



Damanesign

Service d'horodatage électronique

Politique et pratiques d'horodatage

Version 1.1 | Diffusion : public

OID n° 1.3.6.1.4.1.58553.2.8.1

Ce document est la propriété exclusive de Damanesign

Historique du document

Indice	Date de création	Rédacteur(s)	Modifications
1.0	27/06/2024	Fatimazahrae Jalal	Version initiale du document.

Sommaire

1	Introduction	5
1.1	Présentation générale	5
1.2	Définitions	5
1.3	Acronymes	6
1.4	Gestion du document	6
1.4.1	Identification de la PH	6
1.4.2	Point de contact	7
1.4.3	Amendement du document.....	7
1.4.4	Procédure d'approbation.....	7
1.4.5	Publication et consultation	8
1.5	Documents associés	8
1.5.1	Conditions Générales d'Utilisation	8
1.5.2	Documents normatifs.....	8
1.5.3	Politique de Certification.....	9
1.5.4	Politique de Sécurité du Système d'Information	9
1.5.5	Mesures de sécurité	9
2	Dispositions générales	9
2.1	Obligations de l'Autorité d'Horodatage (AH)	9
2.2	Obligations pour l'AC fournissant les certificats des UH	10
2.3	Obligations du Client	10
2.4	Obligations de l'Utilisateur de contremarques de temps.....	10
2.5	Déclarations des pratiques d'horodatage	11
2.6	Conditions Générales d'Utilisation.....	11
2.7	Conformité avec les exigences légales	12
2.8	Règlement des différends	12
2.9	Loi applicable	12
2.10	Responsabilités concernant la mise à disposition des informations devant être publiées	13
2.10.1	Entités chargées de la mise à disposition des informations.....	13
2.10.2	Informations devant être publiées	13
2.10.3	Délais et fréquences de publication	13
2.10.4	Contrôle d'accès aux informations publiées	13
2.11	Gestion des risques.....	13
3	Exigences opérationnelles.....	13
3.1	Organisation interne.....	13
3.1.1	Fiabilité.....	13
3.1.2	Rôles de confiance	13
3.2	Ressources humaines	13
3.3	Gestion des actifs.....	13
3.4	Contrôle d'accès	13
3.5	Cryptographie	13
3.5.1	Génération de clé des UH.....	14
3.5.2	Certification des clés des UH.....	14
3.5.3	Protection des clés privées des UH	14
3.5.4	Destruction des clés des UH	14
3.5.5	Exigences de sauvegarde des clés des UH	14
3.6	Horodatage	14
3.6.1	Gestion des requêtes des contremarques de temps.....	14
3.6.2	Synchronisation de l'horloge	16

3.7	Sécurité physique et environnementale.....	16
3.8	Sécurité opérationnelle	16
3.9	Sécurité réseau	16
3.10	Gestion des incidents.....	16
3.11	Procédure de constitution des données d'audit.....	17
3.12	Continuité d'activité	17
3.13	Fin de vie.....	17
3.14	Conformité	18
4	Exigences de sécurité techniques	18
4.1	Exactitude temps.....	18
4.2	Algorithmes obligatoires.....	18
4.3	Durée de validité des certificats de clé publique des UH.....	19
4.4	Durée d'utilisation des clés privées des UH.....	19
5	Profil des certificats et contremarques de temps.....	19
5.1	Format du certificat d'horodatage	19
5.2	Format des contremarques de temps	19
6	Réglementation	20

1 Introduction

1.1 Présentation générale

L'objectif de ce document est de définir les engagements et les pratiques que Damanesign, 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 vise la qualification par l'organe de contrôle national du service d'horodatage de Damanesign, appelé « Service » dans la suite du document.

Le service d'Horodatage de Damanesign peut être utilisé par ses clients :

- Inclus dans l'offre de signature électronique Damanesign, 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.

La présente Politique d'Horodatage est conforme au plan du document [ETSI EN 319 421 v1.1] et au Règlement eIDAS.

