Politique d’horodatage et déclaration des pratiques d’horodatage

V1.2 – Janvier 2022

IDEMIA

Introduction

Le présent document décrit les politiques et pratiques publics d'horodatage de l'AH IDEMIA.

Numéro de version	Auteur	Commentaire
V1.0	PRO	Version initiale du document.
V.1.1	PRO	Modification du §2.3 >
V.1.2	JMD	Transfert DOCAPOSTE

Sommaire

1 / Introduction 5

1.1 > Identification du document 5
1.2 > Publication du document 6
1.3 > Gestion de la PH et de la DPH 6
1.4 > Point de contact 6
1.5 > Généralités 6
1.5.1 > Définitions 6
1.5.2 > Abréviations 7

2 / Dispositions générales 9

2.1 > Obligations de l'Autorité d'Horodatage 9
2.2 > Obligations de l'abonné 9
2.3 > Obligations de l'utilisateur de contremarques de temps 9
2.4 > Obligations pour les AC fournissant les certificats des UH 10
2.5 > Déclarations des pratiques d'horodatage 10
2.6 > Conditions Générales d'Utilisation 10
2.7 > Conformité avec les exigences légales 11

3 / Exigences opérationnelles 12

3.1 > Gestion des requêtes de contremarques de temps 12
3.2 > Fichiers d'audit 12
3.3 > Gestion de la durée de vie de la clé privée 12
3.4 > Synchronisation de l'horloge 12
3.5 > Exigences du contenu d'une contremarque de temps 13
3.6 > Compromission de l'AH 13
3.7 > Fin d'activité 14

4 / Exigences physiques et environnementales, procédurales et organisationnelles 15

4.1 > Exigences physiques et environnementales 15
4.2 > Exigences procédurales 16
4.3 > Manipulation et sécurité des supports 16
4.4 > Planification de système 16
4.5 > Rapport d'incident et réponse 16
4.6 > Procédures de fonctionnement et responsabilités 16
4.7 > Exigences organisationnelles 17

5 / Exigences de sécurité techniques 19

5.1 > Exactitude temps 19

5.2 > Génération de clé 19
5.3 > Certification des clés de l’unité d’horodatage 19
5.4 > Protection des clés privées des unités d'horodatage 19
5.5 > Exigences de sauvegarde des clés des unités d'horodatage 20
5.6 > Destruction des clés des unités d'horodatage 20
5.7 > Algorithmes obligatoires 20
5.8 > Vérification des contremarques de temps 20
5.9 > Durée de validité des certificats de clé publique des unités d'horodatage 21
5.10 > Durée d’utilisation des clés privées des UH 21

6 / Profil des certificats et contremarques de temps 22
6.1 > Format du certificat d’horodatage pour l’AH qualifiée 22
6.2 > Format des contremarques de temps pour l’AH qualifiée 22
6.3 > Format du certificat d’horodatage pour l’AH non qualifiée 23
6.4 > Format des contremarques de temps pour l’AH non qualifiée 23

7 / Annexe 1 : Documents cités en référence 24
7.1 > Réglementation 24
7.2 > Documents techniques 24

1 / Introduction

IDEMIA, en tant que prestataire de services de confiance au sens du Règlement nº 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 nº 1999/93/CE (dit « Règlement eIDAS »), met en œuvre

- Un service d'horodatage visant à être qualifié au sens du Règlement eIDAS ;
- Un service d'horodatage non qualifié.

A la suite de la cession des activités de signature électronique de IDEMIA à la société Docaposte Trust & Sign, cession qui comprend le personnel en charge de ces activités, la gestion de la continuité des services est assurée par Docaposte Trust & Sign à partir du 1 janvier 2022.
L'accord d'autorisation entre IDEMIA et Docaposte Trust & Sign engage Docaposte Trust & Sign à opérer les services selon le cadre déjà audité.

Cette Politique d'Horodatage est conforme à la Politique d'Horodatage type décrite dans le document [ETSI_TIMESTAMP] et identifiée par l'OID BTSP 0.4.0.2023.1.

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

- Inclus dans l'offre de signature électronique IDEMIA, pour fournir des dates fiables, donnant ainsi une bonne assurance sur la qualité des dates associées aux actes de signature,
- Directement, en tant que service à part entière.

L'objectif de ce document est de définir les engagements que l'AH, respecte dans la délivrance et la gestion de contremarques de temps, ainsi que les obligations des autres participants. Le respect de ces engagements permet, après audit de conformité selon les processus établis dans le règlement eIDAS (cf. [ETSI_TSP]), la qualification du service d'horodatage d'IDEMIA par l'organe de contrôle national.

La structure de la présente Politique d'Horodatage est basée sur les documents issus de l'ETSI (cf. [ETSI_TIMESTAMP]) et du RGS v2 de l'ANSSI.

