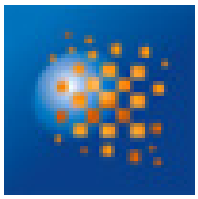
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'EUROPE ET DES
AFFAIRES ÉTRANGÈRES

Politique d'Horodatage de l'Autorité d'Horodatage

Politique d'Horodatage



OID : 1.2.250.1.214.69.3.1.3.5.1.1.

Cotation Archive : E.3.1.3.5

Version 1.3 du 06/09/2019

État : validé

Matrice de responsabilité/validation/diffusion					
Statut : I : Initiateur, R : Rédacteur, C : Contributeur					
Bureau/Société	**NOM, Prénom**	**Qualité**	**Statut**	**Validation**	**Diffusion**
DSI/MSA	SOUABEG Nadir	RSSI	C	✓	
DSI/PSI/OPT	HENNINOT Armand	Responsable IGC	I	✓	

NB. : La validation est automatique en l'absence de retour dans les 3 jours ouvrés à compter de la date de communication du document.

Suivi des mises à jour			
Version	**Date**	**Auteur**	**Commentaire(s)**
0.1	25/02/2014	Solucom	Création du document
1.0	04/11/2014	Solucom	Ajout des éléments communiqués par la MOE et par le MAE.
1.1	16/02/2015	Solucom	Mise à jour
1.2	25/07/2018	MEAE	Mise à jour
1.3	06/09/2019	MEAE	Mise à jour

SOMMAIRE

OID : 1.2.250.1.214.69.3.1.3.5.1.1.
Cotation Archive : E.3.1.3.5

FIGURES

TABLEAUX

DOCUMENTS DE REFERENCE

Renvoi	En ligne	Joint	Titre
[1]	☑	☐	Référentiel Général de Sécurité – version 2.0 – Annexe A5 – Politique d'Horodatage Type – version 3.0
[2]	☑	☐	Politique de Certification des AC INFRASTRUCTURE – Profil « signature jeton d'horodatage » – version 1.0.4

1 INTRODUCTION

1.1 PRESENTATION GENERALE

Le Ministère des Affaires Étrangères dispose d'une infrastructure de gestion de clés (IGC DIPLOMATIE), qui assure la fourniture de certificats électroniques destinés à l'ensemble des agents ou les composants techniques du MINISTÈRE.

L'IGC DIPLOMATIE est constituée d'une hiérarchie d'Autorités de Certification :

- l'AC RACINE DIPLOMATIE ;
- trois AC Déléguées et leurs renouvellements en version 2 : AC UTILISATEURS, AC INFRASTRUCTURE, et AC UTILISATEURS RENFORCÉE ;

Chacune des AC émet plusieurs types de certificats, selon différents profils.

L'AC INFRASTRUCTURE émet notamment des certificats « Signature de jetons d'horodatage ». Ces certificats sont destinés à la signature de jetons émis par l'Autorité d'Horodatage du Ministère.

Le présent document constitue la Politique d'Horodatage de l'Autorité d'Horodatage du service d'horodatage du Ministère.

Cette Politique d'Horodatage a vocation à être consultée et examinée par les personnes qui utilisent les contremarques de temps pour les aider à apprécier le degré de confiance qu'elles peuvent placer dans ces contremarques de temps.

Ce document respecte le plan type de la « Politique d'Horodatage type – version 3.0» du RGS v2.0 [1]. La PH type mentionnée a été élaborée sur la base de la politique d'horodatage de l'ETSI [ETSI_PH].

Cette Politique d'Horodatage est un document public et est mise à disposition du public sous format électronique sur le site Web du Ministère.

1.2 IDENTIFICATION DU DOCUMENT

La présente PH porte le titre suivant :

Politique d'Horodatage de l'Autorité D'Horodatage

La présente politique d'horodatage est identifiée par l'OID suivant : 1.2.250.1.214.69.3.1.3.5.1.1

Le dernier chiffre permet de faire évoluer le numéro de version du document.

1	2	250	1	214	69	3	1	3	5	1	1
ISO	member-body	France	Type org	MAE	Sécurité des SI	Documents normalisés	IGC Diplomatie				N° de version

OID : 1.2.250.1.214.69.3.1.3.5.1.1.
Cotation Archive : E.3.1.3.5

1.3 GESTION DE LA PH

1.3.1 ENTITE GERANT LA PH

La PH de l'Autorité d'Horodatage est élaborée et mise à jour par le Responsable de la Sécurité de l'Information du Ministère.

Cette PH est soumise à l'approbation du Comité SSI (COSSI) notamment pour :

- valider les usages et restrictions d'usage des contremarques des temps émises par cette AH ;
- vérifier sa conformité aux évolutions technologiques et aux exigences fonctionnelles ou réglementaires.

La périodicité minimale de révision de cette PH est de deux (2) ans.
Un tableau indiquant les différentes versions de la PH, les dates de révisions et les principales modifications apportées par rapport à sa version antérieure est présenté en page 2 du présent document.

1.3.2 POINT DE CONTACT

Pour toute information relative à la présente PH, il est possible de contacter :

Ministère des Affaires Étrangères
Direction des Systèmes d'Information
Autorité d'Horodatage
37 quai d'Orsay
75700 PARIS 07 SP

Le tableau suivant indique les coordonnées des entités responsables de la PH du Ministère.

Rôle	Entité	Coordonnées
Entité juridique responsable	MAE- DSI	37, quai d'Orsay 75700 Paris 07 SP
Personne physique responsable	Fabien FIESCHI - DSI	37, quai d'Orsay 75700 Paris 07 SP
Entité gérant la conformité de la DPH avec la PH	COSSI	37, quai d'Orsay 75700 Paris 07 SP
Entité représentant le Comité d'Approbation des Politiques de Certification & d'Horodatage	Nadir SOUABEG - RSSI	37, quai d'Orsay 75700 Paris 07 SP

Tableau 1 : Points de contact de la Politique d'Horodatage

1.3.3 ENTITE DETERMINANT LA CONFORMITE DE LA DPH AVEC CETTE PH

L'entité gérant la conformité de la DPH avec la présente Politique d'Horodatage est le Comité SSI (COSSI).

