Qualification eIDAS 2017

Dossier Horodatage

Section Politiques et pratiques

Politique d'Horodatage du service ClearBUS

Version	Date	Description	Auteurs	Société
1.0	27/04/2018	Rédaction initiale	Céline Burgod	**ClearBUS**
1.1	28/05/2018	Intégration des commentaires	Guy Dubrisay	**ClearBUS**
1.2	23/07/2018	Corrections suite à l'audit	Céline Burgod	**ClearBUS**
1.3	11/09/2018	Modification du PSCE	Céline Burgod	**ClearBUS**
1.4	10/12/2018	Modification du profil de certificat cachet d'UH	Céline Burgod	**ClearBUS**
1.5	11/02/2020	Modification relative à la certification des modules cryptographiques	Céline Burgod	**ClearBUS**
1.6	25/03/2020	Modification OID politique de certification	Céline Burgod	**ClearBUS**
1.7	12/02/2022	Corrections mineures	Céline Burgod	**ClearBUS**
1.8	05/01/2024	Mise à jour des références	Céline Burgod	**ClearBUS**
1.9	28/03/2025	Mise à jour des références (RFC 5816)	Céline Burgod	**ClearBUS**

Etat du document	**Classification**
Final	C1
OID du document	
1.3.6.1.4.1.38116.1.1.1.2	
Diffusion	
Document public	

SOMMAIRE

1 INTRODUCTION

1.1 Présentation générale

ClearBUS met en œuvre un service d'échange de courrier numérique qui nécessite l'horodatage des différentes transactions pour assurer aux utilisateurs du service un niveau de garantie non répudiable. La règlementation en vigueur amène **ClearBUS** à faire qualifier son service de Recommandé Electronique (au sens du règlement eIDAS) ce qui exige corrélativement une qualification de son horodatage. Ce service postal numérique est appelé « **ClearBUS-SRE** » dans la suite du document.

ClearBUS se positionne dans ce contexte en tant qu'Autorité d'Horodatage (ci-après « AH ») et délivre des jetons d'horodatage pour les besoins de **ClearBUS-SRE**. La solution d'Horodatage est mise en œuvre par les équipes techniques **ClearBUS**, qui se positionnent alors comme Prestataire de Service d'Horodatage Electronique (**ClearBUS-SHE**) pour **ClearBUS-SRE**.

Le présent document constitue la politique d'horodatage de **ClearBUS-SHE** (ci-après « PH ») présentant ce service d'horodatage.

Dans le cadre de la présente PH, le principal utilisateur du service d'horodatage est le service **ClearBUS-SRE** lui-même, pour la gestion des courriers à un niveau secondaire, les jetons délivrés par **ClearBUS-SHE** sont également utilisés pour horodater les différents logs produits par les systèmes et sous-systèmes de **ClearBUS**.

L'objectif de ce document est de définir les engagements que **ClearBUS-SHE**, en tant qu'AH, respecte dans la délivrance et la gestion de jetons d'horodatage. Le respect de ces engagements démontre à l'ensemble des utilisateurs du service Postal **ClearBUS** la qualité et le niveau de sécurité du marquage temporel des transactions réalisées.

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

Une DPH expose les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la PH, en particulier les processus qu'une Unité d'Horodatage (« UH ») emploiera pour la création des jetons d'horodatage et le maintien de l'exactitude de ses horloges. L'AH **ClearBUS-SRE** peut mettre en œuvre plusieurs UH pour supporter son service d'horodatage.

Cette PH n'impose pas d'exigences sur le lien entre l'empreinte numérique à horodater et le contenu de la donnée électronique qui en est à l'origine. Cette vérification est à la charge du service **ClearBUS-SRE**.

L'Autorité d'Horodatage se conforme aux normes [EN_319401] et [EN_319421] et met en œuvre des profils de jetons d'horodatage conformes à [EN_319422].

En sus et dans le cadre de la qualification eIDAS de son service d'horodatage en France, l'AH se conforme également aux exigences prévues par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) dans les référentiels suivants :

- [PSCO_QUALIF]
- [PSCO_HORO]

1.2 Gestion du document

1.2.1 Identification du document

La présente « Politique d'Horodatage **ClearBUS** » est identifiée, au sein du référentiel documentaire de l'infrastructure de confiance **ClearBUS**, par un numéro d'identification unique, l'OID : **1.3.6.1.4.1.38116.1.1.1.2.**

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

D'autres éléments, plus explicites, (nom, numéro de version, date de mise à jour) permettent également de l'identifier.

1.2.2 Publication du document

Avant toute publication officielle, la Politique d'Horodatage est validée par le Comité d'Approbation **ClearBUS-SHE**.

La présente Politique d'Horodatage est publiée sur l'URL : https://www.clearbus.fr/Telechargement/PH_Clearbus_1.3.6.1.4.1.38116.1.1.1.2.pdf.

L'ensemble des informations associées notamment les versions antérieures publiques de ces documents, sont également publiées sur le site interne à la société **ClearBUS**. Les versions antérieures publiques peuvent être fournies sur requête effectuée par courriel à l'adresse suivante : horodatage@clearbus.fr.

1.2.3 Composition du comité d'approbation

Le Comité d'Approbation est composé de membres dirigeants de **ClearBUS** et des experts techniques du service **ClearBUS-SHE** couvrant les compétences de sécurité, réseaux, systèmes nécessaires au service d'horodatage.

Ce Comité approuve la présente Politique d'Horodatage.

1.2.4 Processus de mise à jour

1.2.4.1 Circonstances rendant une mise à jour nécessaire

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

La Politique d'Horodatage est réexaminée à minima tous les deux (2) ans.

1.2.4.2 Prise en compte des mises à jour

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

horodatage@clearbus.fr

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

1.2.4.3 Information des acteurs

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

Indépendamment de ce mode de communication, les acteurs peuvent à tout moment se renseigner auprès du Comité d'Approbation pour obtenir plus d'informations, en envoyant un courriel à horodatage@clearbus.fr.

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

- Document au format PDF ;
- OID du document ;
- Date et heure exacte d'entrée en vigueur.

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

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

Lorsqu'une nouvelle version de la Politique d'Horodatage est mise en ligne, tous les utilisateurs des infrastructures d'horodatage de **ClearBUS-SHE** sont informés de la nature, de la date et de l'heure du changement, par courriel ou via une publication officielle sur le site www.clearbus.fr.

La nouvelle version de la Politique d'Horodatage entre en vigueur après sa mise en ligne et reste valide jusqu'à l'entrée en vigueur d'une nouvelle version.

1.2.6 Cohérence de la documentation

Cette Politique d'Horodatage décrit le contexte de production de jetons d'horodatage et, de fait, ne constitue qu'une brique du référentiel documentaire de **ClearBUS-SHE**.

Le Comité d'Approbation s'assure de la cohérence de ce référentiel documentaire et de l'adéquation de la présente Politique d'Horodatage avec les autres documents.

1.3 Principe du service d'horodatage ClearBUS-SHE

Un jeton d'horodatage permet d'attester de la réalité, à une date et une heure donnée, de l'existence d'une empreinte numérique (ou « hash ») qui est soumise au service d'horodatage. Les jetons d'horodatage sont délivrés et signés électroniquement par l'AH à l'aide d'Unité(s) d'Horodatage.

