Politique d'Horodatage du service ClearBUS

Version	Date	Description	Auteurs	Société
1.0	07/12/11	Rédaction initiale	Jean-Marc Lefebvre	ClearBUS
1.1	07/03/12	Première version publique	Jean-Marc Lefebvre	ClearBUS
1.2	15/05/13	Modification référentiel	Jean-Marc Lefebvre	ClearBUS

Etat du document	Classification
Validé	C1
OID du document	
1.3.6.1.4.1.38116.1.1.1.1	
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. Ce service postal numérique est appelé le « service **ClearBUS** » dans la suite du document.

ClearBUS se positionne en tant qu'Autorité d'Horodatage (ci-après « AH ») et délivre des contremarques de temps pour les besoins de son service. La solution d'Horodatage est mise en œuvre par les équipes techniques **ClearBUS**, qui se positionnent alors comme Prestataire de Service d'Horodatage Electronique (PSHE) pour **ClearBUS**.

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

Dans le cadre de la présente PH, le seul utilisateur du service d'horodatage est le service **ClearBUS** lui-même.

L'objectif de ce document est de définir les engagements que **ClearBUS**, en tant qu'AH, respecte dans la délivrance et la gestion de contremarques de temps. Le respect de ces engagements démontre à l'ensemble des utilisateurs du service **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 contremarques de temps et le maintien de l'exactitude de ses horloges. L'AH **ClearBUS** 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**.

L'Autorité d'Horodatage est prestataire de service d'horodatage au sens du décret n° 2011-434 du 20 avril 2011. Elle se conforme aux exigences de l'article 3 de ce même décret.

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 : **1.3.6.1.4.1.38116.1.1.1.1.**

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

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

1.2.2 Publication du document

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

La présente Politique d'Horodatage est publiée sur l'URL : www.clearbus.fr/Telechargements/Politique_Horodatage.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 des membres dirigeants de **ClearBUS** et des responsables techniques du service **ClearBUS**, dont le service d'horodatage fait parti. Ce dernier 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 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.1.3).

Indépendamment de ce mode de communication, les acteurs peuvent à tout moment se renseigner auprès du Comité d'Approbation pour obtenir plus d'informations, en envoyant un 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**, et tous les représentants de ses principaux partenaires, 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 contremarques de temps et, de fait, ne constitue qu'une brique du référentiel documentaire de **ClearBUS**.

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 de ClearBUS

Une contremarque de temps permet d'attester de la réalité, à une date et une heure donnée, de l'existence d'une empreinte numérique (ou « hash ») qui est soumise au service d'horodatage. Les contremarques de temps sont délivrées et signées électroniquement par l'AH à l'aide d'Unité(s) d'Horodatage.

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

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

Les certificats d'horodatage installés sur les unités d'horodatage du service d'horodatage de **ClearBUS** sont émis par **ClearBUS**.

Dans le cadre de cette PH, la date et le temps de chaque contremarque de temps sont synchronisés avec le temps UTC avec une précision de 1 seconde. La présente PH applique un format de contremarque de temps standard défini par le [RFC 3161]. La gestion de la synchronisation de l'horloge du service d'horodatage est détaillée au chapitre 6.2.4.

1.4 Etablissement de la confiance dans le service d'horodatage de ClearBUS

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** les engagements que prend l'autorité d'horodatage, notamment ceux pris en matière de sécurité, et décrit de façon macroscopique les moyens mis en œuvre pour tenir ces engagements. Elle revêt une grande importance car elle incarne le niveau de confiance atteint par le service d'horodatage. Elle traduit la reconnaissance formelle de l'importance accordée par l'autorité d'horodatage à la sécurité du service. Les exigences

pour les services d'horodatage décrits dans ce document incluent des exigences portant, à la fois sur la gestion de l'horodatage et sur le fonctionnement des unités d'horodatage qui publient les contremarques de temps. L'Autorité d'horodatage, telle qu'identifiée dans la contremarque de temps, a la responsabilité d'assurer que ces exigences sont remplies.