1.3.4 PROCEDURES D'APPROBATION DE LA CONFORMITE DE LA DPH

L'entité approuvant la conformité de la DPH est le Comité SSI (COSSI).

1.4 QU'EST-CE QUE L'HORODATAGE ?

L'horodatage permet d'attester qu'une donnée existe à un instant donné. Pour cela, il convient d'associer une représentation sans équivoque d'une donnée, par exemple une valeur de hachage associée à un identifiant d'algorithme de hachage, à un instant dans le temps. La garantie de cette association est fournie au moyen d'une contremarque de temps qui est une structure signée contenant en particulier
:

- l'identifiant de la politique d'horodatage sous laquelle la contremarque de temps a été générée ;
- la valeur de hachage et l'algorithme de hachage de la donnée qui a été horodatée ;
- la date et le temps UTC ;
- l'identifiant du certificat de l'Unité d'horodatage (UH) qui a généré la contremarque de temps (qui contient aussi le nom de l'Autorité d'horodatage).

La clé privée ou les clés utilisées pour générer les contremarques de temps sont gérées par l'Autorité d'Horodatage qui conserve la pleine et entière responsabilité pour satisfaire aux exigences définies dans la présente Politique d'Horodatage. Une Autorité d'Horodatage peut faire fonctionner plusieurs unités d'horodatage (UH). Chaque unité d'horodatage dispose de sa propre bi-clé.

1.5 COMMENT ETABLIR LA CONFIANCE EN L'HORODATAGE

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 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 le 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.

1.6 PRESENTATION DES ROLES ET RELATIONS

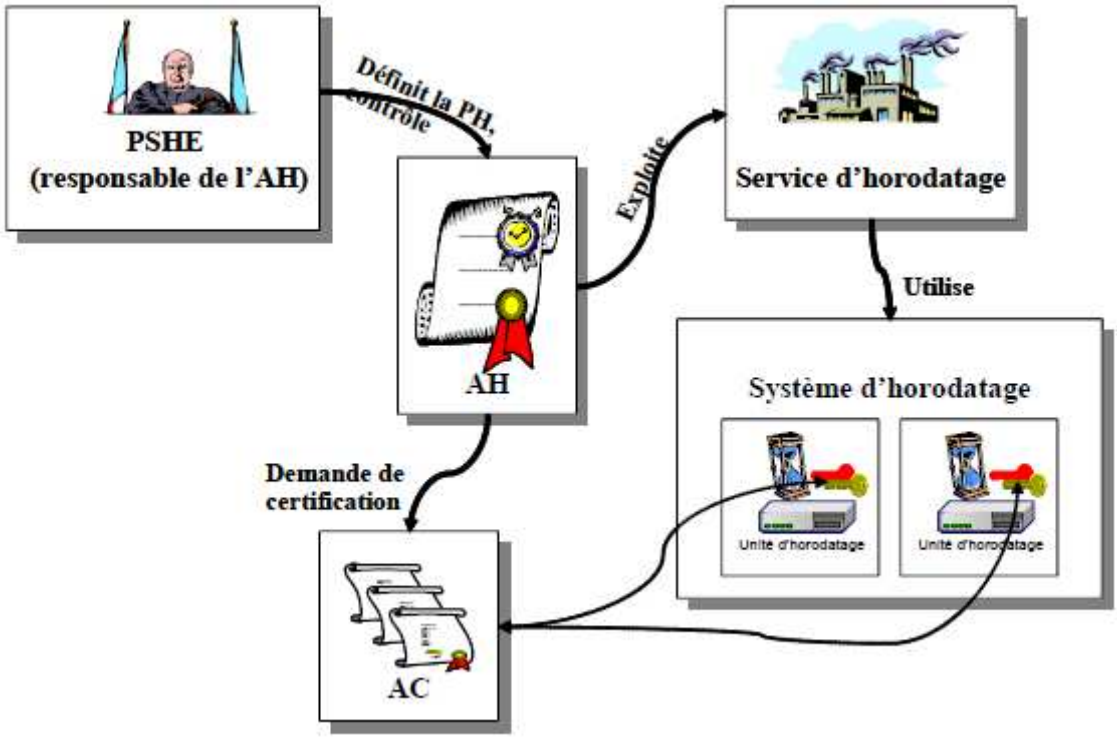


Figure 1. Présentation des rôles et relations

La notion d'Autorité d'Horodatage (AH) telle qu'utilisée dans la présente PH est définie au chapitre 2.1 ci-dessous.

L'AH exploite l'ensemble des services d'horodatage qui regroupent les diverses prestations organisationnelles et techniques nécessaires à la génération et à la gestion des contremarques de temps. Chaque UH signe ses contremarques de temps à l'aide d'une clé privée dont la clé publique correspondante a été certifiée au préalable par l'Autorité de Certification Infrastructure. Les clés privées sont conservées et mises en œuvre dans des modules d'horodatage.

1.7 AUTRES ASPECTS

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

2 GENERALITES

2.1 DEFINITIONS

Abonné - Entité ayant besoin de faire horodater des données par une Autorité d'horodatage et qui a accepté les conditions d'utilisation de ses services.

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 de 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) - Une Autorité d'Horodatage a en charge l'application d'au moins une politique d'horodatage en s'appuyant sur une ou plusieurs Unités d'Horodatage.

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) - Échelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5 [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 client 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.

OID : 1.2.250.1.214.69.3.1.3.5.1.1.
Cotation Archive : E.3.1.3.5

Politique de Certification (PC) – Désigne l'ensemble des règles et engagements énoncés et publiées par l'AC décrivant les caractéristiques générales des services de certification 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 dpar 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.

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 [DécretRGS]. Le [RGS] précise les trois processus de qualification : qualification de niveau élémentaire, qualification de niveau standard et qualification de niveau renforcé.

Ressource cryptographique - Désigne le produit de sécurité comportant une ressource cryptographique matérielle et qui est dédiée 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 des 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 tempos 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 de 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.

