# INFRASTRUCTURE DE CONFIANCE NATIONALE
# AC TECHNIQUE
## POLITIQUE D'HORODATAGE (PH)

| Version | Date | Description | Auteurs | Service |
|---|---|---|---|---|
| 0.1 | 13/08/2021 | Version initiale | SH | DSN |
| 0.9 | 16/11/2021 | Version mise à jour | SH - FG | DSN - AMSN |
| 0.91 | 17/11/2021 | Version mise à jour | SH - LB | DSN |
| 0.92 | 10/12/2021 | Version mise à jour | LB | DSN |
| 1.0 | 27/01/2022 | Alignements PH - RGS | LB | DSN |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| État du document - Classification | Référence |
|---|---|
| En cours – Publique | 2.16.492.1.1.1.1.6.11.2 |

Ce document comporte 21 pages.

# Sommaire

# 1 INTRODUCTION

## 1.1 PRESENTATION GENERALE

Le service d'Horodatage de la DIRECTION DES SERVICES NUMÉRIQUES (DSN) peut être utilisé par ses « clients » :

- inclus dans l'offre de signature électronique de la DSN, pour fournir des dates fiables, donnant ainsi une bonne assurance sur la qualité des dates associées aux actes de signature,

- directement, en tant que service à part entière.

L'objectif de ce document est de définir les engagements que la DSN, en tant qu'AH, respecte dans la délivrance et la gestion de contremarques de temps, ainsi que les obligations des autres participants. Le respect de ces engagements permet, après audit de conformité selon les processus établis dans le règlement eIDAS, la qualification du service d'horodatage de la DIRECTION DES SERVICES NUMÉRIQUES par l'organe de contrôle national.

La structure de la présente Politique d'Horodatage est basée sur les documents issus de l'ETSI et du [RGSP].

Le présent document intègre, pour sa partie mise en œuvre, la Déclaration des Pratiques d'Horodatage. Ainsi il expose les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la PH, en particulier les processus qu'une UH emploiera pour la création des contremarques de temps et le maintien de l'exactitude de ses horloges.

Le présent document est complété par les Conditions Générales d'Utilisation du Service d'Horodatage [CGU-SH].

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 de l'utilisateur du service d'horodatage.

## 1.2 IDENTIFIANT DU DOCUMENT

La présente PH est dénommée « Politique d'Horodatage de la DSN ».

La présente PH est identifié par l'Identifiant d'Objet (OID): 2.16.492.1.1.1.1.6.11.2

## 1.3 PUBLICATION DU DOCUMENT

La présente Politique d'Horodatage est publiée sur l'URL : https://mconnect.gouv.mc/technique

## 1.4 GESTION DE LA PH

L'entité en charge de l'administration et de la gestion de la politique d'horodatage (PH) est l'autorité d'horodatage (AH) . L'AH est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PH de sa déclaration des pratiques d'horodatage.

## 1.5 POINT DE CONTACT

Toute demande relative à la présente Politique d'Horodatage est à adresser à :

Direction des Services Numériques
2 rue du Gabian, immeuble "Les Industries"
BP 673 MC
98014 Monaco Cedex

## 1.6 GENERALITES

### 1.6.1 Définitions

**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. Cette notion est valable pour les hypothèses où la contremarque de temps est demandée directement à l'AH.

**Autorité de Certification (AC) -** Entité émettant des Certificats après vérification de l'identité de la personne ou du représentant du système applicatif, ou de la procédure ayant mené à son identification. L'AC est responsable de l'ensemble des composantes matérielles, humaines et organisationnelles utilisées dans le processus de création et de gestion des Certificats.

**Autorité d'Horodatage (AH) -** Entité responsable de la gestion de l'environnement d'horodatage et de la production des jetons d'horodatage sur les données qui lui sont présentées afin d'attester de l'existence de ces données à la date de la marque de temps.

L'AH est une entité subordonnée au PSHE et ne dispose pas nécessairement de la personnalité juridique.

**Contremarque de temps ou jeton 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. La déclaration de ces pratiques est incluse dans ce présent document.

**Horodatage :** Service qui associe de manière sûre un événement et une heure afin d'établir de manière fiable l'heure à laquelle cet événement s'est réalisé.

**Horodatage électronique** : des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant ;

**Horodatage électronique qualifié,** un horodatage électronique qui satisfait aux exigences fixées à l'article 32 et 33 du [RGSP].

**Jeton d'horodatage -** Voir contremarque de temps.

**Liste de Certificats Révoqués (LCR)** – Liste de certificats ayant fait l'objet d'une révocation avant la fin de leur période de validité.