La garantie de cette association est fournie au moyen d'un jeton d'horodatage qui est une structure signée qui contient en particulier :

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

Les certificats installés sur les unités d'horodatage du service **ClearBUS-SHE** sont émis par l'AC CertEurope eID Corp, dont la Politique de Certification est consultable à l'adresse suivante : https://www.certeurope.fr/chaine-de-confiance/.

Dans le cadre de cette PH, la date et le temps de chaque jeton d'horodatage sont synchronisés avec le temps UTC avec une précision d'une (1) seconde. La présente PH applique un format de jeton d'horodatage standard défini par les [RFC_3161, RFC_5816]. La gestion de la synchronisation de l'horloge du service d'horodatage est détaillée au chapitre 6.2.4.

1.4 Etablissement de la confiance dans le service ClearBUS-SHE

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

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

Les jetons d'horodatage émis par le service **ClearBUS-SHE** sont demandés et à destination du service **ClearBUS-SRE,** ou à destination de ses différents sous-systèmes pour l'horodatage des logs. Les Unités d'Horodatage mises en œuvre par **ClearBUS** ne délivrent pas de jetons d'horodatage pour des applications externes à **ClearBUS**.

1.5 Entités intervenant dans le service d'horodatage

ClearBUS est le responsable de l'Autorité d'Horodatage qui est exploitée et maintenue en condition opérationnelle par ses équipes techniques.

L'Autorité d'Horodatage utilise dans son service d'horodatage des serveurs de temps reliés aux serveurs UTC(k) qui font référence en la matière et qui assurent un niveau de performance conforme aux exigences exprimées dans [EN_319421]. La solution d'horodatage **ClearBUS-SHE** met en œuvre des mécanismes de contrôle, notamment au niveau de la gestion de la dérive et de la précision de temps fournies dans les jetons d'horodatage.

ClearBUS-SHE installe des certificats électroniques sur ses UH émis par l'AC CertEurope. Cette AC est qualifiée conforme à [EN_319411-2] pour le profil « Cachet ».

La représentation schématique est alors la suivante :

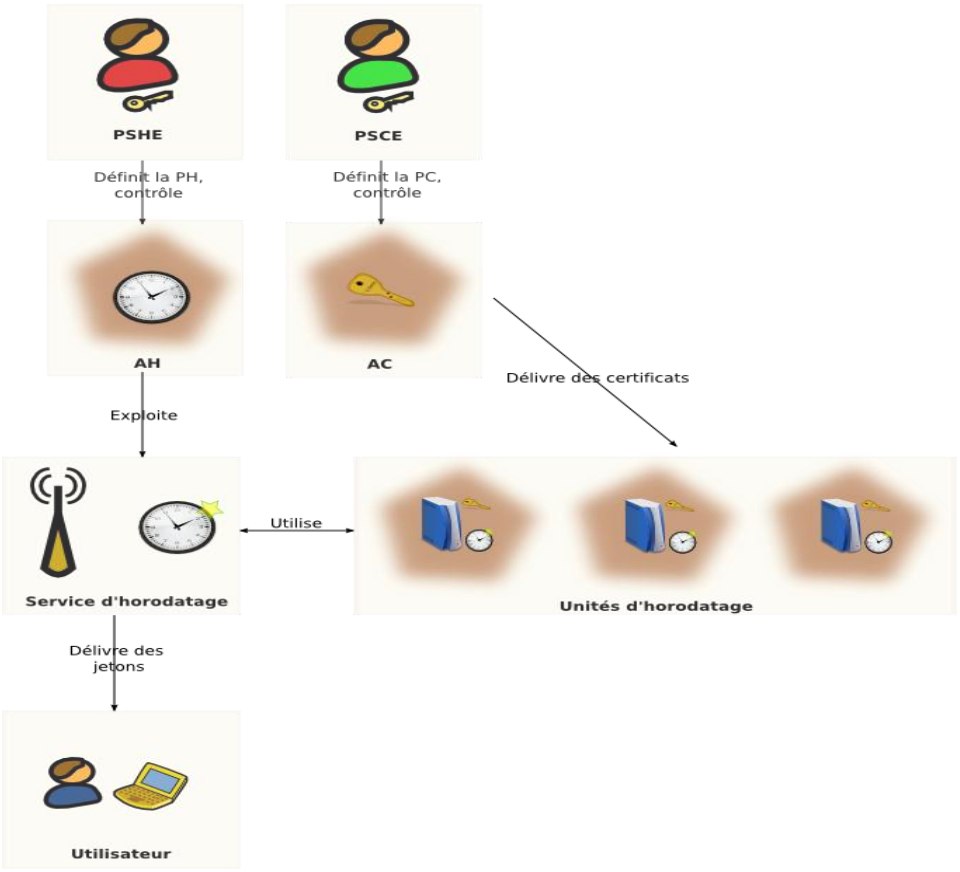

Figure 1 - Entités intervenant dans le service d'horodatage

Les rôles se répartissent de la manière suivante :

	Applications Utilisatrices
PSHE	Service **ClearBUS-SRE** et sous-systèmes (log)
ClearBUS-SHE	
PSCE	Unités d'Horodatage **ClearBUS-SHE**
AC **CertEurope**	

1.6 Autres aspects

Les unités d'horodatage utilisent des boîtiers cryptographiques matériels pour générer et stocker les clés privées des certificats électroniques de signature de jeton d'horodatage. Ces boitiers sont certifiés Critères Communs pour le niveau d'assurance EAL4+.

2 GENERALITES

2.1 Définitions

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

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

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

Certification (qualification) d'un prestataire de services - Le règlement européen n°910/2014 permet à un PSCO d'être contrôlé sur ses pratiques de manière à être certifié pour que les services qu'il fournit soient dits « qualifiés ».

Contremarque de temps - Voir jeton d'horodatage.

Coordinated Universal Time (UTC) - Echelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5.

Nota - Pour la plupart des usages, le temps UTC est équivalent au temps solaire au méridien principal (0°). De manière plus précise, le temps UTC est un compromis entre le temps atomique particulièrement stable (Temps Atomique International -TAI) et le temps solaire dérivé de la rotation irrégulière de la terre lié au temps moyen sidéral de Greenwich (GMST) par une relation de convention.

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

Demande de jeton d'horodatage - Désigne la requête qui est soumise par un utilisateur à l'AH pour l'émission d'un jeton d'horodatage. Cette requête contient au minimum l'empreinte numérique à horodater.

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

Jeton d'horodatage - Donnée signée qui lie une représentation d'une donnée à un temps particulier, exprimé en heure *UTC*, établissant ainsi la preuve que la donnée existait à cet instant-là.

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

Module d'horodatage - Produit de sécurité comportant une ressource cryptographique et qui est dédié à la mise en œuvre des fonctions d'horodatage de l'UH, notamment la génération, la conservation et la mise en œuvre de la clé privée de signature de l'UH ainsi que la génération des jetons d'horodatage.

Politique de Certification (PC) - Désigne l'ensemble des règles et engagements énoncées et publiées par l'AC décrivant les caractéristiques générales des services de certification et des certificats d'UH qu'elle délivre.

Politique d'horodatage (PH) - Ensemble de règles, identifié par un nom (*OID*), définissant les exigences auxquelles une AH se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un jeton d'horodatage à une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes. Une PH peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les utilisateurs de jetons d'horodatage.

