CERTIGNA by tessi

POLITIQUE D'HORODATAGE CERTIGNA TSA

Edité le :	01/09/2022
Version :	1.4
OID :	1.2.250.1.177.2.9.1
Auteurs :	J. Allemandou
Classification :	Publique

tessi

SOMMAIRE

1 INTRODUCTION

1.1 Présentation générale

CERTIGNA s'est dotée d'une Autorité d'horodatage (AH) nommée « Certigna TSA » pour délivrer des contremarques de temps.

La présente Politique d'horodatage (PH) expose les pratiques que l'AH applique et s'engage à respecter dans le cadre de la fourniture de son service d'horodatage. La Politique d'Horodatage identifie également les obligations et exigences portant sur les autres intervenants et les utilisateurs des contremarques de temps.

L'attention du lecteur est attirée sur le fait que la compréhension de la présente PH suppose qu'il soit familiarisé avec les notions liées à la technologie des Infrastructures de Gestion de Clés (IGC) et à l'horodatage.

La présente PH vise la conformité :

- au règlement européen eIDAS N°910/2014 pour le service d'horodatage qualifié ;
- à la PC Type « *Politique d'Horodatage Type* » du Référentiel Général de Sécurité (RGS) élaboré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ;
- à la politique nommée « Best Practices Policy for Time-Stamp (BTSP) » décrite dans les spécifications de l'ETSI EN 319 421 et identifiée par l'OID suivant : 0.4.0.2023.1.1 (*itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1))*.

1.2 Nom et identification du document

La présente PH peut être identifiée par le nom de l'AH « Certigna TSA » ainsi que par son OID : 1.2.250.1.177.2.9.1. Plusieurs Unités d'Horodatage (UH) sont mises en œuvre pour signer les contremarques de temps délivrées par l'AH. Ces UH utilisent des certificats de cachet d'horodatage émis par l'Autorité de Certification (AC) « Certigna Entity CA » et visant la conformité à l'ETSI EN 319 411-2. Les certificats utilisés sont identifiables par l'un des OID suivants :

- 1.2.250.1.177.2.6.1.6.1 : certifié ETSI EN 319411-2 niveau QCP-l-qscd
- 1.2.250.1.177.2.6.1.9.1 : certifié ETSI EN 319411-2 niveau QCP-l

1.2.1 Révision du document

Version	Date	Modifications apportées
1.0	08/06/2017	Création
1.1	12/02/2019	Précisions sur : - La conformité à la politique BTSP (cf. 1.1) ; - La protection des données personnelles (cf. 3.7.1) ; - La gestion des copies de secours des clés (cf. 5.1.8).
1.2	09/06/2020	Nouvelle charte graphique TESSI et précisions sur : - Conformité visée à la PH du RGS (cf. 1.1) ; - Ajout d'un OID de certificats utilisés par les UH (cf. 1.2) ; - Limite de responsabilité (cf. 3.8),

1.3	02/11/2020	Révision du document et précisions sur : - Normes ciblées par les certificats des UH (cf. 1.2) ; - Révocation des certificats d'UH en fin de vie de l'AH (cf. 4.8).
1.4	01/09/2022	Nouvelle charte graphique TESSI, révision et précisions sur les qualifications des HSM à utiliser.

1.3 Qu'est-ce que l'horodatage ?

L'horodatage permet d'attester qu'une donnée existe à un instant donné. Pour cela, on associe à une représentation sans équivoque de la donnée à horodater, un instant dans le temps. Par exemple, la représentation d'une donnée peut être sa valeur de hachage associée à un identifiant d'algorithme de hachage.

La garantie de cette association est fournie au moyen d'une structure signée appelée « contremarque de temps ». Cette contremarque de temps contient notamment :

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

Les utilisateurs finaux ont accès aux informations de validité des certificats d'horodatage (chaînes de certification, Listes des Certificats Révoqués (LCR), …) pour vérifier les contremarques de temps.

Les clés utilisées pour générer les contremarques de temps sont gérées par l'AH qui conserve la pleine et entière responsabilité pour satisfaire aux exigences définies dans cette PH. L'Autorité d'horodatage peut faire fonctionner plusieurs unités d'horodatage (UH). Chaque unité d'horodatage dispose de sa propre bi-clé.

1.4 La confiance en l'horodatage

La garantie apportée par l'AH s'appuie sur des éléments techniques et des règles de gestion qui sont présentées dans cette PH. Celle-ci présente aux utilisateurs les engagements que prend l'AH, notamment en matière de sécurité, et décrit de façon macroscopique les moyens mis en œuvre pour tenir ces engagements.

La PH présente le niveau de confiance atteint par le service d'horodatage. Elle traduit la reconnaissance formelle de l'importance accordée par l'AH à la sécurité du service.

Les exigences pour les services d'horodatage décrits dans cette PH incluent des exigences portant, à la fois sur la gestion de l'horodatage et sur le fonctionnement des unités d'horodatage qui publient les contremarques de temps.

L'AH a la responsabilité d'assurer que ces exigences sont remplies et peut sous-traiter à d'autres parties un sous-ensemble du service d'horodatage.

1.5 Entités intervenant dans l'IGC

1.5.1 Autorité d'horodatage

Un Prestataire de Services de Confiance (PSCO) fournissant des services d'horodatage au public est appelée un « Prestataire de Service d'Horodatage Electronique » (PSHE). La PSHE comporte une ou plusieurs Autorité d'horodatage qui a la responsabilité de fournir des services d'horodatage et est responsable des opérations d'une ou plusieurs TSU qui génèrent et signent des contremarques de temps au nom de l'AH.

L'AH assure tout ou partie de ces fonctions directement ou en les sous-traitant. Dans tous les cas, l'AH en garde la responsabilité. L'AH s'engage à respecter les obligations décrites dans la présente PH. Elle s'engage également à ce que les composants de l'AH, internes ou externes à l'AH, auxquels elles incombent les respectent aussi.

L'AH garantit la conformité des exigences et des procédures prescrites dans cette politique, même quand les fonctionnalités d'horodatage sont remplies par des sous-traitants.

L'AH garantit l'adhésion aux obligations complémentaires indiquées dans la contremarque de temps ou bien directement ou bien incorporée par référence.

L'Autorité d'horodatage fournie des services d'horodatage conformément à la présente PH et à la DPH associée.

L'AH remplie tous ses engagements tels que stipulés dans les Conditions Générales d'Utilisation.

1.5.2 Autorité de certification

L'AC a en charge la fourniture des prestations de gestion des certificats des Unités d'horodatage tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation, …) et s'appuie pour cela sur une infrastructure technique : une IGC. L'AC est responsable de la mise en application de la PC à l'ensemble de l'IGC qu'elle a mise en place.

Pour les certificats d'horodatage signés en son nom, l'AC assure les fonctions suivantes :

- Fonctions d'enregistrement et de renouvellement ;
- Fonction de génération des certificats ;
- Fonction de génération d'éléments secrets ;
- Fonction de publication des conditions générales, de la Politique de Certification, des certificats d'AC et des formulaires de demande de certificat ;
- Fonction de gestion des révocations ;
- Fonction d'information sur l'état des certificats via la liste des certificats révoqués (LCR) mise à jour à intervalles réguliers et selon un mode requête/réponse en temps réel (OCSP).

L'AC assure ces fonctions directement ou en les sous-traitant, tout ou partie. Dans tous les cas, l'AC en garde la responsabilité. L'AC s'engage à respecter les obligations décrites dans la Politique de Certification. Elle s'engage également à ce que les composants de l'IGC, internes ou externes à l'AC, auxquels elles incombent les respectent aussi.

1.5.3 Abonné

Personne morale ou personne physique ayant besoin de faire horodater des données par l'Autorité d'horodatage et qui a accepté les conditions d'utilisation de ce service.

