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

Version	Date	Description	Auteurs	Service
0.1	13/08/2021	Version initiale	SH	DSN
0.2	23/08/2021	Modifications	SH	DSN
0.3	06/10/2021	Modifications (DPH en cours de rédaction)	SH	DSN
0.4	15/10/2021	Relecture conjointe AMSN/DSN	SH	DSN
0.5	18/10/2021	Modifications DSN	SH	DSN
0.6	26/10/2021	Modifications DSN	SH	DSN
0.61	2/11/2021	Modifications Profils des certificats	SH	DSN
1.0	4/11/2021	Version applicable	SH	DSN

État du document - Classification	Référence
En cours – Publique	2.16.492.1.1.1.1.6.1

Ce document comporte 33 pages.

Sommaire

INTRODUCTION

L'horodatage électronique est un service de sécurité qui permet d'attester que des données sous forme électronique existaient bien à un instant donné.

Ce service consiste à associer à une représentation sans équivoque des données concernées, un instant dans le temps suivant une précision prédéfinie par rapport au temps universel.

Cette association est réalisée à travers un mécanisme de signature électronique, la « représentation sans équivoque » des données concernées étant réalisé grâce à un algorithme de hachage. Les données ainsi horodatées peuvent être de n'importe quel type (texte brut, fichier bureautique, document électronique comportant une signature électronique, fichier multimédia, etc.), le type dépendant du service à valeur ajoutée qui s'appuie sur l'horodatage électronique.

L'horodatage électronique est réalisé sous le contrôle et sous la responsabilité d'un Prestataire de Service d'Horodatage Électronique (PSHE) qui peut mettre en œuvre une ou plusieurs Autorité d'Horodatage (AH) lesquelles signent les jetons d'horodatage conformément à une Politique d'Horodatage (PH) qui leur est propre. (Techniquement, la création des jetons horodatage électronique d'une AH est réalisée par une ou plusieurs « Unité d'Horodatage » (UH), comportant chacune un « module d'horodatage »).

Quelle que soit l'organisation retenue, le PSHE reste responsable vis-à-vis des utilisateurs du service d'horodatage électronique rendu.

Le service d'horodatage électronique est sollicité par des « services demandeurs » qui ont en charge la fourniture, à leurs « utilisateurs finaux » (Services de l'Etat et acteurs autorisés), de services à valeur ajoutée qui intègrent le service d'horodatage électronique.

Ainsi, l'AH est en relation directe avec les services demandeurs, et indirectement avec les utilisateurs finaux.

Un service d'horodatage est un service électronique de confiance. Il est nécessaire que les services demandeurs et, indirectement, les utilisateurs finaux puissent avoir confiance dans l'AH pour la fourniture de services d'horodatage fiables.

Cette fiabilité nécessite la mise en œuvre de moyens techniques, humains et organisationnels adéquats. L'AH s'engage et est responsable vis-à-vis des services demandeurs sur la mise en œuvre de ces moyens.

1.1 PRESENTATION GENERALE

Au sein de la Principauté de Monaco, l'Agence Monégasque de Sécurité du Numérique (AMSN) est responsable de la chaîne de certification de l'État. Dans ce cadre, elle génère et opère les Autorités de Certification (AC) Opérationnelles pour le compte des Directions Métiers. Ces Autorités de Certification sont émises par une Autorité de Certification Racine dont les conditions de gestion sont définies dans la Politique de Certification associée [AMSN_PC_RACINE].

Les certificats finaux mis en œuvre par le Gouvernement monégasque sont générés par ces Autorités de Certification Opérationnelles également appelées Autorités de Certification Déléguées (ACD). L'ensemble constitue une hiérarchie de certification.

Techniquement, l'AMSN recourt à une Infrastructure à Gestion de Clés (IGC) en ligne pour la gestion des clés des AC Opérationnelles.

Un responsable est désigné pour chaque Autorité de Certification.

La présente Politique Horodatage (PH) définit les engagements que prend la DIRECTION DES SERVICES NUMERIQUES quant aux opérations de son ACD, appelée AC TECHNIQUE, en tant qu'AH (Autorité d'Horodatage).

L'objet de la présente Politique d'Horodatage est de formaliser les engagements de l'AH.

Cette Politique d'Horodatage, qui définit donc les « objectifs et les engagements » de l'AH pour assurer la fiabilité des services d'horodatage fournis, est un document public accessible librement par les services demandeurs et les utilisateurs finaux. Contractuellement, ce document engage la DIRECTION DES SERVICES NUMERIQUES (DSN) vis-à-vis des services demandeurs. Il appartient ensuite aux services

demandeurs de retranscrire les éléments pertinents de la présente Politique d'Horodatage dans leurs propres relations contractuelles avec leurs utilisateurs finaux.

La présente Politique d'Horodatage est conforme au plan du document [EN_319_421], au [RGSP].

Lorsque cela n'est pas précisé, le terme « AC » désigne dans le présent document l'AC TECHNIQUE, représentée par la DSN.

1.2 IDENTIFIANT DU DOCUMENT

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

La présente PH est identifiée par l'Identifiant d'Objet (OID): 2.16.492.1.1.1.1.6.1

Les certificats et les jetons d'horodatage émis par les services d'horodatage de la DSN comportent l'OID ci-dessus.

1.3 DOCUMENTS DE 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 Disponible sur : http://www.etsi.org 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) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers Disponible sur http://www.etsi.org : https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.02.00_20/en_319401v020200a.pdf *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. https://www.ietf.org/rfc/rfc3161.txt

1.4 ENTITES INTERVENANT DANS L'IGC

1.4.1 Autorité de certification (AE)

L'entité en charge de l'AC TECHNIQUE (AC) est la DIRECTION DES SERVICES NUMERIQUES.

Cette AC opérationnelle dépend de l'AC Racine qui relève de la responsabilité de l'AMSN.

Un comité de suivi nommé « comité de suivi des services de confiance » (C2SC) est mis en œuvre sous la responsabilité du Conseiller de Gouvernement-Ministre de l'Intérieur. Ce comité est le garant de l'application de la PH et de la bonne concordance avec les autres référentiels documentaires, la Déclaration des Pratiques d'Horodatage (DPH) notamment.

Ce comité est constitué des parties prenantes suivantes :

- Le responsable de l'AC Racine ;
- Les responsables de chacune des ACD ;
- Le Responsable de la Sécurité des Systèmes d'Information du Gouvernement ;
- Le Responsable de la Sécurité des Systèmes d'Information de la Direction de la Sûreté Publique ;
- Le Responsable de la Sécurité des Systèmes d'Information de la Mairie.

Le responsable de l'Opérateur Technique ou toutes personnes jugées utiles en lien avec l'ordre du jour d'une réunion du C2SC peuvent, le cas échéant, y être conviés.