Précision - Désigne la différence maximale autorisée entre la date et l'heure UTC fournie par la source de temps externe et la date et heure de la source interne de l'UH qu'il utilise pour générer les jetons d'horodatage.

Prestataire de services de confiance (PSCO) – Le règlement européen n°910/2014 dit « règlement eIDAS » introduit et définit les prestataires de service de confiance (PSCO). Un prestataire de services de confiance est défini comme toute personne ou entité offrant des services tendant à la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique.

Prestataire de services d'horodatage (PSHE) - Un PSHE est un type de PSCO particulier. Un PSHE se définit comme toute personne ou entité qui est responsable de la génération et de la gestion de jetons d'horodatage, vis-à-vis des utilisateurs de ces jetons d'horodatage. Un PSHE peut fournir différentes familles de jetons d'horodatage correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSHE comporte au moins une AH mais peut en comporter plusieurs en fonction de son organisation. Un PSHE est identifié dans les certificats de clés publiques des UH dont il a la responsabilité au travers de ses AH.

Produit de sécurité - Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Référencement - Opération réalisée par l'ANSSI qui atteste que l'offre d'horodatage du PSCO est utilisable avec tous les systèmes d'information qui requièrent ce type d'offre. Une offre référencée peut être utilisée dans toutes les applications d'échanges dématérialisés requérant un service d'horodatage. Pour les utilisateurs, le référencement permet de connaître quelles offres d'horodatage ils peuvent utiliser pour quels échanges dématérialisés.

Ressource cryptographique - Désigne le produit de sécurité comportant une ressource cryptographique matérielle et qui est dédié à la mise en œuvre des fonctions

d'horodatage de l'UH, notamment la génération, la conservation et la mise en œuvre de la clé privée de signature de l'UH ainsi que la génération des jetons d'horodatage.

Service d'horodatage - Ensemble des prestations nécessaires à la génération et à la gestion de jetons d'horodatage.

Source de temps - Désigne la composante qui fournit une date et une heure (temps). On distingue deux sortes de sources de temps :

- La source de temps externe : Source extérieure au système d'information, qui fournit un temps UTC reconnu comme sûr (antenne GPS, onde radio, serveur NTP, ...) ;
- La source de temps interne : Source interne au système d'horodatage, qui fournit un temps (Cf. date et heure UH) sur la base d'éléments uniquement internes au système d'information.

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

Système d'horodatage - Ensemble des unités d'horodatage et des composants d'administration et de supervision utilisés pour fournir des services d'horodatage.

Unité d'Horodatage (UH) - Ensemble de matériel et de logiciel en charge de la création de jetons d'horodatage caractérisé par un identifiant de l'unité d'horodatage accordé par une AC, et une clé unique de signature de jetons d'horodatage.

UTC(k) - Temps de référence réalisé par le laboratoire "k" et synchronisé avec précision avec le temps UTC, dans le but d'atteindre une précision de ±100 ns, selon la recommandation S5 (1993) du Comité Consultatif pour la définition de la Seconde. (Rec. ITU-R TF.536-1).

Nota - Une liste des laboratoires UTC(k) est indiquée dans la section 1 de la Circulaire T publiée par le BIPM et est disponible sur le site web du BIPM (www.bipm.org).

Usager - Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et ayant souscrit ou utilisant le service **ClearBUS-SRE** pour relever son courrier numérique. Le dit service **ClearBUS-SRE** de courrier numérique est lui-même usager de jetons d'horodatage pour dater de façon fiable les étapes clef de l'acheminement.

Utilisateur de jetons d'horodatage – Entité (personne ou système) qui fait confiance à un jeton d'horodatage émis sous une politique d'horodatage donnée par une autorité d'horodatage donnée. Dans le cadre de la présente Politique d'Horodatage, l'utilisateur principal de jetons d'horodatage est le service de courrier numérique **ClearBUS-SRE**.

Utilisateur final - Utilisateur de jetons d'horodatage.

Vérification d'un jeton d'horodatage - Désigne l'action de l'utilisateur de jeton d'horodatage qui consiste à vérifier que le jeton est valide

2.2 Abréviations

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

AC	Autorité de Certification
AH	Autorité d'horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CGUH	Conditions Générales d'utilisation du service d'horodatage
Delta-LRC	Liste de Révocation des Certificats partielle
DPC	Déclaration des Pratiques de Certification
DPH	Déclaration des Pratiques d'Horodatage
ETSI	*European Telecommunications Standards Institute*
LCR	Liste des Certificats Révoqués
IGC	Infrastructure de Gestion de Clés
OID	*Object Identifier*
OSC	Opérateur de Service de Certification
OSH	Opérateur de Service d'Horodatage
PC	Politique de Certification
PH	Politique d'Horodatage
PP	Profil de Protection
PSHE	Prestataire de Services d'Horodatage
UH	Unité d'Horodatage
UTC	*Coordinated Universal Time*

3 POLITIQUE D'HORODATAGE

Pour cette politique, la date et le temps de chaque jeton d'horodatage doivent être synchronisés avec le temps *UTC* avec une exactitude d'une (1) seconde.

La présente PH impose un format de jeton d'horodatage spécifique, qui doit répondre aux exigences du chapitre 8.

Cette politique impose l'usage d'un protocole d'horodatage spécifique pour demander et obtenir un jeton d'horodatage auprès d'une AH définie dans [RFC_3161] et profilé dans le document [EN_319422].

Les caractéristiques principales de cette politique sont les suivantes :

- La protection des clés et de l'horloge doit respecter les exigences spécifiées par l'[EN_319421] ;
- A l'exception de copies de secours, la sauvegarde et l'import des clés privées sont interdits ;
- L'AC générant les certificats de clé publique pour les unités d'horodatage doit gérer le service de révocation pour chaque certificat publié.

4 DECLARATION DES PRATIQUES D'HORODATAGE

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

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

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

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

La déclaration des pratiques d'horodatage est toujours approuvée par le Comité **ClearBUS** en charge de ce service, avant la mise en production du service d'horodatage.

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

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

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

Ces informations publiques sont intégrées aux conditions générales d'utilisation du service d'horodatage (cf. 5).

5 CONDITIONS GENERALES D'UTILISATION

Compte tenu de la complexité de lecture d'une PH pour des utilisateurs non-spécialistes du domaine, l'AH définie également des conditions générales d'utilisation correspondant aux *« TSA Disclosure Statement » (TDS)* définis dans l'annexe B de [EN_319421].

Ces conditions générales d'utilisation ne sont pas destinées à remplacer la politique d'horodatage mais sont destinées à des utilisateurs de jetons d'horodatage non-techniciens afin qu'ils puissent facilement comprendre l'information essentielle dont ils doivent avoir connaissance.

Les conditions générales d'utilisation peuvent aider une Autorité d'horodatage à démontrer comment elle répond aux exigences réglementaires, en particulier celles liées à la protection du consommateur.

L'Autorité d'horodatage spécifie dans ses conditions générales d'utilisation les identifiants des politiques d'horodatage supportées.

L'Autorité d'horodatage définit ses propres conditions générales d'utilisation et les rend disponibles aux utilisateurs de jetons d'horodatage sous une forme lisible, compréhensible et pérenne. Ces CGUH sont complémentaires aux Conditions Générales de **ClearBUS** qui sont acceptées par ses clients, considérant qu'elles portent sur les conditions d'utilisation par ClearBUS-SRE des services offerts par ClearBUS-SHE

Malgré cette indirection, les CGUH peuvent être téléchargées sur le site www.clearbus.fr.