Lorsque l'abonné est une organisation, il comprend plusieurs utilisateurs finaux ou un utilisateur final et certaines obligations s'appliquant à l'organisation s'appliquent également aux utilisateurs finaux. Dans tous les cas, l'organisation sera tenue responsable si les obligations ne sont pas correctement respectées par les utilisateurs finaux et, par conséquent, une telle organisation doit informer de manière appropriée ses utilisateurs finaux.

Lorsque l'abonné est un utilisateur final, l'utilisateur final est directement responsable si les obligations ne sont pas correctement respectées.

Il est recommandé que l'abonné, au moment de l'obtention d'une contremarque de temps, vérifie que le certificat de l'unité d'horodatage n'est pas révoqué.

1.5.4 Utilisateur

Entité (personne ou système) qui fait confiance à une contremarque de temps émise sous la PH. 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'unité d'horodatage est valide à l'instant de la vérification.
- Tenir compte des limitations sur l'utilisation de la contremarque de temps indiquées dans la présente Politique d'Horodatage et les Conditions Générales d'Utilisation.

1.6 Définitions et acronymes

1.6.1 Définitions

Les termes utiles à la bonne compréhension de la PH sont les suivants :

Abonné - Personne morale ou personne physique ayant besoin de faire horodater des données par l'Autorité d'horodatage et qui a accepté les conditions d'utilisation de ce service.

Autorités administratives (AA) - Ce terme générique désigne les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.

Autorité de Certification (AC) – Au sein d'un Prestataire de Service de Confiance (PSCO) une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCO, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ « issuer » du certificat).

Autorité d'horodatage (AH) - Autorité en charge du service d'horodatage en conformité avec la Politique d'horodatage et en s'appuyant sur une ou plusieurs unités d'horodatage.

Cachet électronique – Signature numérique effectuée par un serveur applicatif sur des données dans le but de pouvoir être utilisée, soit dans le cadre d'un service d'authentification de l'origine des données, soit dans le cadre d'un service de non-répudiation.

Certificat électronique - Fichier électronique attestant du lien entre une clé publique et l'identité de son propriétaire (personne physique ou service applicatif). Cette attestation prend la forme d'une signature électronique réalisée par un PSCO. Il est délivré par une AC. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Composante - Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptographie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

Contremarque de temps (CT) - Donnée signée électroniquement 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.460-6.

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 du service d'horodatage et en conformité avec la politique d'horodatage qu'elle s'est engagée à respecter.

Infrastructure de Gestion de Clés (IGC) - Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une AC, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, ...

Liste des Autorités révoquées (LAR) - Liste comprenant les numéros de série des certificats des autorités intermédiaires ayant fait l'objet d'une révocation, et signée par l'AC racine.

Liste des Certificats Révoqués (LCR) - Liste comprenant les numéros de série des certificats ayant fait l'objet d'une révocation, et signée par l'AC émettrice.

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.

Politique de certification (PC) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une 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 et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les Porteurs et les utilisateurs de certificats.

Politique d'horodatage (PH) – Ensemble de règles qui indique l'applicabilité d'une contremarque de temps à une communauté particulière et/ou une catégorie d'application avec des exigences de sécurité commune.

Produit de sécurité - Un dispositif logiciel ou matériel qui met en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information ou d'un système.

Responsable du certificat (RC) - Personne en charge et responsable du certificat électronique de service applicatif.

RSA - Algorithme à clés publiques du nom de ses inventeurs (Rivest, Shamir et Adleman).

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

Système de la TSA - Ensemble des unités d'horodatage et des composants d'administration et de supervision utilisés pour fournir le service d'horodatage.

Système d'Information (SI) - Tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.

Unité d'Horodatage (UH) - Ensemble de matériels et de logiciels 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.

Utilisateur de contremarque de temps - Entité (personne ou système) qui fait confiance à une contremarque de temps émise sous la Politique d'Horodatage.

Utilisateur final - Abonné ou utilisateur de contremarques de temps.

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

Nota - Dans la suite du document le terme « entité » est utilisé pour désigner une entreprise ou une administration. La dénomination « entreprise » recouvre les entreprises au sens le plus large, à savoir toutes personnes morales de droit privé : sociétés, associations ainsi que les artisans et travailleurs indépendants.

1.6.2 Acronymes

Les acronymes utiles à la bonne compréhension de ce document sont les suivants :

AA	Autorité Administrative
AC	Autorité de Certification
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
AH	Autorité d'Horodatage

ANSSI	Agence nationale de la sécurité des systèmes d'information
CGU	Conditions Générales d'Utilisation
CNIL	Commission Nationale de l'Informatique et des Libertés
CSR	Certificate Signature Request
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de Gestion de Clés (= PKI : Public Key Infrastructure)
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de Certification
PCA	Plan de Continuité d'Activité
PP	Profil de Protection
PKCS	Public Key Cryptographic Standards
PSCO	Prestataire de Services de Confiance
RSA	Rivest Shamir Adleman
SSI	Sécurité des Systèmes d'Information
UH	Unité d'Horodatage
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

2 GESTION DES RISQUES

Une appréciation des risques est réalisée par l'AH afin d'identifier, d'analyser et d'évaluer les risques liés au service d'horodatage, en prenant en compte les enjeux commerciaux et techniques.

L'AH prend en compte les résultats de l'appréciation des risques pour déterminer les mesures de traitement permettant d'assurer que le niveau de sécurité est adapté au niveau de risque.

L'AH détermine toutes les exigences de sécurité et procédures opérationnelle nécessaires pour implémenter les mesures de sécurité sélectionnées, comme documenté dans la Politique de sécurité de l'information et dans la déclaration des pratiques d'horodatage.

L'appréciation des risques relative au service d'horodatage est revue et révisée à minima une fois par an, à l'issue de quoi, l'appréciation est approuvée et le risque résiduel identifié est accepté.

3 POLITIQUE ET PRATIQUES

3.1 Politique d'horodatage

Pour cette politique, la date et le temps de chaque contremarque de temps sont synchronisés avec le temps UTC avec une précision d'une seconde.

La présente PH implique l'usage du format de contremarque de temps décrit au chapitre 5.5.2 et d'un protocole d'horodatage conforme à la RFC 3161.

3.2 Déclaration des pratiques d'horodatage

La déclaration des pratiques d'horodatage (DPH) expose les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la PH, en particulier les processus que l'Autorité d'horodatage emploie pour la création des contremarques de temps et le maintien de l'exactitude de ses horloges.

La DPH est une description détaillée des pratiques opérationnelles de l'Autorité d'horodatage mise en œuvre pour la délivrance des contremarques de temps et la gestion du service d'horodatage.

La DPH définit comment l'Autorité d'horodatage se conforme aux exigences physiques, environnementales, procédurales, organisationnelles et techniques identifiées dans cette politique d'horodatage.

Cette PH est ainsi un document moins spécifique que la DPH correspondante. La PH est définie indépendamment des détails particuliers de l'environnement spécifique d'exploitation de l'Autorité d'horodatage, tandis que la DPH est façonnée à la structure organisationnelle, aux procédures d'exploitation, aux équipements et à l'environnement de travail de l'Autorité d'horodatage.

3.3 Conditions générales d'utilisation

Compte tenu de la complexité de lecture d'une PH et d'une DPH pour des utilisateurs non-spécialistes du domaine, l'AH fournit également des conditions générales d'utilisation (CGU) correspondant aux "TSA Disclosure Statement".

Les CGU ne sont pas destinées à remplacer cette PH ou la DPH mais sont destinées aux abonnés et aux utilisateurs des contremarques de temps non-techniciens afin qu'ils puissent facilement comprendre l'information essentielle dont ils doivent avoir connaissance.

