Politique d'Horodatage

Universign Trust Network
7, rue du Faubourg Poissonnière, 75009 Paris, France

OID: 1.3.6.1.4.1.15819.5.2.(2/3)

VERSION : 2.2	DIFFUSION : PUBLIQUE	Date d'entrée en vigueur :15/05/2019

Table des matières

1 Introduction **7**
1.1 Présentation générale 7
1.2 Identification du document 9
1.3 Entités intervenant dans l'UTN 9
1.3.1 Autorités de Certification 9
1.3.2 Autorité d'Enregistrement 9
1.3.3 Porteurs de Certificats 10
1.3.4 Autorités d'Horodatage 10
1.3.5 Parties Utilisatrices 10
1.3.6 Responsable de Certificat 10
1.4 Usage des Certificats 11
1.4.1 Domaines d'utilisation applicables 11
1.4.2 Domaines d'utilisation interdits 11
1.5 Gestion de la Politique 12
1.5.1 Entité gérant ce document 12
1.5.2 Point de contact 12
1.5.3 Entité déterminant la conformité des pratiques avec la PH 12
1.5.4 Procédures d'approbation de la conformité de la DPH . . 12
1.6 Définitions et acronymes 12

2 Responsabilités concernant la mise à disposition des informations devant être publiées **14**
2.1 Entités chargées de la mise à disposition des informations 14
2.2 Informations publiées 14
2.3 Délais et fréquences de publication 14
2.4 Contrôle d'accès aux informations publiées 15

3 Section laissée vide **15**

4 Exigences opérationnelles **15**
4.1 Synchronisation de l'horloge 15
4.2 Algorithmes obligatoires 16

5 Mesures de sécurité non techniques **16**
5.1 Mesures de sécurité physique 16
5.1.1 Situation géographique et construction des sites 16
5.1.2 Accès physiques 16
5.1.3 Alimentation électrique et climatisation 16
5.1.4 Exposition aux dégâts des eaux 17

5.1.5 Prévention et protection incendie . . . 17
5.1.6 Conservation des supports de données . . . 17
5.1.7 Mise hors service des supports . . . 17
5.1.8 Sauvegarde hors site . . . 17
5.2 Mesures de sécurité procédurales . . . 18
5.2.1 Rôles de confiance . . . 18
5.2.2 Nombre de personnes requises par tâches . . . 18
5.2.3 Identification et authentification pour chaque rôle . . . 19
5.2.4 Rôles exigeant une séparation des attributions . . . 19
5.2.5 Analyse de risque . . . 19
5.3 Mesures de sécurité vis à vis du personnel . . . 19
5.3.1 Qualifications, compétences et habilitations requises . . . 19
5.3.2 Procédures de vérification des antécédents . . . 20
5.3.3 Exigences en matière de formation initiale . . . 20
5.3.4 Exigences et fréquence en matière de formation continue 20
5.3.5 Fréquence et séquence de rotation entre différentes attributions . . . 20
5.3.6 Sanctions en cas d'actions non autorisées . . . 20
5.3.7 Exigences vis-à-vis du personnel des prestataires externes 20
5.3.8 Documentation fournie au personnel . . . 21
5.4 Procédures de constitution des données d'audit . . . 21
5.4.1 Type d'événements à enregistrer . . . 21
5.4.2 Fréquence de traitement des journaux d'événements . . . 21
5.4.3 Période de conservation des journaux d'événements . . . 21
5.4.4 Protection des journaux d'événements . . . 21
5.4.5 Procédure de sauvegarde des journaux d'événements . . . 22
5.4.6 Système de collecte des journaux d'évènements . . . 22
5.4.7 Notification de l'enregistrement d'un événement au responsable de l'événement . . . 22
5.4.8 Evaluation des vulnérabilités . . . 22
5.5 Archivage des données . . . 22
5.5.1 Types de données à archiver . . . 22
5.5.2 Période de conservation des archives . . . 23
5.5.3 Protection des archives . . . 23
5.5.4 Procédure de sauvegarde des archives . . . 23
5.5.5 Exigences d'horodatage des données . . . 23
5.5.6 Système de collecte des archives . . . 23
5.5.7 Procédures de récupération et de vérification des archives 23
5.6 Changement de clés . . . 23
5.7 Reprise suite à compromission et sinistre . . . 24

5.7.1 Procédures de remontée et de traitement des incidents et des compromissions . . . 24
5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) . . . 24
5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante . . . 24
5.7.4 Capacités de continuité d'activité suite à un sinistre . . . 24
5.8 Fin de vie de l'AH . . . 25

6 Mesures de sécurité techniques 25
6.1 Génération et installation de bi-clés . . . 25
6.1.1 Génération des bi-clés . . . 25
6.1.2 Transmission de la clé privée au Porteur . . . 26
6.1.3 Transmission de la clé publique à l'AC . . . 26
6.1.4 Transmission de la clé publique de l'AC aux Parties Utilisatrices . . . 26
6.1.5 Tailles des clés . . . 26
6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité . . . 26
6.1.7 Objectifs d'usage de la clé . . . 26
6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques . . . 26
6.2.1 Standards et mesures de sécurité pour les modules cryptographiques . . . 26
6.2.2 Contrôle de la clé privée par plusieurs personnes . . . 27
6.2.3 Séquestre de la clé privée . . . 27
6.2.4 Copie de secours de la clé privée . . . 27
6.2.5 Archivage de la clé privée . . . 27
6.2.6 Transfert de la clé privée vers / depuis le module cryptographique . . . 27
6.2.7 Stockage de la clé privée dans un module cryptographique 27
6.2.8 Méthode d'activation de la clé privée . . . 28
6.2.9 Méthode de désactivation de la clé privée . . . 28
6.2.10 Méthode de destruction des clés privées . . . 28
6.2.11 Niveau de qualification du module cryptographique et des dispositifs de protection de clés privées . . . 28
6.3 Autres aspects de la gestion des bi-clés . . . 28
6.3.1 Archivage des clés publiques . . . 28
6.3.2 Durées de vie des bi-clés et des Certificats . . . 28
6.4 Données d'activation . . . 29
6.4.1 Génération et installation des données d'activation . . . 29