6 EXIGENCES RESPECTEES PAR L'AUTORITE D'HORODATAGE

6.1 Dispositions générales

6.1.1 Obligation de l'Autorité d'Horodatage

Vis-à-vis de la présente Politique, l'Autorité d'Horodatage :

- Génère et signe les jetons d'horodatage conformément à la PH ;
- Respecte et se conforme aux exigences et procédures définies dans la présente PH et dans les Conditions Générales d'Utilisation applicables ;
- Garantit que la mise en œuvre des exigences exprimées dans le présent document est faite conformément à ce qui est décrit dans sa Déclaration des Pratiques d'Horodatage ;
- Met à disposition l'ensemble des informations nécessaires permettant de vérifier les jetons d'horodatage qu'elle aura émises.

6.1.2 Obligation de l'Utilisateur de Jeton d'Horodatage

Le service courrier numérique **ClearBUS-SRE** tout comme les sous-systèmes utilisateurs :

- Vérifie que le jeton d'horodatage été correctement signé et que le certificat de l'UH est valide à l'instant de la vérification ;
- Identifie comme tels les jetons émis par **ClearBUS-SHE** ;
- Assume les limitations connues et documentées du service **ClearBUS-SHE** ;
- Détecte l'indisponibilité de **ClearBUS-SHE**, l'obligeant à mettre éventuellement en œuvre une solution de secours pour récupérer les jetons d'horodatage sur les UH d'un prestataire d'horodatage électronique qualifié.

Les jetons d'horodatage de secours sont émis par le prestataire d'horodatage qualifié Luxtrust, suivant la politique d'horodatage « LuxTrust Time Stamping V2 Policy » (OID : 1.3.171.1.1.1.10.8).

6.1.3 Obligations des Autorités de Certification fournissant des certificats aux Unités d'Horodatage

L'Autorité de Certification AC CertEurope délivrant des certificats aux unités d'horodatage fournit un service de révocation. Les engagements de l'AC CertEurope sont consultables à travers sa Politique de Certification (https://www.certeurope.fr/chaine-de-confiance/).

L'AC CertEurope met à disposition les informations de gestion des certificats, dont le statut de révocation des certificats. Les points de distribution des CRL (HTTP et LDAP) sont précisés dans la Politique de Certification correspondante, consultable à l'adresse suivante : https://www.certeurope.fr/chaine-de-confiance/.

L'AC CertEurope met également en œuvre un service OCSP exposé sur Internet.

L'AC CertEurope est qualifiée conforme à [EN_319411-2] pour le profil « Cachet ».

6.1.4 Déclaration des Pratiques d'Horodatage

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

- L'AH a rédigé une analyse des risques de son service d'horodatage ;
- L'AH adresse l'ensemble des exigences décrites dans la présente PH ;
- La DPH décrit toutes les exigences que doivent respecter les éventuelles tierces parties dans le cadre du service d'horodatage ;
- L'AH **ClearBUS-SHE** met à disposition de **ClearBUS-SRE**, qui aurait à répondre sur ce point à ses propres utilisateurs les données nécessaires à la validation des jetons d'horodatage, soit :
    - Les certificats de signature des unités d'horodatage ;
    - Les CRL de l'AC CertEurope ;
    - Le certificat de l'AC CertEurope ;
    - Toutes les versions des politiques d'horodatage avec leur date de validité.
- L'AH organise un audit interne pour attester que la DPH est conforme à la PH ;
- L'audit organisé par l'AH prend en compte le contrôle des mesures techniques, non techniques et organisationnelles ;
- L'AH garantit qu'elle mettra à jour la PH en cas de changements majeures des pratiques d'horodatage de son service ;
- L'AH publiera les nouvelles versions de la PH sur le site www.clearbus.fr ;
- L'AH garantit que tout changement majeur dans ses pratiques d'horodatage fera l'objet d'une notification auprès de l'organe de contrôle ayant délivré la qualification eIDAS du service d'horodatage.

6.1.5 Conditions Générales d'Utilisation d'Horodatage

L'AH **ClearBUS-SHE** définit des CGUH qui reprennent les grands principes décrits dans la présente PH. Ces CGUH sont basées sur le modèle défini dans l'annexe B de [EN_319421]. L'AH décrit dans ces CGUH les informations suivantes :

- Le cadre d'application des CGUH et le contexte global des engagements de l'AH via la PH et la DPH ;
- Les coordonnées de l'AH ;
- Les types et le cadre d'utilisation des jetons d'horodatage, en précisant notamment :
    - L'exactitude du temps fourni dans les jetons d'horodatage par rapport au temps UTC ;
    - Au moins un algorithme de hachage autorisé pour constituer l'objet horodaté ;
    - La période de temps minimum durant laquelle les jetons d'horodatage sont vérifiables par l'utilisateur de jetons d'horodatage, à compter de leur date de génération. Ce temps ne tient pas compte des éventuelles procédures de révocation du certificat d'une unité d'horodatage ;

- Les limites de confiance, notamment :
  - Les engagements sur la précision des jetons ;
  - La période de conservation des données d'audit ;
- Les obligations de **ClearBUS-SRE** en tant qu'Utilisateur, notamment :
  - Les informations nécessaires pour vérifier les jetons d'horodatage ;
- Les informations pour permettre la vérification du statut du certificat de l'UH ;
- Les limites de garantie et limites de responsabilité de l'AH ;
- La PH et la DPH appliquée :
- Les règles appliquées en matière de protection des informations confidentielles ;
- Les règles appliquées en termes d'assurance de l'AH ;
- Les lois applicables et les procédures de résolution des litiges ;
- Les niveaux de certifications et les audits obtenus par l'AH.

6.1.6 Conformité avec les exigences légales

6.1.6.1 Droit applicable

Le présent document est régi par la loi française.

6.1.6.2 Règlement des différends

Toutes contestations et litiges survenant dans l'interprétation et la mise en œuvre du présent document seront soumis à la juridiction des tribunaux dont ressort le siège social de **ClearBUS**.

6.1.6.3 Propriété intellectuelle des infrastructures

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

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

6.1.6.4 Données Personnelles

Le service d'horodatage ne traite pas de données personnelles nominatives. Les seules données transmises à **ClearBUS-SHE** sont une empreinte éventuellement calculée d'après les données traitées par le service **ClearBUS-SRE,** sinon bâtie sur des fichiers log. La forme de ces empreintes est représentative des données concernées, mais exclut toute information nominative.

6.2 Exigences opérationnelles

6.2.1 Gestion des requêtes

Les demandes de jetons d'horodatage sont traitées par les UH de l'AH **ClearBUS-SHE** exclusivement et selon le protocole défini par la [RFC_3161]. Ce protocole est conforme à [EN_319422].

Les usagers « personnes physiques », clients de **ClearBUS-SRE**, utilisent le service d'horodatage via le service **ClearBUS-SRE**. Opérationnellement, cette demande

d'horodatage est pilotée par le logiciel serveur du service **ClearBUS-SRE**, et elle consiste à effectuer une connexion en mode HTTP(S) vers le serveur d'horodatage.

Le logiciel **ClearBUS-SRE** produit un condensat (hash) des données à horodater, et les transmet au système d'horodatage sans authentification, le paramétrage initial des applications **ClearBUS** assumant la relation unique **ClearBUS-SRE** / **ClearBUS-SHE**.