**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.

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

**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 [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).

**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.

### 1.6.2 Abréviations

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

AC Autorité de Certification

AH Autorité d'Horodatage

C2SC Comité de Suivi des Services de Confiance

CGU Conditions Générales d'utilisation du service d'Horodatage

DPH Déclaration des Pratiques d'Horodatage

DSN Direction des Services Numériques (Gouvernement Princier)

ETSI European Telecommunications Standards Institute

LCR Liste des Certificats Révoqués

IGC Infrastructure de Gestion de Clés

OID Object Identifier

PH Politique d'Horodatage

PP Profil de Protection

RSSI Responsable de la Sécurité des Systèmes d'Information

UH Unité d'Horodatage

UTC Coordinated Universal Time

# 2 DISPOSITIONS GENERALES

## 2.1 OBLIGATIONS DE L'AUTORITE D'HORODATAGE

L'AH génère et signe les contremarques de temps conformément aux documents suivants : la présente PH et les CGU.

L'AH garantit la conformité pour tout acteur intervenant dans la gestion des contremarques de temps par rapport aux exigences et aux procédures prescrites dans cette PH.

L'AH remplit tous ses engagements tels que stipulés dans ses Conditions générales d'utilisation.

L'AH garantit la conformité des exigences et procédures définies dans la présente PH.

L'AH met à la disposition des abonnés et utilisateurs l'ensemble des informations nécessaires à la vérification des contremarques de temps.

L'AH respecte les conditions de disponibilité du service d'horodatage convenues contractuellement avec les abonnés.

L'AH maintient une information sur la compromission de la Bi-clé des UH.

## 2.2 OBLIGATIONS DE L'ABONNE

Au-delà des exigences spécifiques incluses dans les conditions générales d'utilisation du service d'horodatage, et que doit respecter l'abonné, il est recommandé que ce dernier, au moment de l'obtention d'une contremarque de temps, vérifie que le certificat de l'Unité d'Horodatage n'est pas révoqué.

## 2.3 OBLIGATIONS DE L'UTILISATEUR DE CONTREMARQUES DE TEMPS

Pour faire confiance à une contremarque de temps, l'utilisateur devra :

a) Vérifier que la contremarque de temps a été correctement signée, et que le certificat de l'UH est valide à l'instant de la vérification.

b) tenir compte des limitations sur l'utilisation de la contremarque de temps indiquées dans la PH et les conditions générales d'utilisation.

## 2.4 OBLIGATIONS POUR LES AC FOURNISSANT LES CERTIFICATS DES UHS

Les certificats des UH doivent être qualifiés. Ils sont délivrés par l'AC TECHNIQUE.

## 2.5 DECLARATIONS DES PRATIQUES D'HORODATAGE

L'AH garantit qu'elle possède la fiabilité nécessaire pour fournir le service d'horodatage. En particulier :

a) L'AH a effectué une analyse de risque afin de déterminer les contrôles de sécurité nécessaires et les procédures opérationnelles.

b) L'AH déclare les pratiques et des procédures utilisées pour adresser toutes les exigences identifiées dans la PH supportée.

c) L'AH identifie les obligations de toutes les organisations externes participant à la fourniture du service d'horodatage, y compris la politique applicable et les pratiques. Cela inclut l'AC fournissant les certificats aux UH.

d) L'AH met à la disposition des abonnés et des utilisateurs de contremarques de temps les éléments publics de sa PH, s'il y a lieu, et toute autre documentation appropriée, tel que nécessaire pour évaluer la conformité à la PH.

e) L'AH dispose d'une organisation adéquate pour l'approbation de sa PH et de la déclaration de ses pratiques.

f) Le responsable opérationnel de l'AH garantit que les pratiques sont correctement mises en œuvre.

g) L'AH définit une procédure de contrôle périodique de la conformité des pratiques, y compris les responsabilités, à la déclaration des pratiques d'horodatage.

h) L'AH doit informer les abonnés pour tout changement qu'elle a l'intention de faire dans la partie publique de sa PH et, après l'approbation, immédiatement mettre à la disposition des abonnés et des utilisateurs de contremarques de temps la partie publique révisée de la PH et de sa déclaration des pratiques d'horodatage.

i) Si l'AH a été évaluée pour être en conformité avec la présente PH et si une modification envisagée à l'initiative de l'AH pouvait entraîner une non-conformité avec ladite PH, alors l'AH soumettra cette modification à l'organisme évaluateur indépendant pour avis.

Le processus de révision des politiques de sécurité et chartes liées est annuel. Il fait l'objet d'audit de révision interne ou par un organisme agrée COFRAC tous les ans.

### 2.6 CONDITIONS GENERALES D'UTILISATION

L'AH définit des CGU qui reprennent les grands principes décrits dans la présente PH. Ces CGU sont basées sur le modèle défini dans l'annexe B de l'ETSI 102023 et font office de *TSA disclosure statement*.