6.4.2 Protection des données d'activation 29
6.4.3 Autres aspects liés aux données d'activation 29
6.5 Mesures de sécurité des systèmes informatiques 30
6.5.1 Mesures de sécurité technique spécifiques aux systèmes informatiques 30
6.5.2 Niveau de qualification des systèmes informatiques 30
6.6 Mesures de sécurité des systèmes durant leur cycle de vie 30
6.6.1 Mesures de sécurité liées au développement des systèmes 30
6.6.2 Mesures liées à la gestion de la sécurité 30
6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes 30
6.7 Mesures de sécurité réseau 31
6.8 Exactitude du temps 31

7 Profile des Certificats d'UH et des Contremarques 31
7.1 Profils des Certificats d'UH 31
7.2 Profils des Contremarques 31

8 Audit de conformité et autres évaluations 32
8.1 Fréquences et / ou circonstances des évaluations 32
8.2 Identités / qualifications des évaluateurs 32
8.3 Relations entre évaluateurs et entités évaluées 33
8.4 Sujets couverts par les évaluations 33
8.5 Actions prises suite aux conclusions des évaluations 33
8.6 Communication des résultats 33

9 Autres problématiques commerciales et légales 34
9.1 Tarifs 34
9.1.1 Tarifs pour d'autres services 34
9.1.2 Politique de remboursement 34
9.2 Responsabilité financière 34
9.2.1 Couverture par les assurances 34
9.2.2 Autres ressources 34
9.2.3 Couverture et garantie concernant les entités utilisatrices . 34
9.3 Confidentialité des données professionnelles 34
9.3.1 Périmètre des informations confidentielles 34
9.3.2 Informations hors du périmètre des informations confidentielles 35
9.3.3 Responsabilités en termes de protection des informations confidentielles 35
9.4 Protection des données personnelles 35
9.4.1 Politique de protection des données personnelles 35

9.4.2 Informations à caractère personnel . . . 35
9.4.3 Informations à caractère non personnel . . . 35
9.4.4 Responsabilité en termes de protection des données personnelles . . . 35
9.4.5 Notification et consentement d'utilisation des données personnelles . . . 35
9.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives . . . 36
9.4.7 Autres circonstances de divulgation d'informations personnelles . . . 36
9.5 Droits sur la propriété intellectuelle et industrielle . . . 36
9.6 Interprétations contractuelles et garanties . . . 36
9.6.1 Autorité d'Horodatage . . . 37
9.6.2 Service d'enregistrement . . . 37
9.6.3 Porteur . . . 37
9.6.4 Parties Utilisatrices . . . 37
9.6.5 Autres participants . . . 38
9.7 Limite de garantie . . . 38
9.8 Limite de responsabilité . . . 38
9.9 Indemnités . . . 38
9.10 Durée et fin anticipée . . . 38
9.10.1 Durée de validité . . . 38
9.10.2 Fin anticipée de validité . . . 38
9.10.3 Effets de la fin de validité et clauses restant applicables . . . 38
9.11 Notifications individuelles et communications entre les participants 39
9.12 Amendements . . . 39
9.12.1 Procédures d'amendements . . . 39
9.12.2 Mécanisme et période d'information sur les amendements 39
9.12.3 Circonstances selon lesquelles l'OID doit être changé . . . 39
9.13 Dispositions concernant la résolution de conflits . . . 40
9.14 Juridictions compétentes . . . 40
9.15 Conformité aux législations et réglementations . . . 40
9.16 Dispositions diverses . . . 40
9.16.1 Accord global . . . 40
9.16.2 Transfert d'activités . . . 40
9.16.3 Conséquences d'une clause non valide . . . 40
9.16.4 Application et renonciation . . . 41
9.16.5 Force majeure . . . 41
9.17 Autres dispositions . . . 41
9.17.1 Impartialité . . . 41
9.17.2 Accessibilité . . . 41

1 Introduction

1.1 Présentation générale

La présente Politique d'Horodatage définit les engagements des membres de l'UTN pour la délivrance et la gestion de Contremarques de temps.

Présentation de l'Universign Trust Network

Le réseau Universign Trust Network (UTN) est un réseau d'Autorités de Certification (AC) et d'Autorités d'Horodatage (AH) gouvernées par des politiques communes définies par la société Cryptolog International [1].

Dans ce document, le terme UTN désigne, selon son contexte d'utilisation, le réseau Universign Trust Network ou la société Cryptolog International en charge de son contrôle et de sa gestion.

L'UTN est notamment composé :
— d'Autorités de Certification Primaires (AC Primaires) ;
— d'Autorités de Certification Intermédiaires (AC Intermédiaires) ;
— d'Autorités de Certification Horodatage (AC Horodatage) ;
— d'Autorités d'Horodatage (AH) ;
— de Porteurs de Certificats finaux ;
— de Parties Utilisatrices.

Organisation de l'Universign Trust Network

Les Autorités de Certification fonctionnent selon une chaine de confiance structurée hiérarchiquement. Les AC Primaires délivrent des Certificats aux AC Intermédiaires qui, elles-mêmes, délivrent des Certificats à des personnes physiques ou morales (les Porteurs). Les Unités d'Horodatage (UH) des Autorités d'Horodatage reçoivent des Certificats de la part des AC Horodatages et émettent des Contremarques de temps. Les AC Horodatages peuvent recevoir des Certificats de la part des AC Primaires.

Les Parties Utilisatrices se fient aux informations contenues dans les Certificats des Porteurs et les Contremarques de temps.

L'UTN :
— publie la Politique de Certification régissant les AC ;
— publie la Politique d'Horodatage régissant les AH ;

1. Cryptolog International, société par actions simplifiée au capital de 579 504 €, dont le siège social est situé au 7 rue du Faubourg poissonnière, 75009 Paris, immatriculée au Registre du Commerce et des Sociétés de Paris sous le numéro 439 129 164.

— gère les AC Primaires du réseau.

Les membres de l'UTN :
— publient leurs Déclarations des Pratiques ;
— gèrent les AC et les AH associées aux services qu'ils proposent.