Le service rendu aux sous-systèmes **ClearBUS** se situe fondamentalement au cœur de cette même relation.

L'AH **ClearBUS-SHE** génère le jeton d'horodatage à partir du condensat des données qui lui est transmis par le service demandeur (empreinte de la donnée à horodater) et la lui retourne. Le temps de réponse de **ClearBUS-SHE** est calibré en regard des exigences de performance prévues par le système.

L'AH **ClearBUS-SHE** ne conserve pas le jeton d'horodatage généré.

6.2.2 Fichiers d'audit

Les journaux du service d'horodatage sont conservés sur le serveur d'horodatage depuis sa mise en activité, et alimentent le système de Gestion des Incidents de ClearBUS.

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

- Tous les éléments sauvegardés sont décrits dans une politique d'archivage et de sauvegardes appliquée dans service d'horodatage ;
- Les événements sauvegardés sont protégés en intégrité et en confidentialité ;
- Tous les événements d'administration des serveurs d'horodatage sont tracés et conservés ;
- L'instant précis des événements est tracé ;
- Les événements d'audit sont conservés en sureté de manière à éviter les effacements et la perte de ces données ;
- Les informations nominatives sont conservées et protégées ;
- Tous les événements liés à la gestion du cycle de vie des clés d'horodatage sont tracés (création, renouvellement, destruction, installation sur une UH) ;
- Tous les événements liés à la gestion du cycle de vie des certificats d'horodatage sont tracés (création, renouvellement, destruction, installation sur une UH) ;
- Tous les événements liés à la gestion des serveurs de temps sont tracés (initialisation, dépassement de la dérive maximale, dépassement de la précision autorisée, synchronisation, saut de seconde) ;

6.2.3 Gestion de la durée de vie de la clé privée

Les clés des UH sont générées par **ClearBUS-SHE** qui respecte le chapitre 6.4.2. Les clés publiques correspondantes sont certifiées par l'AC CertEurope qui respecte les différentes clauses de sa PC et de sa DPC.

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

A la fin du contexte d'horodatage, la clé privée est détruite.

Les clés privées ne sont pas exportables.

6.2.4 Synchronisation de l'horloge

Le serveur d'horodatage est synchronisé avec sept (7) serveurs NTP différents sur Internet. La moyenne des informations obtenues détermine l'heure exacte. Les serveurs Internet utilisés sont les suivants :

- ntp-p1.obspm.fr – UTC(OP)
- ntp1.sptime.se – UTC(SP)
- ntp1.inrim.it - UTC(IT)
- hora.roa.es - UTC(ROA)
- ptbtime1.ptb.de - UTC(PTB)
- ntp2.oma.be - UTC(ORB)
- time.ufe.cz - UTC(TP)

ClearBUS assure la maintenance logicielle et matérielle du serveur d'horodatage dont le calibrage de l'horloge, les sauts d'horloge programmés, les synchronisations. Les équipes techniques de **ClearBUS** assurent la supervision de la solution d'horodatage avec l'appui de l'astreinte 24x7 du service d'hébergement, et de ses intervenants dûment identifiés.

L'Autorité d'Horodatage garantit que si une dérive de l'horloge supérieure à la limite fixée apparait, elle sera détectée.

L'Autorité d'Horodatage garantie la calibration des horloges en cas de saut de seconde.

En tout état de cause, les unités d'horodatage sont automatiquement interrompues dans les cas suivants :

- Le calibrage de l'horloge n'est plus respecté ;
- L'horloge est désynchronisée ;
- Le saut de seconde n'a pas été respecté.

L'interruption de service de **ClearBUS-SHE** est détectée par **ClearBUS-SRE** qui doit, pour bénéficier de la continuité de l'activité d'horodatage, mettre en œuvre une solution de secours pour récupérer les jetons d'horodatage sur les UH d'un prestataire d'horodatage qualifié.

6.2.5 Contenu d'un Jeton d'Horodatage

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

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

Les jetons d'horodatage émis par l'AH **ClearBUS** respectent, de base, les exigences correspondantes de [RFC_3161, RFC_5816], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Exigences	Elément contenant	
		Certificat	Jeton
version	1		X
Policy	OID de la PH		X
Pays de l'AH	FR	X	
AC Id	Identifiant de l'AC	X	
AH Id	Identifiant de l'AH	X	
UH Id	Identifiant de l'UH	X	
messageDigest	Condensat (hash) des données à horodater		X
serialNumber	Identifiant unique du jeton d'horodatage		X
GenTime	Heure de génération du jeton d'horodatage calculée par rapport à une source UTC(k)		X
accuracy	Contient la précision fournie par l'UH, égale à une (1) seconde		X
nonce	Identique à celui présenté lors de la demande de génération si celui-ci est présent dans cette dernière		X

Le jeton d'horodatage est signé par l'UH à l'aide du certificat délivré par l'AC CertEurope. Ce certificat et la clé privée correspondante sont utilisés exclusivement pour cet usage.

6.2.6 Compromission de l'Autorité d'Horodatage

La compromission de l'AH peut être due à :

- La compromission des clés privées des UH ;
- La compromission de la clé privée de l'AC CertEurope ayant servi à générer les certificats des UH ;
- Un problème d'exploitation entraînant la divulgation d'éléments secrets.

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

En tout état de cause, le service d'horodatage sera arrêté le temps que les équipes d'exploitation de **ClearBUS-SHE** ait pu remettre le service dans un état sûr ;

Le détail des actions enclenchées par ce type d'événements ainsi que les délais de remise en activité des services sont précisés dans les documents d'exploitation maintenus par **ClearBUS**.

En tout état de cause, l'AH **ClearBUS-SHE** :

- Mettra à disposition de **ClearBUS-SRE** et des utilisateurs du Service Postal **ClearBUS** une description de la compromission ou de la perte de synchronisation détectée ;
- Coupera l'unité d'horodatage suspectée de compromission ;
- Mettra à disposition quand cela est possible les éléments permettant d'identifier les jetons d'horodatage émis qui pourraient être compromis ou suspectés de compromission, à moins que cela ne contrevienne à la sécurité des services d'horodatage ;
- Préviendra dans un délai maximal de 24 heures le point de contact de l'ANSSI selon les modalités précisées sur le site https://cyber.gouv.fr.

6.2.7 Continuité d'activité

En cas de défaillance de **ClearBUS-SHE**, la continuité de l'activité est assurée par un prestataire d'horodatage électronique qualifié.

Les jetons de secours sont émis sous la politique d'horodatage en vigueur suivante : LuxTrust Time Stamping V2 Policy. L'OID de cette politique est : 1.3.171.1.1.1.10.8.

6.2.8 Fin d'activité

En cas de fin d'activité du service d'horodatage, **ClearBUS-SHE** :

- Fera prendre en compte par **ClearBUS-SRE** l'information de la cessation d'activité ;
- Abrogera l'ensemble des autorisations délivrées à des tiers dans le cadre du service d'horodatage ;
- Transfèrera à un organisme fiable les informations d'audit ;
- Fournira à un organisme fiable les informations nécessaires à la vérification des jetons d'horodatage ;
- Détruira les clés privées de toutes les unités d'horodatage de son service d'horodatage.