OID : 1.2.250.1.214.69.3.1.3.5.1.1.
Cotation Archive : E.3.1.3.5

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

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

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 procédant à des échanges électroniques avec des autorités administratives.

Nota - Un agent d'une autorité administrative qui procède à des échanges électroniques avec une autre autorité administrative est, pour cette dernière, un usager.

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.

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 ABREVIATIONS

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

CGU : Conditions Générales d'Utilisation du service d'horodatage

Delta-LRC : Liste de Révocation des Certificats partielle

SGMAP : Secrétariat Général à la Modernisation de l'Action Publique

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

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 100 ms.

La présente PH impose un format de contremarque de temps spécifique, qui doit répondre aux exigences du chapitre 7 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.

Les caractéristiques principales de cette politique sont comme suit :

- la protection des clés et de l'horloge doit respecter les exigences spécifiées au chapitre 8 ci-dessous ;
- 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.

OID : 1.2.250.1.214.69.3.1.3.5.1.1.
Cotation Archive : E.3.1.3.5

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 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 définit comment l'AH se conforme aux exigences physiques, environnementales, procédurales, organisationnelles et techniques identifiées dans une 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 SSI (COSSI) du Ministère des Affaires Étrangères.

Contrairement à la Politique d'Horodatage, la DPH n'est pas publiée.

Cependant, l'AH 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.

OID : 1.2.250.1.214.69.3.1.3.5.1.1.
Cotation Archive : E.3.1.3.5

5 CONDITIONS GENERALES D'UTILISATION

Sans Objet.

6 CONTENU DE LA POLITIQUE D'HORODATAGE

Ce chapitre décrit les dispositions générales ainsi que les exigences opérationnelles, physiques et environnementales, procédurales et organisationnelles et enfin de sécurité technique, auxquelles l'AH se conforme.

6.1 DISPOSITIONS GENERALES

6.1.1 OBLIGATIONS DE L'AUTORITE D'HORODATAGE

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

- génère et signe les contremarques de temps conformément à la PH ;
- se conforme aux exigences et procédures définies dans la présente PH ;
- garantie 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 utilisateurs l'ensemble des informations nécessaires permettant de vérifier les contremarques de temps qu'elle aura émis.

6.1.2 OBLIGATIONS DE L'ABONNE

L'abonné est tenu de respecter les exigences spécifiques incluses dans les conditions d'utilisation du service d'horodatage.

D'autre part, les logiciels métiers sont en capacité de vérifier la validité des contremarques de temps délivrées par l'AH (notamment vérifier que le certificat de l'Unité d'Horodatage n'est pas révoqué).

6.1.3 OBLIGATIONS DE L'UTILISATEUR DE CONTREMARQUES DE TEMPS

Les utilisateurs de contremarques de temps doivent :

- vérifier que la contremarque de temps a été correctement signée, et que le certificat de l'Unité d'Horodatage est valide à l'instant de la vérification ;
- s'assurer que les contremarques de temps sont obtenues auprès des UH mises en place par le MAE ;
- tenir compte des limitations sur l'utilisation de la contremarque de temps indiquées dans la présente PH ainsi que dans la DPH associée.

6.1.4 OBLIGATIONS POUR LES AC FOURNISSANT LES CERTIFICATS DES UNITES D'HORODATAGE

Les Autorité de Certification AC Infrastructure délivrant des certificats aux Unités d'Horodatage fournit un service de révocation. Les engagements des AC Infrastructure sont consultables à travers leur Politique de Certification [OID : 1.2.250.1.214.69.3.1.3.1.21.1].

Le MAE met à disposition les informations de gestion des certificats, dont le statut de révocation des certificats. Les points de distribution des LCR sont précisés dans le Politique de Certification des AC Infrastructure – Profil « Signature jetons d'horodatage ».

Les AC Infrastructure, pour le profil « Signature jetons d'horodatage », sont qualifiées au sens du RGS pour le niveau *.

6.1.5 DECLARATION DES PRATIQUES D'HORODATAGE

L'Autorité d'horodatage garanti qu'elle possède la fiabilité nécessaire pour fournir des services d'horodatage. En particulier :

- l'AH a mené une analyse de risques sur l'ensemble de son service d'horodatage ;
- l'AH a défini un document de Déclaration des Pratiques d'Horodatage décrivant la mise en œuvre des exigences de la présente PH. Ce document interne garantit que l'AH possède la fiabilité nécessaire pour fournir les services d'horodatage ;
- la Déclaration des Pratiques d'Horodatage 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 et des applications utilisatrices les données nécessaires à la validation des contremarques de temps, soit :
    - les certificats de signature des unités d'horodatage ;
    - les LCR des AC Infrastructure – profil « signature jetons d'horodatage » ;
    - le certificat des AC Infrastructure ;
    - toutes les versions des politiques d'horodatage avec leur date de validité ;
- L'AH dispose d'une organisation adéquate pour l'approbation de la déclaration des pratiques d'horodatage et la vérification de la concordance entre cette déclaration et la présente PH ;
- Le responsable opérationnel de l'AH garantit que les pratiques sont correctement mises en œuvre ;
- L'AH définit une procédure de contrôle périodique de la conformité des pratiques, y compris les responsabilités, à la déclaration des pratiques d'horodatage ;
- L'AH garantit qu'elle mettra à jour la PH en cas de changements majeurs 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, RGS notamment.

6.1.6 CONDITIONS GENERALES D'UTILISATION

Sans Objet.

6.1.7 CONFORMITE AVEC LES EXIGENCES LEGALES

6.1.7.1 DROIT APPLICABLE

Le présent document est régi par la loi française.

6.1.7.2 REGLEMENT DES DIFFERENDS

Toutes contestations et litiges survenant dans l'interprétation et la mise en œuvre du présent document, et à défaut d'accord amiable entre les parties, seront soumis à la juridiction des tribunaux compétents de la cour d'appel de Paris.

6.1.7.3 PROPRIETE INTELLECTUELLE DES INFRASTRUCTURES MAE

Sur le plan de la propriété intellectuelle, les produits mis en œuvre par le MAE 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 du MAE.

