numérique est effectué à partir de cet ensemble de données.

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

Jeton d'horodatage : Voir **Contremarque de Temps**.

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

Politique de Certification (PC) : désigne l'ensemble de règles identifiées par un OID et publiées par l'AC décrivant les caractéristiques générales des Certificats qu'elle délivre. Ce document décrit les obligations et responsabilités de l'AC, de l'AE, des utilisateurs de certificats et de toutes les composantes de l'IGC intervenant dans l'ensemble du cycle de vie d'un Certificat.

Les versions applicables des PC des AC sont les versions en vigueurs au jour de l'ouverture du Service et sont consultables à l'adresse web suivante : https://www.docusign.fr/societe/politiques-de-certifications. Les versions successives des PC seront mises à la disposition des Clients et des Vérificateurs sur le site Internet de DocuSign France. Les Clients seront avertis de la modification des PC conformément aux dispositions de l'article 9 de ladite PC.

Politique d'horodatage (PH) : désigne l'ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AH se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'une contremarque de temps avec des exigences de sécurité communes. Une PH peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les Clients et les Vérificateurs de Contremarques de temps.

Précision : désigne la différence maximale autorisée entre la date et l'heure UTC fournie par la Source de temps et la date et heure (Cf. Date et heure d'UH) de l'horloge de l'UH qui est utilisée pour générer les Contremarques de temps.

Prestataire de services d'horodatage (PSHE) : L' [ORDONNANCE] introduit et définit les prestataires de service de confiance (PSCO). Un PSHE est un type de PSCO particulier. Un PSHE se définit comme toute personne ou entité qui est responsable de la génération et de la gestion de contremarques de temps, vis-à-vis de ses abonnés et des utilisateurs de ces contremarques de temps. Un PSHE peut fournir différentes familles de contremarques de temps correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSHE comporte au moins une AH mais peut en comporter plusieurs en fonction de son

organisation. Un PSHE est identifié dans les certificats de clés publiques des UH dont il a la responsabilité au travers de ses AH.

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

Service d'horodatage (ou **Service)** : désigne l'ensemble des prestations réalisées par DocuSign France nécessaires à la génération et le cas échéant à la gestion de contremarques de temps.

Source de temps : désigne la composante qui fournit une date et une heure (temps) UTC avec une précision donnée (antenne GPS, onde radio et serveur source de temps NTP).

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

Système d'horodatage : désigne l'ensemble des UH et des composants d'administration et de supervision utilisés pour fournir des services d'horodatage.

Unité d'Horodatage (UH) : désigne l'ensemble de matériels et de logiciels utilisés pour la création de contremarques de temps. L'UH est caractérisée par une identité certifié par une AC et une clé unique de signature de contremarques de temps. L'UH construit une date et une heure d'UH qu'elle utilise pour les contremarques de temps qu'elle signe.

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 20 Consultatif pour la définition de la Seconde (Rec. ITU-R TF.536-1 [TF.536-1]).

Vérificateur de contremarque de temps (ou **Utilisateur de contremarque de temps** au sens du RGS**)** : désigne l'entité (personne ou système) qui valide une contremarque de temps émise sous une PH et DPH données par une AH donnée afin de s'assurer de l'existence d'une donnée électronique à une date et une heure données.

Validation de contremarque de temps : désigne l'action du Vérificateur de Contremarque de temps qui consiste à vérifier que la contremarque est valide. La vérification d'une signature électronique de contremarque de temps consiste en les opérations suivantes :

- Vérification de la signature de la contremarque de temps ;
- Vérification et extraction de la date et de l'heure contenues dans la contremarque de temps ;
- Identification et extraction du certificat de l'UH ayant émis la contremarque de temps ;
- Vérification que la date à laquelle la contremarque de temps a été émise est comprise dans la période de validité du certificat de l'UH ayant émis la Contremarque de temps ;
- Vérification de l'état de validité du certificat de l'UH ayant émis la contremarque de temps au moment de la génération de la contremarque de temps ;
- Vérification que la date indiquée par l'AH dans la Contremarque de temps est antérieure à la révocation éventuelle du certificat d'UH ayant émis la Contremarque de temps.

Si l'ensemble de ces opérations est positif, alors la contremarque de temps est considérée comme valide.

Vérification d'une contremarque de temps : désigne l'action du Vérificateur de Contremarque de temps qui consiste à vérifier que la contremarque est valide.

2.2 Abréviations

Pour le présent document, les acronymes suivants s'appliquent :

AC	Autorité de Certification
AH	Autorité d'horodatage
DPH	Déclaration des Pratiques d'Horodatage
ETSI	European Telecommunications Standards Institute
LCR	Liste des Certificats Révoqués
OID	Object Identifier
PH	Politique d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Système d'Information
UH	Unité d'Horodatage
UTC	Coordinated Universal Time

3 POLITIQUE D'HORODATAGE

Le présent document contient plusieurs PH (3 au total). Ces trois PH sont distingués à l'intérieur de ce document par des paragraphes dont le titre est l'OID de la PH qui fait l'objet d'exigence spécifique.

Mais des exigences communes sont tout de même à relever. Les caractéristiques communes et principales de ces PH sont comme les suivantes :

- La protection des clés et de l'horloge respecte les exigences spécifiées au chapitre IX de [PH RGS] ;
- La date et le temps de chaque contremarque de temps sont synchronisés avec le temps UTC avec une **précision de 1 seconde** ;
- Le format de contremarque de temps standard défini par le [RFC 3161] ;
- Le protocole définit dans le [RFC3161] est utilisé pour utiliser les services des UH ;
- L'AC générant les certificats de clé publique pour les unités d'horodatage gère le service de révocation pour chaque certificat d'UH.

4 DECLARATION DES PRATIQUES D'HORODATAGE

Une DPH expose les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la PH, en particulier les processus qu'une UH emploiera pour la création des contremarques de temps et le maintien de l'exactitude de ses horloges. L'AH de DocuSign France peut mettre en œuvre plusieurs UH pour supporter son Service d'horodatage.

En raison de la confidentialité d'une partie de son contenu, la DPH est un document à diffusion restreinte, il n'est disponible à la consultation qu'aux personnes habilitées à en prendre connaissance. Toute demande de consultation devra être adressée au Comité des politiques de certification et d'horodatage de DocuSign France.

Cependant, chaque AH publie les parties publiques des DPH et en particulier :

- Le cadre d'application de la DPH ;
- Les coordonnées de l'AH ;
- La PH appliquée (OID) ;
- Les algorithmes de hachage autorisés pour constituer l'objet horodaté ;
- La durée minimum pendant laquelle il est possible de vérifier les contremarques de temps, à compter de leur date de génération ;
- La précision de la date des contremarques de temps par rapport à l'échelle de temps UTC ;
- Les obligations des Clients ;
- Les obligations des Vérificateurs de Contremarque de temps ;
- Les informations permettant de vérifier la Contremarque de temps ;
- Les limitations de responsabilité.

Ces informations publiques sont présentées en étant intégrées aux conditions générales d'utilisation (se reporter au § 5).

5 CONDITIONS GENERALES D'UTILISATION (CGU)

Compte tenu de la complexité de lecture d'une PH et d'une DPH pour des Clients et des Vérificateurs non-spécialistes du domaine, l'AH définit également des conditions générales d'utilsiation (CGU) incluant les "TSA Disclosure Statement" (TDS) définis par [ETSI_PH]. Ces CGU ne sont pas destinées à remplacer les PH ou les DPH mais sont destinées à des Clients et à des Vérificateurs de contremarques de temps non-techniciens afin qu'ils puissent facilement comprendre l'information essentielle dont ils doivent avoir connaissance. Ces conditions générales d'utilisation aident l'AH à démontrer comment elle répond aux exigences réglementaires, en particulier celles liées à la protection du consommateur.