Le présent document inclus la partie publique de la Déclaration des Pratiques d'Horodatage. Il est complété, dans sa partie mise en œuvre, par une version confidentielle de la Déclaration des Pratiques d'Horodatage (DPH) et des Conditions Générales d'Utilisation du service d'horodatage (CGU).
Une DPH expose les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la PH, en particulier les processus qu'une UH emploiera pour la création des contremarques de temps et le maintien de l'exactitude de ses horloges.
Le présent document contient les éléments publics de la DPH.
Cette PH n'impose pas d'exigences sur le lien entre l'empreinte numérique à horodater et le contenu de la donnée électronique qui en est à l'origine. Cette vérification est à la charge de l'utilisateur du service d'horodatage.

1.1 > Identification du document

La présente Politique d'Horodatage/Déclaration des pratiques d'horodatage (PH/DPH) est dénommée « Politique d'Horodatage IDEMIA ». Elle peut être identifiée par son numéro d'identifiant d'objet OID :

1.3.6.1.4.1.54916.2.1.1.1	Pour l'AH visant la qualification eIDAS
1.3.6.1.4.1.54916.2.1.2.1	Pour l'AH non qualifiée.

1.2 > Publication du document

La présente Politique d'Horodatage est publiée sur l'URL :
http://pki.trust.idemia.io/policies/idemia-eidas-tsp.pdf

1.3 > Gestion de la PH et de la DPH

L'entité en charge de l'administration et de la gestion de la politique d'horodatage (PH) et des déclarations de pratique d'horodatage (DPH) est DOCAPOSTE Trust & Sign à partir du 1 janvier 2022. DOCAPOSTE Trust & Sign est responsable du suivi et de la modification, dès que nécessaire, de la présente PH/DPH élaborée par IDEMIA et si nécessaire de la version confidentielle de la DPH.

1.4 > Point de contact

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

DOCAPOSTE Trust & Sign	
Personne à contacter	PKI Information contact
Adresse postale	DOCAPOSTE Trust & Sign 45-47 Boulevard Paul Vaillant Couturier 94200 Ivry-sur-Seine
Numéro de téléphone	+33 1 56 29 70 01
Adresse email	info@docaposte.fr
Site internet:	http://pki.trust.idemia.io

1.5 > Généralités

1.5.1 > Définitions

Abonné – Entité ayant besoin de faire horodater des données par une Autorité d'Horodatage et qui a accepté les conditions d'utilisation de ses services. Cette notion est valable pour les hypothèses où la contremarque de temps est demandée directement à l'AH.
Autorité de Certification (AC) – Entité qui délivre et est responsable des Certificats électroniques signés en son nom.
Autorité d'Horodatage (AH) – Entité en charge de l'émission et de la gestion des contremarques de temps conformément à une Politique d'horodatage.
Contremarque de temps – Donnée signée qui lie une représentation d'une donnée à un temps particulier, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là.
Coordinated Universal Time (UTC) – Echelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5 [TF.460-5].

Déclaration des pratiques d'horodatage (DPH) – Document qui 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 - Service qui associe de manière sûre un événement et une heure afin d'établir de manière fiable l'heure à laquelle cet événement s'est réalisé.
Jeton d'horodatage – Voir Contremarque de temps.
Liste de Certificats Révoqués (LCR) – Liste de certificats ayant fait l'objet d'une révocation avant la fin de leur période de validité.
Politique d'horodatage (PH) – Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AH se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'une contremarque de temps à une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes. Une PH peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les Abonnés et les Utilisateurs de contremarques de temps.
Service d'horodatage – Ensemble des prestations nécessaires à la génération et à la gestion de Contremarques de temps.
Système d'horodatage – Ensemble des Unités d'horodatage et des composants d'administration et de supervision utilisés pour fournir des Services d'horodatage.
Unité d'Horodatage (UH) – Ensemble de matériel et de logiciel en charge de la création de Contremarques de temps caractérisé par un identifiant de l'Unité d'Horodatage accordé par une AC, et une clé unique de signature de contremarques de temps.
UTC(k) – Temps de référence réalisé par le laboratoire "k" et synchronisé avec précision avec le temps UTC, dans le but d'atteindre une précision de ±100 ns, selon la recommandation S5 (1993) du Comité Consultatif pour la définition de la Seconde. (Rec. ITU-R TF.536-1 [TF.536-1]).
Utilisateur de contremarque de temps – Entité (personne ou système) qui fait confiance à une Contremarque de temps émise sous une Politique d'horodatage donnée par une Autorité d'horodatage donnée.