L'AC est responsable des certificats signés en son nom.

En particulier, l'AC a la responsabilité des fonctions suivantes :

- Mise en application de la Politique de Certification ;
- Enregistrement des rôles de confiance et des porteurs de secrets ;
- Émission des Certificats ;
- Gestion du cycle de vie des Certificats ;
- Publication de la Liste des Certificats Révoqués (LCR) ;
- Journalisation et archivage des événements et informations relatives au fonctionnement de l'AC.

1.4.2 Autorité d'Enregistrement (AE)

La DSN (Direction des Services Numériques) pour laquelle l'AC TECHNIQUE a été émise établit les processus de gestion des certificats d'horodatage.

Pour cela, le rôle d'AE peut être délégué par l'AC. Dans ce cas, une convention, appelée « Convention AC-AE » est établie entre les parties.

L'Autorité d'Enregistrement assure les fonctions suivantes :

- Réception des dossiers de demande de génération d'un certificat ;
- Réception des dossiers de demande de révocation d'un certificat ;
- Vérification de l'identité et de l'habilitation du futur porteur de certificats à demander la création du certificat correspondant ;
- Déclenchement de la génération des certificats ;
- Remise au futur porteur des certificats par e-mail;

- Traitement de la révocation des certificats ;
- Déclenchement des fonctions d'archivage des données.

L'Autorité d'Enregistrement habilite formellement des personnes en son sein au rôle d'opérateurs d'enregistrement. Ces personnes sont en charge d'opérer les processus définis par l'Autorité d'Enregistrement dans le cadre, le cas échéant, de la convention établie avec l'Autorité de Certification.

1.5 GESTION DE LA PH

La présente PH couvre les services d'horodatages fournis par la Direction des Services Numériques (DSN) en tant que responsable de l'AC Technique.

1.5.1 Entité gérant la PH

La PH est approuvée par le C2SC et mise en œuvre par l'AC.

1.5.2 Point de contact

Toute information concernant la présente PH ou la gestion de l'AC peut être demandée via le point de contact suivant :

Direction des Services Numériques

23, avenue Albert II

98000 MONACO

1.5.3 Entité déterminant la conformité de la DPH avec la PH

La conformité de la DPH à la PH est validée par le C2SC.

1.5.4 Procédures d'approbation de la conformité

L'approbation de la conformité est prononcée par le responsable du C2SC sur la base de résultats d'audits internes et du plan d'action décidé ou validé par le comité. Les services de confiance font l'objet d'une homologation de sécurité qui atteste que les instances dirigeantes valident la mise en production de l'infrastructure de gestion des clés en ayant connaissance des risques résiduels et en les acceptant.

Chaque ACD doit faire l'homologation sur le périmètre qui la concerne.

1.6 CONFORMITE

Les Autorités de Certification (AC) et Autorités de Certifications Déléguées (ACD) sont pilotées par un Comité de Suivi des Services de Confiance appelé le C2SC.

Le C2SC est responsable de :

- la validation et de la publication de la PH,
- la validation de la DPH, et de sa conformité à la PH,
- la conformité des certificats émis vis-à-vis de la présente PH,
- du respect de tous les principes de sécurité par les différentes composantes de l'IGC, et des contrôles afférents.

La DSN, en tant qu'AC, est responsable, sauf à démontrer qu'il n'a été commis aucune faute intentionnelle ou de négligence, des préjudices causés aux utilisateurs, si :

- les informations contenues dans le certificat ne correspondent pas aux informations d'enregistrement,
- l'AC n'a pas fait procéder à l'enregistrement de la révocation d'un certificat, et n'a pas publié cette information conformément à ses engagements.

1.7 DEFINITIONS ET ACRONYMES

Les acronymes utilisés dans la présente PC sont les suivants :

1.7.1 Abréviations

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

OSH Opérateur de Services d'Horodatage

PH Politique d'Horodatage

PP Profil de Protection

PSHE Prestataire de service d'horodatage

RSSI Responsable de la Sécurité des Systèmes d'Information

UH Unité d'Horodatage

UTC Coordinated Universal Time

1.7.2 Termes communs aux différentes PC/PH et autres documents

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) - Autorité responsable de la gestion de l'environnement d'horodatage et de la production des jetons d'horodatage de la DSN sur les données qui lui sont présentées afin d'attester de

l'existence de ces données à la date de la marque de temps. Il s'agit de la DSN (Direction des Services Numériques) dans le cadre de la présente PH.

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 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.

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 du [RGSP].

Jeton d'horodatage - Voir contremarque de temps.

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.

Opérateur de Service d'Horodatage (OSH) - Opérateur assurant les prestations techniques nécessaires au processus d'horodatage. Il est en charge du bon fonctionnement et de la sécurité des moyens informatiques et techniques. Il est en charge de la sécurité des personnels, des locaux et, plus généralement, du bon respect des procédures, toutes choses indispensables pour garantir un niveau de fiabilité.

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.

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

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

Service demandeur - Entité demandant à l'AH la fourniture de certificats d'horodatage dans la perspective de délivrer des jetons d'horodatage.

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 final - Personne physique ou morale identifiée ou non qui reçoit par l'intermédiaire du service demandeur un jeton d'horodatage correspondant à la fourniture d'un service d'horodatage par l'AH.

2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

2.1 ENTITE CHARGEE DE LA MISE A DISPOSITION DES INFORMATIONS

Le responsable de la publication est chargé de mettre à disposition l'information devant être publiée et décrite dans la section §2.2 du présent document. Dans le cas présent le responsable de publication pour l'AC est la Direction des Services Numériques.

Les informations sont publiées en fonction du cas de figure sur les URL suivantes :

- *http(s)://icn.amsn.mc/icn*
- https://mconnect.gouv.mc/technique
- http://icn.monaco.fr/icn

2.2 INFORMATIONS DEVANT ETRE MISES A DISPOSITION

Sur le périmètre du présent document, les informations publiées sont les suivantes :

- la présente PH ;
- les CGU ;
- les LAR ;
- les LCR ;
- le certificat de l'AC TECHNIQUE ;
- le certificat de l'AC Racine ;
- les éléments constitutifs du dossier d'enregistrement.

La présente PH est publiée au format PDF/A. Les versions obsolètes des éléments définis ci-dessus restent publiées dans un espace dédié du site de publication.

2.3 DELAIS ET FREQUENCES DE PUBLICATION

2.3.1 Procédures de publication et de notification

La présente PH est disponible via l'URL suivante :

https://mconnect.gouv.mc/technique

Les politiques de certification sont remises à jour et publiées en cas de changement majeur et a minima tous les deux ans.