La présente PH est élaborée sur la base des documents issus de l'ETSI TS 102 023 ([ETSI_PH]). Les contremarques de temps émise par le service d'horodatage de **ClearBUS** sont demandées et à destination du service **ClearBUS**. Les Unités d'Horodatage mises en œuvre par **ClearBUS** ne délivrent pas de contremarques de temps pour des applications externes à **ClearBUS**.

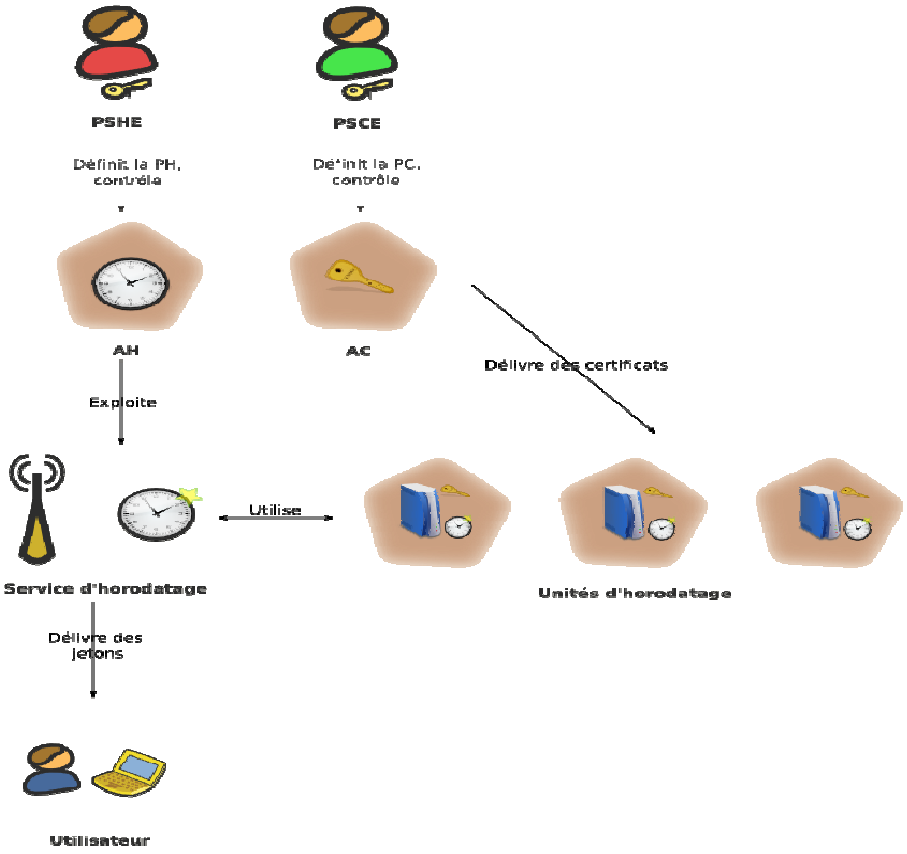
1.5 Entités intervenant dans le service d'horodatage

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 l'[ETSI_PH]. La solution d'horodatage **ClearBUS** 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 contremarques de temps.

ClearBUS installe des certificats électroniques sur ses UH émis par l'AC **ClearBUS**.

La représentation schématique est alors la suivante :



Les rôles se répartissent de la manière suivante :

	Applications Utilisatrices
PSHE	Service **ClearBUS**
ClearBUS	
PSCE	Unités d'Horodatage **ClearBUS**
AC **ClearBUS**	

1.6 Autres aspects

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

2 GÉNÉRALITÉS

2.1 Définitions

Abonné – Personne physique ou morale bénéficiant, selon des conditions définies et acceptées, d'un service d'horodatage électronique assuré par un prestataire de services d'horodatage électronique. Dans le cadre de la présente Politique d'Horodatage, le seul utilisateur de contremarques de temps est le service de courrier numérique **ClearBUS.**

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

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

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

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

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

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

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

Demande de contremarque de temps - Désigne la requête qui est soumise par un abonné à l'AH pour l'émission d'une contremarque de temps. Cette requête contient au minimum l'empreinte numérique à horodater.