Les CGU intègrent à minima les informations suivantes :
- La politique d'horodatage applicable ;
- Les limites sur l'utilisation du service ;
- Les obligations de l'abonné ;
- Les obligations des utilisateurs des contremarques de temps ;
- La période de temps durant laquelle les journaux d'évènement sont conservés ;
- Les limites de responsabilité ;
- Le système légal applicable ;

- Les procédures pour le règlement des plaintes et des conflits ;
- Le schéma d'évaluation de la conformité de cette politique d'horodatage ;
- Les coordonnées du point de contact de l'AH ;
- 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 ;
- Les dispositions permettant de valider la chaîne de certificat liée aux certificats des UH ;
- Le nom du pays dans lequel l'Autorité d'horodatage est établie et l'identifiant de l'Autorité d'horodatage (tel que figurant dans les certificats des unités d'horodatage).

Les CGVU sont accessibles aux abonnés en annexe de leur contrat et aux utilisateurs via le site de CERTIGNA à l'adresse suivante : https://www.certigna.com/politique-horodatage

3.4 Politique de sécurité de l'information

L'AH dispose d'une Politique de Sécurité de l'Information (PSI) qui est documentée, implémentée, maintenue, révisée annuellement et approuvée par la Direction.

Cette politique de sécurité de l'information expose l'approche adoptée par l'organisation pour le management de la sécurité de l'information ainsi que les objectifs de sécurité qui ont été déterminés. Elle est communiquée à l'ensemble du personnel et des intervenants impactés.

3.5 Gestion de la PH et de la DPH

3.5.1 Entité gérant la PH et la DPH

L'AH dispose d'un Comité de Sécurité présidé par un Officier de sécurité.

Ce comité est responsable de l'élaboration, du suivi, de la modification et de la validation de la présente PH et de la DPH associée. Il statue sur toute modification nécessaire à apporter à ces documents à minima une fois par an.

3.5.2 Point de contact

CERTIGNA
20 allée de la Râperie
Zone de la plaine
59650 Villeneuve d'Ascq
France

Contact mail : contact@certigna.fr
Téléphone : 0 806 115 115 (Service gratuit)

3.5.3 Entité déterminant la conformité de la DPH avec la PH

Le Comité de Sécurité s'assure de la conformité de la DPH par rapport à la PH. Il peut le cas échéant se faire assister par des experts externes pour s'assurer de cette conformité.

3.5.4 Procédures d'approbation de la conformité de la DPH

La DPH traduit en termes technique, organisationnel et procédural les exigences de la PH en s'appuyant sur la « Politique de sécurité de l'information » de l'entreprise. Le Comité de Sécurité s'assure que les moyens mis en œuvre et décrits dans la DPH répondent à ces exigences selon le processus d'approbation mis en place. Un contrôle de conformité de la DPH par rapport à la PH est effectué annuellement lors des audits internes et externes réalisés en vue de la qualification de l'AH.

Toute demande de mise à jour de la DPH suit également ce processus.

Toute nouvelle version approuvée de la DPH est publiée sans délai.

3.6 Informations auprès des tiers

3.6.1 Entités chargées de la mise à disposition des informations

CERTIGNA met à disposition des utilisateurs et des applications utilisatrices des contremarques de temps signées par les certificats des UH, des informations sur l'état de révocation des certificats des UH utilisés par l'AH. Ces informations sont publiées au travers de plusieurs serveurs :

- Serveurs Web :
    - http://crl.certigna.fr/entityca.crl
    - http://crl.dhimyotis.com/entityca.crl
- Serveurs OCSP :
    - http://entityca.ocsp.certigna.fr
    - http://entityca.ocsp.dhimyotis.com

3.6.2 Informations devant être publiées

L'AH et l'AC publient à destination des abonnés et des utilisateurs :

- Cette politique d'horodatage ;
- La Déclaration des Pratiques d'Horodatage sur demande expresse auprès du contact de CERTIGNA ;
- La politique de certification de l'AC émettant les certificats des UH et la Déclaration des Pratiques de Certification associée ;
- Les Conditions Générales d'Utilisation liées au service d'horodatage ;
- Les Conditions Générales d'Utilisation liées au service de certification ;
- Les certificats des UH et les certificats d'AC associés (AC racine et intermédiaires) ;
- La liste des certificats révoqués (LAR / LCR) ;

Remarque : compte tenu de la complexité de lecture d'une PH pour les abonnés ou les utilisateurs non spécialistes du domaine, l'AH publie des CGU que le futur abonné est dans l'obligation de lire et d'accepter préalablement à la délivrance de contremarques de temps.

3.6.3 Publication de la documentation

3.6.3.1 Publication de la PH, des Conditions Générales d'Utilisation et des formulaires

La PH, les Conditions Générales d'Utilisation et les différents formulaires nécessaires pour la gestion des contremarques de temps sont publiés sous forme électronique à l'adresse https://www.certigna.com.

3.6.3.2 Publication de la DPH

L'AH publie, à destination des abonnés et utilisateurs de contremarques de temps, et sur leur demande, sa DPH pour rendre possible l'évaluation de la conformité avec sa politique d'horodatage. Les détails relatifs à ses pratiques ne sont toutefois pas rendus publics.

3.6.3.3 Publication des certificats d'AC

Les abonnés et les utilisateurs des contremarques de temps peuvent accéder aux certificats d'AC qui ont signé les certificats des UH, à l'adresse suivante : https://www.certigna.com.

3.6.4 Contrôle d'accès aux informations publiées

L'accès aux informations publiées à destination des utilisateurs est libre.

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'AH et de l'IGC, au travers d'un contrôle d'accès fort, basé sur une authentification à deux facteurs.

3.7 Conformité avec les exigences légales

L'AH garantit la conformité avec les exigences légales.

3.7.1 Protection des données personnelles

3.7.1.1 Politique de protection des données personnelles

CERTIGNA conserve les données à caractère personnel pendant une durée de trois ans à compter de la fin des relations commerciales avec le client et 3 ans à compter du dernier contact émanant avec le prospect. Le délai commence à partir de la dernière connexion au compte client ou du dernier envoi d'un courriel au service client, ou d'un clic sur un lien hypertexte d'un courriel adressé par CERTIGNA, d'une réponse positive à un courriel demandant si le client souhaite continuer à recevoir de la prospection commerciale à l'échéance du délai de trois ans.

Conformément à la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée et au règlement européen « 2016/679/ UE 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, vous bénéficiez d'un droit d'accès,

d'opposition, de rectification, de suppression et de portabilité de vos données personnelles. Vous pouvez exercer votre droit en vous adressant par mail à : privacy@certigna.com, ou par courrier à l'adresse suivante :

CERTIGNA, Service du DPO,
20 Allée de Râperie, 59 650 Villeneuve d'Ascq, France.

3.7.1.2 Informations à caractère personnel

Les informations considérées comme personnelles sont les dossiers de demandes de contremarques de temps des abonnés.

3.7.1.3 Notification et consentement d'utilisation des données personnelles

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les abonnés à l'AH ne doivent pas être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable de l'abonné, décision judiciaire ou autre exigence légale.

3.7.1.4 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

La divulgation des informations confidentielles n'est effectuée qu'aux autorités judiciaires ou administratives habilitées officiellement et exclusivement sur leur demande expresse en conformité avec la législation française.

3.7.2 Droits sur la propriété intellectuelle et industrielle

La marque « CERTIGNA » est protégée par le code de la propriété industrielle. L'utilisation de cette marque par l'entité est autorisée uniquement dans le cadre du contrat d'abonnement.

3.8 Limite de responsabilité

L'AH est soumise à une obligation générale de moyens. L'AH ne pourra voir sa responsabilité engagée à l'égard de l'Abonné ou de l'utilisateur que pour les dommages directs qui pourraient lui être imputés au titre des prestations qui lui sont confiées dans le cadre de la présente PH et des CGU associées.