Le présent document est complété, dans sa partie mise en œuvre, par des Conditions Générales d'Utilisation du Service (CGU).

La présente 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.

Damanesign met en œuvre dans le cadre de cette politique un service d'horodatage conforme à l'ETSI EN 319421 mais non qualifié sur la base d'un certificat d'horodatage fourni par l'AC Damanesign Seal2 CA. La qualification est octroyée par l'organe de contrôle national à la suite d'un audit de conformité conforme aux procédures établies par l'Autorité nationale DGSSI.

1.2 Définitions

Application cliente : Application, gérée par le Client, qui envoie une requête d'horodatage au Service et qui récupère la contremarque de temps produite.

Autorité de Certification (AC) : Entité qui délivre et est responsable des Certificats électroniques signés en son nom, conformément à sa Politique de Certification. Dans ce document le terme d'AC concerne plus particulièrement l'AC qui émet les certificats d'UH.

Autorité d'Horodatage (AH) : Entité en charge de l'émission et de la gestion des contremarques de temps conformément à une PH.

Client : Entité légale, ayant contracté avec Damanesign pour bénéficier du Service, qui soumet ou fait soumettre par sa communauté d'utilisateurs des demandes de contremarques de temps pour ses besoins propres.

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

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

Listes de Certificats Révoqués (LCR) : Liste des identifiants des certificats qui ont été révoqués ou invalidés à une certaine date et qui ne sont donc plus dignes de confiance à partir de cette date (cf. RFC 5280 et RFC 6818).

Politique de Certification (PC) : Ensemble de règles identifiées, définissant les exigences auxquelles un AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière ou à une classe d'applications avec des exigences de sécurité communes.

Politique d'Horodatage (PH) : Ensemble de règles définissant les objectifs et les engagements d'une Autorité d'Horodatage pris pour assurer la fiabilité des services d'horodatage fournis. La PH est un document public accessible librement par les services demandeurs et les utilisateurs finaux.

Service : Service de confiance, opéré par Damanesign, sous la responsabilité de l'AH, qui émet des contremarques de temps conformément à la présente PH.

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]).

Utilisateur : Entité (personne physique ou morale) qui dispose d'une contremarque de temps émise par le Service selon la présente PH et qui a accepté les CGU du Service.

1.3 Acronymes

AC	Autorité de Certification
AH	Autorité d'Horodatage
CGU	Conditions Générales d'Utilisation
LCR	Liste des Certificats Révoqués
HSM	Hardware Security Module
PC	Politique de Certification
PH	Politique d'Horodatage
UH	Unité d'Horodatage
PSCO	Prestataire de service de confiance
OID	Object Identifier
UTC	Universal Time Coordinated

1.4 Gestion du document

1.4.1 Identification de la PH

La présente PH peut être identifié par son numéro d'identifiant d'objet :

1.3.6.1.4.1.58553.2.8.1

La présente PH est conforme à la politique BTSP (*best practices policy for time-stamp*) de l'ETSI, identifiée par l'OID 0.4.0.2023.1.1 [ETSI_319421].

1.4.2 Point de contact

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

Adresse postale	Damanesign 4 RUE OUED ZIZ 3e ETAGE APPT 7 AGDAL, Rabat
Adresse courriel	contact@damanesign.ma
Numéro de téléphone	+212 5 37 68 68 01

1.4.3 Amendement du document

La présente PH est sous la responsabilité de l'AH qui a en charge l'administration et la gestion de la PH, et qui est en particulier responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PH.

1.1.1.1 Procédure de mise à jour

Le document peut être mis à jour uniquement par l'AH, ou par les personnes mandatées par celle-ci, lors de modifications importantes des pratiques ou du Service, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique, ou corriger toute non-conformité.

Pour ce faire l'AH doit, dans un premier temps, valider ou non le principe de cette modification en fonction de ses objectifs et de ses responsabilités vis-à-vis du Service fourni. L'AH peut s'appuyer autant sur des ressources propres, que sur des ressources externes ayant une expertise dans le domaine, notamment pour l'évaluation de la conformité aux exigences réglementaires et normatives applicables.