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

Jeton d'horodatage - Voir contremarque de temps.

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

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

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

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

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

Prestataire de services d'horodatage (PSHE) - L'ordonnance 2005-1516 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.

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

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

- qualification de niveau élémentaire,
- qualification de niveau standard,
- qualification de niveau renforcé.

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

Référencement - Opération réalisée par l'Administration qui atteste que l'offre d'horodatage du PSCE est utilisable avec tous les systèmes d'information qui requièrent ce type d'offre. Une offre référencée peut être utilisée dans toutes les applications d'échanges dématérialisés requérant un service d'horodatage. Pour les utilisateurs, le

référencement permet de connaître quelles offres d'horodatage ils peuvent utiliser pour quels échanges dématérialisés.

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

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

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

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

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

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

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

UTC(k) - Temps de référence réalisé par le laboratoire "k" et synchronisé avec précision avec le temps UTC, dans le but d'atteindre une précision de ±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** pour relever son courrier numérique. Le dit service **ClearBUS** de courrier numérique est lui-même usager de contremarque de temps pour dater de façon fiable les étapes clef de l'acheminement.

Utilisateur de contremarque de temps – Entité (personne ou système) qui fait confiance à une contremarque de temps émise sous une politique d'horodatage donnée par une autorité d'horodatage donnée. Dans le cadre de la présente Politique d'Horodatage, le seul utilisateur de contremarques de temps est le service de courrier numérique **ClearBUS**.

Utilisateur final - Abonné ou utilisateur de contremarques de temps.

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

2.2 Abréviations

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

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

3 POLITIQUE D'HORODATAGE

Pour cette politique, la date et le temps de chaque contremarque de temps doivent être synchronisés avec le temps *UTC* avec une exactitude de 1 seconde.

La présente PH impose un format de contremarque de temps spécifique, qui doit répondre aux exigences du chapitre ci-dessous.

Cette politique impose l'usage d'un protocole d'horodatage spécifique pour demander et obtenir une contremarque de temps auprès d'une AH définie dans le RFC3161 et profilée dans le document ETSI TS 101 861 V1.2.1.

Les caractéristiques principales de cette politique sont les suivantes :

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

4 DÉCLARATION DES PRATIQUES D'HORODATAGE

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

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

La déclaration des pratiques d'horodatage 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 **ClearBUS** 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 contremarques de temps, à compter de leur date de génération ;
- La précision de la date des contremarques de temps par rapport à l'échelle de temps UTC ;
- Les obligations des abonnés ;
- Les obligations des utilisateurs de contremarque de temps ;
- Les informations permettant de vérifier la contremarque de temps ;
- Les limitations de responsabilité.

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

5 CONDITIONS GÉNÉRALES D'UTILISATION

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

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

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

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

L'Autorité d'horodatage définit ses propres conditions générales d'utilisation et les rend disponibles aux abonnés et aux utilisateurs de contremarques de temps sous une forme lisible, compréhensible et pérenne. Ces CGUH sont complémentaires aux Conditions Générales du Service **ClearBUS** qui sont acceptées par ses clients.

Elles peuvent être téléchargées sur le site www.clearbus.fr.

6 EXIGENCES RESPECTÉES PAR L'AUTORITÉ D'HORODATAGE

6.1 Dispositions générales

6.1.1 Obligation de l'Autorité d'Horodatage

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

- Génère et signe les contremarques de temps conformément à la PH ;
- Respecte et se conforme aux exigences et procédures définies dans la présente PH et dans les Conditions Générales d'Utilisation applicables ;
- 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 de ses clients l'ensemble des informations nécessaires permettant de vérifier les contremarques de temps qu'elle aura émises.

6.1.2 Obligation de l'abonné

Le service **ClearBUS** est en capacité de vérifier la validité des contremarques de temps délivrées par l'AH.

La validité d'une contremarque de temps est matérialisée à l'usager via les interfaces d'accès au service **ClearBUS**.