La responsabilité de l'AH ne pourra pas être recherchée pour tout préjudice indirect, tel que notamment, la perte de chiffre d'affaires, la perte de bénéfice, la perte de commandes, la perte de données, la perte d'une chance, le trouble à l'image ou tout autre dommage spécial ou évènements en dehors de son contrôle ou de tout fait ne lui étant pas imputable.

L'AH n'est responsable que des tâches expressément mises à sa charge. L'AH ne saurait être tenue responsable de quelque manière que ce soit de l'utilisation faite par l'abonné ou l'utilisateur de la contremarque de temps, ni du contenu des documents et des données qui lui sont remis par l'Abonné ou le demandeur.

En aucun cas, la responsabilité de l'AH ne saurait être recherchée pour :

- Faute, négligence, omission ou défaillance de l'AH, qui constituerait la cause exclusive de survenance du dommage,
- Dysfonctionnement ou d'indisponibilité d'un bien matériel ou immatériel dans le cas où celui-ci a été fourni par le Porteur,
- Retard dans la fourniture des données à traiter dû à l'Abonné ;
- Perte de la qualification d'un tiers prestataire qui est indépendant de la volonté de CERTIGNA (Ex : le fournisseur du support cryptographique des certificats d'UH).

De convention expresse entre l'AH et l'Abonné, la responsabilité de l'AH est limitée, tous préjudices confondus, à la somme de deux (2) fois le montant réglé au titre de la commande de contremarques de temps au travers d'un pack ou d'un mois d'abonnement.

L'AH ne pourra être tenue responsable d'une utilisation non autorisée ou non conforme des contremarques de temps délivrées par son service d'horodatage.

L'AH ne sera en aucun cas responsable des éventuels dommages ayant leur origine dans l'utilisation d'une contremarque de temps délivrée par l'AH.

L'AH ne pourra pas être impliquée pour des retards ou pertes que pourraient subir les données transmises sur lesquelles est demandé une contremarque de temps par le service applicatif.

L'AH ne saurait être tenue responsable de problèmes relevant de la force majeure, au sens du Code civil. Si un cas de force majeure a une durée supérieure à quinze jours, l'Abonné sera autorisé à mettre un terme au contrat et il n'y aura pas de préjudice.

Les données transmises dans une requête d'horodatage et la vérification de leur valeur dans la réponse associée restent de la responsabilité des abonnés.

3.9 Règlement de conflits

La validité de la présente PH et toute autre question ou litiges relatifs à son interprétation, à son exécution ou à sa résiliation seront régis par le droit français.

L'AH et l'Abonné s'engagent à consacrer leurs meilleurs efforts à la résolution amiable de toutes les questions ou de tous les litiges qui pourraient les diviser, préalablement à la saisie de la juridiction ci-après désignée.

L'AC et l'Abonné conviennent, pour le cas où un accord amiable serait impossible à arrêter, que les juridictions de Lille auront compétences exclusives pour connaître de tout différend résultant de la validité, de l'interprétation, de l'exécution ou de la résiliation des présentes, et plus généralement de tout litige procédant des présentes qui pourrait les diviser, nonobstant pluralités des défendeurs ou appel en garantie.

4 MESURES DE SECURITE NON TECHNIQUES

RAPPEL - L'AH a mené une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'AH et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Sa DPH a été élaborée en fonction de cette analyse.

4.1 Mesures de sécurité physique

4.1.1 Situation géographique et construction des sites

Ces informations sont précisées dans la DPH.

4.1.2 Accès physique

Un contrôle strict d'accès physique aux composants de l'AH est effectué, avec journalisation des accès et vidéo-surveillance : le périmètre de sécurité défini autour des systèmes d'horodatage 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'AH. En outre, toute personne (prestataire externe, etc.) entrant dans ces zones physiquement sécurisées ne peut pas être laissée, pendant une période de temps significative, sans la surveillance d'une personne autorisée.

4.1.3 Alimentation électrique et climatisation

Des mesures concernant la fourniture d'énergie électrique et de climatisation sont prises pour répondre aux engagements de l'AH décrits dans la présente PH sur la garantie du niveau de disponibilité de ses fonctions.

4.1.4 Vulnérabilité aux dégâts des eaux

Des mesures concernant la protection contre les dégâts des eaux sont prises pour répondre aux engagements de l'AH décrits dans la présente PH sur la garantie du niveau de disponibilité de ses fonctions.

4.1.5 Prévention et protection incendie

Des mesures concernant la prévention et la protection contre les incendies sont prises pour répondre aux engagements de l'AH décrits dans cette PH sur la garantie du niveau de disponibilité de ses fonctions.

4.1.6 Conservation des supports

Les informations et leurs actifs supports intervenant dans les services d'horodatage sont identifiés, inventoriés et leurs besoins de sécurité définis en disponibilité, intégrité et

confidentialité conformément à la politique de classification et de manipulation de l'information.

Des mesures sont mises en place pour éviter la compromission et le vol de ces informations. Les supports correspondant à ces informations sont gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils sont manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés, que ce soit durant leur stockage ou leur éventuel transport.

Des procédures de gestion protègent ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

4.1.7 Mise hors service des supports

Les mesures prises pour la mise hors service des supports d'informations sont en conformité avec le niveau de confidentialité des informations correspondantes.

4.1.8 Sauvegardes hors site

Des sauvegardes externalisées sont mises en œuvre et organisées de façon à assurer une reprise des fonctions de l'AH après incident le plus rapidement possible, et conformément aux engagements de la présente PH notamment en matière de disponibilité et de protection en confidentialité et en intégrité des informations sauvegardées.

4.2 Mesures de sécurité procédurales

4.2.1 Rôles de confiance

Chaque composante du service d'horodatage distingue 7 rôles fonctionnels de confiance :

- Responsable de sécurité : Le responsable de sécurité est chargé de la mise en œuvre et du contrôle de la politique de sécurité de l'AH. Il gère les contrôles d'accès physiques aux équipements des systèmes des composantes. Il est habilité à prendre connaissance des archives et des journaux d'évènements. Il est responsable des opérations de génération et de révocation des certificats qui sont implémentées par les Officiers d'enregistrement.
- Responsable d'application : Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques d'horodatage de l'AH au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
- Administrateur système : Il est chargé de la mise en route, de la configuration, de l'installation et de la maintenance technique des systèmes de l'AH pour la gestion de l'horodatage. Il assure l'administration technique des systèmes et des réseaux du service.
- Opérateur : Un opérateur assure l'exploitation au quotidien des services d'horodatage.
- Contrôleur : Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par l'AH par rapport aux politiques, aux déclarations des pratiques de certification et d'horodatage de CERTIGNA et aux politiques de sécurité applicables.

- Officier d'enregistrement : Il est en charge de l'approbation des actions de génération et de révocation des certificats des UH.
- Porteur de part de secret : Il a la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui lui sont confiées.

Les différents rôles sont définis dans la description des postes propres à chaque entité opérant les services de l'AH sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles déterminent la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilisation des employés.

Des mesures sont mises en place pour empêcher que des équipements, des informations, des supports et des logiciels ayant trait aux services de l'AC soient sortis du site sans autorisation.

4.2.2 Nombre de personnes requises par tâche

Pour des raisons de disponibilité, chaque tâche doit pouvoir être effectuée par au moins deux personnes. Au minimum, chacune des tâches suivantes est affectée sur deux personnes distinctes :

- Administrateur système ;
- Opérateur.

Pour certaines tâches sensibles (par exemple la cérémonie des clés), plusieurs personnes sont requises pour des raisons de sécurité et de « dual control ».