Les certificats de l'AC sont diffusés ou mis en ligne préalablement à toute diffusion de certificats finaux.

Les LAR sont établies tous les mois.

Les LCR de l'AC sont établies a minima toutes les 24h.

Une supervision est mise en place. Elle s'assure que la LCR publiée est non seulement en cours de validité mais qu'il s'agit bien de la dernière.

2.3.2 Procédures de modification de la politique d'horodatage

La présente PH est réactualisée selon le besoin, après validation du C2SC.

Les corrections d'erreurs ou changements suggérés à lecture de ce document sont à adresser au C2SC.

Dans le cas où l'AH serait certifiée conforme au [RGSP], si une modification envisagée à l'initiative de l'Autorité d'horodatage pouvait entraîner une non-conformité avec la politique d'horodatage ou avec la déclaration des pratiques d'horodatage, alors l'Autorité d'horodatage soumettra cette modification à l'organisme évaluateur indépendant pour avis.

De même, toute modification susceptible d'entraîner un écart par rapport aux exigences de [AMSN_PSC] fera l'objet d'une soumission pour avis par l'Autorité d'horodatage à l'organisme évaluateur indépendant et à l'organe de contrôle au sens du règlement eIDAS.

2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

Les informations publiées sont mises à disposition en lecture à l'ensemble de la communauté des Utilisateurs.

Les ajouts, suppressions et modifications sont limités aux personnes autorisées de l'AC. L'accès au service de publication se fait, dans l'idéal, à l'aide d'un moyen d'authentification réunissant au moins 2 facteurs.

3 CONCEPTS GENERAUX

3.1 SERVICE D'HORODATAGE

Les services demandeurs se chargent d'émettre des jetons d'horodatage aux utilisateurs finaux. Un jeton d'horodatage est une structure signée numériquement et qui contient en particulier :

- l'identifiant de la Politique d'Horodatage sous laquelle le jeton d'horodatage a été généré ;
- 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 (certificat qui identifie aussi l'AH).

La signature électronique est réalisée par un algorithme cryptographique asymétrique. Chaque UH dispose de sa propre bi-clé : la clé privée de signature est mise en œuvre au sein du module d'horodatage de l'UH (au sein de son HSM), la clé publique est certifiée dans les conditions fixées par la présente PH.

Les services d'horodatage sont mis en œuvre par un « Opérateur de Services d'Horodatage » (OSH), sous la responsabilité de l'AH.

L'OSH a également en charge la surveillance et le contrôle du fonctionnement des services d'horodatage afin d'assurer la conformité avec les exigences et engagements de l'AH (synchronisation adéquate des horloges des modules d'horodatage avec le temps UTC, mise en œuvre des mesures de sécurité, etc.).

3.2 PRESTATAIRE DE SERVICE D'HORODATAGE

Le PSHE est la Direction des Services Numériques (DSN).

La DSN est responsable de la génération et de la gestion de contremarques de temps vis-à-vis de ses utilisateurs.

3.3 AUTORITE D'HORODATAGE

L'AH réalise la fourniture des services d'horodatage et de la conformité aux engagements définis dans le présent document.

Les clés de signature de l'AH sont utilisées, au sein des UH, pour signer les jetons d'horodatage et l'AH est identifiée comme l'émetteur de ces jetons.

L'AH peut faire appel à d'autres entités pour réaliser tout ou partie des services. Elle en conserve cependant l'entière responsabilité et s'assure que les exigences décrites dans la présente politique sont satisfaites.

3.4 SERVICES DEMANDEURS

C'est l'entité qui demande à l'AH la fourniture de services d'horodatage.

Les services demandeurs utilisent ensuite ces jetons d'horodatage soit pour eux-mêmes, soit pour les fournir à leurs utilisateurs dans le cadre de services à valeur ajoutée. Les utilisateurs des services demandeurs sont appelés « utilisateurs finaux » dans le présent document.

3.5 UTILISATEURS FINAUX

Les utilisateurs finaux sont les utilisateurs des services demandeurs. L'AH n'a pas de relations directes avec ces utilisateurs finaux.

3.6 POLITIQUE D'HORODATAGE ET DECLARATION DES PRATIQUES D'HORODATAGE DE L'AH

Une PH définit les engagements de l'AH en matière de niveau de service d'horodatage et de niveau de sécurité correspondant. Une PH identifie ainsi les objectifs à atteindre, indépendamment de toute implémentation des services d'horodatage.

Une DPH identifie les pratiques d'horodatage qui doivent être mises en œuvre dans le fonctionnement des services d'horodatage. Une DPH identifie « ce qu'il faut faire » pour être conforme aux engagements pris dans la PH applicable. Une DPH dépend de l'implémentation des services d'horodatage.

4 OBLIGATIONS ET RESPONSABILITES

4.1 OBLIGATIONS DE L'AH

4.1.1 Obligations générales

L'AH :

- S'assure que toutes les exigences détaillées dans les chapitres qui suivent sont mises en place ;
- Garantit l'application des procédures découlant de la présente politique, que les fonctionnalités de l'AH soient sous-traitées auprès de sociétés externes ou non ;
- S'assure que les moyens mis en œuvre, décrits dans la DPH, répondent complètement aux exigences de la PH ;
- S'engage à respecter la confidentialité des éléments précisés dans la DPH. Concernant la génération des jetons d'horodatage, l'AH s'assure que l'OSH :
- Respecte et répond aux exigences de la présente PH telles que traduits dans la DPH ;
- Accepte les audits périodiques de contrôle de conformité par rapport à la présente PH réalisés par l'AH ou par des entités d'audit externes.

En outre l'OSH s'engage au respect des obligations suivantes :

- Respecter le contrat de prestation de services qui le lie à l'AH ;
- N'utiliser les clés privées de l'AH que pour la signature des jetons d'horodatage destinés à des Services Demandeurs ayant contractualisés avec l'AH dans le cadre de la présente PH et ce, selon les règles et avec les moyens qui y sont spécifiés;

- Protéger contre toute compromission les clés privées de l'AH utilisées pour la signature des jetons d'horodatage ;
- Assurer le bon fonctionnement et la sécurité des moyens informatiques et techniques mis en œuvre dans le cadre des services d'horodatage ;
- Garantir le respect des caractéristiques opérationnelles de la fonction d'horodatage qui lui est confiée par l'AH dans le cadre des services d'horodatage. Ces caractéristiques sont détaillées dans le présent document et dans le contrat de prestation de services associé ;
- Se conformer aux résultats des contrôles de conformité effectués sur demande de l'AH et remédier aux non-conformités que ceux-ci révéleraient ;
- Documenter ses procédures internes d'exploitation ;
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles il s'engage.

4.2 OBLIGATIONS DES SERVICES DEMANDEURS

Le service demandeur s'engage à vérifier le certificat d'horodatage dès sa réception.