6.1.3 Obligation de l'Utilisateur de Contremarque de Temps

Le service courrier numérique **ClearBUS** :

- 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 ;
- s'assure que les contremarques de temps sont obtenues auprès des UH mises en place par **ClearBUS.**

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

L'AC **ClearBUS** délivrant des certificats aux unités d'horodatage fournit un service de révocation disponible uniquement pour le service d'exploitation de **ClearBUS**.

6.1.5 Déclaration des Pratiques d'Horodatage

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

- L'AH a rédigé une analyse des risques de son service d'horodatage ;
- L'AH adresse l'ensemble des exigences décrites dans la présente PH ;
- La DPH décrit toutes les exigences que doivent respecter les éventuelles tierces parties dans le cadre du service d'horodatage ;
- L'AH met à disposition des abonnés, sur demande par courriel envoyé à horodatage@clearbus.fr, les données nécessaires à la validation des contremarques de temps, soit :

  - Les certificats des unités d'horodatage ;
  - Les CRL de l'AC **ClearBUS** ;
  - Le certificat de l'AC **ClearBUS** ;
  - Toutes les versions des politiques d'horodatage avec leur date de validité.
- L'AH organise un audit interne pour attester que la DPH est conforme à la PH ;
- L'audit organisé par l'AH prend en compte le contrôle des mesures techniques, non techniques et organisationnelles ;
- L'AH garantit qu'elle mettra à jour la PH en cas de changements majeures des pratiques d'horodatage de son service ;
- L'AH garantit que tout changement majeur dans ses pratiques d'horodatage fera l'objet d'une notification auprès de l'organisme qui lui a délivré les différentes qualifications.

6.1.6 Conditions Générales d'Utilisation d'Horodatage

L'AH 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 l'ETSI 102023. L'AH décrit dans ces CGUH les informations suivantes :

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

6.1.7 Conformité avec les exigences légales

6.1.7.1 Droit applicable

Le présent document est régi par la loi française.

6.1.7.2 Règlement des différends

Toutes contestations et litiges survenant dans l'interprétation et la mise en œuvre du présent document seront soumis à la juridiction des tribunaux de Grenoble.

6.1.7.3 Propriété intellectuelle des infrastructures

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

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

6.1.7.4 Données nominatives

Le service d'horodatage ne traite pas de données nominatives. Les seules données transmises sont une empreinte des données traitées par le service **ClearBUS**.

6.2 Exigences opérationnelles

6.2.1 Gestion des requêtes

Les demandes de contremarques de temps sont réalisées par les UH de l'AH **ClearBUS** exclusivement et selon le protocole défini par le [RFC 3161]. Ce protocole est conforme à [ETSI_TSP].

Les usagers « personnes physiques », clients de **ClearBUS**, utilisent le service d'horodatage via le service **ClearBUS**. Opérationnellement, cette demande d'horodatage est pilotée par le logiciel serveur du service **ClearBUS**, et elle consiste à effectuer une connexion en mode TCP ou HTTP vers le serveur d'horodatage. Cette opération est généralement réalisée à l'issue d'une opération de signature électronique.

Le logiciel **ClearBUS** produit un condensat (hash) des données à horodater, et les transmet au système d'horodatage sans authentification.

L'AH **ClearBUS** génère la contremarque de temps à partir du condensat des données qui lui est transmis par le service **ClearBUS** (empreinte de la donnée à horodater) et la lui retourne. La durée de création de la contremarque de temps n'excède pas quelques secondes suite à la réception d'une requête d'horodatage.

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

6.2.2 Fichiers d'audit

Les journaux du service d'horodatage sont conservés sur le serveur d'horodatage depuis sa mise en activité.

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 du 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** qui respecte le chapitre 6.4.2.

Ces clés privées sont exclusivement utilisées pour des certificats d'horodatage dans le cadre du service d'horodatage de **ClearBUS**. 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 automatiquement détruite.

Les clés privées ne sont pas exportables.

6.2.4 Synchronisation de l'horloge

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

- ntp1.sp.se - UTC(SP)
- ntp1.inrim.it - UTC(IT)
- hora.roa.es - UTC(ROA)
- ptbtime3.ptb.de - UTC(PTB)
- ntp2.oma.be - UTC(ROB)
- time.ufe.cz - UTC(TP)
- hercules.eim.gr - UTC(EIM)

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.