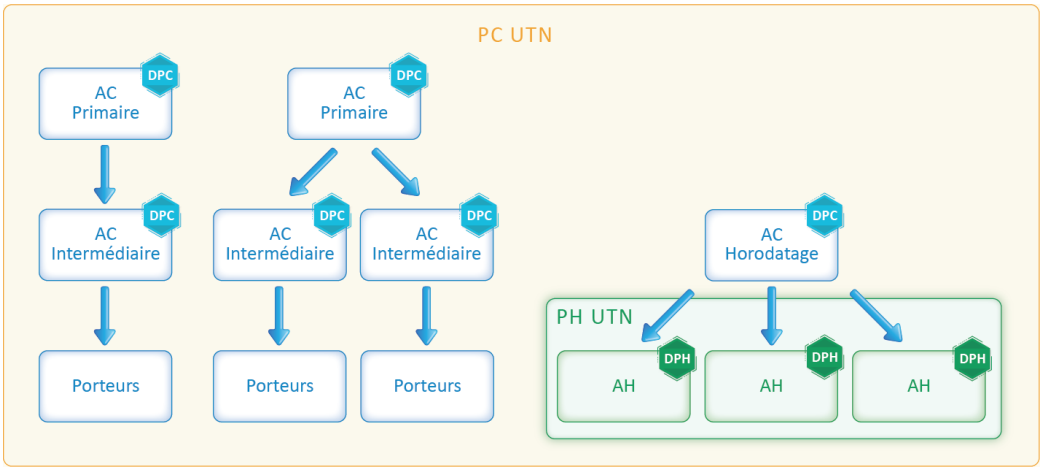

FIGURE 1: Organisation de l'UTN

L'UTN assure la validation, la gestion et la mise en application de la PC et de la PH. L'UTN veille également à la cohérence des référentiels documentaires associés (Accord d'Utilisation, DPC, DPH, ...) à ses Politiques. Chaque autorité membre de l'UTN définit une ou des Déclarations des Pratiques, conformes à la Politique de l'UTN.

Toute demande de rattachement au réseau ou de révocation d'un Certificat d'une AC ou d'une UH du réseau doit être adressée à l'UTN. Les éléments constitutifs du dossier de demande d'un rattachement au réseau ou révocation sont communiqués par l'UTN aux organismes éligibles qui en font la demande.

L'UTN suit les audits et/ou les contrôles de conformité réalisés par les membres du réseau. L'UTN décide des actions à mener et veille à leur mise en application. Il arbitre les litiges entre ses membres.

L'UTN peut auditer ses membres. Les Certificats (AC intermédiaires ou UH) des membres de l'UTN peuvent être révoqués, à tout moment, dans les cas prévus par cette PC.

L'UTN peut déléguer tout ou partie de ses fonctions.

1.2 Identification du document

Ce document est la Politique d'Horodatage de l'UTN.

La présente Politique d'Horodatage (PH) est commune à l'ensemble des Autorités d'Horodatage membres de l'UTN. Elle définit les engagements des AH membres du réseau en termes de sécurité et d'organisation des processus d'émission et de gestion des Contremarques de temps que les AH membres émettent.

Un OID est utilisé pour les Contremarques de temps délivrées par les AH membres de l'UTN.

— Les Contremarques, délivrées en conformité avec [**ETSI 319 421**] et selon la présente PH portent l'OID 1.3.6.1.4.1.15819.5.2.2 ou l'OID 1.3.6.1.4.1.15819.5.2.3 [2] ;

Cette politique est conforme à la Politique d'Horodatage de l'ETSI référencée par l'OID 0.4.0.2023.1.1.

1.3 Entités intervenant dans l'UTN

1.3.1 Autorités de Certification

Une Autorité de Certification (AC) désigne l'autorité en charge de la création, la délivrance, la gestion et la révocation des Certificats au titre de la Politique de Certification.

Chaque membre de l'UTN définit une instance de gouvernance par AC : le Comité d'Approbation. Il est doté des habilitations nécessaires pour :

— définir et approuver des pratiques de certification de l'AC (DPC) conformes à la présente PC ;
— définir le processus de mises à jour de la DPC ;
— informer et mettre à disposition de l'UTN la DPC et ses révisions.

1.3.2 Autorité d'Enregistrement

L'Autorité d'Enregistrement (AE) est une composante de l'AC, responsable de l'identification et de l'authentification des demandeurs de Certificats.

2. Ces deux familles de Contremarques sont reconnues comme qualifiées au sens du règlement eIDAS (EU) No 910/2014.

1.3.3 Porteurs de Certificats

Le Porteur de Certificat est la personne physique ou morale détentrice du Certificat. Le Porteur a nécessairement adhéré aux conditions prévues par l'Accord de Souscription.

1.3.4 Autorités d'Horodatage

Une Autorité d'Horodatage (AH) désigne l'autorité chargée de la création et la délivrance des Contremarques de temps au titre de la Politique d'Horodatage.

Chaque membre de l'UTN définit une instance de gouvernance par AH : le Comité d'Approbation. Il est doté des habilitations nécessaires pour :
- définir et approuver des pratiques de certification de l'AH (DPH) conformes à la présente PH ;
- définir le processus de mises à jour de la DPH ;
- informer et mettre à disposition de l'UTN la DPH et ses révisions.

Les Autorités de Certification délivrent des Certificats pour les Unités d'Horodatage des AH. Ces Certificats permettent aux Parties Utilisatrices d'identifier l'AH. Les Certificats des UH sont délivrés par une AC Horodatage de l'UTN.

1.3.5 Parties Utilisatrices

Les Parties Utilisatrices sont les personnes, physiques ou morales, souhaitant, pour leur propre besoin, se baser sur les informations contenues dans un Certificat ou une Contremarque de temps ou vérifier la validité de la Contremarque ou du Certificat. Il appartient aux Parties Utilisatrices de vérifier les informations relatives au statut de révocation du Certificat.

Les Parties Utilisatrices sont soumises aux stipulations de l'Accord d'Utilisation.

1.3.6 Responsable de Certificat

Un Responsable de Certificat est une personne physique qui :
- accomplit les démarches relatives au cycle de vie d'un Certificat de personne morale (de la demande de Certificat à sa révocation) ;
- contrôle l'utilisation de la clé privée correspondant à ce Certificat.

Le Responsable de Certificat est mandaté par le Porteur du Certificat. Le Responsable de Certificat a un lien contractuel, hiérarchique ou réglementaire avec la personne morale détentrice du Certificat et doit être expressément mandaté par

elle. Le Responsable de Certificat est soumis aux conditions prévues par la présente PC, par le mandat qui le lie au Porteur et par l'Accord de Souscription.