6.1.7.4 DONNÉES NOMINATIVES

En conformité avec les dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le traitement automatisé des données nominatives, réalisé à partir des plates-formes d'horodatage du MAE a fait l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés [CNIL].

Conformément à l'article 32 de la loi n° 78-17 du 6 janvier 1978, les utilisateurs sont informés que les données personnelles qu'ils communiquent pourront être transmises et exploitées par le MAE et les différents partenaires intervenant dans les échanges concernés.

Les utilisateurs sont informés qu'ils disposent d'un droit d'accès, de rectification et d'opposition portant sur les données le concernant en contactant l'entité définies en 1.3.2.

Les utilisateurs du service d'horodatage du MAE sont tenus de respecter les dispositions de la loi relative à l'informatique, aux fichiers et aux libertés, dont la violation est passible de sanctions disciplinaires et pénales.

Ils doivent notamment s'abstenir, s'agissant des informations nominatives auxquelles ils accèdent, de toute collecte, de toute utilisation détournée et, d'une manière générale, de tout acte susceptible de porter atteinte à la vie privée ou à la réputation des personnes.

6.2 EXIGENCES OPERATIONNELLES

6.2.1 GESTION DES REQUETES DE CONTREMARQUES DE TEMPS

Les demandes de contremarques de temps sont réalisées selon le protocole défini par le [RFC3161]. L'application demandeuse de contremarque de temps et l'AH s'authentifient mutuellement au préalable de toute transmission de demande de contremarque de temps.

La communication établie garantit l'intégrité et la confidentialité de la demande.

Lorsque l'authentification est positive, l'AH génère la contremarque de temps à partir des données qui lui sont transmises par l'application demandeuse et 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 ne conserve pas la contremarque de temps générée.

6.2.2 FICHIERS D'AUDIT

L'AH garantit que toutes les informations appropriées concernant le fonctionnement du service d'horodatage sont enregistrées pendant une période de temps suffisante et précisée dans la DPH associée à la présente PH, en particulier dans le but de fournir une preuve en cas de litige ou d'enquête judiciaire.

En particulier :

Général

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

Gestion des clés

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

Synchronisation de l'horloge

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

6.2.3 GESTION DE LA DUREE DE VIE DE LA CLE PRIVEE

La durée de vie des clés privées des certificats de signature d'UH et des certificats de signature d'UH est fixée en accord avec les recommandations faites par les autorités nationales compétentes en la matière, comme par exemple celles issues du SGDN/ANSSI et précisées dans le document [RGS 2.0 – Annexe B1].

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

OID : 1.2.250.1.214.69.3.1.3.5.1.1.
Cotation Archive : E.3.1.3.5

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

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

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

6.2.4 SYNCHRONISATION DE L'HORLOGE

L'AH garantit que son horloge est synchronisée avec le temps UTC selon l'exactitude déclarée.
En particulier :

- le calibrage de chaque horloge d'UH est maintenu de telle manière que les horloges ne puissent pas normalement dériver à l'extérieur de l'exactitude déclarée ;
- les horloges des UH sont protégées contre les menaces relatives à leur environnement pouvant aboutir à ne désynchronisation avec le temps UTC en dehors de l'exactitude déclarée ;
- l'AH garantit que, si son horloge interne ne respecte plus l'exactitude déclarée, alors cela sera détecté. Une information de ce type est publiée à destination des utilisateurs de contremarques de temps ;
- si l'horloge d'une UH est détectée comme étant en dehors de l'exactitude annoncée, alors les contremarques de temps ne sont plus générées ;
- l'Autorité d'horodatage garantit que la synchronisation de l'horloge est maintenue lorsqu'un saut de seconde est programmé comme notifié par l'organisme approprié. Le changement pour tenir compte du saut de seconde est effectué durant la dernière minute du jour où le saut de seconde est programmé. Un enregistrement du temps exact (selon l'exactitude déclarée) de l'instant de ce changement est effectué.

  Nota - Un saut de seconde est un ajustement par rapport au temps UTC effectué en sautant ou en ajoutant une seconde durant la dernière minute d'un mois UTC. On donne la première préférence à la fin de décembre et juin et on donne la seconde préférence à la fin de mars et septembre.

Les conditions détaillées de synchronisation par rapport au temps UTC et de maintien de la précision des horloges de l'AH du MAE sont détaillées dans la DPH qui supporte la présente PH.

6.2.5 EXIGENCES DU CONTENU D'UNE CONTREMARQUE DE TEMPS

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

- la contremarque de temps inclut l'identifiant du certificat de l'UH. Ce certificat inclut :
  - un identifiant du pays dans lequel l'AH est établie, en l'occurrence FR ;
  - un identifiant de l'AH ;
  - une identification de l'UH qui génère les contremarques de temps.
- la contremarque de temps contient l'OID de la PH ;
- chaque contremarque de temps comporte un identifiant unique ;

OID : 1.2.250.1.214.69.3.1.3.5.1.1.
Cotation Archive : E.3.1.3.5

- les informations de temps portées dans les contremarques de temps sont reliées à au moins un temps fourni par une source UTC (k) ;
- le temps inclus dans une contremarque de temps est synchronisé avec le temps UTC au moins avec l'exactitude définie dans la DPH ;
- la contremarque de temps inclut une représentation de la donnée à horodater (la valeur de hachage et l'identifiant d'algorithme de hachage) telle que fournie par le demandeur ;
- la contremarque de temps est signée par l'UH à l'aide du certificat délivré par l'AC Infrastructure ;
- la contremarque de temps respecte les exigences du chapitre 7 ci-dessous.