1.5.2 > Abréviations

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

AC	Autorité de Certification
AH	Autorité d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
BTSP	Best practices policy for time-stamp
CGU	Conditions Générales d'Utilisation du service d'horodatage
CRL	Liste des Certificats Révoqués (Certificate revocation list)
DN	Distinguished Name (nom distinctif)
DPH	Déclaration des Pratiques d'Horodatage
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de gestion de clés
LCR	Liste des Certificats Révoqués
OCSP	Online Certificate Status Protocol
OID	Object Identifier (identifiant d'objet)
PC	Politique de Certification
PH	Politique d'Horodatage

PSHE	Prestataire de Services d'Horodatage Électronique
SSI	Sécurité des Systèmes d’Information
UH	Unité d’horodatage
URL	Uniform Resource Locator (adresse universelle)
UTC	Coordinated Universal Time

2 / Dispositions générales

2.1 > Obligations de l'Autorité d'Horodatage

L'AH génère et signe les contremarques de temps conformément aux documents suivants : la présente PH / DPH, la DPH confidentielle associée et les CGU.
L'AH garantit la conformité pour tout acteur intervenant dans la gestion des contremarques de temps par rapport aux exigences et aux procédures prescrites dans cette PH / DPH et dans la DPH confidentielle associée.
L'AH remplit tous ses engagements tels que stipulés dans ses Conditions Générales d'Utilisation.
L'AH garantit la conformité des exigences et procédures définies dans sa DPH confidentielle avec la présente PH / DPH.
L'AH met à la disposition des abonnés et utilisateurs l'ensemble des informations nécessaires à la vérification des contremarques de temps.
L'AH respecte les conditions de disponibilité du service d'horodatage convenues contractuellement avec les abonnés.
L'AH maintient une information sur la compromission de la bi-clé des UH.

2.2 > Obligations de l'abonné

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

2.3 > Obligations de l'utilisateur de contremarques de temps

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

a) Vérifier que la contremarque de temps a été correctement signée, et que le certificat de l'UH est valide à l'instant de la vérification[1]. En particulier, cette vérification consistera à :
   a. Recalculer le haché du document horodaté et le comparer avec celui-présent dans la contremarque de temps.
   b. Vérifier la signature électronique présente dans la contremarque de temps à l'aide du certificat d'unité d'horodatage inclus dans la contremarque
   c. Vérifier le statut de révocation de l'unité d'horodatage et la validité de l'ensemble de la chaîne de confiance.
b) Tenir compte des éventuelles limitations sur l'utilisation de la contremarque de temps indiquées dans la PH/DPH, et les conditions générales d'utilisation, en particulier,
   a. 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

[1] Différents outils du marché, tel qu'Acrobat Reader ou les librairies OpenSource SD-DSS et OpenSSL, permettent de réaliser ces vérifications sur les jetons générés par IDEMIA.

b. En prenant en compte la limite de validité du certificat d'UH[2].

2.4 > Obligations pour les AC fournissant les certificats des UH

Les certificats des UH doivent être délivrés par l'AC IDEMIA définie ci-dessous. La description de cette AC et les obligations qu'elle respecte sont définis dans les documents :

- [PC AC IDEMIA Qualifiée], pour l'AH visant à être qualifiée
- [PC AC IDEMIA NCP+], pour l'AH non-qualifiée

2.5 > Déclarations des pratiques d'horodatage

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

a) L'AH a effectué une analyse de risque afin de déterminer les contrôles de sécurité nécessaires et les procédures opérationnelles.
b) L'AH a une Déclaration des pratiques et des procédures utilisées pour adresser toutes les exigences identifiées dans chaque PH/DPH supportée.
c) La DPH identifie les obligations de toutes les organisations externes participant à la fourniture du service d'horodatage, y compris la politique applicable et les pratiques. Cela inclut l'AC fournissant les certificats aux UH.
d) L'AH met à la disposition des abonnés et des utilisateurs de contremarques de temps les éléments publics de sa DPH, s'il y a lieu, et toute autre documentation appropriée, tel que nécessaire pour évaluer la conformité à la PH/DPH.
e) L'AH dispose d'une organisation adéquate pour l'approbation des DPH et la vérification de concordance entre les DPH et la PH/DPH.
f) Le responsable opérationnel de l'AH garantit que les pratiques sont correctement mises en œuvre.
g) L'AH définit une procédure de contrôle périodique de la conformité des pratiques, y compris les responsabilités, à la déclaration des pratiques d'horodatage.
h) L'AH doit informer 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.
i) Si l'AH a été évaluée pour être en conformité avec la présente PH/DPH et si une modification envisagée à l'initiative de l'AH pouvait entraîner une non-conformité avec ladite PH/DPH ou avec la version confidentielle DPH, alors l'AH soumettra cette modification à l'organisme évaluateur indépendant pour avis.