Le présent document contient des PH différentes, mais seule la PH certifiée a des CGU publiées.

6 CONTENU DE LA POLITIQUE D'HORODATAGE

6.1 Dispositions générales

6.1.1 Obligations de l'Autorité d'horodatage

Dans le cadre des présentes PH, l'AH :

- Ne modifie pas les empreintes contenues dans les Demandes de contremarques de temps ;
- Génère et signe les contremarques de temps conformément à la PH et à la DPH choisies de DocuSign France, ainsi qu'aux CGU (seulement pour le service certifié) ;
- Respecte et se conforme aux exigences et procédures définies dans la PH et la DPH choisies et les CGU (seulement pour le service certifié) ;
- Garantit la conformité des exigences et des procédures décrites dans la DPH avec la PH choisie même quand les fonctionnalités d'horodatage sont remplies par des sous-traitants ;
- Met à disposition de ses Clients l'ensemble des informations nécessaire à vérifier les contremarques de temps qu'elle aura émises, selon les modalités indiquées au paragraphe 6.4.8 et le précisées dans les CGU (seulement pour le service certifié) ;
- Respecte, les conditions de disponibilité du Service d'horodatage convenues contractuellement avec ses Clients dans les CGU (seulement pour le service certifié) ;
- Garanti l'adhésion aux obligations complémentaires indiquées dans la contremarque de temps par l'intermédiaire des CGU signé du Client (seulement pour le service certifié) ;
- Maintient une information sur la compromission de la bi-clé des UH, même après la date de fin de validité des certificats des UH ;
- Utilise des certificats pour les UH sous sa responsabilité qui sont délivrés par les AC autorisées par les PH ;
- Le cas échéant lorsque le Client a choisi cette option, authentifie les demandes de contremarques de temps à l'aide des certificats déclarés par le Client auprès de l'AH.

6.1.2 Obligations du Client

Dans le cadre des présentes PH, le Client :

- Identifie et habilite les Applications utilisatrices qui vont soumettre des Demandes de contremarque de temps auprès d'une ou des UH de l'AH ;
- Déclare, le cas échéant en cas d'authentification des demandes de contremarques de temps, les AC et les certificats que l'AH utilise pour authentifier les entités qui soumettent des Demandes de contremarques de temps ;
- Demande à l'Application utilisatrice de protéger en confidentialité et en intégrité les informations confidentielles qu'elle détient et qui lui servent pour l'authentification auprès de l'UH ;
- Garantit que les informations contenues dans la Demande de contremarque de temps que l'Application utilisatrice fournit à l'UH sont complètes et correctes et respectent le format de Demande de contremarque de temps ;
- Informe sans délai l'AH en cas de compromission de ses données d'authentification utilisées pour l'authentification auprès de l'UH ;
- Fait garantit la sécurité des plates-formes de l'Application utilisatrices qui procède au Demande de contremarque de temps ;
- Respecte les obligations de la PH, et des CGU associées (seulement pour le service certifié), utilisée par l'AH ;
- Indique à l'AH l'algorithme qu'il utilise pour calculer les empreintes numériques des données électroniques qu'il souhaite faire horodater ;
- Vérifie, au moment de l'obtention d'une contremarque de temps, que le certificat de l'UH n'est pas révoqué et qu'il est délivré par l'ACH conformément à la PC de l'ACH ;

- Le cas échéant en cas d'authentification des Demande de contremarques de temps, respecte les modalités applicables de la politique de certification de l'AC ayant délivré les certificats utilisés pour s'authentifier lors de la Demande de contremarque de temps.

6.1.3 Obligations du Vérificateur de contremarques de temps

Dans le cadre des présentes PH, le Vérificateur de contremarques de temps :

- Vérifie que la Contremarque de temps a été correctement signée et que le certificat de l'UH est valide à l'instant de la vérification ;
- Tient compte des limitations sur l'utilisation de la contremarque de temps indiquées dans la PH et les CGU utilisées (seulement pour le service certifié).

6.1.4 Obligations pour les ACH fournissant les certificats des unités d'horodatage

6.1.4.1 OID 1.3.6.1.4.1.22234.2.6.5.1.1 et 1.3.6.1.4.1.22234.2.6.5.4

L'ACH délivrant des certificats de clés publiques pour les UH fournit un service de révocation mis à jour soit :

- Sur une base quotidienne en employant au moins un mécanisme de publication de LCR en cas d'utilisation de l'AC « KEYNECTIS KH » ;
- Sur une base annuelle en employant un mécanisme de publication de LAR en cas d'utilisation de l'AC « CDS CA » ;

L'ACH s'engage à conserver pendant au moins 1 an après expiration des certificats des UH, tous les journaux d'événement liés à la délivrance des certificats d'UH.

6.1.4.2 OID 1.3.6.1.4.1.22234.2.6.5.3, 1.3.6.1.4.1.22234.2.6.5.5, 1.3.6.1.4.1.22234.2.6.5.6, 1.3.6.1.4.1.22234.2.6.5.7 et 1.3.6.1.4.1.22234.2.6.5.8

Les certificats des clés publiques délivrés aux UH sont délivrés par des AC (PSCE) conformes au RGS v2 pour la Politique de Certification Type "cachet serveur" et ETSI 319 411-1 LCP. Les certificats sont des certificats de production (1.3.6.1.4.1.22234.2.6.5.3, 1.3.6.1.4.1.22234.2.6.5.7, 1.3.6.1.4.1.22234.2.6.5.8) ou de test (1.3.6.1.4.1.22234.2.6.5.5 et 1.3.6.1.4.1.22234.2.6.5.6) en fonction de l'OID de la PH.

6.1.5 Déclarations des Pratiques d'Horodatage (DPH)

DocuSign France garanti que les AH possèdent la fiabilité nécessaire pour fournir des Services d'horodatage. En particulier :

- Effectue 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 ;
- Possède les DPH et des procédures utilisées pour adresser toutes les exigences identifiées dans les PH supportées ;
- Identifie dans les DPH les obligations de toutes les organisations externes participant à la fourniture des Services d'horodatage, y compris la politique de sécurité et les pratiques applicable. Cela inclut l'AC fournissant les certificats aux UH ;
- Met à la disposition des Clients et des Vérificateurs de contremarques de temps les éléments publics de sa DPH, s'il y a lieu, et toute autre documentation appropriée, tel que nécessaire pour évaluer la conformité aux PH ;
- Dispose d'une organisation adéquate pour l'approbation des DPH et la vérification de la Concordance entre ces déclarations et les PH ;
- Garanti que les pratiques sont correctement mises en œuvre ;
- Définit une procédure de contrôle périodique de la conformité des pratiques, y compris les responsabilités, à la DPH ;

- Informe au préalable les Clients pour tout changement qu'elle a l'intention de faire dans la partie publique de sa DPH et, après l'approbation, immédiatement mettre à la disposition des Clients et des Vérificateurs de contremarques de temps la partie publique révisée des DPH ;
- Garanti que si l'AH a été évaluée pour être en conformité avec une PH identifiée et si une modification envisagée à l'initiative de l'AH pouvait entraîner une non-conformité avec la PH ou avec les DPH, alors l'AH indique qu'elle soumettra cette modification à l'organisme évaluateur indépendant pour avis.