Le service demandeur s'engage également à vérifier que les données sur lesquelles portent le scellement d'horodatage sont bien celles transmises pour horodatage.

4.3 OBLIGATIONS DES UTILISATEURS FINAUX

Les utilisateurs finaux n'ont pas d'obligation vis-à-vis de l'AH dans le cadre de la présente politique.

Il leur est cependant recommandé de valider les jetons d'horodatage.

4.4 RESPONSABILITES

Les responsabilités respectives de l'AH et des services demandeurs sont définies dans les Conditions Générales d'Utilisation (CGU).

A noter : des CGUs sont également disponibles spécifiquement pour les utilisateurs finaux des jetons de temps.

4.5 CONFORMITES AVEC LES EXIGENCES LEGALES

4.5.1 Droit applicable

Le présent document est régi par la loi Monégasque.

4.5.2 Règlement des différents

Toute contestation et tout litige pouvant naître à l'occasion de l'exécution de la présente PH seront du ressort exclusif des cours et des tribunaux monégasques avec seule application de la loi monégasque.

4.5.3 Données nominatives

Sans objet.

L'UH ne contient aucune donnée nominative ou personnelle.

5 EXIGENCES CONCERNANT LES PRATIQUES D HORODATAGE

5.1 DECLARATION DES PRATIQUES D'HORODATAGE ET CONDITIONS GENERALES D'UTILISATION

5.1.1 Déclarations des pratiques d'horodatage et conditions générales d'utilisation

L'AH doit démontrer qu'elle possède la fiabilité nécessaire pour la fourniture de service d'horodatage.

5.1.2 Conditions Générales d'utilisation

L'AH publie, en complément des éléments de la présente PH, deux contrats de Conditions Générales d'Utilisation (CGU) :

1. Des CGUs qui régissent la relation entre l'AH et les Services Demandeurs
2. Des CGUs qui régissent la relation entre les Services Demandeurs et les Utilisateurs Finaux.

1. Les CGUs qui régissent la relation entre l'AH et les Services Demandeurs doivent notamment comporter les informations suivantes :

- Les coordonnées de l'AH ;
- La PH appliquée ;
- Les obligations de l'AH ;
- Les obligations des services demandeurs ;

2. Les CGUs qui régissent la relation entre les Services Demandeurs et les Utilisateurs Finaux doivent notamment comporter les informations suivantes :

- Les coordonnées de l'AH ;
- La PH appliquée ;
- La fonction de hachage utilisée pour constituer l'objet horodaté ;
- La durée de vie attendue des clés privées de signature utilisées pour signer le jeton d'horodatage ;
- Les obligations des services demandeurs ;
- Les obligations des utilisateurs finaux ;
- Les informations permettant de vérifier le jeton d'horodatage ;
- Les limitations de responsabilité.

Les CGUs sont disponibles via l'URL suivante : https://mconnect.gouv.mc/technique

6 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CLES DE L'AH

6.1 CYCLE DE VIE DES CLES DE L'AH

6.1.1 Génération des clés par l'AH

L'AH s'assure que la génération des clés cryptographiques est effectuée en conformité avec les normes existantes en la matière.

En particulier :

- La génération des clés de signature de l'AH est réalisée dans un environnement physiquement sécurisé par du personnel autorisé ayant des rôles définis.
- La procédure de génération des clés de signature de l'AH est exécutée sous contrôle d'au moins deux personnes ayant un rôle de confiance et elle fait l'objet d'une trace systématique.
- Les propriétés du module d'horodatage dans lequel est réalisée la génération des clés de signature de l'AH sont conformes aux exigences de cette PH.
- L'algorithme de génération des clés, la longueur des clés obtenue et l'algorithme de signature utilisés pour la signature des jetons d'horodatage sont conformes au minimum aux exigences du RGSP.

6.1.2 Protection des clés privées des UH

L'AH s'assure de la confidentialité des clés privées de signature et maintient leur intégrité.

6.1.3 Distribution des clés publiques des UH

Les clés publiques d'UH sont distribuées au travers de certificats fournis par une AC qualifiée vis-à-vis du RGSP pour les certificats d'horodatage.

6.1.4 Renouvellement des clés des UH

La durée de vie des bi-clés d'horodatage de l'AH, qui correspond à la durée de vie du certificat associé, est de 3 ans.

Ces bi-clés et les certificats associés doivent être renouvelés avant la fin de leur durée de vie.

La période d'activité des clés privées d'horodatage de l'AH, qui correspond à la période durant laquelle les clés privées d'horodatage de l'AH sont utilisées pour émettre des jetons dans le cadre de la présente PH, est de 3 ans.

Elle coïncide avec la période de renouvellement des clés de l'AH, qui est également de 3 ans.

6.1.5 Fin du cycle de vie des clés des UH

L'AH s'assure que ses clés privées d'horodatage ne sont pas utilisées au-delà de la fin de leurs périodes d'activité.

Les procédures techniques et opérationnelles de l'OSH permettent la mise en place d'une nouvelle bi-clé sur demande de l'AH.

6.1.6 Gestion du cycle de vie des modules d'horodatage

L'AH assure la sécurité des modules d'horodatage (UH) durant leur cycle de vie. En particulier, l'AH prend les mesures nécessaires visant à :

- Assurer que chaque UH utilisée pour la signature des jetons d'horodatage n'est pas modifié durant sa livraison ;
- Assurer que chaque UH utilisée pour la signature des jetons d'horodatage n'est pas altéré avant et lors de sa mise en fonction et lors de toute mise à jour ultérieure effectuée sur ce module ;
- Garantir que l'activation des clés de signature de l'AH dans chaque UH n'est réalisée que par du personnel autorisé ayant des rôles définis et au moins sous double contrôle (cf. *5.2.1 Génération des clés par l'AH*), au sein d'un environnement physiquement sécurisé ;
- Assurer le fonctionnement correct des UH de signature des jetons d'horodatage ;

6.1.7 Certification des clés de l'unité d'horodatage

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

L'AH s'assure que la demande de certificat d'UH contient notamment 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.

7 PRODUCTION DES JETONS D'HORODATAGE

7.1 JETON D'HORODATAGE

L'AH s'assure que les jetons d'horodatage sont émis de manière sécurisée et qu'ils présentent une garantie suffisante de fiabilité à la seconde.