Le Responsable de Certificat peut être amené à changer pendant la durée de validité du Certificat (départ du Responsable de Certificat de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc.). Le Porteur doit notifier sans délai à l'AC le départ ou la révocation d'un Responsable de Certificat et désigner un nouveau Responsable de Certificat. L'AC doit révoquer un Certificat pour lequel le Responsable de Certificat n'est plus identifié.

1.4 Usage des Certificats

1.4.1 Domaines d'utilisation applicables

Bi-clés et Certificats des AC

Les bi-clés associées aux Certificats des AC peuvent être utilisées pour signer :

- les Certificats des AC Intermédiaires (pour les AC Primaires) ;
- les Certificats des Porteurs (pour les AC Intermédiaires) ;
- les LCR et/ou les réponses OCSP de l'AC ;
- les Certificats des composantes techniques de son infrastructure.

Bi-clés et Certificats des Porteurs

Les bi-clés associées aux Certificats émis par l'AC sont destinées à être utilisées par les Porteurs pour :

- signer au moyen d'une signature électronique des documents (pour les Certificats de personnes physiques émis par une AC Intermédiaire) ;
- sceller au moyen d'un cachet électronique des documents (pour les Certificats de personnes morales émis par une AC Intermédiaire) ;
- émettre des Contremarques de temps (pour les Certificats émis par une AC Horodatage).

1.4.2 Domaines d'utilisation interdits

Tout autre usage que ceux prévus au paragraphe 1.4.1 est interdit.

1.5 Gestion de la Politique

1.5.1 Entité gérant ce document

Universign Trust Network
Universign
7, rue du Faubourg Poissonnière, 75009 Paris, France

contact@universign.com

1.5.2 Point de contact

Les questions relatives à ce document sont à adresser à :

Le responsable des Politiques
Universign Trust Network
Universign
7, rue du Faubourg Poissonnière, 75009 Paris, France

contact@universign.com

1.5.3 Entité déterminant la conformité des pratiques avec la PH

L'UTN détermine l'adéquation d'une DPH à la PH.

1.5.4 Procédures d'approbation de la conformité de la DPH

L'UTN prononce la conformité des DPH à la PH selon un processus d'approbation qu'il définit librement. Ce processus d'approbation prévoit les audits réalisés par l'UTN.

1.6 Définitions et acronymes

Les termes utilisés dans ce document sont les suivants :

Accord d'Utilisation
Désigne l'accord régissant les relations entre l'UTN et les Parties Utilisatrices.

Accord de Souscription
Désigne l'accord régissant les relations entre l'AC et le Porteur.

Autorité de Certification (AC)
Désigne l'autorité chargée de la création, la délivrance, la gestion et la révocation des Certificats au titre de la Politique de Certification.

Autorité d'Enregistrement (AE)
Désigne l'autorité chargée de la mise en œuvre des procédures d'identification et de l'authentification des demandeurs de Certificats ;

Autorité d'Horodatage (AH)
Désigne l'autorité chargée de la création et la délivrance des Contremarques de temps au titre de la Politique d'Horodatage.

Certificat
Désigne le fichier électronique délivré par l'Autorité de Certification comportant les éléments d'identification de son Porteur et une clé cryptographique permettant la vérification de la Signature Électronique ou du Cachet Électronique pour lequel il est utilisé.

Contremarque de temps ou Contremarque
Désigne le fichier électronique délivré par l'Autorité d'Horodatage qui lie la représentation d'une donnée à un temps particulier, établissant ainsi la preuve que la donnée existait à cet instant-là.

Déclaration des Pratiques de Certification (DPC)
Désigne les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) appliquées par l'AC pour la mise en œuvre de son service de certification électronique. Ces pratiques sont conformes à la ou aux PC que l'AC s'est engagée à respecter.

Déclaration des Pratiques d'Horodatage (DPH)
Désigne les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) appliquées par l'AH pour la mise en œuvre de son service d'horodatage. Ces pratiques sont conformes à la ou aux PH que l'AH s'est engagée à respecter.

Liste des Certificats Révoqués (LCR)
Désigne la liste identifiant les Certificats émis par l'Autorité de Certification et révoqués.

Object IDentifier (OID)
Désignent les numéros d'identification uniques organisés sous forme hiérarchique permettant notamment de référencer les conditions applicables au service de certification ou d'horodatage, e. g. Politique de Certification, ou d'Horodatage, famille de Certificats, Déclaration de Pratiques de Certification ou d'Horodatage.

Online Certificate Status Protocol (OCSP) Un protocole permettant aux Parties Utilisatrices de vérifier le statut d'un Certificat.

Politique de Certification (PC)
Désigne l'ensemble des règles auxquelles l'AC se conforme pour la mise en œuvre du service de certification.

Politique d'Horodatage (PH)
Désigne l'ensemble des règles auxquelles l'AH se conforme pour la mise en œuvre du service d'horodatage.

Unité d'Horodatage (UH)
Ensemble des matériels et des logiciels utilisés par l'AH pour la création de Contremarques de temps. L'UH est identifiée au moyen d'une clé unique de scellement de Contremarques de temps.

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

2.1 Entités chargées de la mise à disposition des informations

L'AH assure la publication des informations relatives au service qu'elle fournit (cf. 2.2).

L'UTN assure la publication de la PH en cours de validité et de ses versions antérieures ainsi que l'Accord d'Utilisation.

2.2 Informations publiées

L'AH s'engage à porter à la connaissance des Parties Utilisatrices :
— la PH applicables aux Contremarque qu'ils utilisent ;
— les conditions d'utilisation du service d'horodatage ;
— la DPH afférente à la PH applicable ;
— les Certificats des UH en cours de validité.

L'UTN met à disposition de l'AH un site de publication accessible à l'adresse `http://docs.universign.eu` pour la mise à disposition des informations publiées.

2.3 Délais et fréquences de publication

Les délais et les fréquences de publication varient selon les informations concernées :
— Les Certificats des UH sont diffusés ou mis en ligne avant leur utilisation.

— La PH, la DPH et l'Accord d'Utilisation sont publiés après chaque mise à jour.

2.4 Contrôle d'accès aux informations publiées

Les informations publiées sont mises à disposition du public conformément à la section 2.1. Elles sont libres d'accès en lecture.

Les ajouts, suppressions et modifications de ces informations sont limités aux personnes autorisées par l'entité en charge des informations publiées.