4.2.3 Identification et authentification pour chaque rôle

Chaque attribution de rôle à un membre du personnel de l'AH est acceptée formellement. L'AH fait vérifier l'identité et les autorisations de tout membre de son personnel avant l'attribution des privilèges relatifs à ses fonctions. L'attribution d'un rôle à un membre du personnel de l'AH suit une procédure stricte avec signature de procès-verbaux pour l'attribution de tous les éléments nécessaires à l'exécution de ce rôle dans l'AH (clés, codes d'accès, clés cryptographiques, etc.).

4.2.4 Rôle exigeant une séparation des attributions

Concernant les rôles de confiance, les cumuls suivants sont interdits au sein de l'AH :

- Responsable de sécurité et administrateur système/opérateur ;
- Contrôleur et tout autre rôle ;
- Administrateur système et opérateur.

4.3 Mesures de sécurité vis-à-vis du personnel

4.3.1 Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'AH sont soumis à une clause de confidentialité vis-à-vis de l'employeur. L'adéquation des compétences

professionnelles des personnels intervenant dans l'AH est vérifiée en cohérence avec les attributions.

Le personnel d'encadrement, le responsable sécurité, les administrateurs système, disposent des expertises nécessaires à l'exécution de leur rôle respectif et sont familiers aux procédures de sécurité appliquées à l'exploitation de l'AH.

L'AC informe tout employer intervenant dans des rôles de confiance de l'AH de ses responsabilités relatives aux services de l'AH et des procédures liées à la sécurité du système et au contrôle du personnel.

4.3.2 Procédures de vérification des antécédents

L'AH s'assure que tout employé intervenant sur l'AH n'a pas subi de condamnation de justice en contradiction avec ses attributions. Les employés fournissent une copie du bulletin n°3 de leur casier judiciaire préalablement à leur affectation. Cette vérification est renouvelée périodiquement. De plus, l'AH s'assure que les personnels ne souffrent pas de conflits d'intérêts préjudiciables à l'impartialité de leurs tâches.

L'AH peut décider en cas de refus du personnel de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions du personnel, de lui retirer ces attributions.

4.3.3 Exigences en matière de formation initiale

Une formation initiale aux logiciels, matériels et procédures internes de fonctionnement et de sécurité est dispensée aux employés, formation en adéquation avec le rôle que l'AH leur attribue. Une sensibilisation sur les implications des opérations dont ils ont la responsabilité est également opérée.

Le personnel de gestion employé possède :
- La connaissance de la technologie de l'horodatage ;
- La connaissance de la technologie de la signature numérique ;
- La connaissance des mécanismes pour le calibrage ou la synchronisation des horloges des UH avec le temps UTC.

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 est requise.

4.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation.

4.3.5 Sanctions en cas d'actions non autorisées

Tout membre du personnel de l'AH agissant en contradiction avec les politiques et les procédures établies et les processus et procédures internes de l'AH, soit par négligence, soit

par malveillance, verra ses privilèges révoqués et fera l'objet de sanctions administratives, voire de poursuites judiciaires.

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

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'AH doit également respecter les exigences du chapitre. Ceci est traduit en clauses adéquates dans les contrats avec ces prestataires. Le cas échéant, si le niveau d'intervention le requiert, il peut être demandé au prestataire de signer la charte interne de sécurité et/ou de fournir des éléments de vérification d'antécédents.

4.3.7 Documentation fournie au personnel

Chaque membre du personnel dispose de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. En particulier, l'AH lui remet les politiques de sécurité l'impactant. Les opérateurs disposent notamment des manuels d'opérateurs correspondant aux composantes sur lesquelles ils interviennent.

4.4 Organisation interne

L'AH est une personne morale conformément à la législation nationale.

L'AH dispose d'un système de management de la qualité et de la sécurité de l'information adapté aux services d'horodatage qu'elle fournit. Elle emploie suffisamment de personnel ayant l'éducation, la formation, les connaissances techniques et l'expérience nécessaires en ce qui concerne le type, la portée et le volume de travail nécessaires pour fournir des services d'horodatage.

L'organisation de l'AH est fiable. Les pratiques de service de confiance que l'AH opère ne sont pas discriminatoires.

L'AH rend ses services accessibles à tous les utilisateurs dont les activités relèvent de leur domaine d'activité déclaré et qui acceptent de respecter leurs obligations, conformément aux Conditions Générales d'Utilisation de l'AH.

L'AH maintient des ressources financières suffisantes et dispose d'une assurance responsabilité appropriée, conformément à la législation nationale, pour couvrir les coûts liés à ses opérations et/ou de ses activités.

L'AH a la stabilité financière et les ressources nécessaires pour fonctionner conformément à cette politique.

L'AH dispose des politiques et des procédures pour la résolution des plaintes et des litiges reçus des clients ou d'autres parties prenantes sur la fourniture des services ou toute autre question connexe.

L'AH dispose d'un accord documenté et d'une relation contractuelle en place lorsque la fourniture des services implique de la sous-traitance, de l'externalisation ou d'autres arrangements de tiers.

4.5 Procédures de constitution des données d'audit

Les événements pertinents intervenant dans la gestion et l'exploitation de l'AH sont enregistrés sous forme manuscrite ou sous forme électronique (par saisie ou par génération automatique) et ce, à des fins d'audit.

4.5.1 Type d'événements à enregistrer

Les systèmes d'exploitation des serveurs de l'AH journalisent les événements suivants, automatiquement dès leur démarrage et sous forme électronique (liste non exhaustive) :

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes ;
- Démarrage et arrêt des systèmes informatiques et des applications ;
- Evénements liés à la journalisation : actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres événements sont aussi recueillis. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques :

- Les accès physiques (enregistrés électroniquement) ;
- Les accès logiques aux systèmes ;
- Les actions de maintenance et de changement de la configuration des systèmes enregistrés manuellement ;
- Les changements apportés au personnel ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs).

Des événements spécifiques aux différentes fonctions de l'AH sont également journalisés :

- Evénements liés au fonctionnement des services d'horodatage ;
- Evénements liés aux cycles de vie des clés des UH et aux certificats d'AC associés ou aux données d'activation (génération, sauvegarde et récupération, révocation, destruction, destruction des supports, ...) ;
- Evènements liés à la synchronisation des horloges au temps UTC, incluant les informations concernant le recalibrage ou la synchronisation normale des horloges utilisées pour l'horodatage et les détections de perte de synchronisation.

Les opérations de journalisation sont effectuées au cours du processus. En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'événement. Les évènements et données spécifiques à journaliser sont documentés par l'AH.

4.5.2 Période de conservation des journaux d'événements

Le délai de conservation des journaux d'événements sur site est de 1 mois. L'archivage des journaux d'événements est effectué au plus tard 1 mois après leur génération.

4.5.3 Protection des journaux d'événements

Seuls les membres dédiés de l'AH sont autorisés à traiter ces fichiers.

Les systèmes générant les journaux d'événements (exceptés les systèmes de contrôle d'accès physique) sont synchronisés sur une source fiable de temps UTC.

4.5.4 Procédure de sauvegarde des journaux d'événements

Des mesures de sécurité sont mises en place par chaque entité opérant une composante de l'AH afin de garantir l'intégrité et la disponibilité des journaux d'événements pour la composante considérée, conformément aux exigences de la présente PH. Une sauvegarde est effectuée à fréquence élevée afin d'assurer la disponibilité de ces informations.

4.5.5 Evaluation des vulnérabilités

Les journaux d'événements sont contrôlés une fois par jour ouvré pour identifier des anomalies liées à des tentatives en échec (accès ou opération).

Les journaux sont analysés dans leur totalité à la fréquence d'au moins 1 fois toute les 2 semaines et dès la détection d'une anomalie. Un résumé d'analyse est produit à cette occasion.