En particulier :

- Le jeton d'horodatage contient un identifiant de la PH : 2.16.492.1.1.1.1.6.1.
- La précision de l'heure contenue dans le jeton d'horodatage vis-à-vis de l'échelle de temps UTC (une seconde) n'est pas indiquée dans le jeton d'horodatage ;
- Le jeton d'horodatage contient l'empreinte numérique de l'objet horodaté, cet objet étant fourni par le service demandeur ;
- Les clés utilisées pour signer les jetons d'horodatage ne servent qu'à cet usage ;
- Le protocole utilisé pour les demandes et les réponses de fourniture de jetons d'horodatage est le protocole défini dans [RFC 3161] et profilé dans [EN_319_421].
- L'AH est identifiée dans le certificat d'horodatage contenu dans le jeton d'horodatage. Cette identification comprend :
- Un identifiant du pays dans lequel l'AH est établi (champ DN du certificat) ;
- Un identifiant de l'AH :
- Un identifiant de l'UH.

7.2 SYNCHRONISATION DES HORLOGES AVEC L'UTC

L'AH s'assure de la précision de l'horloge des services d'horodatage vis-à-vis de l'échelle de temps UTC.

En particulier :

- Les propriétés du module d'horodatage opérant l'horloge sont conformes aux exigences de la [PH-TYPE] et [AMSN_PSC] ;
- L'AH dispose de deux sources de temps fiables :
  - une souveraine issue de l'Infrastructure de Confiance Nationale (ICN) et de ses sources de temps en Principauté
  - du pool NTP de référence international (NTP Pool Project)
- L'AH s'assure que la source de temps ne dévie pas de la précision annoncée;
- La précision par rapport au temps UTC est d'une seconde ;

7.3 VERIFICATION D'UN JETON D'HORODATAGE

La vérification d'un jeton d'horodatage est réalisable de façon autonome par le service demandeur pendant la période de publication en ligne des LCR délivrées par l'AC émettant les certificats d'horodatage :

- La vérification d'un jeton d'horodatage s'effectue à partir des informations publiées par l'AC émettrice du certificat d'UH qu'il comprend ;
- Les LCR de l'AC, qui comportent tous les certificats révoqués depuis le début de l'existence de l'AC, sont accessibles sur son site Internet pendant leur période de publication.

7.4 PROCEDURE DE VERIFICATION AUTONOME D'UN JETON D'HORODATAGE

La procédure de vérification autonome d'un jeton d'horodatage à l'aide d'outils appropriés doit au minimum permettre de garantir que :

- Le jeton d'horodatage émane bien des services d'horodatage de l'AH concernée par la présente PH en contrôlant :
  - La provenance du certificat d'horodatage (provient bien de l'AC Technique) ;
  - La correspondance du champ OID du jeton d'horodatage avec l'OID de la présente PH ;
  - La signature apposée sur le jeton d'horodatage est correcte (vérification de l'intégrité du jeton d'horodatage) ;
  - Les attributs du certificat d'horodatage sont bien spécifiques à l'horodatage ;
  - Le certificat d'horodatage est valide en contrôlant :
    - Sa non-révocation auprès de l'AC émettrice (interrogation de CRL) ;
    - La signature apposée sur le certificat par l'AC émettrice (vérification de l'intégrité des données du certificat) ;
    - La période de validité du certificat ;
    - Les certificats de l'ensemble de la chaîne de certification sont valides ;
    - L'empreinte présente dans le jeton d'horodatage est bien celle des données présentées au Service d'horodatage.

7.5 ALGORITHMES DE PRODUCTION DU JETON D'HORODATAGE

Les algorithmes suivants sont acceptés pour l'empreinte numérique des données horodatées (cette empreinte est réalisée par l'utilisateur final et transmise dans la requête) :

- SHA-256 ;

Les contremarques de temps sont signées en utilisant des algorithmes et des longueurs de clés conformes à l'état de l'art et aux exigences de [AMSN_PSC] et [RGSP]. Les bi-clés RSA des unités d'horodatage ont une longueur de 2048 bits. La signature des contremarques utilise une fonction de hachage de la famille SHA-2.

8 MESURE DE SECURITE NON-TECHNIQUES

8.1 MESURES DE SECURITE PHYSIQUE

8.1.1 Situation géographique et construction des sites

La localisation géographique des sites ne nécessite pas de mesures particulières face à des risques de type tremblement de terre, explosion, risque volcanique ou crue. Les environnements de l'AMSN sont installés sur des sites sécurisés de production informatique.

L'hébergement de l'IGC est réparti entre deux sites dont un principal et un secondaire dédié au secours et à la reprise d'activité localisé sur le territoire monégasque. Il n'existe pas de risque géographique particulier pour le site principal ni pour le site de secours, ces derniers ne sont pas situés à proximité d'un quelconque site à risque ni en zone inondable. La gestion de ce type de risque est contractuellement sous la responsabilité du bailleur.

8.1.2 Accès physique

Les salles d'hébergement bénéficient d'un niveau de sécurité physique double. L'accès physique au site se fait nécessairement avec l'accompagnement d'une personne autorisée de l'AMSN.

Les accès physiques aux zones d'hébergement de l'IGC font l'objet de journalisation et de vidéo-surveillance : le périmètre de sécurité défini autour des machines hébergeant les composantes de l'IGC n'est accessible qu'aux personnes disposant d'un rôle de confiance.

En dehors des heures ouvrables, la mise en œuvre de moyens de détection d'intrusion physique et logique renforce la sécurité de l'IGC.

8.1.3 Alimentation électrique et climatisation

Des mesures de secours sont mises en œuvre de manière à ce qu'une interruption de service d'alimentation électrique, ou une défaillance de climatisation ne portent pas atteinte aux engagements pris par l'AC en matière de disponibilité (gestion des révocations et informations relatives à l'état des certificats en particulier).

8.1.4 Vulnérabilité aux dégâts des eaux

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

8.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre l'incendie permettent de respecter les engagements pris par l'AC en matière de disponibilité (gestion des révocations et informations relatives à l'état des certificats en particulier), et de pérennité de l'archivage.

8.1.6 Conservation des supports

Les moyens de conservation des supports permettent de respecter les engagements pris par l'AC en matière de restitution et de pérennité de l'archivage.

8.1.7 Mise hors service des supports

Les supports recensés comme sensibles en termes de confidentialité font l'objet de mesures de destruction, ou peuvent être réutilisés dans un contexte opérationnel identique, pour un même niveau de sensibilité.

8.1.8 Sauvegardes hors site

Des sauvegardes externalisées sont mises en œuvre et organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conformément aux engagements de la présente PC notamment en matière de disponibilité et de protection en confidentialité et en intégrité des informations sauvegardées. Les supports de sauvegarde font l'objet d'une mise sous coffre hors site plusieurs fois par an.

8.2 MESURES DE SECURITE PROCEDURALES

8.2.1 Rôles de confiance

L'AMSN définit explicitement les rôles de confiance requis pour assurer le fonctionnement et la sécurité de ses services. Les définitions des rôles de confiance sont rendues disponibles à l'ensemble des personnels concernés.