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

- Le calibrage de l'horloge n'est plus respecté ;

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

6.2.5 Contenu d'une Contremarque de Temps

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

Le tableau ci-dessous reprend les champs d'un `TimeStampToken` tels que définis dans le [RFC 3161].

Les contremarques de temps émises par l'AH **ClearBUS** respectent, de base, les exigences correspondantes du [RFC 3161], 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 de la contremarque de temps		X
GenTime	Heure de génération de la contremarque de temps calculée par rapport à une source UTC(k)		X
accuracy	absent car égal à 1 seconde		X
nonce	Identique à celui présenté lors de la demande de génération si celui-ci est présent dans cette dernière		X

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 **ClearBUS** ayant servi à générer les certificats des UH ;
- Un problème d'exploitation entraînant la divulgation d'éléments secrets.

En tout état de cause le service d'horodatage sera arrêté le temps que les équipes d'exploitation de **ClearBUS** est 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, **ClearBUS** :

- Mettra à disposition des abonnés et des utilisateurs de contremarque de temps 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 contremarques de temps émises qui pourraient être compromises ou suspectées de compromission.

6.2.7 Fin d'activité

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

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

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**.

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.

L'accès physique au système d'horodatage supportant ces fonctions est limité aux seules personnes autorisées par la mise en place d'un périmètre de sécurité physique,

permettant la séparation des rôles entre les différents intervenants, et par la mise en place d'un contrôle d'accès électronique par badge ou clé.

La traçabilité des accès est assurée par l'enregistrement des utilisations des badges électroniques.

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

6.3.1.3 Alimentation électrique et climatisation

Des mesures de secours sont mises en œuvre par **ClearBUS**, de manière à ce qu'une interruption de service ne porte pas atteinte aux engagements pris par l'AH en matière de disponibilité (signature et délivrance des contremarques de temps) :

- alimentation électrique : mise en œuvre de moyens techniques tels que des onduleurs et groupes électrogènes, avec redondance des équipements ;
- défaillance de climatisation : redondance climatiseurs, alarmes de dysfonctionnement.

6.3.1.4 Exposition aux dégâts des eaux

La définition du périmètre de sécurité prend en considération les risques inhérents aux dégâts des eaux. Des moyens de protection sont mis en œuvre pour parer les risques résiduels (installation sur un plancher en surélévation pour parer une rupture de canalisation par exemple).

6.3.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre l'incendie permettent de respecter les engagements pris par l'AH en matière de disponibilité (signature et délivrance des contremarques de temps), et de pérennité de l'archivage, en mettant en œuvre des moyens de prévention (sensibilisation et formation du personnel), de détection (détecteur fumée et incendie) et de lutte contre l'incendie (signalisation et disposition d'extincteur dans les lieux sensibles).

6.3.1.6 Conservation des supports

Les documents de l'AH **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 hébergé sur le même environnement mais sur un serveur physique séparé.

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**, qui prend les mesures nécessaires à la remise en service de l'UH défaillante, ou à la bascule sur le site de secours ;
- En cas de problèmes bloquants, les équipes techniques de **ClearBUS** 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 Rôles de confiance

Les rôles de confiance suivant sont définis :

6.3.3.1.1AH

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.

6.3.3.1.2Prestataire 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.

Le Comité de Pilotage a notamment pour mission de :

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

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 ;
- chargé de la sécurité informatique : responsabilité complète d'administrer la mise en œuvre des pratiques de sécurité ;
- techniciens d'exploitation : suivi et maintien en conditions opérationnelles du service d'horodatage ;
- techniciens d'administration : suivi et réalisation des opérations d'administration sur les serveurs d'horodatage ;
- technicien de supervision réseau et système ;
- auditeur système : suivi et revue des incidents 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.

6.3.3.2 Identification et authentification pour chaque rôle

Des mesures d'identification et d'authentification sont mises en place afin de supporter la mise en œuvre de la politique de contrôle d'accès et la traçabilité des opérations ; la

politique de contrôle d'accès limite l'accès aux seules personnes autorisées conformément à leur besoin d'en connaître.