6.1.6 Conditions Générales d'Utilisation (CGU)

L'AH met à disposition de tous ses Clients et des Vérificateurs potentiels de contremarques de temps, pour chaque PH supportée par l'AH, des CGU (seulement pour le service certifié) qui contiennent les informations suivantes :

- Une information sur un point de contact pour l'AH ;
- Une description ou une référence de la PH appliquée ;
- Au moins un algorithme de hachage qui peut être utilisé pour représenter la donnée à horodater ;
- La période de temps minimum, hors cas de révocation, durant laquelle les Contremarques de temps seront vérifiables ;
- L'exactitude du temps dans les Contremarques de temps par rapport au temps UTC ;
- N'importe quelles limitations sur l'utilisation du Service d'horodatage ;
- Les obligations du Client, si elles ne font partie ni du contrat avec l'abonné, ni de la DPH ;
- Les obligations des Vérificateurs de contremarques de temps, si elles ne font partie ni du contrat avec les Vérificateurs de contremarques de temps, ni de la DPH ;
- L'information sur la manière de vérifier les Contremarques de temps de telle façon que le Vérificateur de Contremarques de temps puisse "raisonnablement avoir confiance" dans les contremarques de temps ainsi que les restrictions possibles sur sa période de validité ;
- La période de temps pendant laquelle les fichiers d'audit de l'AH sont conservés ;
- Le système légal applicable ;
- Les limitations de responsabilité ;
- Les procédures pour les plaintes et le règlement des conflits ;
- Le nom de l'organisme de qualification et de certification indépendant ayant validé la conformité avec la PH type du RGS et celle de l'ETSI ;
- Les éléments permettant de valider la chaîne de certificats (du certificat de l'unité d'horodatage au certificat auto-signé) ;
- Le nom du pays dans lequel l'AH est établie et l'identifiant de l'AH (tel que figurant dans le certificat de l'UH).

6.1.7 Conformité avec les exigences légales

L'inapplicabilité d'une stipulation des présentes PH n'affecte en rien la validité des autres stipulations. En conséquence, l'ensemble des stipulations des présentes PH continueront à s'appliquer à la seule exception de la stipulation déclarée inapplicable.

Les intitulés de chaque Article ne servent qu'à la commodité de la lecture et ne peuvent en aucun cas être le prétexte d'une quelconque interprétation ou dénaturation des clauses sur lesquelles ils portent.

En cas de conflit d'interprétation entre les intitulés et leur contenu, le contenu des clauses prévaudra.

6.1.7.1 Exonération des droits

Les exigences définies dans les présentes PH et ses DPH doivent être appliquées par les Clients, l'AH, l'AC et les Vérificateurs de contremarque de temps dans le respect des stipulations des présentes PH et des DPH associées sans qu'aucune exonération des droits, dans l'intention de modifier tout droit ou obligation prescrit, ne soit possible.

6.1.7.2 Loi applicable et juridictions compétentes

Les dispositions de la PH sont régies par le droit français.

En cas de litige relatif à l'interprétation, la formation ou l'exécution des présentes PH, et faute de parvenir à un accord amiable, tout différend sera porté devant les tribunaux compétents de Paris.

6.1.7.3 Droits de propriété intellectuelle

Tous les droits de propriété intellectuelle relatifs au service d'horodatage détenus par l'AH et ses fournisseurs sont protégés par la loi, règlement et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctifs, droits d'auteur (par exemple : logiciels, pages Web, bases de données, textes originaux, …etc.) est sanctionnée par les articles L 716-1 et suivants du Code de la propriété intellectuelle.

6.1.7.4 Protection des données à caractère personnel

DocuSign France a mis en place et respecte des procédures de protection des données personnelles pour garantir la sécurité des informations caractérisées comme personnelles dans le cadre du Service d'horodatage. Les données considérées comme personnelles sont les informations personnelles des Clients.

A cet égard, l'AH respecte notamment la législation et la réglementation en vigueur sur le territoire français, en particulier, la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés révisée 2006.

En application de l'article 34 de la loi Informatique et Libertés du 6 janvier 1978, les porteurs disposent d'un droit d'accès, de modification, de rectification et de suppression des données qui les concernent comme convenu et décrit dans la demande de certificat et les CGU associés (seulement pour le service certifié). Pour l'exercer, les porteurs doivent s'adresser à DOCUSIGN FRANCE par courrier électronique à cil@docusign.com.

Pour toute autre information relative à l'exercice de leurs droits en matière de données à caractère personnel, les signataires peuvent s'adresser au Correspondant Informatique et Libertés de DocuSign France par e-mail : legal-france@docusign.com.

Aucune des données à caractère personnel communiquées lors de l'enregistrement ne peut être utilisée par l'AH, pour une autre utilisation autre que celle définie dans le cadre de la PH, sans consentement exprès et préalable de la part du Client. Le consentement du Client, pour l'utilisation desdites données pour celle définie dans le cadre de la PH est considéré comme obtenu lors de la conclusion du contrat avec DocuSign France.

Le Client accepte que les données personnelles les concernant recueillies lors de la demande d'ouverture du Service fassent l'objet d'un traitement informatique aux seules fins : d'être authentifié par l'AH, de permettre les vérifications nécessaires à l'ouverture du Service et d'apporter les preuves nécessaires à la gestion du Service au profit du Client.

Les infractions aux dispositions de la loi Informatique et Libertés du 6 janvier 1978 sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

6.1.7.5 Assurance

DOCUSIGN FRANCE déclare avoir souscrit une assurance responsabilité civile professionnelle, auprès d'une compagnie d'assurance notoirement solvable et établie en France, pour tous dommages corporels, matériels et immatériels causés dans le cadre de l'exécution des présentes.

6.1.8 Limite de responsabilité

Les présentes PH ne traitent que le cas de la signature de Contremarque de temps par des UH conformément aux présentes PH.

L'AH ne saurait être tenue responsable en cas de validation d'une Contremarque de temps avec un certificat déclaré révoqué à l'AC mais non encore pris en compte au niveau de la CRL émise par l'AC. Le Vérificateur doit appliquer une période de précaution et procéder à des vérifications auprès des AC impliquées et de l'AH afin de valider une Contremarque de temps.

L'AH ne saurait être tenue responsable en cas de validation et d'utilisation d'une Contremarque de temps avec une cryptographie qui ne serait plus considéré comme valide par l'ANSSI (se référer au document [ANSSI_ALGO]). L'AH émet des Contremarque de temps qui sont valides, au moment de leur émission, d'un point de vue cryptographique par rapport au référentiel de l'ANSSI. L'AH suit les recommandations de l'ANSSI afin de n'émettre que des Contremarque de temps dont la validation des certificats et des signatures repose sur des algorithmes et paramètres cryptographiques qui sont conformes au référentiel de l'ANSSI. Cependant les attaques évoluent et les référentiels évoluent en conséquence.

Il est donc de la responsabilité du Vérificateur et du Client de prendre l'ensemble des précautions nécessaires en fonction des besoins de leur application et des données horodatées dont la conservation des caractéristiques d'intégrité et d'existence à partir d'une date et d'une heure particulière sont à conserver dans une durée plus ou moins longue dans le temps.

Seules le Vérificateurs et le Client impliqués dans le Service peuvent rechercher la responsabilité de l'AH au titre du Service horodatage.

En aucun cas, l'AH ne sera responsable des dommages indirects.

La responsabilité de l'AH ne saurait être engagée en cas de force majeure ou de cas fortuit au sens de l'article 1148 du Code civil et la jurisprudence des cours et tribunaux français, qui échappent raisonnablement à son contrôle.

Dans le cas où la responsabilité de l'AH serait retenue, il est expressément convenu que l'AH ne serait tenue à réparation que des dommages directs certains et immédiats au sens de l'article 1151 du Code civil, dans la limite d'un montant qui ne saurait excéder le montant annuel des prestations précisé dans la ou les convention(s) et/ou les contrats conclu entre avec chacune des entités de la communauté d'utilisateurs.