6.2.6 COMPROMISSION DE L'AH

L'AH garantit dans le cas d'événements qui affectent la sécurité des services d'horodatage, incluant la compromission de la clé privée de signature d'une UH ou la perte détectée de calibrage pouvant affecter des contremarques de temps émises, qu'une information appropriée est mise à la disposition des abonnés et des utilisateurs de contremarques de temps. En particulier :

- le plan de secours de l'AH traite le cas de la compromission réelle ou suspectée de la clé privée de signature d'une UH ou la perte de calibrage de l'horloge d'une UH, pouvant affecter des contremarques de temps émises ;
- en cas de compromission, réelle ou suspectée, ou d'une perte de calibrage d'une UH, pouvant affecter des contremarques de temps émises, l'AH met à la disposition de tous les abonnés et utilisateurs de contremarques de temps une description de la compromission survenue ;
- en cas de compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité d'horodatage, pouvant affecter des contremarques de temps émises, l'AH prend les mesures nécessaires pour que les contremarques de temps de cette unité ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation ;
- en cas d'un évènement majeur dans le fonctionnement de l'AH ou d'une une perte de calibrage, qui pourrait affecter des contremarques de temps émises, chaque fois que cela est possible, l'AH met à la disposition de tous ses abonnés et des utilisateurs de contremarques de temps toute information pouvant être utilisée pour identifier les contremarques de temps qui pourraient avoir été affectées, à moins que cela ne contrevienne à la vie privée des abonnés ou à la sécurité des services d'horodatage ;
- l'AH doit également prévenir directement et sans délai le point de contact de la DGME identifié sur le site : http://www.references.modernisation.gouv.fr.

6.2.7 FIN D'ACTIVITE

En cas de fin d'activité du service d'horodatage :

- l'Autorité d'horodatage rendra disponible à tous ses abonnés et aux utilisateurs de contremarques de temps l'information concernant sa fin d'activité ;
- l'AH abroge les éventuelles autorisations données aux sous-traitants d'agir pour son compte dans l'exécution de n'importe quelles fonctions touchant au processus de génération des contremarques de temps ;
- l'AH transfère à un organisme fiable ses obligations de maintien des fichiers d'audit et des archives nécessaires pour démontrer son fonctionnement correct durant une période raisonnable, si elle ne les maintient pas elle-même ;
- l'AH maintien ou transfère à un organisme fiable ses obligations de rendre disponible aux utilisateurs de contremarques de temps pendant une période raisonnable ses clés publiques ainsi que ses certificats ;

- les clés privées des UH sont détruites de telle façon que les clés privées ne puissent pas être recouvrées ;
- l'AH doit également prévenir directement et sans délai le point de contact de la SGMAP identifié sur le site : https://www.references.modernisation.gouv.fr.

6.3 EXIGENCES PHYSIQUES ET ENVIRONNEMENTALES, PROCEDURALES ET ORGANISATIONNELLES

6.3.1 EXIGENCES PHYSIQUES ET ENVIRONNEMENTALES

6.3.1.1 SITUATION GEOGRAPHIQUE ET CONSTRUCTION DES SITES

L'infrastructure du service d'horodatage est hébergée sur le site nominal dans un local sécurisé vis-à-vis des risques naturels.

6.3.1.2 ACCES PHYSIQUE

Les zones hébergeant les systèmes informatiques de l'AH sont physiquement protégées. L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.
Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant un tel accès.

6.3.1.3 ALIMENTATION ELECTRIQUE ET CLIMATISATION

Le serveur hébergeant l'AH sur le site nominal ainsi que son module cryptographique sont branchés électriquement en permanence.
Les locaux hébergeant l'AH sont climatisés.
Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'AH telles que fixées par leurs fournisseurs.

6.3.1.4 VULNERABILITE AUX DEGATS DES EAUX

Les locaux hébergeant l'AH sont protégés contre les dégâts des eaux par le plan de prévention des inondations.

6.3.1.5 PREVENTION ET PROTECTION INCENDIE

Les locaux hébergeant l'AH bénéficient des moyens de prévention et de lutte contre les incendies par des dispositifs de détection d'incendie et d'extinction.

6.3.1.6 CONSERVATION DES SUPPORTS

Les sauvegardes des données et de l'application opérant l'AH sont conservées dans une enceinte sécurisée, accessible aux seules personnes habilitées, autorisées et désignées à ces fins.
Les supports papier de l'AH sont également conservés avec des mesures de sécurité compatibles avec leur niveau de sensibilité.

La DPH identifie les différentes informations et données intervenant dans les activités de l'AH, ainsi que les mesures de sécurité qui leur sont appliquées, afin d'en garantir la confidentialité, l'intégrité et la disponibilité.

6.3.1.7 MISE HORS SERVICE DES SUPPORTS

Les supports papier et électroniques de l'AH en fin de vie sont systématiquement détruits par des moyens appropriés, permettant d'éviter toute perte de confidentialité.
Les matériels et supports informatiques de l'AH ne seront pas utilisés à d'autres fins avant destruction complète des informations liées à l'AH qu'ils sont susceptibles de contenir.

6.3.1.8 SAUVEGARDE HORS SITE

La procédure de sauvegarde des données et logiciels appliquée permet de garantir la continuité d'activité de l'AH, y compris en cas de destruction des sauvegardes situées sur le site nominal.

6.3.2 EXIGENCES PROCEDURALES

L'ensemble des opérations menées par l'AH pour générer et délivrer des contremarques de temps font l'objet d'une attention toute particulière pendant toute la durée de vie des contremarques de temps et des UH :

- les informations et supports d'informations nécessaires à la bonne conduite des opérations de l'AH ;
- les informations confiées à l'AH à des fins de délivrance de ses services d'horodatage, notamment les informations à caractère personnel ;
- la mise en œuvre des matériels nécessaires à la conduite des opérations d'horodatage ;
- les personnels en charge de la conduite des opérations d'horodatage.

L'AH du Ministères des Affaires Étrangères a dans cette optique adopté une organisation avec séparation des rôles du même type que celle mise en œuvre pour les AC Déléguées.

En complément de ces mesures et afin d'assurer un fonctionnement cohérent, sûr et auditable de l'AH du Ministère des Affaires Étrangères, celle-ci s'engage à ce que soient formalisées et respectées les règles internes relatives à :

- la mise en place, le fonctionnement et la maintenance des systèmes ;
- la protection et le service des systèmes ;
- la prise en compte des incidents et la mise en œuvre des mesures nécessaires à en limiter les impacts sur le service d'horodatage ;
- la traçabilité des évènements ;
- les rôles et responsabilités des personnes en charge des opérations ;
- la mise en œuvre et le contrôle d'accès aux systèmes et installations.