Dans certains cas, un audit interne peut être diligenté pour s'assurer que les nouvelles évolutions ne remettent pas en cause des exigences prises par l'AH dans sa PH.

1.1.1.2 Circonstances selon lesquelles l'OID doit être changé

Toute évolution de la présente PH ayant un impact majeur sur le Service doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement identifier les exigences applicables aux contremarques simples.

1.4.4 Procédure d'approbation

La PH doit être approuvée par l'AH avant d'être promulguée.

La décision est consignée par le comité de pilotage du Service via une procédure d'approbation et de gestion des versions.

La nouvelle version de la PH entre en vigueur à la date indiquée dans sa page de garde et reste valide jusqu'à l'entrée en vigueur d'une nouvelle version.

1.4.5 Publication et consultation

La mise à disposition des informations devant être publiées à destination des Clients et Utilisateurs est réalisée par Damanesign.

La PH est publiée sur l'URL : <https://pki.damanesign.ma/cps.html>

Damanesign peut modifier la présente PH. Dans ce cas Damanesign avisera les Clients de la nature des modifications apportées, par tous moyens à sa convenance dont notamment le site Internet de Damanesign et la messagerie électronique, en fonction de la portée des modifications.

1.5 Documents associés

1.5.1 Conditions Générales d'Utilisation

L'AH définit des CGU qui reprennent les points principaux de la présente PH.

1.5.2 Documents normatifs

[ETSI_319401]	ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf
[ETSI_319421]	ETSI EN 319421 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. http://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf
[EIDAS]	Règlement n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n° 1999/93/CE. http://www.europa.eu
[GDPR]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 https://www.cnil.fr/fr/reglement-europeen-protection-donnees
[RFC_3161]	Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP) https://www.ietf.org/rfc/rfc3161.txt
[RFC_5816]	ESSCertIDv2 Update for RFC 3161 https://www.ietf.org/rfc/rfc5816.txt
[SOGIS-CRYPTO]	SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms – Version 1.0 – May 2016. http://sogis.org

[OPENSSL] Time Stamping Authority command (OpenSSL, Cryptography and SSL/TLS Toolkit)
<https://www.openssl.org/docs/manmaster/man1/openssl-ts.html>

1.5.3 Politique de Certification

[PC] Politique de certification Damanesign Seal2 CA,
OID n° 1.3.6.1.4.1.58553.1.8.1.2

1.5.4 Politique de Sécurité du Système d'Information

[PSSI] Politique de Sécurité des Systèmes d'Information de Damanesign

1.5.5 Mesures de sécurité

[DMSSC] Damanesign – la Partie Mesures de sécurité des services de confiance de la PC

2 Dispositions générales

2.1 Obligations de l'Autorité d'Horodatage (AH)

Le Service est placé sous la responsabilité de l'AH à laquelle incombe les obligations suivantes :

- Générer et signer les contremarques de temps conformément à la présente PH ;
- Respecter et se conformer aux exigences et procédures définies dans la présente PH ;
- Garantir la conformité des exigences et des procédures décrites dans la présente PH ;
- Mettre à disposition de Clients et Utilisateurs l'ensemble des informations nécessaire à la vérification des contremarques de temps qu'elle aura émises, selon les modalités indiquées dans la présente PH ;
- Respecter les conditions de disponibilité du Service convenues contractuellement avec les Clients ;
- Maintenir une information sur la compromission de la bi-clé des UH ;
- Utiliser des certificats pour les UH sous sa responsabilité, conformément aux exigences de la PC de l'AC émettrice de ces certificats ;
- Prévenir les clients de toute modification du service d'horodatage qui altérerait son fonctionnement ;
- Garantir l'intégrité et la fiabilité du service d'horodatage ;
- Authentifier les demandes de contremarques de temps soumises par les Clients à l'AH.