L'AH ne saurait être tenu responsable des caractéristiques et les limites d'Internet, et en particulier :

- Les limites des performances techniques de l'Internet et notamment des temps de réponse pour consulter, interroger ou transférer des informations ;
- Que la communication éventuelle par Internet de mots de passe, codes confidentiels et d'une manière générale, toute information confidentielle est faite à ses risques et périls ;
- Que les données circulant sur Internet pouvant être réglementées en termes d'usage ou être protégées par un droit de propriété, le Client est seul responsable de l'usage des données qu'ils consultent, interrogent et transfèrent sur Internet ;
- Qu'il doit prendre toutes les mesures appropriées de façon à protéger ses propres systèmes informatiques des intrusions non autorisées, des actes de destruction ou d'altération, des contaminations éventuelles par des virus, chevaux de Troie ou autre système causant des failles de sécurité sur Internet.

Ces garanties sont exclusives de toute autre garantie de l'AH dans le cadre du Service d'horodatage.

Chaque partie impliquée dans le Service d'horodatage s'interdit de prendre un engagement au nom et pour le compte de l'autre partie à laquelle elle ne saurait en aucun cas se substituer.

6.2 Exigences opérationnelles

6.2.1 Gestion des requêtes de contremarques de temps

6.2.1.1 Engagements de qualité de service

Les engagements de qualité de service relatifs à la fourniture d'une contremarque de temps en réponse à une demande sont définis dans les CGU définies par l'AH (seulement pour le service certifié).

Dans tous les cas, les réponses de la part d'une AH à une Demande de contremarque de temps n'excède pas quelques secondes, ceci afin de ne pas nuire ni dégrader les usages de l'Application utilisatrice.

6.2.1.2 Authentification des demandes de contremarques de temps

L'authentification du Client est optionnelle et laissée au choix du Client. C'est donc le Client qui choisit d'être authentifié ou pas avant d'utiliser le service d'une AH.

Si le Client choisit l'option d'être authentifié alors toutes les Demandes de contremarques de temps seront authentifiées par l'UH avant d'être traitée.

Si le Client choisit l'option de ne pas être authentifié alors les contremarques de temps ne seront pas authentifiées par l'UH avant d'être traitée.

6.2.1.3 Choix d'une AH et d'une PH

Le Client choisit une AH et un OID de PH. Ensuite il utilise l'UH de l'AH choisie qui met en œuvre la PH choisie.

Dès que le Client a fait son choix alors l'AH communique au Client l'ensemble des informations de connexions aux UH. Si le Client a fait le choix que l'Application utilisatrice soit authentifiée, alors l'AH crée un espace dédié sur l'UH au seul profit du Client.

6.2.1.4 Demande de contremarques de temps

Les Demandes de contremarques de temps sont réalisées par les Applications utilisatrice de l'AH selon le protocole défini par le [RFC 3161]. Ce protocole est conforme au document [ETSI].

Si le Client a fait le choix de faire authentifier l'Application utilisatrice, alors l'Application utilisatrice et l'AH s'authentifient mutuellement, lors d'une session SSL, au préalable de toute transmission de Demande de contremarque de temps.

L'UH génère la Contremarque de temps à partir des données qui lui sont transmises par l'Application utilisatrice et la lui retourne.

La date et l'heure contenue dans la Contremarque de temps est synchronisé avec une seconde d'écart par rapport au temps UTC.

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

6.2.2 Fichiers d'audit

L'AH garantit que toutes les informations appropriées concernant le fonctionnement du Service d'horodatage et les informations pertinentes concernant les données délivrées et reçues, notamment afin de pouvoir fournir des preuves en justice sont enregistrées pendant une période de temps suffisante. Les informations appropriées concernant le fonctionnement du Service d'horodatage sont conservées notamment dans le but de fournir des éléments de preuve en cas de litige ou en cas d'enquête judiciaire. Toute demande en ce sens est à adresser au service juridique de DocuSign France.

La durée garantie de conservation de ces informations est de :

- Au moins 7 an après la fin de période pendant laquelle une contremarque de temps est vérifiable, pour tout évènement lié à la gestion du cycle de vie des Contremarques de temps ;
- Au moins 7 an après expiration des certificats d'UH, pour tout évènement lié à la gestion du cycle de vie des certificats d'UH et de leurs clés privées.

Les événements spécifiques et les données enregistrées doivent être documentés par l'AH.

La confidentialité et l'intégrité des enregistrements d'audit courants et archivés relatifs au fonctionnement du Services d'horodatage est assurée.

6.2.2.1 Général

L'AH conserve en particulier les éléments suivants :

- Les enregistrements relatifs à l'administration des services d'horodatage sont intégralement archivés et de manière adaptée à la sensibilité des informations ;
- Les événements spécifiques et les données enregistrées sont documentés par l'Autorité d'horodatage ;
- La confidentialité et l'intégrité des enregistrements d'audit courants et archivés relatifs au fonctionnement des services d'horodatage sont assurée par l'AH.
- Les enregistrements relatifs au fonctionnement des services d'horodatage sont disponibles si exigé dans le but de fournir une preuve d'un fonctionnement correct des services d'horodatage en cas d'enquêtes légales ;
- L'instant précis d'évènements significatifs concernant l'environnement de l'AH, la gestion des clés, et la synchronisation de l'horloge des UH sont enregistrés ;
- Les enregistrements relatifs à l'administration du Service d'horodatage sont gardés, après la date d'expiration de la validité de la clé de signature de l'unité d'horodatage durant une période de temps appropriée pour fournir des éléments de preuves nécessaires tel qu'indiqué dans les CGU de l'AH (seulement pour le service certifié) ;
- Les événements sont enregistrés de telle façon qu'ils ne puissent pas être facilement supprimés ou détruits (sauf s'ils sont transférés sur un support de sauvegarde) durant la période de temps où l'on exige qu'ils soient conservés ;
- Toute information enregistrée au sujet d'un Client est tenue confidentielle sauf lorsqu'un accord est passé avec le Client pour une publication plus large.

6.2.2.2 Gestion des clés

L'AH conserve en particulier les éléments suivants :

- Les enregistrements concernant tous les événements touchant au cycle de vie des clés doivent être effectués ;
- Les enregistrements concernant tous les événements touchant au cycle de vie des certificats des UH doivent être effectués.

6.2.2.3 Synchronisation de l'horloge

L'AH conserve en particulier les éléments suivants :

- Les enregistrements concernant tous les événements touchant à une synchronisation de l'horloge des unités d'horodatage sont effectués. Cela doit inclure l'information concernant des recalibrages ou des synchronisations normales ;
- Les enregistrements concernant tous les événements touchant à la détection de perte de synchronisation sont effectués.

6.2.3 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 :

- Des procédures opérationnelles et techniques sont mises en place pour assurer qu'une nouvelle paire de clés est mise en place quand la fin de la période d'utilisation d'une clé privée d'UH a été atteinte ;
- Des procédures opérationnelles et techniques sont mises en place pour détruire la clé privée si la fin de la période d'utilisation de cette clé privée a été atteinte.

Les clés privées d'UH sont des éléments sensibles qui font l'objet d'un suivi unitaire de la part de l'AH et bénéficient de mesures de protection particulière afin de les protéger de toute compromission pendant l'ensemble de leur cycle de vie.

La période d'utilisation opérationnelle des clés privées d'UH est plus courte que celle du certificat de sa clé publique associée. L'AH de DocuSign France procède au renouvellement des clés privées d'AH dans le mois précédent la fin de leur utilisation opérationnelle. Lorsqu'une nouvelle clé privée d'UH est générée, un nouveau certificat d'UH est demandé à l'ACH.