2.6 > Conditions Générales d'Utilisation

L'AH définit des CGU qui reprennent les grands principes décrits dans la présente PH/DPH Ces CGU sont basées sur le modèle défini dans l'annexe B de l'ETSI EN 319 421.
Les CGU du service d'horodatage sont mises à disposition des abonnés et utilisateurs (actuels ou potentiels) des contremarques de temps à l'URL suivante :

[2] La durée de vie des clés privées d'UH est limitée à un an pour permettre une période de vérification des contre-marques de temps d'au moins 5 ans.

AH qualifiée
http://pki.trust.idemia.io/agreement/idemia-eidas-tac-tsa.pdf

AH non-qualifiée
http://pki.trust.idemia.io/agreement/idemia-eidas-tac-tsa.pdf

2.7 > Conformité avec les exigences légales

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

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

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

3 / Exigences opérationnelles

3.1 > Gestion des requêtes de contremarques de temps

L'AH IDEMIA fournit une contremarque de temps en réponse à une demande contenant l'empreinte de la donnée à horodater.
La fourniture d'une contremarque de temps en réponse à une demande n'excède pas quelques secondes[3], ceci afin de ne pas nuire ni dégrader l'ergonomie de l'application appelante.
L'AH IDEMIA conserve la contremarque de temps générée.

3.2 > Fichiers d'audit

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

a) Les enregistrements d'audit relatifs à l'administration des services d'horodatage,
b) Les enregistrements d'audit relatifs au fonctionnement du service d'horodatage,
c) Les enregistrements d'audit concernant les événements touchant au cycle de vie des clés et certificats d'UH,
d) Les enregistrements d'audit concernant les événements touchant à une synchronisation de l'horloge des UH, y compris les événements touchant à la détection de perte de synchronisation.

La confidentialité des enregistrements d'audit est assurée par une gestion d'accès physique, système et réseau appropriée. L'intégrité et la protection contre la suppression sont assurées. Les moyens mis en œuvre sont décrits dans la version confidentielle de la DPH.
Les journaux du service d'horodatage sont conservés pendant 7 ans minimum.

3.3 > Gestion de la durée de vie de la clé privée

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

a) Des procédures opérationnelles ou techniques assurent qu'une nouvelle paire de clés est mise en place quand la fin de la période d'utilisation d'une clé privée d'UH a été atteinte.
b) L'AH détruit la clé privée si la fin de la période d'utilisation de cette clé privée a été atteinte.

La durée de vie des clés privées de signature des UH est définie dans le § 5.10 >.

3.4 > Synchronisation de l'horloge

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

La synchronisation utilise des serveurs de temps interne qui sont eux-mêmes synchronisés sur plusieurs sources de temps externes, dont au moins une source de référence UTC(k).

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

Des précisions quant aux modalités de la synchronisation sont fournies dans la version confidentielle de la DPH.
En particulier :

a) Le calibrage de chaque horloge d'UH est maintenu de telle manière que les horloges ne puissent pas normalement dériver en dehors de l'exactitude déclarée.
b) Les horloges des unités d'horodatage sont protégées contre les menaces relatives à leur environnement qui pourraient aboutir à une désynchronisation avec le temps UTC en dehors de l'exactitude déclarée.
c) L'AH s'assure que tout non-respect de l'exactitude déclarée par son horloge interne sera détecté.
d) Si l'horloge d'une UH est détectée comme étant en dehors de l'exactitude annoncée, ou que les serveurs de temps ne sont plus disponibles, alors les contremarques de temps ne seront plus générées.
e) L'AH garantit que la synchronisation de l'horloge est maintenue lorsqu'un saut de seconde est programmé comme notifié par l'organisme approprié. 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.

3.5 > Exigences du contenu d'une contremarque de temps

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

- L'identifiant de l'UH fourni à travers le DN du certificat de l'unité d'horodatage ;
- L'identifiant (OID) de la politique d'horodatage appliquée ;
- Optionnellement, un identifiant unique de la contremarque ;
- Un temps, celui du moment de génération de la contremarque, synchronisé avec le temps de référence référencé en 3.4 >
- L'empreinte et l'algorithme d'empreinte de la donnée horodatée.

La contremarque de temps est signée par l'UH avec sa clé privée, réservée à cet usage.
Les contremarques sont conformes à la RFC 3161 (cf. [RFC_3161]). Le détail du format est donné au §6.2 > Format des contremarques de temps.