L'AH s'appuie sur une organisation interne de Damanesign (communément nommée Opérateur du Service d'Horodatage Électronique) pour la mise en œuvre technique du Service, notamment l'installation et l'exploitation des UH.

2.2 Obligations pour l'AC fournissant les certificats des UH

Les certificats de signature des contremarques de temps, mis en œuvre au sein de chaque UH sont émis par un AC interne à Damanesign ;

Cette AC assume les responsabilités suivantes :

- L'émission des certificats de signature des UH ;
- La mise à disposition de l'AH des services de révocation nécessaires ;
- La publication à destination des Clients et utilisateurs des contremarques de temps des moyens de vérification des certificats, c'est à dire de la chaîne de certification et du statut de révocation des certificats.

La politique de certification applicable est référencée sous le nom : Politique de Certification AC Cachet Damanesign.

2.3 Obligations du Client

Le Client doit respecter les obligations suivantes :

- Accepter et respecter les CGU ;
- Respecter les obligations de la présente PH qui lui sont applicables ;
- Envoyer des requêtes conformes à la [RFC_3161] et aux contraintes exposées dans cette PH, à partir d'une empreinte calculée avec un algorithme conforme à l'état de l'art et autorisé par la PH ;
- S'assurer de la validité des contremarques de temps dès leur réception en vérifiant en particulier la valeur de l'empreinte contenue ainsi que la signature de la contremarque de temps. Il est recommandé que les Clients vérifient que le certificat de l'UH ne soit pas révoqué au moment de l'obtention des contremarques.

D'autre part, le Client assume les responsabilités suivantes :

- La cohérence entre l'empreinte soumise dans la requête et les données horodatées par la contremarque de temps ;
- La conservation des contremarques de temps selon ses besoins propres ;
- La transmission des CGU à ses Utilisateurs ou l'obligation de faire figurer leurs obligations dans un document qui leur est opposable.

2.4 Obligations de l'Utilisateur de contremarques de temps

Pour faire confiance à une contremarque de temps, l'Utilisateur doit :

- 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. En particulier, cette vérification consistera à :
 - Recalculer le hach du document horodaté et le comparer avec celui-présent dans la contremarque de temps.
 - Vérifier la signature électronique présente dans la contremarque de temps à l'aide du certificat d'unité d'horodatage inclus dans la contremarque.
 - Vérifier le statut de révocation du certificat d'horodatage et la validité de l'ensemble de la chaîne de confiance.

- Tenir compte des limitations sur l'utilisation de la contremarque de temps indiquées dans la présente PH et dans les CGU, en particulier,
 - En s'assurant que le service d'horodatage qui a été utilisé pour générer la contremarque est conforme aux exigences légales, réglementaires ou normatives requises par l'utilisateur ;
 - b. En prenant en compte la limite de validité du certificat d'UH.
- Prendre en compte d'éventuelles consignes ou obligations contractuelles s'appliquant à son utilisation du Service.

2.5 Déclarations des pratiques d'horodatage

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

- L'AH a effectué une analyse de risque afin de déterminer les contrôles de sécurité nécessaires et les procédures opérationnelles.
- 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.
- L'AH met à la disposition des abonnés et des utilisateurs de contremarques de temps les éléments publics de sa DPH, s'il y a lieu, et toute autre documentation appropriée, tel que nécessaire pour évaluer la conformité à la PH.
- L'AH dispose d'une organisation adéquate pour l'approbation des DPH et la vérification de concordance entre les DPH et la PH.
- 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.
- L'AH doit informer au préalable les abonnés pour tout changement qu'elle a l'intention de faire dans la partie publique de sa DPH et, après l'approbation, immédiatement mettre à la disposition des abonnés et des utilisateurs de contremarques de temps la partie publique révisée de la DPH.
- L'AH met en œuvre des mécanismes lui permettant de garantir la dérive maximum de son service d'horodatage
- L'AH met en œuvre des mécanismes permettant d'arrêter le service d'horodatage si les jetons sont produits en dehors de la dérive maximale

2.6 Conditions Générales d'Utilisation

Un document, mis à la disposition des abonnés, précise les conditions générales d'utilisation (CGU) du service d'horodatage.