6.3.2.1 MANIPULATION ET SECURITE DES SUPPORTS

Les supports d'information utilisés dans le cadre de la délivrance du service d'horodatage de l'AH font l'objet d'un suivi qui tient notamment compte du niveau de sensibilité des informations qu'ils renferment.
Le cycle de vie des supports contenant des informations sensibles est soumis au respect de principes et procédures qui sont précisés dans la DPH. Seuls les personnels habilités et dûment affectés aux rôles de confiance du service d'horodatage ont accès à ces supports, selon le besoin d'en connaitre.

6.3.2.2 PLANIFICATION DE SYSTEME

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

6.3.2.3 RAPPORT D'INCIDENT ET REPONSE

Le traitement des incidents est assuré au sein de l'AH par une entité spécialisée dont le rôle est de centraliser la prise en compte, le suivi des incidents et la communication auprès des entités concernées.

Chaque incident est clairement identifié, est affecté à une entité de l'AH et fait l'objet d'une fiche de suivi. En fin de traitement, l'incident est clos si la vérification est faite que les systèmes d'horodatage sont revenus dans une configuration normale de fonctionnement.

Les interventions correctives sur les systèmes d'horodatage font également l'objet de fiches de traitement.

Les détails du processus de traitement des incidents sont précisés dans la DPH.

6.3.2.4 PROCEDURES DE FONCTIONNEMENT ET RESPONSABILITES

Les opérations de sécurité sont séparées des autres opérations.

Les opérations de sécurité incluent :

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

Ces opérations sont gérées par du personnel habilité et dûment désigné de l'AH, selon les règles relatives au partage des rôles et des responsabilités au sein du Ministères des Affaires Étrangères.

6.3.2.5 ROLES DE CONFIANCE DE L'AUTORITE D'HORODATAGE

Les rôles de confiance définis au niveau de l'Autorité d'Horodatage sont basés sur les rôles définis pour les AC Déléguées, et sont les suivants :

- **Administrateur central -** Personne chargée de la configuration applicative et du maintien en conditions opérationnelles de l'application d'horodatage, ainsi que de l'analyse régulière des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission.
- **Administrateur local –** Personne chargée des opérations de gestion du cycle de vie des certificats émis par les AC Déléguées (demande initiale, révocation, renouvellement recouvrement des certificats).
- **Auditeur -** Personne désignée par l'Autorité d'Horodatage dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par l'Autorité d'Horodatage par rapport aux Politiques d'Horodatage et Déclarations des Pratiques d'Horodatage correspondantes.
- **Autorité Qualifiée -** Personne chargée de la Sécurité de l'application d'horodatage pour le compte de l'Autorité d'Horodatage.

- **Responsable de l'application d'Horodatage -** Personne chargée de la mise en œuvre de la Politiques d'Horodatage et des Déclarations des Pratiques d'Horodatage, au niveau de l'application d'horodatage. Sa responsabilité couvre l'ensemble des fonctions rendues par l'application d'horodatage et des performances correspondantes.
- **Responsable Qualité -** Personne chargée de la vérification de la cohérence des actions des différents rôles décrits précédemment et de la qualité des processus de l'Autorité d'Horodatage.

6.3.2.6 ROLES DE CONFIANCE MUTUALISES

Les rôles de confiance mutualisés et définis au niveau des AC Déléguées et de l'Autorité d'Horodatage sont les suivants :

- **Administrateur sécurité** - Personne chargée d'assurer la gestion de la sécurité au niveau des systèmes, ainsi que de l'habilitation des administrateurs centraux et locaux.
- **Responsable de salle** - Personne chargée de la gestion des accès physiques aux salles informatiques hébergeant l'infrastructure et aux équipements.
- **Exploitant -** Personne chargée d'assurer l'exploitation, la surveillance et la maintenance des systèmes et des réseaux. Cette personne est également chargée d'assurer l'administration des systèmes, la mise en route et la configuration des équipements composant l'infrastructure. Elle réalise notamment le contrôle des fichiers d'audit du système, ainsi que de l'analyse courante des journaux d'évènements système afin de détecter tout incident, anomalie, tentative de compromission, etc.
- **Fonctionnaire de Sécurité des Systèmes d'Informations (FSSI) -** Personne chargée de la Politique de Sécurité du SI du Ministère.
- **Responsable de production -** Personne chargée du maintien en conditions opérationnelles du système d'information du Ministère.

6.3.2.7 NOMBRE DE PERSONNES REQUISES PAR TACHES

Les rôles liés à la gestion des systèmes sont distincts des rôles de gestion de l'application d'horodatage, ainsi que des rôles intervenants sur les données enregistrées au niveau de l'application. Ces différents rôles sont assurés par des personnes distinctes.
Par ailleurs, toute opération impliquant les secrets principaux de l'AH nécessite l'intervention de trois personnes. La DPH précise les opérations nécessitant l'intervention de plusieurs personnes ainsi que les contraintes que ces personnes doivent respecter.

6.3.2.8 IDENTIFICATION ET AUTHENTIFICATION POUR CHAQUE ROLE, GESTION D'ACCES AU SYSTEME

Tout accès à l'application d'horodatage est soumis à authentification (éventuellement forte), les droits d'accès étant définis en fonction des rôles. Notamment, toute personne susceptible d'intervenir auprès de l'application d'horodatage, et ainsi de modifier des données ou des informations de configuration, est préalablement enregistrée dans l'application d'horodatage et dispose d'un certificat d'authentification.
Pour les autres rôles en relation avec l'horodatage, l'AH fait vérifier l'identité et les autorisations du personnel concerné avant :

- que son nom soit ajouté aux listes de contrôle d'accès aux locaux hébergeant la plate-forme de l'horodatage ;
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans ces systèmes.

Ces contrôles sont décrits dans la DPH associée à cette PH.
Chaque attribution de rôle dans l'application d'horodatage est notifiée par écrit.