L'AC définit les rôles de confiance suivants :

- Responsable d'AC :
  - Il s'agit du responsable de la Direction Métier pour laquelle l'AC opérationnelle est créée
- Administrateur système :
  - Il s'agit d'une personne identifiée formellement chez l'Opérateur Technique en relation contractuelle avec l'AMSN
- Exploitant / superviseur :
  - Ce rôle est délégué à un Opérateur Technique en relation contractuelle avec le Gouvernement. L'exploitant / superviseur est en charge d'assurer le maintien des fonctions de l'IGC en condition opérationnelle
- Administrateur sécurité :
  - Ce rôle est délégué à un Opérateur Technique en relation contractuelle avec le Gouvernement. L'administrateur sécurité est en charge d'assurer le maintien de l'IGC en condition de sécurité. Il doit appliquer les correctifs nécessaires, piloter les audits techniques de sécurité.
- Auditeur système :
  - Ce rôle est partagé entre des personnels formellement identifiés chez l'AMSN et des personnels chez l'Opérateur Technique en relation contractuelle avec l'AMSN. Le rôle de l'auditeur système est de pouvoir accéder aux configurations et aux traces des composants de l'IGC en lecture seulement pour détecter des incidents de sécurité ou des vulnérabilités.

En sus de ces rôles de confiance opérationnels, l'AC identifie des porteurs de secrets qui disposent d'une part des secrets de l'AC répartis selon l'algorithme de SHAMIR avec un quorum de 3 parmi 5.

8.2.2 Nombre de personnes requises par tâche

Selon le type d'opération effectuée, le nombre et les rôles des personnes devant être présentes, en tant qu'acteurs ou témoins, peuvent varier. En effet, certaines tâches sensibles, telles que la génération du certificat d'une AC, nécessitent plus d'une personne occupant un rôle de confiance au sein de l'ICN pour des raisons de sécurité. Certains rôles de confiance sont occupés par plusieurs personnes pour permettre à l'AMSN d'assurer la continuité des services de l'ICN sans dégrader la sécurité des services offerts.

8.2.3 Identification et authentification pour chaque rôle

Chaque personnel en rôle de confiance est clairement identifié par l'AMSN au travers d'un inventaire des rôles.

Chaque entité opérant une composante d'un service de confiance vérifie, pour chacun de ses composants, l'identité et les autorisations de tout membre du personnel ainsi que d'éventuelles personnes extérieures intervenant sur les tâches sensibles.

Avant d'utiliser une application critique contribuant à un service de confiance, tout personnel est obligatoirement identifié et authentifié au préalable. Toutes les opérations réalisées sur les systèmes par les personnels font l'objet d'une traçabilité garantissant l'imputabilité des actions. Chaque attribution d'un rôle de confiance à un membre du personnel est notifiée et documentée par écrit.

Les rôles de confiance assurés par l'Opérateur Technique sont établis concrètement et acceptés formellement par les personnes ayant ces rôles. L'Opérateur Technique tient à jour l'inventaire et le produit au Gouvernement sur simple demande dans les 48h suivant la demande en jours ouvrés.

8.2.4 Rôles exigeant une séparation des attributions

Il est autorisé par la présente politique que plusieurs rôles soient opérés par une même personne. Cependant, pour des raisons de sécurité, certains rôles ne peuvent pas être opérés par la même personne. De façon générale, les rôles et responsabilités sont attribués sur le principe du moindre privilège afin de limiter le risque de conflit d'intérêts et limiter les opportunités de réalisation d'actions non autorisées ou de mauvaise utilisation des biens mis en œuvre par le service de confiance.

Le rôle d'auditeur système ne peut pas être cumulé.

Le rôle d'« exploitant / superviseur » est cumulé avec le rôle d'« Administrateur système ».

8.3 MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

8.3.1 Qualifications, compétences et habilitations requises

Tout intervenant amené à occuper un rôle identifié comme sensible est soumis à une clause de confidentialité. Les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles. Le personnel d'encadrement possède l'expertise appropriée, et est familier des procédures de sécurité. Toute personne intervenant dans des rôles de confiance est informée de ses responsabilités (description de poste), et des procédures liées à la sécurité du système et au contrôle du personnel.

8.3.2 Procédures de vérification des antécédents

Des procédures de vérification des antécédents sont mises en place pour les personnes appelées à occuper un rôle sensible.

Des procédures de vérification des antécédents sont mises en place pour les personnes appelées à occuper un rôle sensible. L'AC demande en particulier la production d'une copie du bulletin n°3 de leur casier judiciaire. Ces vérifications sont effectuées préalablement à l'affectation à un rôle de confiance et revues au minimum tous les 3 ans.

8.3.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures de fonctionnement de l'IGC.

8.3.4 Exigences et fréquence en matière de formation continue

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux intervenants dans la mesure où cette évolution impacte le mode de travail de ces intervenants. Les intervenants sont formés à la gestion des incidents et sont au fait de l'organisation de remontée d'incidents.

8.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

8.3.6 Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont énoncées dans la définition de poste ou la charte de sécurité du personnel pour les rôles sensibles tenus par le personnel de l'AC.

8.3.7 Exigences vis-à-vis du personnel des prestataires externes

Les exigences vis-à-vis des prestataires externes sont contractualisées.

Chaque prestataire transmet à l'ensemble de ses sous-traitants les règles de sécurité qui doivent être respectées dans le cadre de la mission qui leur est sous-traitée. Ces règles de sécurité font l'objet d'une acceptation formelle par les différents sous-traitants.

8.3.8 Documentation fournie au personnel

Les règles de sécurité sont communiquées au personnel lors de leur prise de poste, en fonction du rôle affecté à l'intervenant. Les personnes appelées à occuper un rôle opérationnel dans l'IGC disposent des procédures correspondantes. Les porteurs de rôles, appelés également rôles de confiance, signent dès leur prise de fonction une attestation dans laquelle ils reconnaissent avoir obtenu la formation nécessaire à la conduite de leur rôle.

Cela s'applique à l'ensemble des personnes intervenant sur l'IGC.

9 MESURE DE SECURITE TECHNIQUES

9.1 MANAGEMENT DE LA SECURITE

L'AH s'assure que les procédures administratives et les procédures de gestion de l'OSH sont mises en œuvre, et correspondent aux normes et bonnes pratiques existant en la matière.