3.6 > Compromission de l'AH

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

a) L'AH traite le cas de la compromission réelle ou suspectée de la clé privée de signature d'une UH ou la perte de calibrage de l'horloge d'une UH, qui pourrait affecter des contremarques de temps émises dans le cadre d'un plan de secours
b) Dans le cas d'une compromission, réelle ou suspectée, l'AH mettra à la disposition de tous les abonnés et utilisateurs de contremarques de temps une description de la compromission qui est survenue.
c) Dans le cas d'une perte de calibrage d'une UH, qui pourrait affecter des contremarques de temps émises, l'AH prendra les mesures nécessaires pour que les contremarques de temps de cette UH ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.

d) Dans le cas d’une perte de connexion prolongés avec les serveurs de temps, l’AH prendra les mesures nécessaires pour que les contremarques de temps de cette UH ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.
e) Dans le cas d'un événement majeur dans le fonctionnement de l'AH ou d'une perte de calibrage qui pourrait affecter des contremarques de temps émises, chaque fois que cela sera possible, l’AH mettra à la disposition de tous ses abonnés et utilisateurs de contremarques de temps toute information pouvant être utilisée pour identifier les contremarques de temps qui pourraient avoir été affectées, à moins que cela ne contrevienne à la vie privée des abonnés ou à la sécurité des services d'horodatage.
f) L'AH prévient directement et sans délai le point de contact de l’organe de contrôle national.

3.7 > **Fin d'activité**

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

a) Avant que l’AH ne termine ses services d'horodatage, les procédures suivantes seront exécutées au minimum :
   - L’AH rendra disponible à tous ses abonnés et utilisateurs de contremarques de temps l'information concernant sa fin d'activité ;
   - L’AH abrogera les autorisations données aux sous-traitants d'agir pour son compte dans l'exécution de n'importe quelles fonctions touchant au processus de génération des contremarques de temps ;
   - L’AH transférera à un organisme fiable ses obligations de maintien des fichiers d'audit et des archives nécessaires pour démontrer son fonctionnement correct durant une période raisonnable ;
   - L’AH maintiendra ou transférera à un organisme fiable ses obligations de rendre disponibles aux utilisateurs de contremarques de temps pendant une période raisonnable ses clés publiques ainsi que ses certificats ;
   - Les clés privées des UH seront détruites de telle façon que les clés privées ne puissent pas être recouvrées.
b) L’AH prend les mesures nécessaires pour couvrir les dépenses pour accomplir ces exigences minimales dans le cas où l’AH tomberait en faillite ou pour d'autres raisons serait incapable de couvrir les dépenses par elle-même.
c) L'AH prévient directement et sans délai le point de contact de l’organe de contrôle national.

4 / Exigences physiques et environnementales, procédurales et organisationnelles

4.1 > Exigences physiques et environnementales

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

a) A la fois pour la fourniture du service d'horodatage et la gestion de l'horodatage :
   - L'accès physique aux équipements concernés par les services d'horodatage est limité aux individus autorisés ;
   - Des contrôles sont mis en œuvre pour éviter la perte, des dégâts ou la compromission d'actifs et l'interruption des activités et ;
   - Des contrôles sont mis en œuvre pour éviter la compromission ou le vol d'informations ou d'équipements informatiques.

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

c) Les contrôles suivants complémentaires sont appliqués à la gestion du service d'horodatage :
   - Le système d'horodatage fonctionne dans un environnement qui protège physiquement les services de la compromission au moyen d'un accès non autorisé aux systèmes ou aux données ;
   - La protection physique est réalisée par la création d'un périmètre de sécurité dédié clairement défini (c'est-à-dire des barrières physiques) autour des unités d'horodatage ;
   - Des contrôles de sécurité physique et environnementale sont mis en œuvre pour protéger l'environnement qui abrite les ressources du système, les ressources du système elles-mêmes et les équipements utilisés pour remplir leur fonction ; la politique de sécurité physique et environnementale de l'Autorité d'horodatage pour les systèmes concernés par la gestion de l'horodatage concerne :
     - Le contrôle d'accès physique ;
     - La protection vis à vis des catastrophes naturelles ;
     - Les facteurs de sécurité liés au feu ;
     - La défaillance d'alimentation électrique ;
     - La défaillance de connexions réseau ;
     - L'écroulement de la structure ;
     - Les fuites de plomberie ;
     - La protection contre le vol, la casse et la pénétration ;
     - Le rétablissement de la sécurité après un désastre.
   - Des contrôles sont mis en œuvre pour empêcher des équipements, de l'information, des médias et du logiciel touchant aux services d'horodatage d'être enlevés du site sans autorisation

4.2 > Exigences procédurales

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

a) L'intégrité des composants du système d'horodatage et l'information sont protégés contre les virus, les logiciels malveillants et non autorisés
b) Un rapport d'incident et des procédures de réponse aux incidents sont employés d'une telle façon que les dégâts liés aux incidents de sécurité et aux défaillances soient réduits au minimum.
c) Les supports employés dans les systèmes d'horodatage sont manipulés de manière sécuritaire pour les protéger des dégâts, du vol, de l'accès non autorisé et de l'obsolescence
d) Des procédures sont établies et mises en œuvre pour tous les rôles de confiance et administratifs qui impactent la fourniture des services d'horodatage