Une information sur un point de contact pour l'Autorité d'horodatage.

- L'OID de la PH appliquée
- Au moins un algorithme de hachage qui peut être utilisé pour représenter la donnée à horodater.

- La période de temps minimum, hors cas de révocation, durant laquelle les contremarques de temps seront vérifiables.
- L'exactitude du temps dans les contremarques de temps par rapport au temps UTC.
- Toutes les limitations sur l'utilisation du service d'horodatage ;
- Les obligations de l'abonné, si elles ne font partie ni du contrat avec l'abonné, ni de la déclaration des pratiques d'horodatage.
- Les obligations des utilisateurs de contremarques de temps, si elles ne font partie ni du contrat avec les utilisateurs de contremarques de temps, ni de la déclaration des pratiques d'horodatage.
- L'information sur la manière de vérifier les contremarques de temps de telle façon que l'utilisateur de contremarques de temps puisse "raisonnablement avoir confiance" dans les contremarques de temps ainsi que les restrictions possibles sur sa période de validité.
- La période de temps pendant laquelle les fichiers d'audit de l'Autorité d'horodatage sont conservés.
- Le système légal applicable.
- Les limitations de responsabilité.
- Les procédures pour les plaintes et le règlement des conflits.
- Les éléments permettant de valider la chaîne de certificats (du certificat de l'unité d'horodatage au certificat auto-signé).
- Le nom du pays dans lequel l'Autorité d'horodatage est établie et l'identifiant de l'Autorité d'horodatage (tel que figurant dans le certificat de l'unité d'horodatage)

2.7 Conformité avec les exigences légales

L'AH garantit la conformité avec les exigences légales. En particulier, elle permet de :

- Mettre en œuvre des mesures techniques appropriées et organisationnelles contre le traitement non autorisé ou illégal des données à caractère personnel contre la perte accidentelle, la destruction de données personnelles ou les dégâts commis aux données à caractère personnel.
- Garantir que les informations fournies par les services demandeurs à l'autorité d'horodatage ne seront pas divulguées, sauf accord de leur part, décision judiciaire ou exigence légale.

2.8 Règlement des différends

La résolution des litiges entre les parties découlant de l'interprétation, l'application ou l'exécution de la présente PH ou du contrat souscrit entre l'AH et le service demandeur, et à défaut d'accord amiable entre les parties ci-avant, sont du ressort du Tribunal de Casablanca

2.9 Loi applicable

Les dispositions de la PH associée sont régies par le droit Marocain.

2.10 Responsabilités concernant la mise à disposition des informations devant être publiées

2.10.1 Entités chargées de la mise à disposition des informations

Voir [DMSSC].

2.10.2 Informations devant être publiées

Damanesign s'engage à publier au minimum les informations suivantes à destination des Utilisateurs et des tiers ayant à déterminer la validité des contremarques produites par le Service :

- Le présent document, décrivant la politique et les pratiques du Service ;
- Les CGU ;
- Les certificats des UH.

2.10.3 Délais et fréquences de publication

Voir [DMSSC].

2.10.4 Contrôle d'accès aux informations publiées

Voir [DMSSC].

2.11 Gestion des risques

Voir [DMSSC].

3 Exigences opérationnelles

3.1 Organisation interne

3.1.1 Fiabilité

Voir [DMSSC] (« Responsabilité financière »).

3.1.2 Rôles de confiance

Les rôles de confiance sont attribués aux personnes sur lesquelles repose la sécurité du Service.

Voir [DMSSC] (« Mesures de sécurité procédurales »).

3.2 Ressources humaines

Voir [DMSSC].

3.3 Gestion des actifs

Voir [DMSSC].

3.4 Contrôle d'accès

Voir [DMSSC].

3.5 Cryptographie

Voir [DMSSC].