Un rapprochement entre les différents journaux d'événements de fonctions qui interagissent entre-elles est effectué à la fréquence d'au moins 1 fois par mois et ce, afin de vérifier la concordance entre événements dépendants et contribuer ainsi à révéler toute anomalie. Le contrôleur se fait assister si besoin par une personne disposant des compétences liées aux différents environnements utilisés.

4.6 Archivage des données

4.6.1 Types de données à archiver

L'AH archive :
- Les journaux d'événement des différentes composantes de l'AH ;
- La PH ;
- La DPH ;
- Les certificats émis pour les UH et les AC associées ;
- Les LCR émises pour les UH et les AC associées ;

4.6.2 Période de conservation des archives

4.6.2.1 Certificats, LCR / LAR et réponses OCSP émis par l'AC

Les certificats de clés des TSU et d'AC, ainsi que les LCR / LAR produites, sont archivés pendant au moins sept ans après leur expiration.

Les réponses OCSP produites sont archivées pendant au moins deux ans après leur expiration.

4.6.2.2 Journaux d'événements

Les journaux d'événements traités au chapitre 4.5.1 sont archivés pendant au moins sept ans après leur génération.

4.6.3 Protection des archives

Pendant tout le temps de leur conservation, les archives sont protégées en intégrité. Elles peuvent être relues et exploitées par les membres dédiés de l'AH. L'accès en écriture à ces fichiers est protégé (gestion des droits). L'accès en lecture à ces journaux n'est possible qu'à partir d'une machine identifiée et autorisée des réseaux internes.

4.6.4 Procédure de sauvegarde des archives

Le procédé de « réplication » (automatique ou manuel en cas de reprise) garantit l'existence d'une copie de secours de l'ensemble des archives.

4.6.5 Système de collecte des archives

L'archivage est réalisé sur des serveurs d'archivage qui assurent la disponibilité, l'intégrité et la confidentialité des archives.

4.6.6 Procédures de récupération et de vérification des archives

Les archives peuvent être récupérées uniquement par les membres dédiés de l'AH autorisés à traiter ces fichiers dans un délai maximal de deux jours ouvrés.

Les données concernant les abonnés peuvent être récupérées à leur demande.

4.7 Gestion des incidents et reprise après sinistre

4.7.1 Procédures de remontée et de traitement des incidents

Les procédures de remontée et de traitement d'incidents sont employées de telle sorte que les dommages causés par les incidents de sécurité et les dysfonctionnements soient minimisés.

L'AH répond à toute vulnérabilité critique qui n'a pas été précédemment adressée dans les heures qui suivent sa découverte. Si cela est proportionné compte tenu de l'impact, l'AH créera et mettra en œuvre un plan pour atténuer la vulnérabilité ou l'AH documentera les raisons pour lesquelles la vulnérabilité ne sera pas traitée.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'événement déclencheur est la constatation

de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AH.

L'AH informera les parties appropriées conformément aux règles réglementaires applicables en cas de violation de la sécurité ou de la perte d'intégrité qui a un impact important sur le service de confiance fourni et sur les données personnelles qui y sont maintenues dans les 24 heures qui suivent la violation.

Lorsque le manquement à la sécurité ou à la perte d'intégrité est susceptible de nuire à une personne physique ou morale à qui le service de confiance a été fourni, l'AH informe également la personne physique ou morale de la violation de la sécurité ou de la perte d'intégrité sans délai injustifié.

4.7.2 Compromission de l'AH

Dans le cas d'un incident majeur qui affecte la sécurité des services d'horodatage, incluant la compromission (réelle ou suspectée) de la clé privée de signature d'une unité d'horodatage ou la perte détectée de calibrage qui pourrait affecter des contremarques de temps émises, l'AH a défini et maintient un plan de continuité d'activité.

L'AH prendra les mesures nécessaires pour que les contremarques de temps de cette unité ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.

Chaque fois que cela sera possible, l'AH mettra à la disposition de tous ses abonnés et des utilisateurs de contremarques de temps toute information pouvant être utilisée pour identifier les contremarques de temps qui pourraient avoir été affectées, à moins que cela ne contrevienne à la vie privée des abonnés ou à la sécurité des services d'horodatage.

Le contact identifié sur le site de l'ANSSI (https://www.ssi.gouv.fr) sera immédiatement informé.

4.7.3 Capacité de continuité d'activité suite à un sinistre

L'AH dispose des moyens nécessaires permettant d'assurer la continuité des services d'horodatage en conformité avec les exigences de cette PH.

L'AC s'appuie sur la redondance de ses systèmes d'informations sur plusieurs sites et sur ses plans de continuité d'activité pour assurer la continuité des services.

4.8 Fin de vie de l'IGC

Une ou plusieurs composantes de l'AH peuvent être amenées à cesser leur activité ou à la transférer à une autre entité. Le transfert d'activité est défini comme :

- La fin d'activité d'une composante de l'AH ne comportant pas d'incidence sur la validité des certificats d'UH et des contremarques de temps émis antérieurement au transfert ;
- La reprise de cette activité organisée par l'AH en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'AH comportant une incidence sur la validité des certificats d'UH et contremarque de temps émis antérieurement à la cessation concernée.

Afin d'assurer un niveau de confiance constant pendant et après de tels événements, l'AH prend les mesures suivantes :

- L'AH rendra disponible à tous ses abonnés et aux utilisateurs de contremarques de temps l'information concernant son transfert ou sa cessation 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 disponible aux utilisateurs de contremarques de temps pendant une période raisonnable ses clés publiques ainsi que ses certificats ;
- L'AH révoquera les certificats des UH ;
- L'AH détruira les clés privées des UH et leurs copies de telle façon qu'elles ne puissent pas être recouvrées.
- L'AH indiquera dans sa PH les dispositions prises pour la fin du service incluant :
  - Un avis aux abonnés et aux utilisateurs de contremarques de temps
  - Un transfert des obligations de l'AH à d'autres organismes.
- Elle effectue une information auprès des autorités administratives. En particulier le contact de l'ANSSI est averti (https://www.ssi.gouv.fr). L'AC l'informera notamment de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus de transfert ou de cessation d'activité.
- L'AH prendra 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.

Si l'AH est en faillite, c'est au tribunal de commerce de décider de la suite à donner aux activités de l'entreprise. Néanmoins, le cas échéant, l'AH s'engage à accompagner le tribunal de commerce dans les conditions suivantes : avant une faillite, il y a une période préalable, générée la plupart de temps, soit par plusieurs procédures d'alerte du commissaire aux comptes, soit par un redressement judiciaire ; pendant cette période, l'AC s'engage à préparer pour le tribunal de commerce, le cas échéant, une proposition de transfert des certificats des UH vers une autre autorité disposant d'une certification d'un niveau au moins égal au sien.

5 MESURES DE SECURITE TECHNIQUES

5.1 Gestion des clés du UH

5.1.1 Génération des bi-clés des UH

L'AH garantit que toutes les clés cryptographiques des UH sont produites dans des circonstances contrôlées et décrites par la PC de l'AC.

La génération des clés de signature des UH :
- est effectuée dans un environnement sécurisé physiquement par du personnel de confiance et à minima en dual control ;
- est effectuée dans un module cryptographique répondant aux exigences du chapitre 5.3 ci-dessous.

Les clés des UH peuvent être stockées sur plusieurs systèmes pour des besoins de disponibilité. Dans ce cas, leurs certificats de clés publiques sont identiques.

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

5.1.2 Algorithmes obligatoires

L'AH, dans la limite des algorithmes qu'elle reconnaît :
- Supporte des valeurs de hachage générées par des clients et employant les algorithmes de hachage conformes aux exigences de l'ANSSI et des spécifications techniques de l'ETSI. L'AH supporte à minima les algorithmes suivants : SHA256, SHA384, SHA512.
- Génère des contremarques de temps signées selon les algorithmes et les longueurs de clé conformes aux exigences de l'ANSSI et des spécifications techniques de l'ETSI. Les bi-clés des UH ont les caractéristiques suivantes : RSA 2048 bits / Algorithme de hachage SHA-256 (256 bits).