4.3 > Manipulation et sécurité des supports

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

4.4 > Planification de système

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

4.5 > Rapport d'incident et réponse

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

4.6 > Procédures de fonctionnement et responsabilités

Les opérations de sécurité sont séparées des autres opérations. Elles incluent :

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

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

Gestion d’accès au système

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

- Des contrôles (par pare-feux) sont être mis en œuvre pour protéger le réseau interne de l’AH d'accès non autorisés incluant l'accès par des abonnés et des tierces personnes. Les pare-feux sont aussi configurés pour bloquer tous les protocoles et les accès non nécessaires au fonctionnement de l’AH.
- L’AH effectue une administration efficace des utilisateurs (opérateurs, administrateurs et auditeurs), pour maintenir la sécurité du système, y compris la gestion des comptes des utilisateurs, l'audit, et la modification ou le retrait rapide d'accès.
- L’AH garantit que l'accès aux fonctions du système, à l'information et aux applications est limité conformément à la politique de contrôle d'accès et que le système d'horodatage possède les contrôles informatiques de sécurité suffisants pour la séparation des rôles de confiance identifiés dans les pratiques d'horodatage, y compris la séparation des fonctions d'administrateur de sécurité et des fonctions opérationnelles. En particulier, l'utilisation de programmes systèmes utilitaires sera limitée et très contrôlée.
- Le personnel de l’AH est dûment identifié et authentifié avant d'utiliser des applications critiques liées à l'horodatage.
- Le personnel de l’AH sera tenu responsable de ses activités, par exemple en conservant des fichiers d'audit.

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

- L'Autorité d'horodatage garantit que des composants de réseau locaux (par exemple les routeurs) seront mis dans un environnement physiquement sûr et que leurs configurations sont périodiquement vérifiées pour la conformité avec les exigences indiquées par l’AH.
- Une surveillance permanente et des équipements d'alarme doivent être mis en œuvre pour permettre à l’AH de détecter, d'enregistrer et de réagir rapidement à n'importe quelle tentative non autorisée et/ou irrégulière d'accès à ses ressources.

Déploiement et Maintenance

L’AH emploie des produits et systèmes de confiance.

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

4.7 > **Exigences organisationnelles**

L’AH garantit que le personnel et les pratiques d'embauche améliorent et concourent à la fiabilité des opérations de l’AH. En particulier :

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

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

- Le personnel de gestion employé possède :

- La connaissance de la technologie de l'horodatage et ;
- La connaissance de technologie de la signature numérique et ;
- La connaissance des mécanismes pour le calibrage ou la synchronisation des horloges des unités d'horodatage avec le temps de référence et ;
- Pour le personnel avec des responsabilités de sécurité, une bonne connaissance des procédures de sécurité, et ;
- L'expérience avec la sécurité de l'information et l'évaluation des risques.

- Tout le personnel de l'AH dans des rôles de confiance est libre de conflit d'intérêt qui pourrait porter préjudice à l'impartialité des opérations de l'AH.
- Les rôles de confiance incluent les rôles qui impliquent les responsabilités suivantes :
  - Les officiers chargés de la sécurité : responsabilité complète d'administrer la mise en œuvre des pratiques de sécurité ;
  - Les administrateurs système : autorisés à installer, configurer et maintenir les modules d'horodatage de l'AH pour la gestion de l'horodatage ;
  - Les opérateurs système : responsables pour faire fonctionner les modules d'horodatage de l'AH de manière quotidienne et autorisés pour effectuer les opérations de sauvegarde et des secours ;
  - Les auditeurs de système : autorisés à consulter les archives et les fichiers d'audit des modules d'horodatage.
- Le personnel de l'AH est formellement nommé aux rôles de confiance par la direction responsable de la sécurité.
- L'AH s'interdit de nommer aux rôles de confiance ou de gestion toute personne connue pour avoir une condamnation pour un crime sérieux ou une autre infraction qui affecte son adéquation avec la position. Le personnel n'a pas accès aux fonctions de confiance avant que les contrôles nécessaires ne soient achevés

5 / Exigences de sécurité techniques

5.1 > Exactitude temps

Voir section 3.4 > Synchronisation de l'horloge.

5.2 > Génération de clé

L'AH garantit que les clés cryptographiques des UH sont produites dans des circonstances et un environnement contrôlé, faisant l'objet d'un compte-rendu d'exécution signé des deux rôles de confiance.