Les CGU du service d'horodatage sont mises à disposition des abonnés et utilisateurs (actuels ou potentiels) des contremarques de temps à l'URL suivante : https://mconnect.gouv.mc/technique

### 2.7 CONFORMITE AVEC LES EXIGENCES LEGALES

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

a) Des mesures techniques appropriées et organisationnelles sont prises contre le traitement non autorisé ou illégal des données à caractère personnel (cf. [CCIN]), contre la perte accidentelle, la destruction de données à caractère personnel ou les dégâts commis aux données à caractère personnel.

b) Les informations fournies par les abonnés à l'AH ne sont pas divulguées, à moins de leur accord, d'une décision judiciaire ou d'une exigence légale.

## 3 EXIGENCES OPERATIONNELLES

### 3.1 GESTION DES REQUETES DE CONTREMARQUES DE TEMPS

L'AH fournit une contremarque de temps en réponse à une demande contenant l'empreinte de la donnée à horodater.

La fourniture d'une contremarque de temps en réponse à une demande n'excède pas quelques secondes[1], ceci afin de ne pas nuire ni dégrader l'ergonomie de l'application appelante.

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

[1] Ce temps de réponse est le délai écoulé entre la réception de la requête et la signature de la contremarque de temps résultante.

Le service d'horodatage est géré selon une convention de service garantissant une qualité de service avec une disponibilité permanente. En cas de force majeure les contremarques de temps ne seront plus générées. Dans ce cas une communication sur l'indisponibilité du service est faite le temps de restaurer les fonctionnalités.

## 3.2 FICHIERS D'AUDIT

L'AH enregistre les informations appropriées concernant le fonctionnement du service d'horodatage, en particulier :

a) Les enregistrements d'audit relatifs à l'administration des services d'horodatage,

b) Les enregistrements d'audit relatifs au fonctionnement du service d'horodatage,

c) Les enregistrements d'audit concernant les événements touchant au cycle de vie des clés et certificats d'UH,

d) Les enregistrements d'audit concernant les événements touchant à une synchronisation de l'horloge des UH, y compris les événements touchant à la détection de perte de synchronisation.

Les journaux d'évènements du service d'horodatage sont conservés pendant 1 an.

La confidentialité des enregistrements d'audit est assurée par une gestion d'accès physique, système et réseau appropriée. L'intégrité et la protection contre la suppression sont assurées par un système de rotation de journaux ainsi que par la centralisation des journaux d'évènements dans un puit de log.

Les modalités de gestion des traces de l'intégrité de logs sont consignées dans Dossier d'Architecture Technique [OID-2.16.492.1.1.1.1.20.6.1] de la solution et dans son complément [OID_2.16.492.1.1.1.1.20.7.9]

## 3.3 GESTION DE LA DUREE DE VIE DE LA CLE PRIVEE

L'AH garantit que les clés privées de signature des UH ne sont pas employées au-delà de la fin de leur cycle de vie. En particulier :

a) Des procédures opérationnelles ou techniques assurent qu'une nouvelle paire de clés est mise en place quand la fin de la période d'utilisation d'une clé privée d'UH a été atteinte. Le responsable de l'UH organise ainsi le renouvellement de la bi clé et du certificat tous les ans.

b) Le Système d'horodatage détruit la clé privée si la fin de la période d'utilisation de cette clé privée a été atteinte.

La durée de vie des clés privées de Signature des UH est définie dans la section 5.10.

Aucun jeton de temps n'est émis au-delà de la période de validité du certificat.

## 3.4 SYNCHRONISATION DE L'HORLOGE

L'AH garantit que son horloge est synchronisée avec le temps UTC selon l'exactitude déclarée d'une seconde.

La synchronisation utilise des serveurs de temps qui sont eux-mêmes synchronisés sur plusieurs sources :

- une source de temps souveraine issue de dispositifs locaux. Cette source de temps dispose d'un récepteur sur trois constellations de satellites : GPS (USA) / GLONASS (RUSSIE) / Beidou (CHINE), équipée en plus d'un oscillateur OCXO qui garantit la stabilité avec une dérive de moins de 25 microsecondes en cas de perte d'un des trois signaux satellite ou d'un défaut sur le récepteur satellite. Cette source de temps alimente un serveur NTP qui distribue l'heure directement à l'UH.
- du pool NTP de référence international (NTP Pool Project) fr.pool.ntp.org

En particulier :

a) Le calibrage de chaque horloge d'UH est maintenu de telle manière que les horloges ne puissent pas normalement dériver en dehors de l'exactitude déclarée.

b) Les horloges des unités d'horodatage sont protégées contre les menaces relatives à leur environnement qui pourraient aboutir à une désynchronisation avec le temps UTC en dehors de l'exactitude déclarée.