D'autre part, les contrôles complémentaires suivants sont appliqués au système d'horodatage :

- des contrôles (par exemples des firewalls) sont mis en œuvres pour protéger le réseau interne de l'Autorité d'Horodatage d'accès non autorisés incluant l'accès par des abonnés et des tierces personnes ;
- l'Autorité d'Horodatage garantit que des composants de réseaux locaux (par exemples des routeurs) sont mis en œuvre dans un environnement physiquement sûr et que leurs configurations sont périodiquement vérifiées pour la conformité avec les exigences indiquées par l'AH ;
- une surveillance permanente et des équipements d'alarme sont mis en œuvre pour permettre à l'AH de détecter, d'enregistrer et de réagir rapidement à n'importe quelle tentative non autorisée et / ou irrégulière d'accès à ses ressources

6.3.2.9 ROLES EXIGEANT UNE SEPARATION DES ATTRIBUTIONS

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre, et dans le respect des règles de non-cumul définis dans la partie 6.3.2.7.

Les attributions associées à chaque rôle sont décrites dans la DPH de l'AH.

Les règles de non-cumul des rôles de confiance sont décrites au sein de la DPH.

6.3.2.10 DÉPLOIEMENT ET MAINTENANCE

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

6.3.3 EXIGENCES ORGANISATIONNELLES

6.3.3.1 QUALIFICATIONS, COMPÉTENCES ET HABILITATIONS REQUISES

Tout intervenant amené à occuper un rôle de confiance est soumis à une clause de confidentialité.
Le responsable de l'AH s'assure que les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles, et tient à jour une liste des personnels intervenant dans le cadre du service d'horodatage.
Le personnel d'encadrement possède l'expertise appropriée à son rôle et est familier des procédures de sécurité en vigueur au sein de l'AH.
L'AH informe, par une lettre de mission signée par l'AH, toute personne intervenant dans des rôles de confiance de l'AH :

- de ses responsabilités relatives aux services de l'AH ;
- des procédures liées à la sécurité du système et au contrôle du personnel.

Les personnels employés sur le service d'horodatage du MAE possèdent des connaissances suffisantes :

- sur la technologie de l'horodatage ;

- sur la technologie de la signature numérique ;
- sur les mécanismes pour le calibrage ou la synchronisation des horloges des UH avec le temps UTC ;
- pour le personnel avec des responsabilités de sécurité sur les procédures de sécurité ;
- sur la sécurité de l'information et l'évaluation des risques.

6.3.3.2 PROCEDURES DE VERIFICATION DES ANTECEDENTS

Le personnel amené à assurer un rôle de confiance vis-à-vis de l'AH fait l'objet lors de son entrée en fonction, d'une vérification de ses antécédents par les services du Ministère.

Il est notamment vérifié que :

- les personnels concernés ne possèdent pas de condamnation incompatible avec leurs attributions ;
- les personnels ayant un rôle de confiance ne souffrent pas de conflits d'intérêts préjudiciables à l'impartialité de leurs tâches.

6.3.3.3 EXIGENCES EN MATIERE DE FORMATION INITIALE ET CONTINUE

En préalable à leur entrée en fonction, les administrateurs centraux sont formés aux concepts et objectifs de l'AH, ainsi qu'aux procédures à mettre en œuvre.
Les exploitants et administrateurs système sont formés aux concepts et objectifs de l'AH, ainsi qu'aux logiciels, matériels et procédures d'exploitation applicables.

Chaque évolution dans les systèmes, procédures ou organisation 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 DOCUMENTATION FOURNIE AU PERSONNEL

Le personnel dispose de la documentation relative aux procédures opérationnelles ou organisationnelles et aux outils spécifiques qu'il met en œuvre.

6.4 EXIGENCES DE SECURITE TECHNIQUES

6.4.1 EXACTITUDE TEMPS

Si une unité d'horodatage fournit une exactitude différente de la seconde, alors cette exactitude doit être indiquée dans chaque contremarque de temps générée.

6.4.2 GENERATION DE CLE

La génération des bi-clés cryptographiques des UH est réalisée à l'aide de ressources cryptographiques logicielles. À aucun moment, lors de cette génération, les clés privées d'UH ne sont exportées de ces ressources.
La génération des clés de signature des unités d'horodatage doit être effectuée dans un module d'horodatage répondant aux exigences du chapitre 8 ci-dessous.

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

6.4.3 CERTIFICATION DES CLES DE L'UNITE D'HORODATAGE

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

L'Autorité d'Horodatage doit s'assurer qu'une demande de certificat d'Unité d'Horodatage auprès d'une Autorité de Certification contient, en plus des informations exigées dans la PC Type « cachet » pour la partie enregistrement, au moins les informations suivantes :

- le nom (DN) de l'unité d'horodatage pour laquelle la demande de certificat est faite ;
- la valeur de la clé publique (et l'identifiant de l'algorithme) ;
- la durée d'utilisation souhaitée pour la clé privée.

L'Autorité d'Horodatage doit vérifier, lors de l'import du certificat de l'Unité d'Horodatage, qu'il provient bien de l'Autorité de Certification auprès de laquelle la demande de certificat a été effectuée.
L'Autorité d'Horodatage doit s'assurer que l'Unité d'Horodatage ne peut être opérationnelle qu'une fois ces exigences remplies.

6.4.4 PROTECTION DES CLES PRIVEES DES UNITES D'HORODATAGE

L'AH garantit que la clé privée de son unité d'horodatage reste confidentielle et conserve son intégrité. En particulier, la clé de signature de l'unité d'horodatage doit être gardée et utilisée à l'intérieur d'un module d'horodatage répondant aux exigences de l'état de l'art en la matière.

6.4.5 EXIGENCES DE SAUVEGARDE DES CLES DES UNITES D'HORODATAGE

La présente PH ne comporte pas de politique de sauvegarde des clés des UH. Les clés des UH ne sont pas exportables et ne sont de fait pas sauvegardées.

6.4.6 DESTRUCTION DES CLES DES UNITES D'HORODATAGE

En fin de vie d'une clé privée d'UH, normale ou anticipée (révocation), cette clé est détruite afin qu'elle ne puisse être recouvrée et employée au-delà. Elle n'est pas exportable et n'est pas sauvegardée.