3.5.1 Génération de clé des UH

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

Ces clés sont générées et protégées au sein d'un HSM et ne sont pas exportées. La longueur des clés de l'AH est d'au moins 3072 bits avec l'algorithme RSA et la bi-clé cryptographique de l'AC délivrant les certificats des UH est de 4096 bits pour l'algorithme RSA.

Les HSM mis en œuvre sont des boîtiers certifiés EAL 4+.

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

3.5.2 Certification des clés des UH

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 identifiée en 1.5.3.

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.

3.5.3 Protection des clés privées des UH

Les clés privées des UH sont stockées dans un HSM certifié *Common Criteria EAL4+*

Pour la gestion du cycle de vie de ces HSM, voir [DMSSC].

Les HSM sont hébergés dans les sites sécurisées de l'AH et sont gérés exclusivement par les personnes ayant les rôles de confiance requis.

Les clés privées des UH font l'objet d'un suivi unitaire pendant toute la durée de leur vie.

3.5.4 Destruction des clés des UH

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

3.5.5 Exigences de sauvegarde des clés des UH

Les clés privées des UH ne sont pas sauvegardées.

3.6 Horodatage

3.6.1 Gestion des requêtes des contremarques de temps

3.6.1.1 Émission de contremarques de temps

Le Service fournit une contremarque de temps en réponse à une requête valide émise par une application cliente, contenant l'empreinte de la donnée à horodater.

Si la requête contient le champ *certReq* avec la valeur TRUE alors le Jeton d'horodatage contiendra le certificat de l'UH utilisé pour signer ce Jeton d'horodatage sinon il ne contiendra pas le certificat de l'UH.

Si la requête contient le champ *nonce*, sa valeur sera intégrée dans le champ *nonce* du Jeton d'horodatage produit.

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

- L'empreinte et l'algorithme d'empreinte de la donnée horodatée ;
- L'identifiant de l'UH contenu dans la propriété signée « *SigningCertificate* » de la signature du Jeton d'horodatage et dans le DN du certificat de l'UH dans le cas où il est présent dans le Jeton d'horodatage ;
- L'identifiant (OID) de la PH appliquée ;
- Un identifiant unique de la contremarque de temps ;
- La date UTC de génération de la contremarque de temps par l'UH.
- La précision de la date UTC de génération du Jeton d'horodatage ;
- Le « *nonce* » (dans le cas où il a été renseigné dans la requête) ;

La contremarque de temps est signée par l'UH avec sa clé privée, réservée à cet usage.

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

Il est important de noter que le service se restreint exclusivement à la génération de contremarques de temps.

3.6.1.2 Vérification d'une contremarque de temps

Les Clients et, de manière générale, les Utilisateurs des contremarques de temps sont incités à vérifier la validité des contremarques générées par le Service.

L'AH garantit l'accès à l'information nécessaire pour vérifier la signature numérique des contremarques de temps. En particulier :

- Les certificats des UH sont disponibles sur l'espace de publication de l'AH, et éventuellement sont joints à la contremarque de temps sur demande ;
- La chaîne de certification complète des certificats des UH est disponible sur l'espace de publication de l'AC ;
- Les informations sur le statut de révocation des certificats sont disponibles via les URL présentes dans les extensions *Authority Information Access* et *CRL Distribution Point* des certificats d'UH. Les LCR sont publiées sur l'espace de publication de l'AC.

La vérification d'un Jeton d'horodatage se déroule de la façon suivante :

- Vérifier que le Jeton d'horodatage a été correctement signé, et que le certificat de l'UH est valide à l'instant de la vérification ;
- Vérifier que l'OID contenu dans le Jeton d'horodatage est bien celui qui s'applique pour la présente PH ;

- Vérifier la valeur de l'empreinte contenue dans le Jeton d'horodatage par rapport aux données à laquelle elle se rapporte.

Si le Jeton d'horodatage est contenu dans une signature électronique, il devrait normalement être vérifiée par l'application de vérification de signature utilisée conformément à [ETSI_319102]. Dans tous les cas, un Jeton d'horodatage peut être vérifié avec [OPENSSL].