Ces clés sont générées et protégées au sein de HSM (Hardware Security Module) cryptographiques et ne sont pas exportées à l'exception de l'export initial pour la mise en production. La longueur des clés de l'UH est de 4096 bits avec l'algorithme RSA.

5.3 > 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.

AH qualifiée

Le certificat de l'UH est généré par l'AC Qualifiée IDEMIA

AH non-qualifiée

Le certificat de l'UH est généré par l'AC IDEMIA NCP+

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

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

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

5.4 > Protection des clés privées des unités d'horodatage

AH qualifiée

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

AH non-qualifiée
Les clés privées des UH sont stockées dans un HSM certifié a minima CC EAL4+ ou FIPS140-2 level 2

5.5 > Exigences de sauvegarde des clés des unités d'horodatage

La sauvegarde des clés des UH est interdite.

La seule exception à cette règle est la création d'une sauvegarde à l'issue de la cérémonie des clés permettant l'injection de la clé sur le HSM de production. A l'issue de la mise en production, la sauvegarde utilisée est détruite et toutes autres sauvegardes sont interdites.

5.6 > Destruction des clés des unités d'horodatage

Les clés de signature des UH sont détruites à la fin de leur cycle de vie restreint par la durée d'utilisation de la clé privée.

5.7 > Algorithmes obligatoires

L'AH accepte les empreintes calculées avec les algorithmes souhaités par les abonnés, si ceux-ci sont compatibles avec les meilleures pratiques et les recommandations de l'ANSSI et de l'ETSI et sont supportés par la plate-forme. En particulier, les algorithmes suivants sont supportés actuellement :

- SHA-256
- 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 4096 bits et l'algorithme de signature utilise une fonction de hachage SHA-256 ou supérieur.

5.8 > Vérification des contremarques de temps

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

a) Les certificats des UH sont disponibles, joints à la contremarque de temps.
b) La chaîne de certification complète est disponible à l'URL suivante : https://pki.trust.idemia.io/ca.html
c) Les LCR des AC de la chaîne de certification sont disponibles en activant les URL disponibles dans les certificats dans l'attribut cRLDistributionPoint.

5.9 > Durée de validité des certificats de clé publique des unités d'horodatage

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

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

Par défaut, cette durée est de 6 ans.

5.10 > Durée d’utilisation des clés privées des UH

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

6 / Profil des certificats et contremarques de temps

6.1 > Format du certificat d'horodatage pour l'AH qualifiée

Voir PC de l'AC Qualifiée IDEMIA

6.2 > Format des contremarques de temps pour l'AH qualifiée

Les contremarques de temps respectent le gabarit suivant :

Champ	Commentaires	Valeur
version	Version du format	1
policy	OID de la PH	1.3.6.1.4.1.54916.2.1.1.1
messageImprint	OID de l'algorithme de hash (empreinte) hash des données à horodater	Identiques aux valeurs inclues dans la demande
serialNumber	Identifiant unique de la contremarque de temps	Généré par l'UH
genTime	Heure de la contremarque de temps	Heure de l'UH au moment de la génération
accuracy	Précision déclarée	1 seconde
ordering	Information d'ordonnancement	false
nonce	Donnée anti-rejeu	Identique à celui présent dans la demande si nonce était présent
tsa	Identifiant de l'UH	Non présent dans la version actuelle du service. Les futures versions pourront intégrer le champ "subject" du certificat d'horodatage de l'UH
extensions	Extension supplémentaire optionnelle	Non présent dans la version actuelle du service. Les futures versions pourront intégrer le qcstatement « esi4-qtstStatement-1 »

Tableau 1 : Format des contremarques de temps

6.3 > Format du certificat d'horodatage pour l'AH non qualifiée

Voir PC de l'AC NCP+ IDEMIA

6.4 > Format des contremarques de temps pour l'AH non qualifiée

Les contremarques de temps respectent le gabarit suivant :

Champ	Commentaires	Valeur
version	Version du format	1
policy	OID de la PH	1.3.6.1.4.1.54916.2.1.2.1
messageImprint	OID de l'algorithme de hash (empreinte) hash des données à horodater	Identiques aux valeurs inclues dans la demande
serialNumber	Identifiant unique de la contremarque de temps	Généré par l'UH
genTime	Heure de la contremarque de temps	Heure de l'UH au moment de la génération
accuracy	Précision déclarée	1 seconde
ordering	Information d'ordonnancement	false
nonce	Donnée anti-rejeu	Identique à celui présent dans la demande si nonce était présent
tsa	Identifiant de l'UH	Non présent dans la version actuelle du service. Les futures versions pourront intégrer le champ "subject" du certificat d'horodatage de l'UH
extensions	Extension supplémentaire optionnelle	Aucune extension supplémentaire