5.1.3 Protection des clés privées des UH

L'AH garantit que les clés privées des UH restent confidentielles et conservent leur intégrité. Les clés de signature des UH sont gardées et utilisées à l'intérieur d'un module cryptographique répondant aux exigences du chapitre 5.3 ci-dessous.

5.1.4 Certificats des UH

L'AH garantit l'intégrité et l'authenticité des clés (publiques) de vérification de signature :
- Les clés de vérification de signature de l'UH (publiques) sont mises à la disposition des parties prenantes dans un certificat de clé publique.
- L'UH ne délivre pas de contremarques de temps avant que son certificat de vérification de signature (clé publique) ne soit chargé dans l'UH ou son module cryptographique.
- Lors de l'obtention d'un certificat de vérification de signature (clé publique), l'AH vérifie que ce certificat a été correctement signé (y compris la vérification de la chaîne de certificats à une autorité de certification approuvée).

La durée de validité des certificats des unités d'horodatage est fixée à 3 ans. Cette durée ne doit pas être plus longue que :

- La durée de vie cryptographique de la clé privée associée ;
- Fin de validité du certificat d'AC qui l'a émis.

5.1.5 Durée d'utilisation des clés privées des UH

La durée d'utilisation d'une clé privée d'UH est limitée à 1 an. La durée d'utilisation d'une clé est réduite afin que la validité des contremarques de temps générées avec cette clé puisse être effectuée durant à minima 2 ans.

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 via des procédures mises en place pour assurer qu'une nouvelle bi-clé est mise en place quand la fin de la période d'utilisation d'une clé privée de l'UH a été atteinte.

5.1.6 Destruction des clés privées des UH

L'AH assure la destruction de la clé privée et de ses copies lorsque la fin de la période d'utilisation de cette clé privée a été atteinte.

5.1.7 Archivage des clés privées des UH

Les clés privées des UH ne sont en aucun cas archivées.

5.1.8 Copies de secours des clés privées des UH

Chaque clé privée d'UH dispose d'une copie de secours positionnée dans un autre module cryptographique conforme aux exigences du chapitre 5.3 ci-dessous. Leur export hors du module cryptographique si nécessaire est sous forme chiffrée et avec un mécanisme de contrôle d'intégrité.

Le chiffrement correspondant offre un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, s'appuie sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé.

La copie de secours n'est pas utilisée pour la délivrance de jeton d'horodatage afin que seule la clé privée initiale soit active.

Toutes les clés privées des UH sont manipulées par personnel dans des rôles de confiance en « dual control » et depuis un environnement sécurisé physiquement. Ce personnel autorisé à mettre en œuvre la copie de secours des clés est limité à le faire conformément aux pratiques de l'AH.

5.2 Profils des certificats et LCR des UH

Cf. chapitre 7 de la politique de certification de Certigna Entity CA.

5.3 Gestion du module cryptographique des UH

5.3.1 Gestion du cycle de vie du module cryptographique des UH

L'AH s'assure que :

- Le module cryptographique de signature des contremarques de temps n'est pas altéré pendant l'expédition et n'est pas falsifié quand et pendant qu'il est stocké.
- L'installation, l'activation et la duplication des clés de signature de l'UH dans le module cryptographique sont effectuées uniquement par dans personnel dans des rôles de confiance en utilisant au moins un double contrôle dans un environnement physiquement sécurisé.
- Les clés de signature privées des UH stockées sur le module cryptographique de l'UH sont effacées lors du retrait de l'appareil de manière qu'il soit pratiquement impossible de les récupérer.

5.3.2 Objectifs de sécurité du module cryptographique des UH

Le dispositif utilisé par l'AH pour stocker et mettre en œuvre les clés privées des UH et pour générer les contremarques de temps répond aux exigences de sécurité formulées dans la Politique de Certification correspondante parmi lesquelles figurent les exigences suivantes :

- Garantir que la génération des bi-clés des UH est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- Assurer la confidentialité et l'intégrité des clés privées de signature des UH durant tout leur cycle de vie, et permettre leur destruction sûre en fin de vie ;
- Garantir l'authenticité et l'intégrité des clés publiques lors de leur export hors du module ;
- Lors de son importation dans le module, vérifier la correspondance entre le certificat importé et la clé publique de l'UH contenue dans le module ;
- Être capable d'identifier et d'authentifier ses utilisateurs ;
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- Être capable de mener une série de tests, lors des phases d'initialisation, de personnalisation et d'opération, pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Être capable de détecter les tentatives d'altérations physiques et d'entrer dans un état sûr quand une tentative d'altération est détectée ;
- Permettre de créer une signature numérique, pour signer les contremarques de temps générées par l'UH, qui ne révèle pas les clés privées de l'UH et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- Garantir la synchronisation de son horloge avec le temps UTC suivant la précision définie dans la DPH ;
- Fournir des contremarques de temps conformes aux requêtes reçues.

5.3.3 Qualification du module cryptographique des UH

Le module cryptographique utilisé par les UH répond aux exigences suivantes :

- Le module bénéficie des qualifications et/ou certifications attendues par la Politique de Certification des certificats d'UH utilisés ;
- Le module est certifié FIPS 140-2 Level 3, ou Critères Communs EAL4 ou supérieur.

5.4 Gestion du temps

5.4.1 Exactitude déclarée

L'exactitude déclarée est d'une seconde.

5.4.2 Synchronisation des horloges avec l'UTC

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

- Le calibrage de chaque horloge d'UH est maintenu de telle manière que les horloges ne puissent pas normalement dériver à l'extérieur de l'exactitude déclarée.
- Les horloges des UH sont protégées contre les menaces relatives à leur environnement qui pourraient aboutir à une désynchronisation avec le temps UTC en dehors de l'exactitude déclarée.
- Si l'horloge d'une UH ne respecte plus l'exactitude déclarée, alors cela sera détecté.
- Si l'horloge d'une UH est détectée comme étant en dehors de l'exactitude annoncée, alors les contremarques de temps ne sont plus être générées automatiquement.
- 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 de l'instant (selon l'exactitude déclarée) de ce changement et effectué.
  Note : Un saut de seconde est un ajustement par rapport au temps UTC effectué en sautant ou en ajoutant une seconde durant la dernière minute d'un mois UTC. On donne la première préférence à la fin de décembre et juin et on donne la seconde préférence à la fin de mars et septembre.

5.5 Gestion des contremarques de temps

5.5.1 Gestion des demandes de contremarques de temps

Les contremarques de temps sont délivrées de manière sécurisée et intègrent le temps correct avec l'exactitude déclarée. Les informations de temps portées dans les contremarques de temps sont reliées à au moins un temps fourni par un laboratoire UTC (k).

Note : Le Bureau des International Poids et Mesures (BIPM) calcule UTC sur la base des représentations locales UTC (k) d'un grand ensemble de montres atomiques dans des instituts de métrologie nationaux et des observatoires nationaux astronomiques autour du monde. Le BIPM dissémine le temps UTC par sa Circulaire mensuelle T. Celle-ci est disponible sur le site Web BIPM (www.BIPM.org) qui identifie officiellement tous les instituts ayant des échelles de temps UTC (k) reconnues.

Les contremarques de temps sont signées uniquement en utilisant une clé générée exclusivement pour cet usage. Le système de génération de contremarques de temps rejette toute tentative de délivrance de contremarques de temps lorsque la fin du délai d'utilisation de la clé privée de l'UH a été atteinte.