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

6.3.3.3 Rôles exigeant une séparation des attributions

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

- Le responsable de la sécurité n'est 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.

6.3.3.4 Mesures de sécurité vis à vis du personnel

6.3.3.4.1 Qualifications, compétences, et habilitations requises

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

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.

6.3.3.4.2 Procédures de vérification des antécédents

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

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

6.3.3.4.3 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.

6.3.3.4.4Exigences en matière de formation continue et fréquences des formations

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

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

6.3.3.4.5Fréquence et séquence de rotations entre différentes attributions

Sans objet.

6.3.3.4.6Sanctions en cas d'actions non autorisées

La charte informatique 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**.

6.3.3.4.7Exigences 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.

6.3.3.4.8Documentation 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** est donc synchronisé avec au moins un serveur UTC(k). Ceci permet de mettre en évidence que le temps au sein du système d'horodatage est fiable.

La précision du service d'horodatage est de 1 seconde.

6.4.2 Génération des clés

La génération des bi-clés cryptographiques des UH est réalisée à l'aide de ressources cryptographiques matérielles. A aucun moment, lors de cette génération, les clés privées d'UH ne sont exportées de ces ressources. La génération des clés privées des unités d'horodatage est réalisée durant une cérémonie des clés qui fait l'objet d'un procès-verbal.

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

6.4.3 Certification des clés de l'UH

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

La configuration du serveur utilisé dans l'AH garantit le lien entre le demandeur d'une contremarque et les droits 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-512 ;

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 nCipher nShield 500E. Ce module est certifié FIPS 140-2 niveau 3.

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 des autorités compétentes en la matière comme par exemple [DCSSI_ALGO]. L'algorithme de calcul d'empreinte numérique accepté est SHA-512 ;
- Génère des contremarques de temps signées selon les algorithmes et les longueurs de clé conformes aux exigences des autorités compétentes en la matière comme par exemple [DCSSI_ALGO]. La bi-clé de l'UH est au minimum une bi-clé RSA de 2048 bits utilisant l'algorithme SHA-1.

6.4.8 Vérification des contremarques de temps

Les contremarques de temps sont vérifiées par le logiciel **ClearBUS**.

6.4.9 Durée de vie des clés publiques des UH

La durée de vie des clés publiques des UH est de 4 ans. Cette durée ne pourra être plus longue que :

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

6.4.10 Durée d'utilisation des clés privées des UH

La durée de vie des clés privées des UH est de 3 ans.

7 DOCUMENTS CITÉS EN RÉFÉRENCE

7.1.1 Réglementations

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

7.1.2 Documents techniques

Renvoi	Document
[DCSSI_ALGO]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, DCSSI, version 1.02 du 19 novembre 2004 N°2791 SGDN/DCSSI/SDS/Crypto du 19 novembre 2004 Les informations sont consultables sur le site http://www.ssi.gouv.fr
[ETSI_PH]	ETSI TS 102 023 V1.2.1 (2003-01) Policy requirements for Time-Stamping Authority
[ETSI_TSP]	ETSI TS 101 861 V1.2.1 (2002-03) Time Stamping Profile
[RFC 3161]	IETF - Internet X.509 Public Key Infrastructure - Time-Stamp Protocol - 08/2001
[RGS]	http://www.ssi.gouv.fr/IMG/pdf/RGSv1-0.pdf
[PH_Type]	http://www.ssi.gouv.fr/IMG/pdf/RGS__P_Horodatage-Type_v2-3.pdf

8 EXIGENCES SUR LES FORMATS DES CONTREMARQUES DE TEMPS, DES CERTIFICATS ET DES LCR ET SUR LES ALGORITHMES CRYPTOGRAPHIQUES

8.1 Contremarque de temps

Les contremarques de temps fournies par l'AH **ClearBUS** ont une structure TimeStampToken conforme au [RFC3161].