c) L'AH s'assure que tout non-respect de l'exactitude déclarée par son horloge interne sera détecté.

d) Si l'horloge d'une UH est détectée comme étant en dehors de l'exactitude annoncée, ou que les serveurs de temps ne sont plus disponibles, alors les contremarques de temps ne seront plus générées. Dans ce cas une communication sur l'indisponibilité du service est faite le temps de restaurer la situation.

e) L'AH garantit que la synchronisation de l'horloge est maintenue lorsqu'un saut de seconde est programmé comme notifié par l'organisme approprié (souscription au bulletin C d'annonce des secondes intercalaires de l'observatoire de Paris) . 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 (à la seconde près) de l'instant de ce changement est effectué.

La section *5.1 Exactitude de temps* de ce document précise les moyens de surveillance de la synchronisation des sources de temps de l'UH.

## 3.5 EXIGENCES DU CONTENU D'UNE CONTREMARQUE DE TEMPS

Les contremarques de temps sont générées dans un environnement sûr et contiennent les informations suivantes :

- L'identifiant de l'UH fourni à travers le DN du certificat de l'unité d'horodatage ;
- L'identifiant (OID) de la politique d'horodatage appliquée ;
- Un identifiant unique de la contremarque ;
- Un temps, celui du moment de génération de la contremarque, synchronisé avec le temps UTC avec une précision d'une seconde ;
- L'empreinte et l'algorithme d'empreinte de la donnée horodatée.

Les contremarques sont signées par l'UH avec sa clé privée, réservée à cet usage.

Les contremarques de temps sont qualifié.

La délivrance des contremarques de temps est à la discrétion de l'AH.

Les contremarques sont conformes à la [RFC 3161]. Le détail des attributs est présenté au §5.11 Format des contremarques de temps.

## 3.6 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 qui pourrait affecter des contremarques de temps émises –, qu'une information appropriée est mise à la disposition des abonnés et des utilisateurs de contremarques de temps. En particulier,

a) 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, qui pourrait affecter des contremarques de temps émises dans le cadre d'un plan de secours

b) Dans le cas d'une compromission, réelle ou suspectée, l'AH mettra à la disposition de tous les abonnés et utilisateurs de contremarques de temps une description de la compromission qui est survenue.

c) Dans le cas d'une perte de calibrage d'une UH, qui pourrait affecter des contremarques de temps émises, l'AH prendra les mesures nécessaires pour que les contremarques de temps de cette UH ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.

d) Dans le cas d'une perte de connexion prolongés avec les serveurs de temps, l'AH prendra les mesures nécessaires pour que les contremarques de temps de cette UH ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.

e) Dans le cas d'un événement majeur dans le fonctionnement de l'AH ou d'une perte de calibrage qui pourrait affecter des contremarques de temps émises, chaque fois que cela sera possible, l'AH mettra à la disposition de tous ses abonnés et 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.

f) L'AH prévient directement et sans délai le point de contact de l'organe de contrôle national (C2SC) et engage la procédure de gestion de crise.

En cas de telles compromissions, les informations sont publiées directement sur le site mconnect.gouv.mc et relayés par les canaux de communication habituels du Gouvernement Princier auprès de ses administrés.

## 3.7 FIN D'ACTIVITE

Des procédures de fin d'activité définies par l'AH garantissent que les dérangements potentiels aux abonnés et aux utilisateurs de contremarques de temps seront réduits au minimum suite à la cessation d'activité du service d'horodatage et assurent en particulier la maintenance continue des informations nécessaires pour vérifier la justesse de contremarques de temps. En particulier :

a) Avant que l'AH ne termine ses services d'horodatage, les procédures suivantes seront exécutées au minimum :

- l'AH rendra disponible à tous ses abonnés et utilisateurs de contremarques de temps l'information concernant sa fin d'activité ;

- l'AH abrogera les autorisations données aux sous-traitants d'agir pour son compte dans l'exécution de n'importe quelles fonctions touchant au processus de génération des contremarques de temps ;

- l'AH transférera à un organisme fiable ses obligations de maintien des fichiers d'audit et des archives nécessaires pour démontrer son fonctionnement correct durant une période raisonnable ;

- l'AH maintiendra ou transférera à un organisme fiable ses obligations de rendre disponibles aux utilisateurs de contremarques de temps pendant une période raisonnable ses clés publiques ainsi que ses certificats;

- les clés privées des UH seront détruites de telle façon que les clés privées ne puissent pas être recouvrées.

b) L'AH prend les mesures nécessaires pour couvrir les dépenses pour accomplir ces exigences minimales dans le cas où l'AH tomberait en faillite ou pour d'autres raisons serait incapable de couvrir les dépenses par elle-même.