3 Section laissée vide

4 Exigences opérationnelles

4.1 Synchronisation de l'horloge

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

Plus particulièrement :

1. le calibrage de chaque horloge d'UH est maintenu de telle manière que les horloges ne puissent pas dériver à l'extérieur de l'exactitude déclarée ;
2. 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 ;
3. l'AH garantit que la dérive de l'horloge interne d'une UH au delà de l'exactitude déclarée sera détectée.
4. si l'horloge d'une UH est détectée comme étant en dehors de l'exactitude annoncée, alors les CT ne sont plus générées ;
5. 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 (selon l'exactitude déclarée) de l'instant de ce changement est effectué.

4.2 Algorithmes obligatoires

L'AH accepte les algorithmes de hachage conformes aux exigences des autorités compétentes en la matière. Les algorithmes de hachage acceptés sont les suivants :

— SHA-1 [3]
— SHA-256
— SHA-384
— SHA-512

5 Mesures de sécurité non techniques

L'AH définit sa Politique de Sécurité de l'Information (PSI). Elle décrit l'approche et les solutions à mettre en place en termes de gestion de la sécurité.

La PSI est maintenue à jour et approuvée par l'AH.

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

L'AH héberge ses services dans des locaux sécurisés. Ces sites et locaux disposent de mécanismes de sécurité physique permettant d'assurer une protection forte contre les accès non autorisés.

5.1.2 Accès physiques

L'accès aux zones des services de l'AH est restreint aux seules personnes nommément autorisées.

Les locaux sont composés de plusieurs zones de sécurité physique successives. Chaque zone successive offre un accès plus restreint et de plus grande sécurité physique contre l'accès non autorisé, du fait que chaque zone sécurisée est encapsulée dans la précédente.

5.1.3 Alimentation électrique et climatisation

Des mesures de secours sont mises en œuvre de manière à ce qu'une interruption de service d'alimentation électrique, ou une défaillance de climatisation ne porte pas atteinte aux engagements pris par l'AH en matière de disponibilité.

3. L'utilisation de cet algorithme est encore accepté pour des raisons de compatibilité. Il est aujourd'hui considéré comme faible. Il est recommandé d'utiliser un des autres algorithmes de la liste.

5.1.4 Exposition aux dégâts des eaux

La définition du périmètre de sécurité prend en considération les risques inhérents aux dégâts des eaux. Des moyens de protection sont mis en œuvre par l'hébergeur pour parer les risques résiduels.

5.1.5 Prévention et protection incendie

Les zones sécurisées sont soumises à des mesures de prévention et de protection incendie appropriées.

5.1.6 Conservation des supports de données

Les supports sont conservés de façon sécurisée. Les supports de sauvegarde sont stockés de manière sécurisée dans un site géographiquement éloigné du support original. Les zones contenant les supports de données sont protégées contre les risques d'incendie, d'inondation et de détérioration. Les documents papiers sont conservés par l'AH dans des locaux sécurisés fermés à clé et stockés dans un coffre-fort dont les moyens d'ouverture ne sont connus que du responsable de l'AH et des personnels habilités. L'AH prend des mesures pour se protéger contre l'obsolescence et la détérioration des médias durant la période de rétention des enregistrements.

5.1.7 Mise hors service des supports

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

5.1.8 Sauvegarde hors site

Afin de permettre une reprise après incident conforme à ses engagements, l'AH met en place des sauvegardes des informations et fonctions critiques hors site de production. L'AH garantit que les sauvegardes sont réalisées par des personnes ayant des Rôles de Confiance. L'AH garantit que les sauvegardes sont exportées hors du site de production et bénéficient de mesures pour la protection de la confidentialité et de l'intégrité. L'AH garantit que les sauvegardes sont testées de façon régulière pour assurer que les mesures du plan de continuité d'activité sont respectées.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les Rôles de Confiance définis dans le présent chapitre sont applicables à toutes les AH membres de l'UTN.

Les Rôles de Confiance suivants sont définis :

Responsable de sécurité : il possède la responsabilité de tous les aspects de la sécurité du système d'information.

Responsable de l'Administration Système : il est responsable des administrateurs systèmes. Il possède des droits d'authentification sur l'ensemble des composantes de l'AH.

Administrateur Système : il est en charge de l'administration et de la configuration de l'ensemble des composants techniques de l'AH ainsi que des opérations d'exploitation quotidienne de l'AH. Il est autorisé à réaliser des sauvegardes et des restaurations.

Auditeur : il est autorisé à auditer les archives et l'intégralité des données d'audits de l'AH.

Contrôleur : il est en charge de l'analyse récurrente des évènements intervenant sur les composantes de l'AH.

Porteur de secrets : il assure la confidentialité, l'intégrité et la disponibilité des parts de secrets qui lui sont confiées.

Les personnels en Rôle de Confiance doivent être libres de tous conflits d'intérêt incompatibles avec leurs missions.

5.2.2 Nombre de personnes requises par tâches

L'AH détermine les procédures et le nombre de personnes ayant un Rôle de Confiance nécessaires pour chaque opération sur les opérations sensibles.

5.2.3 Identification et authentification pour chaque rôle

Des mesures d'identification et d'authentification sont prévues afin de mettre en œuvre la politique de contrôle d'accès et la traçabilité des opérations. Les Rôles de Confiance attribués sont notifiés par écrit aux personnes concernées par l'AH. L'AH s'assure régulièrement que l'ensemble des Rôles de Confiance sont pourvus afin d'assurer une continuité de l'activité.

5.2.4 Rôles exigeant une séparation des attributions

L'AH s'assure que les rôles de Responsable de Sécurité et d'Administrateur Système ne sont pas attribués à la même personne.
L'AH s'assure que les rôles de Contrôleur et d'Administrateur Système ne sont pas attribués à la même personne.
L'AH s'assure que les rôles d'Auditeur et d'Administrateur Système ne sont pas attribués à la même personne.

L'AH s'assure que les opérations de sécurité sont séparées des opérations d'exploitation classiques et qu'elles sont réalisées systématiquement sous le contrôle d'une personne ayant un Rôle de Confiance.

5.2.5 Analyse de risque

L'AH réalise une analyse de risque afin d'identifier les menaces sur les services. Cette analyse de risque est revue périodiquement et lors de changements structurels significatifs. De plus, la méthodologie utilisée pour effectuer l'analyse de risque permet de s'assurer que l'inventaire de l'AH est maintenu à jour.