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

Une contremarque de temps conforme à la présente PH respecte, de base, les exigences correspondantes du RFC 3161, moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Exigences
messageImprint	Valeur hachée du message suivant l'algorithme défini dans le paragraphe suivant
Accuracy	Le champ contient la précision du temps délivré dans la contremarque de temps par rapport au temps UTC(k)
Ordering	*Ce champ n'est pas positionné*
Tsa	*Ce champ n'est pas positionné*
Extensions	*Aucune extension n'est marquée critique*

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

8.2 Certificats et LCR

Les gabarits des certificats d'UH sont conformes aux exigences des certificats de type « cachet » dont la clé privée associée est utilisée pour signer des jetons d'horodatage décrites dans les documents [RGS_A_14] et [RGS_A_13].

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 (cf. chapitre VII.1 de RGS_A_14) 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-1. L'algorithme mis en œuvre pour le calcul des hachés dans les contremarques de temps est SHA-512. Ces algorithmes respectent les recommandations en la matière et en vigueur en France.

9 EXIGENCES DE SÉCURITÉ DU MODULE D'HORODATAGE DES UH

9.1 Exigences sur les objectifs de sécurité

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

- Garantir que la génération des bi-clés des UH est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- Assurer la confidentialité et l'intégrité des clés privées de signature des UH durant tout leur cycle de vie, et permettre leur destruction sûre en fin de vie ;
- Garantir l'authenticité et l'intégrité des clés publiques lors de leur export hors du module (à fins de certification par une AC) ;
- Lors de son importation dans le module, vérifier la correspondance entre le certificat importé et la clé publique de l'UH contenue dans le module ;
- 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 contremarques de temps générées par l'UH, qui ne révèle pas les clés privées de l'UH et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- Empêcher toute importation / exportation des clés privée de l'UH ;
- Garantir la synchronisation de son horloge avec le temps UTC suivant la précision définie dans la DPH ;
- Fournir des contremarques de temps conformes aux requêtes reçues.

9.2 Exigences complémentaires

Le module cryptographique utilisé pour stocker les clés privées des UH est qualifié FIPS 140-2 niveau 3.

10 VÉRIFICATION DES CONTREMARQUES DE TEMPS

10.1 Empilement des contremarques de temps

Les contremarques de temps peuvent être validées durant la durée de vie du certificat de l'UH qui a signé la contremarque.

Il n'est pas prévu de prolonger la durée de vérification des contremarques en dehors d'une rupture cryptographique de l'algorithme utilisé pour générer le haché.

Pour pouvoir réaliser ces opérations d'empilement de contremarques de temps et permettre leur vérification, l'AH archive l'ensemble des CRL valides publiées.

10.2 Gestion de la révocation par l'AC

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

11 PRÉCISION DE LA SYNCHRONISATION DE L'HORLOGE

La précision de l'horloge est de 1 seconde par rapport au temps UTC(k). La précision est positionnée dans la contremarque de temps délivrée.

12 PROTOCOLE D'HORODATAGE

12.1 Conformité RFC 3161

La validité de la conformité à la RFC 3161 est obtenue par l'utilisation d'un boîtier d'horodatage conforme aux règlementations et normes en vigueur.

12.2 Conformité ETSI TS 101861

Le profil des contremarques de temps est conforme à l'[ETSI_TSP].

13 COMPATIBILITÉ AVEC [ETSI_PH]

La présente PH est fondé sur l'[ETSI_PH].

14 GABARIT DE CERTIFICAT D'UNE UH

Version :	3
Emetteur :	OU = 002 509608352 O = ClearBUS C = FR
Objet :	CN = **ClearBUS** TSA - UH 001 OU = 0002 509608352 O = **ClearBUS** ST = Rhone-Alpes L = Grenoble C = FR
Durée de validité :	4 ans
Numéro de série :	Numéro unique défini par la PKI
Clé publique :	Générée au moment de la signature de la demande par l'AC
Politique de Certification :	
Liste de révocation :	https://www.clearbus.fr/certs/crls/clearbus_ac_1_horodatage.crl
Utilisation de la clé :	Digital Signature
Extension d'utilisation de la clé :	Id-kp-timestamping