c) L'AH prévient directement et sans délai le point de contact de l'organe de contrôle national (C2SC)

# 4 EXIGENCES PHYSIQUES ET ENVIRONNEMENTALES, PROCEDURALES ET ORGANISATIONNELLES

## 4.1 EXIGENCES PHYSIQUES ET ENVIRONNEMENTALES

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

a) A la fois pour la fourniture du service d'horodatage et la gestion de l'horodatage :

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

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

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

- le système d'horodatage fonctionne dans un environnement qui protège physiquement les services de la compromission au moyen d'un accès non autorisé aux systèmes ou aux données ;
- la protection physique est réalisée par la création d'un périmètre de sécurité dédié clairement défini (c'est-à-dire des barrières physiques) autour des unités d'horodatage ;

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

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

Ces exigences sont implémentées aussi bien sur le centre d'hébergement principal que sur le centre d'hébergement de continuité d'activité redondé.

## 4.2 EXIGENCES PROCEDURALES

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

a) L'intégrité des composants du système d'horodatage et l'information sont protégés contre les virus, les logiciels malveillants et non autorisés

b) Un rapport d'incident et des procédures de réponse aux incidents sont employés d'une telle façon que les dégâts liés aux incidents de sécurité et aux défaillances soient réduits au minimum.

c) Les supports employés dans les systèmes d'horodatage sont manipulés de manière sécuritaire pour les protéger des dégâts, du vol, de l'accès non autorisé et de l'obsolescence

d) Des procédures sont établies et mises en œuvre pour tous les rôles de confiance et administratifs qui impactent la fourniture des services d'horodatage

**Manipulation et sécurité des supports**

e) Tous les supports doivent être traités de manière sécuritaire conformément aux exigences de la classification de l'information. Les supports contenant des données sensibles doivent être retirés de manière sécuritaire quand ils ne sont plus utiles

**Planification de système**

f) Les charges doivent être contrôlées et des projections de charge dans le futur doivent être effectuées pour garantir que les puissances de traitement et de stockage adéquates seront disponibles.

**Rapport d'incident et réponse**

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

Les contrôles complémentaires suivants doivent être appliqués à la gestion de l'horodatage :

**Procédures de fonctionnement et responsabilités**

h) Les opérations de sécurité sont séparées des autres opérations. Elles 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.

Les opérations de sécurité sur les composantes du service d'horodatage sont réalisées par du personnel de confiance.

Gestion d'accès au système

L'Autorité d'horodatage doit garantir que l'accès au système d'horodatage est limité aux individus dûment autorisés. En particulier :

a) Des contrôles (par pares-feux) sont être mis en œuvre pour protéger le réseau interne de l'AH d'accès non autorisés incluant l'accès par des abonnés et des tierces personnes.

Les pares-feux sont aussi configurés pour bloquer tous les protocoles et les accès non nécessaires au fonctionnement de l'AH.

b) L'AH effectue une administration efficace des utilisateurs (opérateurs, administrateurs et auditeurs), pour maintenir la sécurité du système, y compris la gestion des comptes des utilisateurs, l'audit, et la modification ou le retrait rapide d'accès.
c) l'AH garantit que l'accès aux fonctions du système, à l'information et aux applications est limité conformément à la politique de contrôle d'accès et que le système d'horodatage possède les contrôles informatiques de sécurité suffisants pour la séparation des rôles de confiance identifiés dans les pratiques d'horodatage, y compris la séparation des fonctions d'administrateur de sécurité et des fonctions opérationnelles. En particulier, l'utilisation de programmes systèmes utilitaires sera limitée et très contrôlée.
d) Le personnel de l'AH est dûment identifié et authentifié avant d'utiliser des applications critiques liées à l'horodatage.
e) Le personnel de l'AH sera tenu responsable de ses activités, par exemple en conservant des fichiers d'audit.

Les contrôles complémentaires suivants doivent être appliqués à la gestion de l'horodatage :
f) L'Autorité d'horodatage garantit que des composants de réseau locaux (par exemple les routeurs) seront mis dans un environnement physiquement sûr et que leurs configurations sont périodiquement vérifiées pour la conformité avec les exigences indiquées par l'AH.
g) Une surveillance permanente et des équipements d'alarme doivent être mis en oeuvre 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.

Déploiement et Maintenance

L'AH emploie des produits et systèmes de confiance.