Les clés privées d'UH sont détruites dès que la fin d'utilisation opérationnelle de cette clé privée a été atteinte.

6.2.3.1 OID 1.3.6.1.4.1.22234.2.6.5.3, 1.3.6.1.4.1.22234.2.6.5.5, 1.3.6.1.4.1.22234.2.6.5.6, 1.3.6.1.4.1.22234.2.6.5.7 et 1.3.6.1.4.1.22234.2.6.5.8

La durée de vie des clés privées d'UH et des certificats d'UH est fixée en accord avec les recommandations faites par les autorités nationales compétentes en la matière, comme par exemple celles issues de l'ANSSI et précisées dans le document [ANSSI_ALGO].

6.2.4 Synchronisation de l'horloge

L'AH garantit que l'horloge des UH est synchronisée avec le temps UTC fournit par les sources de temps selon l'exactitude déclarée. En particulier :

- Le calibrage de chaque horloge d'UH est maintenu de telle manière que les horloges d'UH ne puissent pas normalement dériver à l'extérieur de l'exactitude déclarée ;
- Les horloges des UH 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. L'AH mène une analyse des risques spécifique, en plus de l'analyse de risques globale sur les services du TSP, conduite sur le système afin d'identifier les menaces contre lesquelles les horloges des UH doivent se protéger. Les menaces incluent des modifications par du personnel non autorisé et des ondes radio ou des chocs électriques ;
- L'AH devra garantir que, que si l'horloge d'une UH ne respecte plus l'exactitude déclarée, alors cela sera détecté ;
- Si l'horloge d'une UH est détectée comme étant en dehors de l'exactitude annoncée, alors les contremarques de temps ne sont plus générées par l'UH ;
- L'AH garantit que la synchronisation de l'horloge des UH 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 (selon l'exactitude déclarée) de l'instant de ce changement est effectué. Un saut de seconde est un ajustement par rapport au temps UTC effectué en sautant ou en ajoutant une seconde durant la dernière minute d'un mois UTC. On donne la première préférence à la fin de décembre et juin et on donne la seconde préférence à la fin de mars et septembre. Le saut de seconde est traité, par exemple en cas d'ajout d'une seconde intercalaire, de la manière suivante par l'AH : au moment du saut de seconde, l'AH gardera la valeur « 00.00 » et on aura donc la séquence suivante ; « 23.59 » (temps donné par l' UH) et « 23.59 » (temps UTC) à « 23.59 » (temps UTC), « 00.00 » (temps donné par l' UH) et « 23.60 » (temps UTC) à « 23.60 » (temps UTC),

« 00.00 » (temps donné par l' UH) et « 00.00 » (temps UTC) et ainsi de suite. Donc l'UH respectera toujours une précision d'une seconde par rapport au temps UTC.

6.2.5 Exigences du contenu d'une contremarque de temps

L'AH garantit que les Contremarques de temps sont générées en toute sécurité et incluent un temps particulier correct. En particulier :

- La Contremarque de temps inclut l'identifiant du certificat de l'UH. Ce certificat d'UH inclut :
    - Un identifiant du pays dans lequel l'AH est établie ;
    - Un identifiant de l'AH ;
    - Une identification de l'UH qui génère les contremarques de temps ;
- La Contremarque de temps inclut un identifiant de la PH utilisé ;
- Chaque contremarque comporte un identifiant unique ;
- Les informations de temps portées dans les Contremarques de temps sont reliées à au moins à un temps fourni par un laboratoire UTC (k). Toutes les sources de temps utilisés pour synchroniser les horloges des UH sont des sources UTC(k) ;
    - *Nota* - Le Bureau des International Poids et Mesures (BIPM) calcule UTC sur la base des représentations locales UTC (k) d'un grand ensemble de montres atomiques dans des instituts de métrologie nationaux et des observatoires nationaux astronomiques autour du monde. Le BIPM dissémine le temps UTC par sa Circulaire mensuelle T. Celle-ci est disponible sur le site Web BIPM (www.BIPM.org) qui identifie officiellement tous les instituts ayant des échelles de temps UTC (k) reconnues ;
- Le temps inclus dans une Contremarque de temps est synchronisé avec le temps UTC au moins avec l'exactitude définie dans le présente document ;
- La Contremarque de temps inclut la représentation de la donnée à horodater (c'est-à-dire la valeur de l'Empreinte et l'identifiant d'algorithme de hachage) telle que fournie par le Demandeur de contremarque de temps ;
- La Contremarque de temps est signée en employant une clé privée produite exclusivement à cette fin ;
- La Contremarque de temps respecte les exigences du chapitre 8 ci-dessous ;
    - *Nota* - Dans le cas de Demande de contremarque de temps survenant durant un intervalle de temps correspondant à l'exactitude de l'horloge de l'UH, l'ordonnancement des Contremarques de temps à l'intérieur de cet intervalle n'est pas requis.

6.2.6 Compromission de l'AH

L'AH garantit dans le cas d'événements qui affectent la sécurité du Service 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 :

- Le plan de secours de l'AH doit traiter 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. En cas de compromission de clé d'UH, le certificat d'UH est révoqué ;
- Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une UH, qui pourrait affecter des contremarques de temps émises, l'AH mettra à la disposition de tous les Clients et Vérificateurs de contremarques de temps une description de la compromission qui est survenue ;

- Dans le cas d'une compromission, réelle ou suspectée, ou 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 unité ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation ;
- En cas d'un évènement majeur dans le fonctionnement de l'AH ou d'une 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 Clients et des Vérificateurs 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 doit également prévenir directement et sans délai le point de contact identifié sur le site : http://www.ssi.gouv.fr. Les vulnérabilités découvertes sont traitées sous 48 heures dès leurs connaissances par la PMA et l'ANSSI est alertée par la PMA en 24H00 dès connaissance de l'incident majeure portant atteinte à la sécurité du service ou des données personnelles.

6.2.7 Fin d'activité

Il est nécessaire de définir les procédures de fin d'activité ou de reprise par un tiers. Dans ce cadre, l'AH garantit que les dérangements potentiels aux Clients et aux Vérificateurs de contremarques de temps seront réduits au minimum suite à la cessation d'activité du Service d'horodatage et assurer en particulier la maintenance continue des informations nécessaires pour vérifier la justesse de Contremarques de temps. En particulier :

- Avant que l'AH ne termine ses Services d'horodatage les procédures suivantes sont mises en œuvres exécutées au minimum :
    - l'AH rendra disponible à tous ses Clients et aux Vérificateurs de contremarques de temps l'information concernant sa fin d'activité ;
    - l'AH abroge 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 disponible aux Vérificateurs de contremarques de temps pendant une période raisonnable ses clés publiques ainsi que ses certificats ;
    - Les clés privées des UH sont détruites de telle façon que les clés privées ne puissent pas être recouvrées ou réutilisées ;
    - Les certificats d'UH encore valides sont révoqués.
- DocuSign France 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 ;
- L'AH indique dans sa PH les dispositions prises pour la fin du service. Cela doit inclure :
    - Un avis aux Clients et aux Vérificateurs de contremarques de temps ;
    - Un transfert des obligations de l'AH à d'autres organismes ;
- L'AH prévient également directement et sans délai le point de contact identifié sur le site : www.ssi.gouv.fr.