Le choix de l'organisme qui récupèrera les données d'audit sera défini dans le cadre du plan de fin d'activité mis en œuvre par l'AH **ClearBUS-SRE**.

L'AH préviendra dès que possible le point de contact précisé sur le site de l'ANSSI https://cyber.gouv.fr de la fin d'activité de son service d'horodatage.

ClearBUS prendra les mesures nécessaires pour provisionner financièrement cette fin d'activité.

6.3 Exigences physiques, environnementales, procédurales et organisationnelle

6.3.1 Exigences physiques et environnementales

6.3.1.1 Situation géographique et construction des sites

La localisation géographique du site ne nécessite pas de mesures particulières face à des risques de type tremblements de terre, explosion, risque volcanique ou crue.

6.3.1.2 Accès physique

L'accès physique aux fonctions d'horodatage (ceci comprend les fonctions de gestion des certificats des Unités d'Horodatage) est strictement limité aux seules personnes nominativement autorisées, personnel de ClearBUS ou personnel identifié du Service d'hébergement

L'accès physique au système d'horodatage supportant ces fonctions est limité aux seules personnes autorisées par la mise en place d'un périmètre de sécurité physique, permettant la séparation des rôles entre les différents intervenants, et par la mise en place d'un contrôle d'accès électronique par badge ou clé assumé par le Service d'hébergement

La traçabilité des accès est assurée par l'enregistrement des utilisations des badges électroniques de ces intervenants dûment identifiés en application du contrat de service convenu entre ClearBUS et son hébergeur.

L'accès physique au système d'horodatage par les personnels **ClearBUS** nécessite une coordination avec les personnels de l'hébergeur, qui permettra cet accès grâce à son propre badge, et tiendra le registre de ces demandes.

En dehors des heures ouvrables, des mesures de détection d'intrusion physique sont mises en œuvre.

6.3.1.3 Alimentation électrique et climatisation

- Les moyens nécessaires au maintien de la disponibilité du système et du service sont pris en compte dans les Conditions du contrat d'hébergement.

6.3.1.4 Exposition aux dégâts des eaux

- Les moyens nécessaires à la protection du matériel sont mis en œuvre contractuellement par l'hébergeur.

6.3.1.5 Prévention et protection incendie

- Les moyens nécessaires au maintien de la disponibilité du système et du service sont pris en compte dans les Conditions du contrat d'hébergement. Son personnel est sensibilisé aux risques incendie, à sa prévention, sa détection et formé à l'utilisation des moyens de lutte.

6.3.1.6 Conservation des supports

Les documents de l'AH **ClearBUS** ne nécessitent pas d'archivage. Les documents sensibles tels que les procès-verbaux de cérémonie des clés des Unités d'Horodatage du service d'horodatage **ClearBUS** sont conservés dans un coffre sécurisé.

6.3.1.7 Mise hors service des supports

Les supports recensés comme sensibles en termes de confidentialité font l'objet de mesures de destruction lorsqu'ils parviennent en fin de vie.

6.3.1.8 Sauvegarde hors site

Les fichiers d'audits sont stockés sur les serveurs d'horodatage puis exportés vers un serveur de traces externe à la plateforme de production. Ce serveur de trace est physiquement séparé.

Une sauvegarde système journalière est de plus opérée par l'hébergeur.

6.3.2 Exigences procédurales

6.3.2.1 Analyse des risques

Le service d'horodatage fait partie du périmètre de l'étude de risques menée régulièrement par **ClearBUS**.

6.3.2.2 Gestion des supports

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

6.3.2.3 Planification de systèmes

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

6.3.2.4 Gestion des incidents

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

- Tout dysfonctionnement du service d'horodatage est identifié par l'équipe « Production » de **ClearBUS-SHE**, qui prend les mesures nécessaires à la remise en service de l'UH défaillante ;
- En cas de problèmes bloquants, les équipes techniques de **ClearBUS-SHE** sont à même d'analyser l'incident et d'apporter de mesures de contournement ou correctives ;
- Les incidents liés au service d'horodatage sont traités selon la procédure de gestion des incidents en vigueur chez **ClearBUS**.

6.3.2.5 Manipulation et sécurité des systèmes

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

6.3.2.6 Procédures de fonctionnement et responsabilités

Les opérations de sécurité sur les composantes du service d'horodatage sont réalisées par du personnel de confiance qui est explicitement mis au courant de ses responsabilités.

Les opérations de sécurité incluent notamment :

- Les procédures opérationnelles et les responsabilités ;
- La planification et la qualification des systèmes sécurisés ;
- La protection vis-à-vis du logiciel malveillant ;
- La maintenance ;
- La gestion du réseau ;
- Le contrôle actif des journaux d'audit, l'analyse des événements et les suites à donner ;
- Le traitement et la sécurité des médias ;
- L'échange des données et du logiciel.

6.3.2.7 Gestion d'accès au système

L'accès aux systèmes du service d'horodatage est réservé aux seules personnes formellement habilitées. Les administrateurs sont munis d'un identifiant personnel permettant de tracer nominativement l'ensemble des accès aux systèmes.

Des équipements de filtrage sont positionnés en amont des serveurs d'horodatage pour garantir que seuls les flux nécessaires et suffisants sont autorisés à accéder à ces serveurs. Les équipements d'infrastructure sont positionnés dans une zone sécurisée.

Toutes les traces liées à l'administration des systèmes sont conservées conformément aux exigences exposées dans le paragraphe 6.2.2. Les incidents sur les serveurs d'horodatage font l'objet de remontées d'alertes vers une équipe en charge de les analyser et de réagir selon des procédures formelles.

6.3.3 Exigences organisationnelles

6.3.3.1 Entités constitutives du système

6.3.3.1.1 Autorité d'Horodatage (AH)

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

6.3.3.1.2 Prestataire de Services d'Horodatage Electronique

Le PSHE est garant de l'application opérationnelle de la PH. **ClearBUS** assure directement ce rôle, et s'organise à partir d'un Comité de Pilotage.

Ce Comité de Pilotage a notamment pour mission de :

- Faire réaliser les analyses de risques sur le périmètre dont il a la charge ;
- Décider de la stratégie de gestion des risques ;
- Valider et suivre les plans d'actions correspondants ;
- Faire réaliser les audits internes sur sa composante, et suivre la mise en place des mesures correctives nécessaires.

Les moyens nécessaires au maintien de la disponibilité du système et du service sont pris en compte dans les Conditions du contrat d'hébergement.

6.3.3.2 Rôles de confiance des intervenants

Les rôles de confiance définis sont au moins :

- Administrateurs de la plateforme d'horodatage : responsabilité de la configuration et du paramétrage des unités d'horodatage ;
- Responsable de la sécurité informatique : responsabilité complète de définir et de contrôler la mise en œuvre des pratiques de sécurité ;
- Opérateur système : suivi et maintien en conditions opérationnelles du service d'horodatage ;
- Administrateur système : suivi et réalisation des opérations d'administration sur les serveurs d'horodatage ;
- Auditeur système : responsabilité de l'analyse récurrente des fichiers d'audit du service d'horodatage.

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

6.3.3.3 Identification et authentification pour chaque rôle

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

Les rôles attribués concernant les services d'horodatage sont notifiés à travers des fiches de postes aux personnes concernées par le Responsable de l'AH **ClearBUS-SHE**.