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

## 4.3 EXIGENCES ORGANISATIONNELLES

L'AH garantit que le personnel et les pratiques d'embauche améliorent et concourent à la fiabilité des opérations de l'AH. En particulier :
a) L'Autorité d'horodatage emploie un personnel qui possède l'expertise, l'expérience et les qualifications nécessaires pour les services offerts, tels que l'exige la fonction.
b) Les rôles de sécurité et les responsabilités, comme spécifié dans la politique de sécurité de l'AH, sont documentés dans des descriptions de poste. Les rôles de confiance, sur lesquels la sécurité du fonctionnement de l'AH repose, sont clairement identifiés.
c) Des descriptions de fonctions sont définies pour le personnel de l'AH (aussi bien provisoire que permanent) du point de vue de la séparation des responsabilités et du principe du privilège minimum, selon la sensibilité de la fonction sur la base des responsabilités et des niveaux d'accès, et indiquent le type d'enquête à effectuer sur le passé, le type de formation appropriée et les particularités de la fonction.
d) Le personnel met en œuvre des procédures administratives et de gestion ainsi que des processus en accord avec les procédures de gestion de sécurité de l'information de l'AH

Les contrôles complémentaires suivants sont appliqués à la gestion de l'horodatage :
e) le personnel de gestion employé possède :
- la connaissance de la technologie de l'horodatage et ;
- la connaissance de technologie de la signature numérique et ;
- la connaissance des mécanismes pour le calibrage ou la synchronisation des horloges des unités d'horodatage avec le temps UTC et ;

- pour le personnel avec des responsabilités de sécurité, une bonne connaissance des procédures de sécurité, et ;
- l'expérience avec la sécurité de l'information et l'évaluation des risques.

f) Tout le personnel de l'AH dans des rôles de confiance est libre de conflit d'intérêt qui pourrait porter préjudice à l'impartialité des opérations de l'AH.

g) Les rôles de confiance incluent les rôles qui impliquent les responsabilités suivantes :
- les officiers chargés de la sécurité : responsabilité complète d'administrer la mise en oeuvre des pratiques de sécurité ;
- les administrateurs système : autorisés à installer, configurer et maintenir les modules d'horodatage de l'AH pour la gestion de l'horodatage ;
- les opérateurs système : responsables pour faire fonctionner les modules d'horodatage de l'AH de manière quotidienne et autorisés pour effectuer les opérations de sauvegarde et des secours ;
- les auditeurs de système : autorisés à consulter les archives et les fichiers d'audit des modules d'horodatage.

h) Le personnel de l'AH est formellement nommé aux rôles de confiance par la direction responsable de la sécurité.

i) L'AH s'interdit de nommer aux rôles de confiance ou de gestion toute personne connue pour avoir une condamnation pour un crime sérieux ou une autre infraction qui affecte son adéquation avec la position. Le personnel n'a pas accès aux fonctions de confiance avant que les contrôles nécessaires ne soient achevés.

# 5 EXIGENCES DE SECURITE TECHNIQUES

## 5.1 EXACTITUDE TEMPS

L'AH garantit que les contremarques de temps sont générées avec une exactitude de temps de 1 seconde par rapport au temps UTC.

Cette précision est obtenue par synchronisation et contrôle des horloges des UH en se basant sur les sources de temps définies au chapitre 3.4.

Surveillance de la synchronisation des horloges :

Un script de synchronisation de l'horloge permet la surveillance régulière de la synchronisation de l'horloge système avec ses sources de temps de référence par le protocole NTP.

L'activation et le paramétrage de ce mécanisme de surveillance sont détaillés dans la solution technique de la solution logicielle de l'UH.

Le document *20220213_Unite Horodatage MROADv1.1_OID_2.16.492.1.1.1.1.6.7.14.docx* présente le fonctionnement de ces mécanismes.

## 5.2 GENERATION DE CLE

L'AH garantit que les clés cryptographiques des UH sont produites dans des circonstances et un environnement contrôlé, qui a fait l'objet d'une cérémonie de clés et d'un procès-verbal.

Ces clés sont générées et protégées au sein de HSM (Hardware Security Module) cryptographiques et ne sont pas exportées. La longueur des clés de l'AH est de 2048 bits avec l'algorithme RSA.

## 5.3 CERTIFICATION DES CLES DE L'UNITE D'HORODATAGE

L'AH s'assure que la valeur de la clé publique et l'identifiant de l'algorithme de signature contenus dans la demande de certificat de l'UH sont égaux à ceux générés par l'UH.

Le certificat de l'UH est généré par l'AC Technique.

La demande de certificat envoyée auprès de l'AC contient, en plus des informations exigées dans la PC de l'AC pour la partie enregistrement, au moins les informations suivantes :

- le nom (DN) de l'UH pour laquelle la demande de certificat est faite ;
- la valeur de la clé publique (et l'identifiant de l'algorithme).

L'AH vérifie lors de l'import du certificat de l'UH qu'il est bien émis par l'AC requise et qu'il est conforme au gabarit attendu. L'AH s'assure que l'UH ne peut être opérationnelle qu'une fois ces vérifications effectuées avec succès.