Tableau 2 : Format des contremarques de temps

7 / Annexe 1 : Documents cités en référence

7.1 > Réglementation

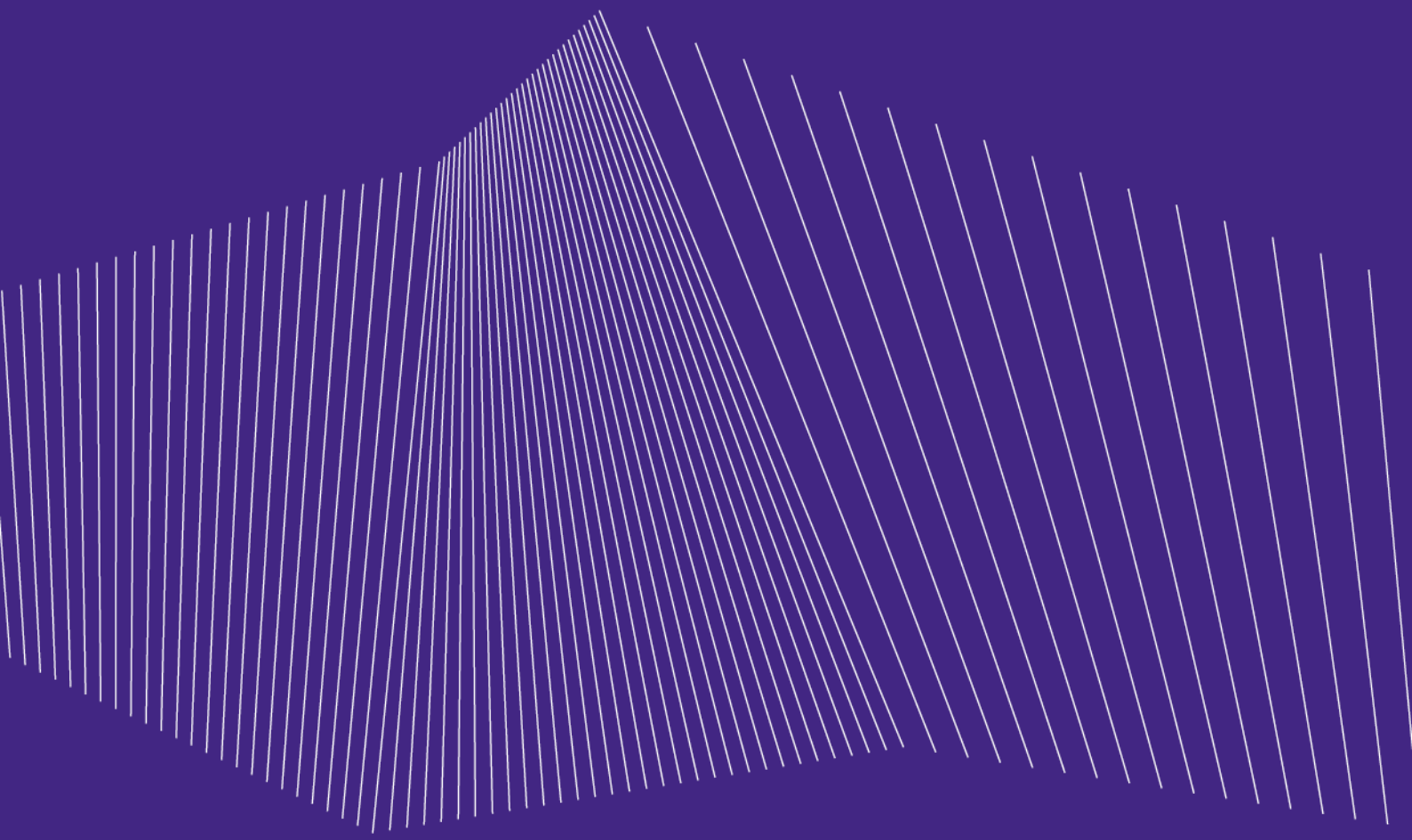
Renvoi	Document
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données dit RGPD).

Tableau 3 : Documents règlementaires

7.2 > Documents techniques

Renvoi	Document
[ETSI_TSP]	ETSI EN 319 401 v2.0.0 : Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI_TIMESTAMP]	ETSI EN 319 421 v1.1.1 : Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[RFC_3161]	IETF - Internet X.509 Public Key Infrastructure - Time-Stamp Protocol -08/2001
[PC AC IDEMIA Qualifiée]	Politique de certification - Autorité de certification AC Qualifiée IDEMIA
[PC AC IDEMIA NCP+]	Politique de certification - Autorité de certification AC NCP+ IDEMIA
[SEC_TSP]	Mesures de sécurité techniques et non techniques - Services de confiance IDEMIA

Tableau 4 : Documents techniques



IDEMIA

www.idemia.com