5.5.2 Format des contremarques de temps

Les contremarques de temps délivrées par l'AH ont une structure TimeStampToken conforme à la RFC 3161.

La contremarque de temps inclut :
- L'identifiant du certificat de l'UH,
- L'identifiant de la présente politique d'horodatage,
- Un identifiant unique lié à la contremarque de temps,
- Une représentation de la donnée à horodater (c'est-à-dire la valeur de hachage et l'identifiant d'algorithme de hachage) telle que fournie par l'abonné.

Champ	Description
version	1
policy	1.2.250.1.177.2.9.1.1
messageImprint	SHA256
serialNumber	N° de série positif
genTime	YYYYMMDDhhmmssZ
accuracy	1 seconde
ordering	Absent
nonce	Identique à la valeur présente dans la requête le cas échéant.
tsa	Subject DN du certificat de l'UH
extensions	id-etsi-tsts-EuQCompliance [Non critique]

5.5.3 Vérification des contremarques de temps

Les utilisateurs de contremarques de temps peuvent avoir accès à l'information utilisable pour vérifier la signature numérique des contremarques de temps au travers des moyens suivants :
- Les certificats des UH sont joints à la contremarque de temps,
- La chaine de confiance associée aux certificats des UH est disponible à l'adresse suivante : https://www.certigna.fr/autorites/

Le certificat de l'UH inclue :
- Un identifiant du pays dans lequel l'AH est établi,
- Un identifiant de l'AH,
- Une identification de l'UH qui génère les contremarques de temps.

5.6 Sécurité opérationnelle

5.6.1 Sécurité des systèmes informatiques

Un niveau minimal d'assurance de la sécurité sur les systèmes informatiques des personnes occupant un rôle de confiance est assuré par :

- Identification et authentification forte des utilisateurs pour l'accès au système (contrôle d'accès physique pour entrer dans la salle + contrôle logique par identifiant / mot de passe ou par certificat pour accéder au système) ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AH, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles) ;
- Protection contre les virus informatiques et toutes formes de logiciel compromettant ou non autorisé et mises à jour des logiciels ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- Protection du réseau contre toute intrusion d'une personne non autorisée à l'aide du firewall ;
- Communication sécurisée inter-sites (tunnel VPN IP Sec) ;
- Fonctions d'audit (non-répudiation et nature des actions effectuées).

Des dispositifs de surveillance et des procédures d'audit des paramétrages du système, notamment des éléments de routage, sont mis en place.

5.6.2 Déploiement et maintenance

L'AH emploie des produits et systèmes de confiance.

Une analyse des exigences de sécurité est effectuée au moment de la conception et de l'étape de spécification des exigences pour tout projet de développement de systèmes entrepris par l'AH ou pour le compte de l'AH pour assurer que la sécurité fait partie du système d'information.

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

5.6.3 Planification de système

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

5.6.4 Contrôle d'accès

L'accès au système du TSP est limité aux personnes autorisées.

Les contrôles protègent les domaines de réseau interne de l'AH contre les accès non autorisés, y compris l'accès des abonnés et des tiers. Les pares-feux sont configurés pour empêcher tous les protocoles et les accès non requis pour le fonctionnement de l'AH.

L’AH administre l'accès des utilisateurs aux opérateurs, aux administrateurs et aux auditeurs du système. L'administration comprend la gestion du compte utilisateur et la modification ou l'élimination en temps opportun de l'accès.

L'accès aux informations et aux fonctions du système d'application est restreint conformément à la politique de contrôle d'accès. Le système d’horodatage fournit des contrôles de sécurité informatique suffisants pour la séparation des rôles fiables identifiés dans les pratiques d’horodatage, y compris la séparation de l'administration de la sécurité et des fonctions opérationnelles. En particulier, l'utilisation des programmes utilitaires est restreinte et contrôlée.

Le personnel de l’AH est identifié et authentifié avant d'utiliser les applications critiques liées au service.

Le personnel de l’AH est responsable de ses activités.

Les données sensibles sont protégées contre le fait que des objets de stockage réutilisés sont accessibles à des utilisateurs non autorisés.

5.7 Mesures de sécurité des systèmes durant leur cycle de vie

5.7.1 Mesures de sécurité liées au développement des systèmes

Conformément à l'analyse de risque menée, lors de la conception de tout nouveau projet de développement, une analyse sur le plan de la sécurité est réalisée et approuvée par le Comité de Sécurité de l'AH.

La configuration des systèmes de l'AH ainsi que toute modification et mise à niveau sont documentées. Le développement est effectué dans un environnement contrôlé et sécurisé exigeant un niveau élevé d'autorisation.

Afin de permettre à ses prospects ou futurs clients de tester ou d’évaluer certaines de leurs applications d'échange dématérialisé, l'AC a mise en place une AC de test émettant des certificats d’UH en tous points identiques aux certificats de production (seul l'émetteur du certificat diffère). Cette AC de test dispose d'une clé privée qui lui est propre. Le certificat de clé publique est auto-signé. Les certificats émis ont une utilisation restreinte à des fins de test exclusivement.

Les solutions de CERTIGNA sont testées en premier lieu au sein d’un environnement de développement/test avant d'être utilisées dans l'environnement de production. Les environnements de production et de développement sont dissociés.

5.7.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'AH est documentée et signalée à l'AH pour validation.

5.8 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement souhaité par l'AH.

L'AH garantit que les composants du réseau local sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de leur conformité avec les exigences spécifiées par l'AH.

Des contrôles sont 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.

L'AH segmente ses systèmes en réseaux ou zones en fonction de l'évaluation des risques en tenant compte des relations fonctionnelles, logiques et physiques (y compris la localisation) entre des systèmes et des services fiables. Le TSA applique les mêmes contrôles de sécurité à tous les systèmes situés dans la même zone.

L'AH restreint l'accès et les communications entre les zones à celles nécessaires à l'exploitation de l'AH. Les connexions et les services non nécessaires sont explicitement interdits ou désactivés. L'ensemble des règles établies sont revues régulièrement.

L'AH conserve tous les éléments de ses systèmes critiques dans une zone sécurisée.

Un réseau dédié pour l'administration de systèmes informatiques séparés du réseau opérationnel est établi. Les systèmes utilisés pour l'administration ne sont pas utilisés à des fins non administratives.

La plate-forme de test et la plate-forme de production sont séparées des autres environnements qui ne concernent pas les opérations en direct.

La communication entre des systèmes de confiance distincts n'est établie que par des canaux fiables qui sont logiquement distincts des autres canaux de communication et qui fournissent une identification assurée de ces terminaux et la protection des flux de données à partir de toute modification ou divulgation.

La connexion réseau externe à Internet est redondante pour assurer la disponibilité des services en cas de panne.

L'AH se soumet à une analyse de vulnérabilité régulière et consigne la preuve que chaque analyse de vulnérabilité a été effectuée par une personne ou une entité ayant les compétences, les outils, la compétence, le code de déontologie et l'indépendance nécessaire pour fournir un rapport fiable.

L'AH se soumet à un test de pénétration sur les systèmes de l'AH lors de la mise en place et après l'évolution de l'infrastructure ou de l'application ou des modifications significatives que l'AH détermine. L'AH consigne la preuve que chaque test de pénétration a été effectué par une personne ou une entité possédant les compétences, les outils, la compétence, le code de déontologie et l'indépendance nécessaire pour fournir un rapport fiable.

L'AH maintient et protège tous ses systèmes dans une zone sécurisée.

L’AH configure tous les systèmes des UH en supprimant ou en désactivant tous les comptes, applications, services, protocoles et ports qui ne sont pas utilisés dans les opérations de l’AH.

Seuls les rôles de confiance peuvent accéder aux zones sécurisées et aux zones de haute sécurité.

[FIN DU DOCUMENT]

CERTIGNA
by tessi

www.certigna.com