## 5.4 PROTECTION DES CLES PRIVEES DES UNITES D'HORODATAGE

Les clés privées des UH sont générées et stockées dans un HSM certifié CC EAL4+ et qualifié par l'ANSSI.

## 5.5 EXIGENCES DE SAUVEGARDE DES CLES DES UNITES D'HORODATAGE

Les clés privées des UH font l'objet d'une copie de secours (sauvegarde) qui ne peut être restaurée que par les administrateurs de sécurité de l'AH. La sécurité de la sauvegarde est assurée par les mécanismes de sécurité intrinsèques au HSM (évalué CC EAL4+ et qualifié).

## 5.6 DESTRUCTION DES CLES DES UNITES D'HORODATAGE

Les clés de signature des UH sont détruites à la fin de leur cycle de vie.

Cette destruction est opérée par le HSM (évalué CC EAL4+ et qualifié).

## 5.7 ALGORITHMES OBLIGATOIRES

L'AH accepte les empreintes calculées avec les algorithmes souhaités par les abonnés, si ceux-ci sont compatibles avec les meilleures pratiques et les recommandations de l'ANSSI et de l'ETSI.

Les contremarques de temps sont signées selon les algorithmes et les longueurs de clé conformes à l'état de l'art. Actuellement, la bi-clé de l'UH est une bi-clé RSA de 2048 bits et l'algorithme de signature utilise une fonction de hachage SHA-256.

## 5.8 VERIFICATION DES CONTREMARQUES DE TEMPS

L'AH garantit que les utilisateurs de contremarques de temps ont accès à l'information utilisable pour vérifier la signature numérique des contremarques de temps. En particulier :

- Les certificats des UH sont disponibles, joints à la contremarque de temps.
- La chaîne de certification complète est disponible à l'URL suivante
  - pour l'AC racine : https://icn.amsn.mc/icn/acr.crt
  - et pour l'AC Technique https://icn.amsn.mc/icn/ac-technique.crt
- Les LCR des AC de la chaîne de certification sont disponibles en activant les URL disponibles dans les certificats dans l'attribut cRLDistributionPoint : http://technique-icn.gouv.mc/crl/technique.crl

## 5.9 DUREE DE VALIDITE DES CERTIFICATS DE CLE PUBLIQUE DES UNITES D'HORODATAGE

La durée de validité des certificats des UH ne peut pas excéder :

- la durée de vie cryptographique de la clé privée associée,
- la date de fin de validité du certificat de l'AC émettrice.

La durée de validité des certificats de l'UH est de 3 ans.

## 5.10 DUREE D'UTILISATION DES CLES PRIVEES DES UH

La durée d'utilisation des clés privées des UH sera limitée en pratique à 1 ans afin de faciliter la vérification autonome des jetons d'horodatage grâce à une période adéquate de validité du certificat.

L'AH opère un renouvellement des clés privées de l'UH et du certificat associé tous les ans.

Les clés privées des certificats de l'UH ont une durée d'utilisation limitée à 1 an alors que les certificats associés ont une durée de vie maximale de 3 ans. L'objectif est bien de laisser 2 ans pour valider de manière autonome les jetons d'horodatage et permettre ainsi de construire des formats de signature étendus.

## 5.11 PROFIL DES CERTIFICATS ET CONTREMARQUES DE TEMPS

### 5.11.1 Format du certificat d'horodatage

Les certificats de signature des contremarques de temps respectent le gabarit suivant :

#### 5.11.1.1 Champs de base du certificat

Le tableau suivant présente les champs de base :

| Champ | Valeur |
|---|---|
| **Version** | 2 (pour version 3) |
| **SerialNumber** | Défini par l'AC |
| **Signature** | Sha256WithRSAEncryption |
| **Issuer** | • CN=AC TECHNIQUE<br>• OU=0206 20A00001<br>• orgID=NTRMC-20A00001<br>• O=AMSN<br>• C=MC |
| **Subject** | • serialNumber=<identifiant unique du responsable de certificat (format 2digit année+TIMESTAMP+numéro sur 5 digits)><br>• CN=<Nom de l'unité d'horodatage><br>• OU=0206 < numéro RCI de l'organisme><br>• orgID=NTRMC-<RCI de l'organisme><br>• O=<Raison sociale de l'organisme> |

| | |
|---|---|
| | • C=MC |
| **Validity** | • notBefore: Date de création<br>• notAfter: notBefore + 3 ans |
| **Subject Public Key Info** | RSA 2048 bits |