En particulier :

- L'AH réalise ou fait réaliser une évaluation de risques pour évaluer les actifs et les menaces pour ces actifs afin de déterminer les mesures de sécurité nécessaires et les procédures opérationnelles ;
- L'AH assume la responsabilité de la fourniture du service d'horodatage au regard de la présente PH, quelles que soient les fonctions sous-traitées ;
- Les responsabilités des tierces parties auprès desquelles des fonctions de l'AH sont sous-traitées sont fixées contractuellement ;
- La gestion de la sécurité est maintenue à toute heure. Tout changement ayant un impact sur le niveau de sécurité fourni est approuvé par le C2SC;
- Les contrôles de sécurité et les procédures opérationnelles concernant la fourniture du service d'horodatage sont documentés, mis en place et maintenus à jour ;

- L'AH s'assure que la sécurité des informations est assurée lorsque des fonctions de l'AH ont été sous-traitées à une autre organisation ou entité ;
- L'analyse de risques est revue et révisée tous les deux ans ;
- La direction du service d'horodatage approuve l'évaluation des risques et accepte les risques résiduels identifiés.

9.2 GESTION DE L'EXPLOITATION

L'AH s'assure que les composantes du système d'horodatage de l'AH sont exploitées correctement et de façon sûre, en minimisant les risques de défaillance.

En particulier :

- L'intégrité des composantes du système d'horodatage de l'AH et des données est protégée contre les codes malveillants et les logiciels non autorisés ;
- Une politique de gestion d'évènements, d'incidents et de gestion de crise est appliquée ;
- Des procédures sont établies et mises en place pour chacune des fonctions sensibles et des fonctions administratives ayant une incidence sur la fourniture de l'horodatage ;

9.2.1 Traitement et sécurité des supports de stockage d'information

Tous les supports de stockage d'information sont manipulés avec précaution en conformité avec les exigences définies par le schéma de classification de l'information. Les médias contenant des données sensibles sont conservés de manière sûre.

9.2.2 Planification des systèmes

Les demandes en termes de capacités sont contrôlées et des planifications concernant les futures exigences en termes de capacité sont effectuées de façon à s'assurer de la disponibilité de celles- ci.

9.2.3 Compte-rendu d'incident et réponse à incident

L'AH s'engage à fournir une réponse rapide, opportune et coordonnée aux incidents afin de limiter les impacts provenant d'incidents de sécurité. Des comptes rendus d'incidents sont effectués dès que possible après la résolution des incidents.

L'AH applique les contrôles additionnels suivants aux services d'horodatage :

9.2.4 Responsabilités et procédures d'exploitation

Les responsabilités d'exploitation de la sécurité de l'AH incluent les éléments suivants :

- Les procédures opérationnelles et les responsabilités associées ;
- La définition de l'architecture de sécurité et moyens permettant de réaliser cette architecture ;
- La protection contre les logiciels dangereux ;
- L'entretien des locaux ;
- La gestion des réseaux ;
- Le contrôle actif des journaux d'événements, l'analyse et le suivi des événements ;
- La sécurité de l'utilisation des supports ;
- Le changement de données ou de logiciels ;

- Les procédures d'exploitation sont gérées par du personnel spécifique dédié à cette fonction. Dans le cas où elles seraient appliquées par du personnel non qualifié, les politiques, les rôles et les responsabilités appliqués sont également définis.
- L'AH vérifie que les correctifs de sécurité soient appliqués dans un délai raisonnable après leur mise à disposition. De même l'AH doit s'assurer que les dits correctifs ne soient pas appliqués s'ils entraînent des vulnérabilités ou instabilités supplémentaires qui l'emportent sur les avantages à les appliquer. L'AH documente les raisons pour lesquelles un correctif de sécurité n'a pas été déployé.
- Toute vulnérabilité sera notifiée dans une analyse de risque ou dans un plan de réduction de risque et une mesure de réduction y sera associée.
- Les procédures de signalement et de réponse aux incidents sont utilisées de manière à ce que les dommages, consécutifs aux incidents de sécurité et dysfonctionnements soient minimisés.

9.2.5 Gestion des accès aux systèmes

L'OSH s'assure que l'accès aux composantes du système d'horodatage de l'AH est limité aux seules personnes autorisées.

En particulier :

- Des contrôles sont mis en place afin de protéger le réseau d'accès aux unités d'horodatage des accès non autorisés des services demandeurs et des tiers ;
- L'OSH assure une administration effective des accès des utilisateurs (qui comprennent les opérateurs, les ingénieurs systèmes et les administrateurs) afin de garantir la sécurité des composantes. L'administration des accès des utilisateurs comprend la gestion des comptes-utilisateurs, l'audit, la création, la modification et la suppression des accès ;
- L'OSH s'assure que l'accès aux informations et aux fonctionnalités systèmes sensibles est défini en accord avec la politique de contrôle d'accès ;
- Les contrôles mis en place par l'OSH permettent de garantir la séparation des fonctions sensibles définie dans la DPH, comme la séparation de l'administration de la sécurité et de l'exploitation. En particulier, l'exploitation des logiciels utilitaires systèmes est restreinte et fortement contrôlée ;
- Le personnel de l'OSH est identifié et authentifié avant toute réalisation de fonctions critiques relatives à l'horodatage ;
- Les activités de surveillance sont mises en place par l'OSH et tiennent compte de la sensibilité de toute information collectée ou analysée.
- L'OSH surveille le démarrage et l'arrêt des fonctions de journalisation ainsi que la disponibilité et l'utilisation des services nécessaires au service.
- L'OSH met en place des mesures permettant d'effectuer des contrôles a posteriori sur l'utilisation par le personnel des applications critiques relatives à l'horodatage. Ces mesures comprennent :
    - L'identification des applications ;
    - L'authentification du personnel ;
    - Les demandes de service ;
    - Les contrôles d'accès aux applications ;
    - La journalisation des événements relatifs aux applications.
- L'OSH sépare les systèmes de production des systèmes utilisés dans le développement et les tests.
- L'OSH garantit un niveau élevé de disponibilité de l'accès externe au service de confiance via la mise en place de technologies permettant la redondance du service en cas de défaillance unique.

- L'OSH s'assure que les composants réseaux sont conservées dans un environnement sécurisé et que leur configuration est périodiquement auditée pour assurer la conformité avec les exigences de l'AH.

9.3 COMPROMISSION DES SERVICES DE L'AH

En cas d'événement affectant la sécurité des services de l'AH, comme la compromission des clés privées des unités d'horodatage ou une perte détectée de la précision de l'horloge de l'AH, l'AH s'assure que l'information appropriée est fournie aux entités responsables des services demandeurs.