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 [RGS 2.0 – Annexe B1]. Les algorithmes de calcul d'empreinte numérique acceptés sont SHA 1 et SHA 2 ;
- 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 [RGS 2.0 – Annexe B1]. La bi-clé de l'UH est au minimum une bi-clé RSA de 2048 bits.

6.4.8 VERIFICATION DES CONTREMARQUES DE TEMPS

L'AH tient à disposition des clients les informations nécessaires à la vérification de la signature électronique des contremarques de temps. L'ensemble des informations et les moyens de leurs mise à disposition par l'AH seront précisés dans la DPH.
La vérification d'une signature électronique de contremarque de temps consiste en les opérations suivantes :

OID : 1.2.250.1.214.69.3.1.3.5.1.1.
Cotation Archive : E.3.1.3.5

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

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

6.4.9 DUREE DE VALIDITE DES CERTIFICATS DE CLE PUBLIQUE DES UNITES D'HORODATAGE

La durée de validité des certificats d'UH est égale à 3 ans.

Cette durée de validité pourra être revue si les recommandations des autorités nationales compétentes sont amenées à évoluer.

6.4.10 DUREE D'UTILISATION DES CLES PRIVEES DES UNITES D'HORODATAGE

La durée d'utilisation opérationnelle d'une clé privée d'UH est au plus égale à la période de validité du certificat de clé publique correspondant.

Dans la pratique elle est réduite afin que la fin de période de vérification de la dernière contremarque de temps qu'elle a signé coïncide avec la fin de validité du certificat de clé publique d'UH auquel elle correspond.

La durée d'utilisation opérationnelle des clés privées d'UH est égale à 3 ans.

Cette durée de validité pourra être revue si les recommandations des autorités nationales compétentes sont amenées à évoluer.

7 ANNEXE 1 : EXIGENCES SUR LES FORMATS DES CONTREMARQUES DE TEMPS, DES CERTIFICATS ET DES LCR ET SUR LES ALGORITHMES CRYPTOGRAPHIQUES

7.1 CONTREMARQUES DE TEMPS

Les contremarques de temps fournies par l'AH MAE 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 [RFC3161], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	**Exigences**
messageImprint	Cf. chapitre 7.3 ci-dessous sur les exigences concernant les fonctions de hachage.
accuracy	Précision de 1 seconde
ordering	False
tsa	CN= FQDN du serveur OU= 0002 12000601000025 O= MINISTERE DES AFFAIRES ETRANGERES C = FR Subject Serial Number= <nom du VLAN> Adresse électronique = <assistance.dsi@diplomatie.gouv.fr>
extensions	Sans Objet

7.2 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 2.0 – Annexe A4] et [RGS 1.0 – Annexe A13].
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 2.0 – Annexe A4]) et l'identifiant propre à l'UH concernée, au sein de l'AH, doit être porté dans l'attribut « commonName » du DN de ce champ (au sein d'une AH, chaque UH doit avoir 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}.

Les LCR qui comportent des numéros de série correspondant à des certificats d'unité d'horodatage supportent l'extension d'entrée LCR : « reasonCode »

OID : 1.2.250.1.214.69.3.1.3.5.1.1.
Cotation Archive : E.3.1.3.5

7.3 ALGORITHMES CRYPTOGRAPHIQUES

Les algorithmes et fonctions cryptographiques (hachage, signature) mis en œuvre pour la génération des différents certificats, pour la génération des contremarques de temps ainsi que la valeur du champ messageImprint dans les contremarques de temps respectent les exigences correspondantes de [RGS 2.0 – Annexe A4].

8 ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE D'HORODATAGE DES UH

8.1 EXIGENCES SUR LES OBJECTIFS DE SECURITE

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 ;
- être 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 ;
- être 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 ;
- être 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.

8.2 EXIGENCES COMPLEMENTAIRES

Sans Objet.

9 ANNEXE 3 : VERIFICATION OU UTILISATION (INFORMATIVE)

Cette politique d'horodatage prévoit la vérification d'une contremarque de temps, pendant la période de validité du certificat de clé publique de l'unité d'horodatage qui l'a générée.

9.1 EMPILEMENT DES CONTREMARQUES DE TEMPS

S'il s'avère nécessaire de prolonger la durée de vie d'une contremarque de temps ou d'en conforter la robustesse, il est possible d'ajouter une contremarque de temps supplémentaire fournie par une autre unité d'horodatage.

Pour cela, il convient de pouvoir prouver que le certificat de l'unité d'horodatage référencé dans la contremarque de temps d'origine n'était pas révoqué au moment où la contremarque de temps supplémentaire a été ajoutée.
Après s'être assuré que l'unité d'horodatage qui a généré la première contremarque de temps n'est pas révoquée, une contremarque de temps supplémentaire sera apposée sur la contremarque précédente.

Les LCR des AC en charge de l'unité d'horodatage sont archivées afin de pouvoir démontrer que l'unité d'horodatage ayant généré la première contremarque de temps n'était pas révoquée à ce moment-là.

Lors d'une vérification ultérieure, un utilisateur de contremarque de temps devra vérifier les deux contremarques de temps et s'assurer que l'unité d'horodatage ayant généré la première contremarque n'était pas révoquée à la date où la seconde contremarque de temps a été apposée. L'utilisateur de contremarque de temps devra en outre s'assurer que le certificat de l'unité d'horodatage ayant généré la seconde contremarque de temps n'est pas révoquée à l'instant de la vérification ultérieure.

9.2 GESTION DE LA REVOCATION PAR LES AUTORITES DE CERTIFICATION

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

10 ANNEXE 4 : PRECISION DE LA SYNCHRONISATION DE L'HORLOGE

La précision de l'horloge est de l'ordre d'une seconde par rapport au temps UTC(k).

11 ANNEXE 5 : PROTOCOLE D'HORODATAGE

11.1 CONFORMITE AU RFC 3161

Le protocole d'horodatage utilisé est conforme au [RFC3161].

11.2 CONFORMITE AU STANDARD ETSI TS 101 861

Le protocole d'horodatage est conforme au standard [ETSI_TSP].