6.3.3.4 Rôles exigeant une séparation des attributions

L'AH **ClearBUS-SHE** met en œuvre une séparation des rôles de confiance de manière à ce que :

- Le responsable de la sécurité n'ait pas de rôle opérationnel directement sur les serveurs du service d'horodatage ;
- L'audit système se fasse par une personne neutre vis-à-vis du service d'horodatage.

6.3.3.5 Mesures de sécurité vis à vis du personnel

6.3.3.5.1 Qualifications, compétences, et habilitations requises

Tout intervenant amené à occuper un rôle identifié comme sensible est soumis à une clause de confidentialité, gérée par l'employeur.

ClearBUS s'assure que les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles.

Le personnel d'encadrement de **ClearBUS** possède l'expertise appropriée, et est familier des procédures de sécurité.

Toute personne intervenant dans des rôles de confiance est informée de ses responsabilités (description de poste) et des procédures liées à la sécurité du système et au contrôle du personnel.

6.3.3.5.2 Procédures de vérification des antécédents

Il est demandé aux personnes appelées à occuper un rôle sensible au sein du service d'horodatage de fournir une déclaration sur l'honneur attestant pour la personne :

- De ne pas avoir de conflit d'intérêt dans le poste qu'elle occupe ;
- De ne pas avoir commis de délits informatiques.

6.3.3.5.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement.

Les personnels participant au service d'horodatage ont notamment des connaissances sur les thèmes suivants :

- Technologie et fonctionnement de l'horodatage ;
- Technologie et principe de la signature électronique ;
- Connaissance des principes de calibration et de synchronisation des horloges de temps ;
- Connaissance et respect des règles de sécurité pour les personnels techniques.

6.3.3.5.4 Exigences en matière de formation continue et fréquences des formations

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux intervenants dans la mesure où cette évolution impacte le mode de travail de ces intervenants.

Les intervenants sont formés à la gestion des incidents et sont au fait de l'organisation de remontée d'incidents.

6.3.3.5.5 Fréquence et séquence de rotations entre différentes attributions

Sans objet.

6.3.3.5.6 Sanctions en cas d'actions non autorisées

Le règlement intérieur prévoit la mise en œuvre de sanctions en cas d'actions non autorisées. Le processus de sanctions appliqué est traité par les ressources humaines de **ClearBUS**.

6.3.3.5.7 Exigences vis à vis du personnel des prestataires externes

Les exigences vis-à-vis des prestataires externes sont contractualisées. Il s'agit essentiellement du personnel réalisant l'hébergement des serveurs de **ClearBUS**.

Les types d'engagement sont des contrats relatifs à la réalisation d'une prestation, des engagements de confidentialité et une charte d'utilisation des moyens informatiques.

6.3.3.5.8 Documentation fournie au personnel

Les règles de sécurité sont communiquées au personnel lors de la prise de poste, en fonction du rôle affecté à l'intervenant. Les personnes appelées à occuper un rôle opérationnel dans le service d'horodatage disposent des procédures correspondantes.

6.4 Exigences de sécurité techniques

6.4.1 Exactitude du temps

Les horloges des UH sont synchronisées localement sur le serveur d'horodatage. Ce dernier se synchronise sur plusieurs serveurs de temps (NTP) différents sur Internet. La moyenne de temps des serveurs NTP permet d'établir l'heure du service d'horodatage.

Les serveurs de synchronisation sont ceux listés dans le chapitre 6.2.4.

Le système d'horodatage de **ClearBUS-SHE** est donc synchronisé avec au moins un serveur UTC(k). Ceci permet de mettre en évidence que le temps au sein du système d'horodatage est fiable.

La précision du service d'horodatage est d'une (1) seconde par rapport au temps UTC(k).

6.4.2 Génération des clés

La génération des bi-clés cryptographiques des UH est réalisée à l'aide de ressources cryptographiques matérielles.

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

Les clés privées d'UH ont une longueur de 2048 bits minimum pour l'algorithme RSA.

Une UH dispose d'une seule clé active de signature de jetons d'horodatage à un instant donné.

6.4.3 Certification des clés de l'UH

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

La configuration du serveur utilisé dans l'AH garantit le lien entre le demandeur d'un jeton d'horodatage et les droits qu'a le serveur d'horodatage à la lui délivrer.

Les informations suivantes font parties de la demande :

- Le nom DN à faire apparaître dans le certificat ;
- La valeur de la clé publique suivant l'algorithme SHA-256 ;

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

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

6.4.4 Protection des clés privées des UH

Les clés privées des UH sont stockées dans un HSM. Le module utilisé est :

- Qualifié au niveau « renforcé » par l'ANSSI ;
- Certifié Critères Communs pour le niveau d'assurance EAL4+ ;

L'installation, la configuration et l'utilisation du HSM sont conformes au périmètre de la certification.

6.4.5 Exigences de sauvegarde des clés des UH

Les clés des UH sont sauvegardées et stockées dans un lieu sécurisé.

6.4.6 Destruction des clés des UH

En fin de vie d'une clé privée d'UH, normale ou anticipée (révocation), cette clé est détruite par une opération d'administration du boîtier HSM. Les copies de sauvegarde de la clé sont également détruites.

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 de l'ANSSI [PSCO_QUALIF] et à [TS_119312]. L'algorithme de calcul d'empreinte numérique accepté est SHA-512 ;
- Génère des jetons d'horodatage signés selon les algorithmes et les longueurs de clé conformes aux exigences de l'ANSSI [PSCO_QUALIF] et à [TS_119312]. La bi-clé de l'UH est au minimum une bi-clé RSA de 2048 bits utilisant l'algorithme de hachage SHA-256.

6.4.8 Vérification des jetons d'horodatage

Les jetons d'horodatage sont vérifiés par le logiciel **ClearBUS-SRE,** seul utilisateur supporté.

6.4.9 Durée de vie des clés publiques des UH

La durée de vie des clés publiques des UH est de trois (3) ans. Cette durée ne pourra être plus longue que :

- La durée de vie cryptographique de l'algorithme utilisé pour la signature ;
- La durée de vie du certificat de l'AC qui l'a émis.

6.4.10 Durée d'utilisation des clés privées des UH

La durée de vie des clés privées des UH est limitée à deux (2) ans. La durée d'utilisation d'une clé est réduite afin que la validité des jetons d'horodatage générés avec cette clé puisse être effectuée durant à un (1) an.

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 via des procédures mises en place pour assurer qu'une nouvelle bi-clé est mise en place quand la fin de la période d'utilisation d'une clé privée de l'UH a été atteinte

7 DOCUMENTS CITES EN REFERENCE

7.1.1 Réglementations

Renvoi	Document
[CNIL]	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la Loi n°2018-493 du 20 juin 2018
[eIDAS]	Règlement n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n°1999/93/CE Disponible sur https://european-union.europa.eu

7.1.2 Documents techniques

Renvoi	Document
[RFC_3161]	IETF - Internet X.509 Public Key Infrastructure - Time-Stamp Protocol - 08/2001 Disponible sur https://www.ietf.org
[RFC_5816]	IETF - ESSCertIDv2 Update for RFC 3161 – 03/2010 Disponible sur https://www.ietf.org
[EN_319401]	General Policy Requirements for Trust Service Providers Disponible sur https://www.etsi.org
[EN_319421]	Policy & security requirements for TSP issuing time-stamps Disponible sur https://www.etsi.org
[EN_319422]	Time-stamping protocol and time-stamp profiles Disponible sur https://www.etsi.org
[TS_119312]	Cryptographic suites Disponible sur https://www.etsi.org
[DPH]	Déclaration des Pratiques d'Horodatage de l'AH ClearBUS
[CGUH]	Conditions Générales d'Utilisation du service d'Horodatage ClearBUS Disponible sur https://www.clearbus.fr

[AnalyseRisques]	Analyse des risques de l'infrastructure des services de confiance ClearBUS
[PSCO_QUALIF]	Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur Disponible sur https://cyber.gouv.fr
[PSCO_HORO]	Services d'horodatage électronique qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur Disponible sur https://cyber.gouv.fr

8 EXIGENCES SUR LES FORMATS DES JETONS D'HORODATAGE, DES CERTIFICATS ET DES LCR ET SUR LES ALGORITHMES CRYPTOGRAPHIQUES

8.1 Jeton d'horodatage

Les jetons d'horodatage fournis par l'AH **ClearBUS-SHE** ont une structure TimeStampToken conforme au [RFC_3161].