En particulier :

- Le plan de reprise après sinistre concerne la compromission, la suspicion de compromission des clés privées des unités d'horodatage et la perte de la précision de l'horloge de l'AH, qui pourraient avoir affecté les jetons d'horodatage qui ont été émis ;
- Dans le cas d'un incident majeur de l'exploitation de l'AH, d'une suspicion de compromission ou de la perte de la précision de l'horloge de l'AH, l'AH doit rendre disponible une description des événements aux entités responsables des services demandeurs, avec l'accord de l'OSH pour ce qui la concerne ;
- Dans le cas d'un incident majeur de l'exploitation de l'AH, d'une suspicion de compromission ou de la perte de la précision de l'horloge de l'AH, l'AH n'émet pas de jetons d'horodatage avant la résolution définitive de l'incident ;
- Dans le cas d'un incident majeur de l'exploitation de l'AH ou de la perte de la précision de l'horloge de l'AH, l'AH doit rendre disponible aux entités responsables des services demandeurs toute information permettant d'identifier les jetons ayant été affectés ;
- L'AH prévient également directement et sans délai l'AMSN et passe dans un fonctionnement de gestion de crise avec le C2SC.
- Lorsque l'atteinte à la sécurité ou la perte d'intégrité est susceptible de nuire à une personne à qui le service de confiance a été fourni, l'AH notifie la personne physique ou morale de la violation de la sécurité ou de la perte d'intégrité dans les plus bref délais.

9.3.1 Conformité avec les exigences légales et règlementaires

L'AH est établie sur le territoire Monégasque. La présente PH est régie par le droit Monégasque.

9.4 POLITIQUE DE SECURITE

L'AH et le PSHE s'assurent que les exigences la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) sont appliquées :

Arrêté Ministériel n° 2018-67 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, modifiée

10 PROFILS DES CERTIFICATS ET DES JETONS DE TEMPS

10.1 PROFIL DES CERTIFICATS

10.1.1.1 Champs de base du certificat de l'AC Technique

Le tableau suivant présente les champs de base :

Champ	Valeur
Version	2 (pour version 3)
SerialNumber	Généré automatiquement lors de la Cérémonie des Clés
Signature	Sha256WithRSAEncryption
Issuer	• CN=AC RACINE PRINCIPAUTE DE MONACO • OU=0206 20A00001 • orgID=NTRMC-20A00001 • O=AMSN • C=MC
Subject	• CN=AC TECHNIQUE • OU= 0206 20A00001 • orgID= NTRMC-20A00001 • O= AMSN • C=MC
Validity	• notBefore: Date de création • notAfter: notBefore + 10 ans
Subject Public Key Info	RSA 4096 bits

10.1.1.2 Extensions du certificat de l'AC Technique

Le tableau suivant présente les extensions :

Champ	OID	Criticité	Valeur
Authority Key Identifier	2.5.29.35	Non	97:B0:7D:B6:FE:4B:A9:55:30:CF:EB:3B:87:7E:0E:66:3A:9C:3D:E9
Subject Key Identifier	2.5.29.14	Non	51:62:BB:6E:3A:B8:97:63:0A:50:38:46:BC:0B:45:D3:6D:8B:F0:9F
Key Usage	2.5.29.15	Oui	keyCertSign, CRLSign, digitalSignature

Basic Contraints	2.5.29.19	Oui	• CA:true • Maximum Path Length : absent
X509v3 CRL Distribution Points	2.5.29.31	Non	Full Name: • URI:http://icn.amsn.mc/icn/icn4096.crl • URI:http://icn.monaco.fr/icn/icn4096.crl
Authority Information Access	1.3.6.1.5.5.7.1.1	Non	CA Issuers - URI:https://icn.amsn.mc/icn/acr.crt

10.1.2 Certificats d'horodatage sur environnement HSM non QSCD

10.1.2.1 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 • OU= 0206 20A00001 • orgID= NTRMC-20A00001 • O= AMSN • C=MC
Subject	• serialNumber=<identifiant unique du responsable de certificat> • CN=DSN • Locality=MONACO • State=MONACO • OU=20A00312 • orgID=NTRMC-20A00312 • O=DSN • C=MC
Validity	• notBefore: Date de création • notAfter: notBefore + 3 ans
Subject Public Key Info	RSA 2048 bits

10.1.2.2 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] méthode [1] : identifiant de la clé publique contenue dans le certificat
Key Usage	2.5.29.15	Oui	DigitalSignature
Extended Key Usage	2.5.29.15	Oui	TimeStamping
Basic Constraints	2.5.29.19	Non	• CA: false • Maximum Path Length : absent
X509v3 Certificate Policies	2.5.29.32	Non	Policy: 2.16.492.1.1.1.1.6.1 • CPS: https://mconnect.gouv.mc/technique Policy : 2.16.492.1.1.1.1.6.4.10
X509v3 CRL Distribution Points	2.5.29.31	Non	Full Name: • http://technique-icn.gouv.mc/crl/technique.crl • 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 OCSP Issuers - URI: http://technique-oscpicn.gouv.mc
QCStatement	1.3.6.1.5.5.7.1.3	Non	id-etsi-qcs-QcCompliance id-etsi-qct-eseal QcEuPDS= https://mconnect.gouv.mc/technique

10.1.3 Profils des contremarques de temps

10.1.3.1 Champs de base des contremarques de temps

Les contremarques de temps fournies par les AH respectant la présente PH Type doivent être 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 cette PH Type doit respecter, de base, les exigences

correspondantes du [RFC3161], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	**Exigences**
Generation time	*Date de l'horodatage*
messageImprint	SHA-256
policy	2.16.492.1.1.1.1.6.1
serial number	Numéro de série de la contremarque
accuracy	Si la synchronisation avec le temps UTC est différente de 1 seconde, ce champ doit être présent et doit préciser l'exactitude de la synchronisation. Si la synchronisation est de 1 seconde, il peut être omis.
gentimeaccuracy	absent
messageimprint	Empreinte des données et OID de l'algorithme utilisé
ordering	Ce champ doit être absent ou bien contenir la valeur false.
tsa	Si ce champ est présent, il doit être identique au champ subject du certificat de l'UH ayant signé la contremarque de temps.
extensions	Des extensions peuvent être incluses par l'AH, mais aucune ne doit être marquée comme critique.
nonce	Valeur incluse si présente dans la requête

10.2 LISTE DES CERTIFICATS REVOQUES

10.2.1 Champ de base

http://technique-icn.gouv.mc/crl/technique.crl

Champ	Valeur
Version	1 (pour version 2)
Signature	SHA256WithRSA
Issuer	• C = MC • O = AMSN • 2.5.4.97 = NTRMC-20A00001 • OU = 0206 20A00001 • CN = AC TECHNIQUE
Validity	5 jours
Revoked Certificates	• Serial Number • Revocation Date

10.2.2 Extensions

Champ	Criticité	Valeur
Authority Key Identifier	non	51:62:BB:6E:3A:B8:97:63:0A:50:38:46:BC:0B:45:D3:6D:8B:F0:9F
CRL Number	non	Défini par l'outil