5.3 Mesures de sécurité vis à vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

L'AH s'assure que les attributions des personnels opérant des Rôles de Confiance correspondent à leurs compétences professionnelles. Le personnel d'encadrement possède l'expertise appropriée et est sensibilisé aux procédures de sécurité. Toute personne intervenant dans des Rôles de Confiance est informée de ses responsabilités (description de poste) et des procédures liées à la sécurité du système et au contrôle du personnel. Les personnels opérant des Rôles de Confiance sont nommés par la direction de l'AH.

5.3.2 Procédures de vérification des antécédents

Avant la nomination d'une personne à un Rôle de Confiance, l'AH procède à la vérification de ses antécédents judiciaires et ses compétences professionnelles, de manière à valider son adéquation au poste à pourvoir. Il est notamment vérifié que :

— la personne n'a pas de conflit d'intérêt préjudiciable à l'impartialité des tâches qui lui sont attribuées ;
— la personne n'a pas commis d'infraction en contradiction avec son Rôle de Confiance.

L'AH sélectionne les personnes remplissant les Rôles de Confiance en tenant compte de leur loyauté, leur sérieux et leur intégrité.

5.3.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement.

5.3.4 Exigences et fréquence en matière de formation continue

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux intervenants dans la mesure où cette évolution impacte leur travail.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont prévues contractuellement. La nature de ces sanctions sont portées à la connaissance des personnes qui remplissent un Rôle de Confiance.

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

Les exigences vis-à-vis des prestataires externes sont contractualisées. Les contrats conclus avec les prestataires prévoient des engagements en matière de confidentialité et de sécurité ainsi que des mesures relatives à l'utilisation des moyens informatiques.

5.3.8 Documentation fournie au personnel

Les règles et procédures de sécurité documentées sont soumises à l'approbation du Comité d'Approbation de l'AH. Les règles de sécurité sont communiquées au personnel lors de la prise de poste, en fonction du rôle affecté à l'intervenant. Les personnes appelées à occuper un rôle opérationnel au sein de l'AH disposent d'un accès aux procédures correspondantes et sont tenues de les respecter.

5.4 Procédures de constitution des données d'audit

5.4.1 Type d'événements à enregistrer

L'AH prend les mesures nécessaires pour enregistrer les évènements suivants :
— la génération de Contremarques ;
— l'ensemble des évènements liés au cycle de vie des UH (gestion du contexte, gestion des clés, import de certificat, ...) ;
— les arrêts / relances des UH ;
— les désynchronisation des horloges des UH.

Ces journaux permettent d'assurer la traçabilité et l'imputabilité des actions effectuées, en particulier en cas de demande émanant d'une autorité judiciaire ou administrative. L'AH décrit dans ses procédures internes le détail des évènements et des données enregistrées. Les procédures de traçabilité mises en place par l'AH sont robustes et permettent l'agrégation des traces issues de différentes sources, la détection d'intrusion et un plan de monitoring.

5.4.2 Fréquence de traitement des journaux d'événements

Les journaux d'événements sont exploités systématiquement en cas de remontée d'événement anormal.

5.4.3 Période de conservation des journaux d'événements

Les journaux d'évènements sont conservés pendant la durée nécessaire aux besoins de preuve dans le cadre de procédures administratives et judiciaires.

5.4.4 Protection des journaux d'événements

Les journaux d'événements sont rendus accessibles uniquement au personnel autorisé. Ils ne sont pas modifiables.

5.4.5 Procédure de sauvegarde des journaux d'événements

Les journaux sont sauvegardés régulièrement sur un système externe.

5.4.6 Système de collecte des journaux d'évènements

Les systèmes de collecte des journaux d'évènements de l'AH ont pour but de fournir des éléments de preuves dans le cadre de procédures judiciaires et en cas de contrôle administratif. Ils contribuent également à assurer la continuité du service. Les informations collectées sont conservées pendant une période appropriée, y compris après la cessation des activités de l'AH. Elles sont pertinentes et proportionnées au regard de leurs finalités.

5.4.7 Notification de l'enregistrement d'un événement au responsable de l'événement

Il n'y a pas de notification des évènements.

5.4.8 Evaluation des vulnérabilités

L'AH met en place des contrôles permettant de détecter :
— les accès non autorisés ;
— les anomalies techniques ;
— les incohérences entre les différents évènements de l'AH.

5.5 Archivage des données

5.5.1 Types de données à archiver

Les données archivées sont les suivantes :
— la DPH ;
— les journaux d'évènements, contenant notamment :
  — les évènements relatifs à un changement significatif de l'environnement de l'AH et le moment précis d'occurrence de l'évènement ;
  — les évènements relatifs aux opérations sur les clés des UH et le moment précis d'occurrence de l'évènement.

L'AH décrit dans ses procédures internes le détail des données et évènements qui sont conservés.

5.5.2 Période de conservation des archives

L'ensemble des archives est conservé en conformité avec la législation en vigueur (voir Sect. 9.4.1) et les obligations inhérentes à l'AH (voir Sect. 5.8).

5.5.3 Protection des archives

Quel que soit leur support, les archives sont protégées en intégrité et ne sont accessibles qu'aux personnes autorisées. Ces archives sont consultables et exploitables pendant toute la durée de leur cycle de vie et sont conservées dans un environnement sécurisé.

5.5.4 Procédure de sauvegarde des archives

Des sauvegardes régulières des archives sous forme électronique sont réalisées par les personnes ayant des Rôles de Confiance. Ces sauvegardes sont exportées hors du site de production et bénéficient de mesures de protection de la confidentialité et de l'intégrité.

5.5.5 Exigences d'horodatage des données

Les enregistrements des évènements doivent contenir la date et l'heure de l'évènement. Cependant, il n'y a pas d'exigence d'horodatage cryptographique de ces évènements.

5.5.6 Système de collecte des archives

Les systèmes de collecte des archives de l'AH sont internes.

5.5.7 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) peuvent être récupérées dans un délai inférieur à deux jours ouvrés. Ces archives sont conservées et traitées par des équipes de l'AH.

5.6 Changement de clés

L'AH n'a pas de procédure automatique de renouvellement de clé, cependant une AH doit générer de nouvelles bi-clés d'UH et effectuer des demandes de Certificats auprès d'une AC Horodatage de l'UTN avant la fin de la période d'utilisation de la clé privée d'une l'UH.