6.3 Exigences physiques et environnementales, procédurales et organisationnelles

6.3.1 Exigences physiques et environnementales

L'AH garantit 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 :

- A la fois pour la fourniture du Service d'horodatage et la gestion de l'horodatage :
    - L'accès physique aux équipements concernés par le Services d'horodatage sont limité aux seules personnes autorisées ;
    - Des contrôles sont mis en œuvre pour éviter la perte, des dégâts ou la compromission d'actifs et l'interruption des activités ;
    - Des contrôles sont mis en œuvre pour éviter la compromission ou le vol d'informations ou d'équipements informatiques ;
- Des contrôles d'accès sont appliqués aux UH pour remplir les exigences de sécurité des UH. Les contraintes sur l'environnement d'exploitation, identifiées dans la documentation liée à la certification d'un module d'UH (PP, cible de sécurité, …) sont remplies ;
- Les contrôles suivants complémentaires doivent être appliqués à la gestion du service d'horodatage :
    - Le système d'horodatage doit fonctionner dans un environnement qui protège physiquement les services de la compromission au moyen 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 UH. Les ressources cryptographiques des UH sont dans des baies uniquement accessible sous double contrôle ;
    - 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'AH 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 sont 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.

6.3.2 Exigences procédurales

L'AH garantit que les composants du UH 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 ;
- Des procédures sont établies et mises en œuvre pour tous les rôles de confiance et administratifs qui impactent la fourniture des Services d'horodatage.

6.3.2.1 Manipulation et sécurité des supports

Tous les supports sont 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.

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.

Chaque membre du personnel avec des responsabilités de gestion est responsable de la planification et de l'exécution effective des PH et des DPH qui lui incombent.

6.3.2.2 Planification de Système

Les charges 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 pour les UH. La disponibilité du service d'UH est de 99,9.

6.3.2.3 Rapport d'incident et réponse

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

Les composantes de l'AH doivent être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée. Les journaux d'évènements sont contrôlés régulièrement afin d'identifier des anomalies liées à des tentatives en échec. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

Pour l'analyse, les règles suivantes s'appliquent :

- Mettre en œuvre des contrôles de détection et de prévention sous le contrôle de l'OSC pour protéger les systèmes UH contre les virus et logiciels malveillant ;
- Documenter et suivre un processus de correction de la vulnérabilité qui traite de l'identification, l'examen, la réponse, et la résolution des vulnérabilités ;
- Effectuer une analyse de vulnérabilité (i) après tout changement de système ou réseau suivant la décision de la PMA qui décide si les changements sont importants pour les UH, et (ii) au moins une fois par semaine, sur les adresses IP publics et privés identifiés par les systèmes de l'UH ;
- Effectuer un test de pénétration sur les systèmes de l'UH sur au moins une base annuelle et suite à une modification de l'infrastructure ou des applications qui sont jugées important par la PMA pour l'AH ;
- Enregistrer les preuves de la réalisation des analyses de vulnérabilités et des tests de pénétration ;
- Enregistrer les preuves de la réalisation des analyses de vulnérabilités et des tests de pénétration ; par des personnes qualifiées, avec des outils adéquates, et suivant une démarche indépendante afin de garantir la qualité et la pertinence des analyses et des tests ;
- Procéder à une veille sur les vulnérabilités et les résoudre en fonction de la politique de sécurité de l'OSC et de l'analyse de risque de l'OSC.

6.3.2.4 Procédures de fonctionnement et responsabilités

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

- Les procédures opérationnelles du Service d'horodatage ;
- La planification et l'évaluation des systèmes sécurisés ;
- La protection vis-à-vis de 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 de logiciel.

Ces opérations doivent être gérées par du personnel de confiance de l'Autorité d'horodatage, mais, peuvent aussi être exécutées par du personnel opérationnel non-spécialiste (sous surveillance), comme défini dans la politique de sécurité appropriée et, les documents sur les rôles et les responsabilités.

6.3.2.5 Gestion d'Accès au Système

L'AH garantit que l'accès aux UH est limité aux individus dûment autorisés. En particulier :

- Des contrôles (pares-feux - firewalls, …) sont mis en œuvre pour protéger le réseau interne de l'AH d'accès non autorisés ncluant l'accès par des Clients et des tierces personnes (Vérificateurs de contremarques de temps entre autres) ;
- Les pares-feux (firewalls) sont configurés pour bloquer tous les protocoles et les accès non nécessaires au fonctionnement de l'Autorité d'horodatage ;
- L'AH garantit une administration efficace des rôles de confiance (cela inclut les opérateurs, les administrateurs et les auditeurs), pour maintenir la sécurité de l'UH, y compris la gestion des comptes des rôles de confiance, l'audit, et la modification ou le retrait rapide d'accès ;
- L'AH garantit que l'accès aux fonctions de l'UH, à l'information et aux applications est limité conformément à la politique de contrôle d'accès et que l'UH possède les contrôles informatiques de sécurité suffisants pour la séparation des rôles de confiance identifiés, y compris la séparation des fonctions d'administrateur de sécurité et des fonctions opérationnelles ;
- Le personnel de l'AH est correctement identifié et authentifié avant d'utiliser des fonctions de l'UH ;
- Le personnel de l'AH sera tenu responsable de ses activités en conservant des fichiers d'audit ;
- L'AH garantit que des composants de réseau locaux (par exemple les routeurs) ont mis dans un environnement physiquement sûr et que leurs configurations sont périodiquement vérifiées ;
- Une surveillance permanente et des équipements d'alarme sont mis en œuvre 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.

6.3.2.6 Déploiement et Maintenance

L'AH emploiera des produits et systèmes de confiance qui permettent aux l'UH de répondre aux exigences du chapitre IX de la [PH RGS].

En particulier :

- 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'AH pour assurer que la sécurité fait partie du système d'information ;
- Des procédures de contrôle de changement sont appliquées pour les nouvelles versions, les modifications et les corrections d'anomalies de n'importe quel logiciel opérationnel.

6.3.3 Exigences organisationnelles

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

- L'AH emploie un personnel qui possède l'expertise, l'expérience et les qualifications nécessaires pour les services offerts, tels que l'exige la fonction ;

- 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 ;
- 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 indiquer le type de vérification à effectuer sur le personnels, le type de formation appropriée et les particularités de la fonction ;
- Le personnel met en œuvre les procédures de fonctionnement et d'administration de l'UH définies par l'AH ;
- le personnel de gestion employé possède :
    - La connaissance de la technologie de l'horodatage ;
    - La connaissance de technologie de la signature électronique ;
    - La connaissance des mécanismes pour le calibrage ou la synchronisation des horloges des unités d'horodatage avec le temps UTC ;
    - Pour le personnel avec des responsabilités de sécurité, une bonne connaissance des procédures de sécurité et une expérience dans le domaine de la sécurité de l'information et de l'évaluation des risques ;
- Tout le personnel de l'AH dans des rôles de confiance doit être libre de conflit d'intérêt qui pourrait porter préjudice à l'impartialité des opérations de l'AH ;
- Les rôles de confiance incluent les rôles qui impliquent les responsabilités suivantes :
    - Le responsable de sécurité : responsabilité complète d'administrer la mise en œuvre et la configuration des rôles pour les PH et les DPH ;
    - Les Administrateur système : responsables pour installer, faire fonctionner les UH de l'AH de manière quotidienne et autorisés à effectuer les opérations de sauvegarde ;
    - Les Administrateur UH : 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 : autorisés à consulter les archives et les fichiers d'audit des AH ;
- Le personnel de l'AH est formellement nommé aux rôles de confiance par DocuSign France ;
- L'AH 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. Quand cela est nécessaire, ces descriptions de fonctions font la différence entre les fonctions générales et les fonctions spécifiques à l'AH.

6.4 Exigences de sécurité techniques

6.4.1 Exactitude temps

L'exactitude de temps des AH de DocuSign France est de 1 seconde par rapport au temps UTC. La précision des horloges des UH est assurée par le mécanisme de synchronisation de l'horloge d'UH avec les sources de temps.