Les contremarques de temps ne sont vérifiables que pendant la période de validité des certificats des UH émettrices.

3.6.2 Synchronisation de l'horloge

L'heure intégrée dans une contremarque de temps est donnée par l'horloge de l'UH produisant cette contremarque. Cette horloge est synchronisée avec le temps UTC via plusieurs sources de référence.

L'AH garantit que son horloge est synchronisée avec le temps UTC selon l'exactitude déclarée de 1 (une) seconde, et garantit les propriétés suivantes :

- 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 ;
- Les horloges des UH 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 ;
- Tout non-respect de l'exactitude déclarée par son horloge interne sera détecté ;
- Aucune contremarque de temps ne sera générée par une UH dès lors que l'horloge de cette UH est détectée comme étant en dehors de l'exactitude annoncée, ou que l'exactitude ne peut plus être garantie ;
- La synchronisation de l'horloge est maintenue lorsqu'un saut de seconde est programmé comme notifié par l'organisme approprié. Le changement pour tenir compte du saut de seconde est effectué durant la dernière minute du jour où le saut de seconde est programmé. Un enregistrement du temps exact (à la seconde près) de l'instant de ce changement est effectué.

3.7 Sécurité physique et environnementale

Voir [DMSSC].

3.8 Sécurité opérationnelle

Voir [DMSSC].

3.9 Sécurité réseau

Voir [DMSSC].

3.10 Gestion des incidents

Voir [DMSSC].

L'AH garantit, dans le cas d'événements qui affectent la sécurité du Service – 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 Clients 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 ses Clients et Utilisateurs une description de la compromission 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 prolongée 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 Clients et Utilisateurs 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 Clients ou à la sécurité du Service.

3.11 Procédure de constitution des données d'audit

Voir [DMSSC].

Les traces générées et collectées par le Service comprennent notamment les traces d'événement relatives :

- Au cycle de vie des clés et des certificats d'UH ;
- Aux requêtes d'horodatage et contremarques de temps produites ;
- À la synchronisation entre les UH et le temps UTC, y compris les sauts de seconde, les calibrations et les pertes de synchronisation.

Les traces sont protégées en intégrité et en confidentialité.

3.12 Continuité d'activité

Voir [DMSSC].

3.13 Fin de vie

En cas de cessation d'activité de son AH, Damanesign doit s'assurer que l'impact sur les utilisateurs soit réduit au maximum et doit assurer la maintenance continue des informations nécessaires pour vérifier la justesse des contremarques de temps.

À ce titre, Damanesign a mis en œuvre un plan de fin de vie adressant l'ensemble des actions à exécuter :

- L'AH fournira à tous ses Clients et Utilisateurs, ainsi qu'à tous les partenaires et parties concernées, l'information concernant sa fin d'activité ;
- L'AH prévient directement et sans délai le point de contact de l'organe de contrôle national (D.G.S.S.I.) ;

- 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 s'efforcera de proposer à ses Clients un transfert du Service vers un autre prestataire de service de confiance d'horodatage ;
- 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, pendant une période raisonnable, ses clés publiques ainsi que ses certificats :
 - Les certificats de signature des UH seront révoqués ;
 - Les clés privées des UH seront détruites de telle façon que les clés privées ne puissent pas être recouvrées ;
- L'AH prend les mesures nécessaires pour couvrir les dépenses nécessaires à l'accomplissement de ces exigences minimales dans le cas où l'AH serait en faillite ou dans l'incapacité de couvrir les dépenses par elle-même.
- L'AH indique dans sa PH les dispositions prises pour la fin du service. Cela inclut :
 - Un avis aux abonnés et aux utilisateurs des contremarques de temps ;
 - Un transfert des obligations de l'AH à d'autres organismes.

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

Le plan de fin de vie appliqué sera celui en vigueur au moment de l'annonce de la fin d'activité

Le plan de fin de vie est tenu à jour. Il est revu annuellement et lors de tout changement majeur.