#### 5.11.1.2 Extensions du certificat

Le tableau suivant présente les extensions :

| Champ | OID | Criticité | Valeur |
|---|---|---|---|
| **Authority Key Identifier** | 2.5.29.35 | Non | 51:62:BB:6E:3A:B8:97:63:0A:50:38:46:BC:0B:45:D3:6D:8B:F0:9F |
| **Subject Key Identifier** | 2.5.29.14 | Non | [RFC 5280] : identifiant de la clé publique contenue dans le certificat (Hash de la clé publique du sujet) |
| **Key Usage** | 2.5.29.15 | Oui | Authentification : digitalSignature |
| **Extended Key Usage** | 2.5.29.37 | Oui | id-kp-timestamping |
| **Basic Constraints** | 2.5.29.19 | Non | • CA: false<br>• Maximum Path Length : absent |
| **X509v3 Certificate Policies** | 2.5.29.32 | Non | Policy: 2.16.492.1.1.1.1.6.1<br>• CPS: https://mconnect.gouv.mc/technique<br>Policy : 2.16.492.1.1.1.1.6.4.10 |
| **X509v3 CRL Distribution Points** | 2.5.29.31 | Non | Full Name:<br>• http://technique-icn.gouv.mc/crl/technique.crl<br>• http://technique-icn.monaco.fr/crl/technique.crl |
| **Subject Alternative Name** | 2.5.29.17 | Non | [RFC822]=<optionnel> <courriel du responsable du certificat ou adresse générique de l'entité> |
| **Authority Information Access** | 1.3.6.1.5.5.7.1.1 | Non | CA Issuers - URI: https://icn.amsn.mc/icn/ac-technique.crt<br>OCSP Issuers - URI: http://technique-oscpicn.gouv.mc |
| **QCStatement** | 1.3.6.1.5.5.7.1.3 | Non | id-etsi-qcs-QcCompliance<br>id-etsi-qct-eseal<br>QcEuPDS= https://mconnect.gouv.mc/technique |

### 5.11.2 Format des contremarques de temps

Les contremarques de temps respectent le gabarit suivant :

| Champ | Commentaires | Valeur |
|---|---|---|
| ***version*** | Version du format | 1 |
| ***policy*** | OID de la PH | 2.16.492.1.1.1.1.6.11.2 |
| ***messageImprint*** | OID de l'algorithme de hash (empreinte)<br>hash des données à horodater (Message data) | Hash Algorithm: sha256<br>Identiques aux valeurs incluses dans la demande |
| ***serialNumber*** | Identifiant unique de la contremarque de temps | Généré par l'UH |
| ***genTime*** | Heure de la contremarque de temps | Heure de l'UH au moment de la génération |
| ***accuracy*** | Précision déclarée | 1 seconde |
| ***ordering*** | Information d'ordonnancement | false |
| ***nonce*** | Donnée anti-rejeu | Identique à celui présent dans la demande si nonce était présent |
| ***tsa*** | Identifiant de l'UH | champ "subject" du certificat d'horodatage de l'UH |
| ***extensions*** | Extension supplémentaires optionnelles | Aucune extension supplémentaire |

# 6 ANNEXE : DOCUMENTS CITES EN REFERENCE

| Renvoi | Document |
|---|---|
| **[RGSP]** | RÉFÉRENTIEL GÉNÉRAL DE SÉCURITÉ DE LA PRINCIPAUTÉ DE MONACO (RGSP) - Règles applicables aux systèmes d'information aux services de confiance pour les transactions électroniques - Annexes à l'arrêté ministériel n° 2020-461 du 6 juillet 2020 |
| **[AMSN_PSC]** | AM n° 2018-67 du 30 janvier 2018 JO n°8368 - Critères d'évaluation de la conformité au RGS des services d'horodatage électronique qualifiés |
| **[PSCO_QUALIF]** | Arrêté ministériel n° 2018-66 du 30 janvier 2018 portant application de l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, relatif aux critères d'évaluation de la conformité au règlement général de sécurité des prestataires de services de confiance qualifiés |
| **[EN_319_421]** | Norme européenne ETSI EN 319 421 v1.1.1 (2016-03), Electronic Signatures and Infrastructures (ESI) ; Policy and Security Requirements for Trust Service Providers issuing Time-Stamps<br>Disponible sur : http://www.etsi.org<br>https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf |

| | |
|---|---|
| **[EN_319_401]** | Norme européenne ETSI EN 319 4201 V2.2.0 (2017-08)<br>Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers<br>Disponible sur http://www.etsi.org :<br>https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.02.00_20/en_319401v020200a.pdf<br>*Ce document est encore à l'état de projet* |
| **[RFC3161]** | La norme RFC 3161 définit un protocole d'horodatage applicable par une autorité d'horodatage.<br>https://www.ietf.org/rfc/rfc3161.txt |
| **[CGU-SH]** | Conditions Générales d'Utilisation – Service Horodatage |
| **[DPH]** | Déclaration des Pratiques d'Horodatage<br>La DPH identifie les pratiques 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 |