Le mécanisme de synchronisation des UH garanti que l'horloge des UH :

- Délivrent une Date et une heure avec la précision de 1 seconde par rapport au temps UTC ;
- Est uniquement synchronisée par rapport à plusieurs types de sources de temps externes.

6.4.2 Génération de clé

La génération des bi-clés cryptographiques des UH est réalisée à l'aide de ressources cryptographiques matérielles (RCM). A aucun moment, lors de cette génération, les clés privées d'UH ne sont exportées des RCM.

La génération de bi-clés est effectuée par des personnels habilités de DocuSign France et dûment affectés à cette tâche, dans des zones dédiées et sous double contrôle minimum.

L'activation de la clé privée d'UH est contrôlée par au moins 2 personnes détenant des données d'activations et qui sont dans des rôles de confiance. Les personnes de confiance participant à l'activation de la clé privée d'UH font l'objet d'une authentification forte. L'UH est activée dans un boîtier cryptographique afin qu'elle puisse être utilisée par les seul rôles de confiances qui peuvent émettre des certificats.

Les clés privées d'UH ont une longueur de 2048 bits pour l'algorithme RSA au minimum. Cette longueur est fixée en accord avec les recommandations issues de l'ANSSI et précisées dans le document [CRYPTO]. Elle pourra être revue si les recommandations faites sont amenées à évoluer.

La RCM est certifiée :

- OID 1.3.6.1.4.1.22234.2.6.5.1 : FIPS 140 - 2 level 2 ;
- OID 1.3.6.1.4.1.22234.2.6.5.3, 1.3.6.1.4.1.22234.2.6.5.4, 1.3.6.1.4.1.22234.2.6.5.5, 1.3.6.1.4.1.22234.2.6.5.6 et 1.3.6.1.4.1.22234.2.6.5.7 : EAL4+ qualifié renforcé selon le schéma de l'ANSSI ou FIPS 140 – 2 level 3.
- OID 1.3.6.1.4.1.22234.2.6.5.8 : EAL4+ qualifié renforcé selon le schéma de l'ANSSI.

6.4.3 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.

L'AH s'assure qu'une demande de certificat d'UH auprès d'une 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'unité d'horodatage pour laquelle la demande de certificat est faite ;
- La valeur de la clé publique (et l'identifiant de l'algorithme) ;
- La durée d'utilisation souhaitée pour la clé privée.

L'AH vérifie, lors de l'import du certificat de l'UH, qu'il provient bien de l'AC auprès de laquelle la demande de certificat a été effectuée. L'AH s'assure que l'UH n'est opérationnelle qu'une fois ces exigences remplies.

Les dates de validité des certificats d'UH sont clairement indiquées dans les certificats d'UH et font l'objet d'une attention particulière de l'AH. Un certificat d'UH reste valide au-delà de la durée d'utilisation opérationnelle de la clé privée associée à la clé publique qu'il certifie.

6.4.3.1 OID 1.3.6.1.4.1.22234.2.6.5.1.1 et 1.3.6.1.4.1.22234.2.6.5.4

Il y a deux AC qui émettent les certificats d'UH pour cette OID :

- L'AC KEYNECTIS KH dont les informations sont les suivantes :
  - Identité de l'AC :
    - CN = AC_KEYNECTIS_KH
    - OU = Autorite de Certification Horodatage
    - O = KEYNECTIS
    - C = FR
  - La CLR est disponible à : http://trustcenter-crl.certificat2.com/KEYNECTIS/AC_KEYNECTIS_KH.crl ;

- Bi-clé et certificat de l'AC : RSA 2048 et SHA-1 ;
- Empreinte de la clé publique de l'AC « KEYNECTIS_KH » : 07 b5 ca d7 9a eb 16 5d ea 0c 3a 90 f2 29 42 52 c8 ca b8 e1 ;

- L'AC CDS CA dont les informations sont les suivantes :
  - Identité de l'AC :
    - CN = KEYNECTIS CDS CA
    - OU = KEYNECTIS for Adobe
    - O = KEYNECTIS
    - C = FR
  - La CLR est disponible à : http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_CDS_CA.crl ;
  - Bi-clé et certificat de l'AC : RSA 2048 et SHA-1 minimum ;
  - Empreinte de la clé publique de l'AC « CDS CA » : 9f 22 78 d7 71 1b de 33 b0 7f c9 20 7a a9 a8 e0 4e 62 e3 fb ;
  - Empreinte de la clé publique de l'AC Racine Adobe : 82 b7 38 4a 93 aa 9b 10 ef 80 bb d9 54 e2 f1 0f fb 80 9c de.

Les certificats d'UH, conformément à la PC de l'ACH, contiennent les extensions suivantes pour définir l'usage de la clé privée :

- « Key Usage » : « digitalSignature » et « nonRepudiation » ;
- « Extended Key Usage » : qui ne contient que l'identifiant « timeStamping ».

6.4.3.2 OID 1.3.6.1.4.1.22234.2.6.5.3, 1.3.6.1.4.1.22234.2.6.5.5, 1.3.6.1.4.1.22234.2.6.5.6, 1.3.6.1.4.1.22234.2.6.5.7 et 1.3.6.1.4.1.22234.2.6.5.8

L'AC qui émet les certificats d'UH est la suivante :

- Identité de l'AC :
  - C = FR
  - O = Keynectis
  - OU = 0002 478217318
  - OU = Keynectis CDS
  - CN = Keynectis CDS CA for timestamping
- OID de la PC : 1.3.6.1.4.1.22234.2.8.3.5 ;
- Chemin de certification est disponible à l'URL : https://www.docusign.fr/societe/politiques-de-certifications ;
- La CLR pour vérifier le certificat de l'AC est disponible à :
  - URL= http://get-crl.certificat.com/public/opentrustcaforaatlg1.crl ;
- La CLR pour vérifier le certificat de l'UH est disponible à :
  - http://trustcenter-crl.certificat2.com/Keynectis/Keynectis_CDS_CA_for_timestamping.crl ;
- La PC est disponible à : https://www.docusign.fr/societe/politiques-de-certifications ;
- Bi-clé et certificat de l'AC : RSA 2048 et SHA-2 ;

- Empreinte de la clé publique de l'AC « Keynectis CDS CA for timestamping » : 5f a8 71 60 bf 55 89 58 b5 e3 ed 20 99 e1 67 37 48 a9 b1 e1 ;
- Empreinte de la clé publique de l'ACI « OpenTrust CA for AATL G1 » : 78 7f 6e 54 aa cc e8 38 b8 fd 27 c6 e7 85 15 c1 05 87 8d 16 ;
- Empreinte de la clé publique de l'ACR « OpenTrust Root CA G1 » : 97 46 21 57 21 35 da 36 55 c7 f3 f1 37 70 e5 08 f6 93 29 b6 ;

Le DN (identité) de l'UH est construit de la manière suivante :

- C = FR
- O = DocuSign France
- 2.5.4.97 (OI) = VATEU-FR71812611150
- OU = 0002 812611150
- Dans les certificats de test on trouve en plus : OU = FOR TEST PURPOSES ONLY ;
- CN =
    - UH Qualifiee : nom UH - AAAAMMJJ ;

Le certificat de l'UH est signé en SHA-2.

Les certificats d'UH, conformément à la PC de l'ACH, contiennent les extensions suivantes pour définir l'usage de la clé privée :

- « Key Usage » : « digitalSignature » ;
- « Extended Key Usage » : qui ne contient que l'identifiant « timeStamping ».

6.4.4 Protection des clés privées des unités d'horodatage

L'AH garantit que des clés privées des UH restent confidentielles et conservent leur intégrité.