3.14 Conformité

Voir [DMSSC].

4 Exigences de sécurité techniques

4.1 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 des sources de temps externes de type GPS, DCF77, et références UTC(k).

4.2 Algorithmes obligatoires

L'Autorité d'Horodatage (AH) admet les empreintes obtenues grâce aux algorithmes préférés des utilisateurs, pour autant qu'ils respectent les normes préconisées par la DGSSI et l'ETSI.

Par ailleurs, l'AH accepte de générer des contremarques de temps pour les empreintes calculées avec les algorithmes suivants :

- SHA-256 ;

- SHA-384 ;
- SHA-512.

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 SHA256.

4.3 Durée de validité des certificats de clé publique des UH

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.

Par défaut, cette durée est de 5 ans.

4.4 Durée d'utilisation des clés privées des UH

La durée d'utilisation des clés privées des UH sera limitée en pratique à 2 ans afin de faciliter la vérification des jetons d'horodatage grâce à une période adéquate de validité du certificat.

5 Profil des certificats et contremarques de temps

5.1 Format du certificat d'horodatage

Les certificats des UH, pour la signature des Jetons d'horodatage, sont des certificats au format X.509 v3.

Voir [PC Seal2 CA].

5.2 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	OID de la présente PH (1.3.6.1.4.1.58553.2.8.1)
messageImprint	OID de l'algorithme de hash (empreinte) hash des données à horodater	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'ordonnement	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 Réglementation

Nous nous engageons fermement à assurer la conformité de nos services d'horodatage aux normes et exigences légales en vigueur. À cet égard, nous attestons que notre service d'horodatage, en conformité avec la Politique d'Horodatage (PH) établie, répond intégralement aux dispositions de la loi 43.20 du droit marocain régissant les services d'horodatage. Cette conformité englobe également une stricte adhésion aux référentiels de ladite loi. Il est important de souligner que cette déclaration est soumise à un processus formel de reconnaissance, avec la qualification délivrée par l'organe de contrôle national, suite à un audit de conformité rigoureux exécuté selon les procédures établies par l'Autorité nationale DGSSI. Nous percevons cette démarche comme une garantie de transparence, de fiabilité, et de conformité aux normes, renforçant ainsi la confiance de nos utilisateurs et des parties prenantes.

- Référentiel d'exigences générales de conformité des prestataires fournissant des services de confiance:
 - Se référer à la version la plus récente publiée sur le site de la DGSSI : <https://www.dgssi.gov.ma/fr/prestations-et-produits-reglementes>
 - A titre indicatif, la version la plus récente au moment de la rédaction des documents est la suivante : <https://www.dgssi.gov.ma/sites/default/files/2023-09/Ref1.pdf>

- Référentiel d'exigences de conformité relatives au service d'horodatage électronique :
 - Se référer à la version la plus récente publiée sur le site de la DGSSI : <https://www.dgssi.gov.ma/fr/prestations-et-produits-reglementes>
 - A titre indicatif, la version la plus récente au moment de la rédaction des documents est la suivante : <https://www.dgssi.gov.ma/sites/default/files/2023-09/Ref3.pdf>

- ETSI EN 319 401 : Electronic Signatures and Infrastructures (ESI) ; General Policy Requirements for Trust Service Providers :
 - Se référer à la version la plus récente publiée sur le site de l'ETSI : https://www.etsi.org/deliver/etsi_en/319400_319499/319401/
 - A titre indicatif, la version la plus récente au moment de la rédaction des documents est la suivante (v2.3.1) : https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.03.01_60/en_319401v020301p.pdf

- ETSI EN 319 421 v1.2.1 : Electronic Signatures and Infrastructures (ESI) ; Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
 - Se référer à la version la plus récente publiée sur le site de l'ETSI : https://www.etsi.org/deliver/etsi_en/319400_319499/319421
 - A titre indicatif, la version la plus récente au moment de la rédaction des documents est la suivante (v1.2.1) : https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.02.01_60/en_319421v010201p.pdf