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

Un jeton d'horodatage conforme à la présente PH respecte, de base, les exigences correspondantes du [RFC_3161], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Exigences
messageImprint	Valeur hachée du message suivant l'algorithme défini au paragraphe 6.4.7
Accuracy	Le champ contient la précision du temps délivré dans le jeton d'horodatage par rapport au temps UTC(k) Ce champ est positionné et contient une valeur égale à 1 seconde
Ordering	*Ce champ n'est pas positionné*
Tsa	Ce champ est positionné et contient le sujet DN du certificat de l'UH
Extensions	*Aucune extension n'est marquée critique*

Les champs en italique, optionnels vis-à-vis de l'ETSI, ne sont pas contenus dans les jetons d'horodatage conformes à la présente PH.

8.2 Certificats et LCR

Les gabarits des certificats d'UH sont conformes aux exigences des certificats de type « Cachet » dont la clé privée associée est utilisée pour signer des jetons d'horodatage.

Il est rappelé ici que :

- L'extension « Extended Key Usage » est présente, marquée critique, et ne contient que l'identifiant « id-kp-timeStamping » à l'exclusion de toute autre ;
- Le champ « DN Subject » identifie l'AH suivant les mêmes règles que l'identification des AC et l'identifiant propre à l'UH concernée, au sein de l'AH, est porté dans l'attribut commonName du DN de ce champ (au sein d'une AH, chaque UH a un identifiant unique) ;

- La durée de vie maximale est bornée selon le couple {durée de vie cryptographique de la clé ; fin de validité de la durée de vie de l'AC émettrice}.

8.3 Algorithmes cryptographiques

L'algorithme mis en œuvre pour la génération des certificats est SHA-256. L'algorithme mis en œuvre pour le calcul des hachés dans les jetons d'horodatage est SHA-512. Ces algorithmes respectent les exigences prévues dans [TS_119312].

9 EXIGENCES DE SECURITE DU MODULE D'HORODATAGE DES UH

9.1 Exigences sur les objectifs de sécurité

Le module d'horodatage, utilisé par l'AH pour générer et mettre en œuvre les clés de signature des UH et pour générer les jetons d'horodatage, répond aux exigences de sécurité suivantes :

- Garantir que la génération des bi-clés des UH est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- Assurer la confidentialité et l'intégrité des clés privées de signature des UH durant tout leur cycle de vie, et permettre leur destruction sûre en fin de vie ;
- Garantir l'authenticité et l'intégrité des clés publiques lors de leur export hors du module (à fins de certification par une AC) ;
- Lors de son importation dans le module, vérifier la correspondance entre le certificat importé et la clé publique de l'UH contenue dans le module ;
- Etre capable d'identifier et d'authentifier ses utilisateurs ;
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- Etre capable de mener une série de tests, lors des phases d'initialisation, de personnalisation et d'opération, pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Etre capable de détecter les tentatives d'altérations physiques et d'entrer dans un état sûr quand une tentative d'altération est détectée ;
- Permettre de créer une signature numérique, pour signer les jetons d'horodatage générés par l'UH, qui ne révèle pas les clés privées de l'UH et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- Empêcher toute importation / exportation des clés privée de l'UH ;
- Garantir la synchronisation de son horloge avec le temps UTC suivant la précision définie dans la DPH ;
- Fournir des jetons d'horodatage conformes aux requêtes reçues.

9.2 Exigences complémentaires

Le module cryptographique utilisé pour stocker les clés privées des UH fait l'objet d'une certification Critères Communs pour le niveau d'assurance EAL4+.

10 VERIFICATION DES JETONS D'HORODATAGE

10.1 Empilement des jetons d'horodatage

Les jetons d'horodatage peuvent être validés durant la durée de vie du certificat de l'UH qui a signé le jeton.

Pour maintenir la capacité de vérifier un jeton d'horodatage après la durée de vie du certificat de l'UH qui a signé ce jeton, il convient de procéder à un réhorodatage du jeton initial.

Il n'est pas prévu de prolonger la durée de vérification des jetons d'horodatage.

10.2 Gestion de la révocation par l'AC

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

11 PRECISION DE LA SYNCHRONISATION DE L'HORLOGE

La précision de l'horloge est inférieure ou égale à une (1) seconde par rapport au temps UTC(k). La précision est positionnée dans le jeton d'horodatage délivré, à travers le champ « accuracy ».

12 PROTOCOLE D'HORODATAGE

12.1 Conformité RFC 3161

La validité de la conformité à la [RFC_3161] est obtenue par l'utilisation d'une application d'horodatage conforme aux règlementations et normes en vigueur.

12.2 Conformité EN 319422

Le profil des jetons d'horodatage est conforme à [EN_319422].

13 COMPATIBILITE AVEC [EN_319421]

La présente PH est conforme à la politique de l'ETSI [EN_319421] dont l'OID est le suivant 0.4.0.2023.1.1.

14 GABARIT DE CERTIFICAT D'UNE UH

14.1 En cours de validité

Le profil de certificat qualifié ETSI EN 319 411-2 est de niveau QCP-L pour cette version, car actuellement aucun dispositif de création de cachet électronique n'a été qualifié en France pour permettre la transition vers le niveau QCP-L-QSCD.

Dès l'obtention de la qualification nécessaire de son dispositif de création de cachet, **ClearBUS** fera évoluer le profil de son certificat d'UH vers le niveau QCP-L-QSCD.

Champ	Description
Version :	3
Emetteur :	CN = CertEurope eID Corp OU = 0002 434202180 O = CertEurope C = FR
Objet :	CN = **ClearBUS** - UH <id> OU = 0002 509608352 O = **ClearBUS** C = FR
Durée de validité :	3 ans
Numéro de série :	Numéro unique défini par l'AC
Clé publique :	Générée au moment de la signature de la demande par l'AC
Politique de Certification :	(Défini par l'AC) OID = 1.2.250.1.105.24.411.2.2.1.1.0 CPS = https://www.certeurope.fr/chaine-de-confiance/
Liste de révocation :	(Défini par l'AC) URI:https://www.certeurope.fr/reference/certeurope_eid_corp.crl
Accès aux informations de l'autorité :	(Défini par l'AC) caIssuers = http://www.certeurope.fr/reference/eid_corp.crt URL =
Utilisation de la clé :	Non repudiation

14.2 Historique