L'AH doit appliquer toutes les actions nécessaires pour éviter tout arrêt de ses opérations.

5.7 Reprise suite à compromission et sinistre

5.7.1 Procédures de remontée et de traitement des incidents et des compromissions

L'AH met en place des procédures et des moyens de remontée et de traitement des incidents. Ces moyens permettent de minimiser les dommages en cas d'incidents.

L'AH met en place un plan de réponse en cas d'incident majeur, tel qu'une compromission de ses mécanismes de publication ou de son mécanisme d'émission de Certificat.

Un incident majeur, tels qu'une perte, une suspicion de compromission ou un vol de la clé privée de l'UH est immédiatement notifié au Comité d'Approbation, qui, si cela s'avère nécessaire, peut décider de faire une demande de révocation du certificat de l'UH auprès de l'UTN et de mettre fin à l'UH.

5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Un plan de continuité est mis en place permettant de répondre aux exigences de disponibilité des différentes composantes de l'AH. Ce plan est testé régulièrement.

5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Ce point est couvert par les plans de continuité et de reprise d'activité. La compromission d'une clé d'UH entraîne immédiatement la révocation de son Certificat et l'arrêt de cette UH. Dans ce cas, les différents acteurs et entités concernées seront avertis du caractère non sûr des Contremarques signées par la clé compromise de l'UH. Des mesures similaires sont prises si la robustesse de l'algorithme utilisé ou celle des paramètres utilisés par l'UH devient insuffisante.

5.7.4 Capacités de continuité d'activité suite à un sinistre

La capacité de continuité de l'activité suite à un sinistre est traitée par le plan de reprise et le plan de continuité d'activité. Suite à un sinistre, l'AH met en place ce plan afin de restaurer les services touchés. En particulier, l'AH a une architecture redondée pour ses services critiques. De plus, l'AH gère un stock

de matériel de rechange afin de palier toute panne matérielle. En cas d'incident majeur, l'AH possède un plan de reprise d'activité lui permettant de mettre en place une nouvelle AH dans une durée raisonnable. Ce plan s'appuie sur une salle d'hébergement secondaire.

A la reprise d'activité, l'AH met en œuvre l'ensemble des mesures nécessaires pour éviter qu'un sinistre similaire se reproduise. Les opérations de restauration sont réalisées par des personnels occupant des Rôles de Confiance.

Le Plan de Reprise d'Activité est testé régulièrement.

5.8 Fin de vie de l'AH

En cas d'arrêt définitif, l'AH met en place un plan de fin de vie. Ce plan de fin de vie traite des aspects suivants :

— la notification de l'arrêt aux personnes et organismes concernés par le plan ;
— la notification de l'arrêt à l'UTN ;
— la potentielle révocation de tous les Certificats émis encore en cours de validité au moment de la décision de l'arrêt de l'activité ;
— la destruction des clés privées des UH ;
— les dispositions nécessaires pour transférer ses obligations relatives aux archives des données d'audit ;
— la mise à disposition des informations pour les Parties Utilisatrices.

Ce plan est vérifié et maintenu à jour régulièrement.

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

Les clés des UH sont générées :

— lors d'une cérémonie des clés ;
— sous le contrôle d'au moins deux personnes ayant des Rôle de Confiance (voir Sect. 5.2.1) ;
— dans des locaux sécurisés (voir Sect. 5.1) ;
— au sein d'un HSM répondant aux exigences définies dans la section 6.2.11.

La génération des clés est réalisée selon une procédure précise et donne lieu à la rédaction d'un procès-verbal en fin de cérémonie.

Les clés publiques des UH sont transmises à l'AC conformément à la PC de l'UTN.

6.1.2 Transmission de la clé privée au Porteur

Sans objet.

6.1.3 Transmission de la clé publique à l'AC

La clé publique à certifier est transmise à l'AC de façon à garantir l'intégrité et l'origine de cette clé.

6.1.4 Transmission de la clé publique de l'AC aux Parties Utilisatrices

Sans objet.

6.1.5 Tailles des clés

Les clés des UH doivent être conformes (ou être cryptographiquement supérieures ou égales) aux caractéristiques ci-dessous. Elles doivent également être conformes aux exigences de la PC de l'UTN.

Certificat	Taille des clésKey Size	Format
UH	2048 4096 (pour les clés générées après le 1er janvier 2019)	RSA RSA

6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité

Les AH doivent utiliser du matériel certifié (voir Sect. 6.2.11) et des algorithmes dont les paramètres respectent les normes de sécurité idoines.

6.1.7 Objectifs d'usage de la clé

Voir chapitre 7.1.

6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

Les modules cryptographiques utilisés par l'AH pour la génération et la mise en œuvre de ses clés de signature sont des modules cryptographiques matériels

certifiés répondant aux exigences de la section 6.2.11. L'AH s'assure de la sécurité de ces modules tout au long de leur cycle de vie. En particulier, l'AH met en place les procédures nécessaires pour :

— s'assurer de leur intégrité durant leur transport depuis le fournisseur ;
— s'assurer de leur intégrité durant leur stockage précédant la cérémonie des clés ;
— s'assurer que les opérations d'activation des clés de signature sont réalisées sous le contrôle de deux personnels ayant des Rôles de Confiance ;
— s'assurer qu'ils sont en bon état de fonctionnement ;
— s'assurer que les clés qu'ils contiennent sont détruites lorsqu'ils sont décommissionnés.

6.2.2 Contrôle de la clé privée par plusieurs personnes

La clé privée d'une UH est contrôlée par des données d'activation stockées sur des cartes à puce remises à des porteurs de secrets lors de la cérémonie des clés. Un partage de secret du HSM est mis en œuvre par l'AH.

6.2.3 Séquestre de la clé privée

Les clés privées ne font pas l'objet de séquestre.

6.2.4 Copie de secours de la clé privée

Les clés privées des UH ne font pas l'objet de copies de sauvegarde.

6.2.5 Archivage de la clé privée

Les clés privées de l'AH ne sont pas archivées.

6.2.6 Transfert de la clé privée vers / depuis le module cryptographique

Sans objet.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées des UH sont stockées dans un module cryptographique.