La RCM est certifiée :

- OID 1.3.6.1.4.1.22234.2.6.5.1 : FIPS 140 - 2 level 2 ;
- OID 1.3.6.1.4.1.22234.2.6.5.3, 1.3.6.1.4.1.22234.2.6.5.5, 1.3.6.1.4.1.22234.2.6.5.6 et 1.3.6.1.4.1.22234.2.6.5.7 : EAL4+ qualifié renforcé selon le schéma de l'ANSSI ou FIPS 140 – 2 level 3.
- OID : 1.3.6.1.4.1.22234.2.6.5.8 : EAL4+ qualifié renforcé selon le schéma de l'ANSSI.

Les clés d'UH sont générées, activées et stockées dans des ressources cryptographiques matérielles ou sous forme chiffrées. Quand elles ne sont pas stockées dans des ressources cryptographiques ou lors de leur transfert, les clés privées d'UH sont chiffrées au moyen de l'algorithme conforme à [CRYPTO]. Une clé privée d'UH chiffrée ne peut être déchiffrée sans l'utilisation d'une ressource cryptographique matérielle et la présence de multiples personnes dans des rôles de confiance.

Les clés privées des UH font l'objet d'un suivi unitaire pendant toute la durée de leur vie.

Les supports des clés privées d'UH sont positionnés dans des lieux et opérés dans des systèmes dont les accès physique et logique sont contrôlés et protégés.

6.4.5 Exigences de sauvegarde des clés des unités d'horodatage

La bi-clé d'UH est sauvegardée sous le contrôle de plusieurs personnes à des fins de reprise d'activité. Les sauvegardes des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles. Les sauvegardes sont rapidement transférées sur site sécurisé de sauvegarde délocalisé afin de fournir et maintenir la capacité de reprise d'activité de l'UH. Les sauvegardes de clés privées d'UH sont stockées dans des ressources cryptographiques matérielles ou sous forme de fichier chiffrée avec des algorithmes conformes à [CRYPTO].

Les opérations de chiffrement et de déchiffrement doivent être 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.

6.4.6 Destruction des clés des unités d'horodatage

L'AH garantit que les clés de signature des UH sont détruites à la fin de leur cycle de vie.

Cette opération est effectuée par des rôles de confiance de manière sécurisée et seulement dans les locaux du PSHE.

Les clés privées d'UH sont détruites quand elles ne sont plus utilisées ou quand les certificats auxquels elles correspondent sont expirés ou révoqués. La destruction d'une clé privée implique la destruction des copies de sauvegarde, des données d'activation et l'effacement de la ressource cryptographique qui la contient, de manière à ce qu'aucune information ne puisse être utilisée pour la retrouver.

6.4.7 Algorithmes obligatoires

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

- Accepte des valeurs de hachage générées par des clients et employant les algorithmes de hachage conformes aux exigences des autorités compétentes en la matière comme par exemple [CRYPTO].
- Génère des Contremarques de temps signées avec l'algorithme et les longueurs de clé conformes aux exigences de l'ANSSI [CRYPTO] :
    - OID 1.3.6.1.4.1.22234.2.6.5.1 : SHA-1 minimum ;
    - OID 1.3.6.1.4.1.22234.2.6.5.3, 1.3.6.1.4.1.22234.2.6.5.5, 1.3.6.1.4.1.22234.2.6.5.6, 1.3.6.1.4.1.22234.2.6.5.7 et 1.3.6.1.4.1.22234.2.6.5.8 : SHA-256.

6.4.8 Vérification des contremarques de temps

Pendant la durée de validité des certificats d'UH, l'AH garantit que les Vérificateurs de contremarques de temps peuvent avoir accès à l'information utilisable pour vérifier la signature numérique des contremarques de temps. En particulier :

- Les certificats des AC sont disponibles sur le site internet de DocuSign France : https://www.docusign.fr/societe/politiques-de-certifications ;
- Les certificats des UH sont joints à la contremarque de temps si l'Application utilisatrice le demande dans la Demande de contremarque de temps ;
- Les certificats du chemin de certification qui sont utilisables pour valider un certificat d'UH sont publiés par l'AC (se reporter au § 6.4.3) ;
- Les informations de révocations des certificats d'UH et d'AC sont publiées par l'AC (se reporter au § 6.4.3).

Pendant la durée de validité des certificats d'UH et suite à la fin de validité des certificats d'UH, le Vérificateur vérifie régulièrement que les algorithmes et les paramètres cryptographiques qui ont été utilisés le jour de l'émission de la Contremarque de temps sont toujours valides.

Suite à la fin de la validité de tous les certificats utilisés pour une Contremarque de temps, l'AH ne s'engage plus sur les informations nécessaires à la validation de la signature de cette Contremarque de temps.

6.4.9 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 ;
- Fin de validité du certificat d'AC qui l'a émis.

6.4.9.1 OID 1.3.6.1.4.1.22234.2.6.5.1

L'AC « KEYNECTIS KH » émet des certificats d'UH d'une durée de 11 ans maximum.

6.4.9.2 OID 1.3.6.1.4.1.22234.2.6.5.3, 1.3.6.1.4.1.22234.2.6.5.5, 1.3.6.1.4.1.22234.2.6.5.6, 1.3.6.1.4.1.22234.2.6.5.7 et 1.3.6.1.4.1.22234.2.6.5.8

L'AC « Keynectis CDS CA for timestamping » émet des certificats d'UH d'une durée de 6 ans maximum.

6.4.10 Durée d'utilisation des clés privées des unités d'horodatage

La durée d'utilisation d'une clé privée d'UH 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. La durée d'utilisation de la clé privée peut être définie soit au moment de l'initialisation du boîtier de l'unité d'horodatage, soit en définissant cette durée dans le certificat avec l'extension « PrivateKeyUsagePeriod ».

L'AC émet des certificats d'UH dont la durée d'utilisation de la clé privée est d'une durée de 1 an. Cette information est portée dans le certificat d'UH dans l'extension « PrivateKeyUsagePeriod ».

7 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

Les documents référencés sont les suivants :

- [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 ;
- [ORDONNANCE] : Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électronique entre les usagers et les autorités administratives et entre les autorités administratives ;
- [DécretRGS] : Décret relatif à l'Ordonnance n° 2005-1516 du 8 décembre 2005 ;
- [RGS] : Référentiel Général de Sécurité – Arrêté ou version de travail publiée. ;
- [PROG_ACCRED] : COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – version publiée cf. www.cofrac.fr.

8 ANNEXE 2 : FORMATS DES CONTREMARQUES DE TEMPS

Les contremarques de temps fournies par les AH respectant les présentes PH ont une structure `TimeStampToken` conforme au [RFC3161].

Le tableau ci-dessous reprend l'ensemble des champs d'un `TimeStampToken` tels que définis dans le [RFC3161]. Une contremarque de temps conforme à la PRIS respecte, de base, les exigences correspondantes du [RFC3161], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

De plus, toutes les contremarques de temps contiennent l'empreinte du certificat de l'UH, le numéro de série du certificat de l'UH et le DN complet de l'AC qui a émis le certificat d'UH.

Champ	**Exigences**
version	1
policy	OID de la PH applicable
messageImprint	Contient l'identifiant de l'algorithme d'empreinte utilisé par l'Application pour calculer une représentation de la donnée à horodater.
serialNumber	Renseigné par l'UH avec numéro de série unique.
genTime	Contient la date et l'heure UTC
accuracy	Non présent.
ordering	Ce champ est absent et donc non renseigné.
nonce	Renseigné seulement si l'Application utilisatrice transmet une valeur pour ce champs qui est en ce cas reprise à l'identique dans ce champs.
tsa	Non renseigné.
extensions	Aucunes extensions renseignées.