6.2.8 Méthode d'activation de la clé privée

L'activation des clés privées est contrôlée par des données spécifiques dites données d'activation. Elle est réalisée au sein d'un module cryptographique répondant aux exigences de la section 6.2.11 sous le contrôle de deux personnes ayant des Rôles de Confiance.

6.2.9 Méthode de désactivation de la clé privée

La désactivation de la clé privée s'opère lors de l'arrêt du module cryptographique.

6.2.10 Méthode de destruction des clés privées

La destruction de la clé privée d'une UH est effectuée à partir de son module cryptographique. L'AH s'assure que toutes les copies de secours correspondantes sont également détruites.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs de protection de clés privées

Module cryptographique des UH : Les modules cryptographiques des UH satisfont aux exigences de certification suivantes :

- EAL 4+ aux Critères Communs ISO/CEI 15408 (conforme au Profil de Protection CWA 14169 ou certifié conforme au Profil de protection Secure Signature Creation Device (SSCD) par une entité gouvernementale européenne) ;
- FIPS 140-2 level 3
- QSealCD au sens du règlement eIDAS (EU) No 910/2014.
- ou équivalent.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

L'AH archive les clés publiques de ses UH selon les exigences de la section 5.5.

6.3.2 Durées de vie des bi-clés et des Certificats

La durée de vie maximale des Certificats est de :

- 30 ans pour les Certificats d'AC Racine ;

— 20 ans pour les Certificats d'AC Horodatage ;
— 15 ans pour les Certificats d'AC Intermédiaire ;
— 5 ans pour les Certificats de personne physique et les Certificats de personne morale ;
— 11 ans pour les Certificats de personne morale destinés à l'horodatage.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Les données d'activation de la clé d'une UH sont générées durant la cérémonie des clés. Ces données d'activation sont stockées sur des cartes à puce et remises à des porteurs de secret.

Chaque porteur de secrets prend les mesures nécessaires pour se prémunir contre la perte, le vol, l'utilisation non autorisée ou la destruction non autorisée de sa carte à puce et des données d'activation qu'elle contient.

6.4.2 Protection des données d'activation

Les données d'activation sont stockées sur une carte à puce nominative et personnelle. La responsabilité de cette carte à puce incombe à la personne à qui la carte est remise. La carte est protégée par un mot de passe personnel au porteur de secret. Les cartes à puce sont ensuite stockées dans un coffre-fort sécurisé individuel. Chaque porteur de secret est responsable de sa part de secret d'activation. Il exprime son consentement en signant un formulaire définissant ses responsabilités.

6.4.3 Autres aspects liés aux données d'activation

Transmission des données d'activation : La transmission des cartes à puce contenant des données d'activation d'un porteur de secret vers un nouveau porteur de secret doit être réalisée de façon à protéger les données d'activation contre la perte, le vol, la modification, la divulgation non autorisée ou l'utilisation non autorisée de ces données.

Destruction des données d'activation : Les données d'activation sont décommissionnées de façon à se prémunir du vol, de la perte, de la modification, de la divulgation non autorisée ou de l'utilisation non autorisée de ces données.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Mesures de sécurité technique spécifiques aux systèmes informatiques

L'AH met en place, en fonction du système à protéger, des mécanismes de contrôle appropriés à la plate-forme à sécuriser (afin de se protéger contre l'exécution de code non autorisé ou potentiellement dangereux sur son système).

L'AH met en place des mécanismes de contrôle d'accès et d'authentification pour tous les rôles permettant la génération de nouveaux certificats. Elle maintient ces systèmes de sécurité en permanence.

Ces mécanismes sont décrits dans la DPH.

6.5.2 Niveau de qualification des systèmes informatiques

Sans objet.

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

Tous les composants logiciels de l'AH sont développés dans des conditions et suivant des processus de développement garantissant leur sécurité. L'AH met en œuvre des processus qualité au cours de la conception et du développement de ses logiciels. L'AH s'assure, lors de la mise en production d'un élément logiciel, de son origine et de son intégrité et assure une traçabilité de l'ensemble des modifications apportées sur son système d'information.

Les infrastructures de développement et d'essai sont distinctes des infrastructures de production de l'AH.

6.6.2 Mesures liées à la gestion de la sécurité

L'AH s'assure que la mise à jour des logiciels est réalisée de façon à assurer la sécurité du système. Les mises à jour sont réalisées par des personnels ayant un Rôle de Confiance de l'AH.

6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

6.7 Mesures de sécurité réseau

Les communications réseaux véhiculant des informations confidentielles font l'objet de mesures de protection contre l'écoute des informations. Les règles régissant ces contrôles sont vérifiées régulièrement.

Des mesures de sécurité sont mises en place afin de protéger les composantes locales du système d'information des accès non autorisés, en particulier les données sensibles.

L'AH met en place des procédures de gestion des accès d'administration de la plate-forme afin de maintenir la sécurité à un niveau élevé. Ces mesures incluent l'authentification des administrateurs, la production de traces pour les audits, l'utilisation de canaux sécurisés de type VPN ainsi que la possibilité de modifier à tout instant les droits d'accès. L'AH met également en place un réseau d'administration déconnecté du réseau nominal.

L'AH met en place des procédures de contrôle d'accès pour séparer les fonctions d'administration et les fonctions opérationnelles. L'utilisation des applications (publication, génération de certificat, révocation) nécessite une authentification des utilisateurs ou des entités. Une politique de contrôle d'accès est mise en place pour limiter l'accès de ces applications aux seules personnes autorisées.

6.8 Exactitude du temps

Les horloges des UH sont supervisées localement par des serveurs de temps de référence. Ces serveurs sont autonomes et bénéficient d'une procédure de synchronisation avec des références UTC(k). Les mécanismes utilisés permettent de se prémunir des attaques visant à désynchroniser les systèmes de temps, y compris les attaques majeures visant à brouiller les signaux radios ou satellitaires.

L'AH garantit que les CT générées par ses UH ont un décalage de temps inférieur à une seconde par rapport à UTC.

7 Profile des Certificats d'UH et des Contremarques

7.1 Profils des Certificats d'UH

Le profil des Certificats des UH est défini dans la PC de l'UTN.

7.2 Profils des Contremarques

version	Version 1
policy	OID : 1.3.6.1.4.1.15819.5.2.(2/3)

messageImprint	OID de l'algorithme de hash et l'empreinte numérique données à horodater. NB : Ces informations sont fournies dans la requête.
serialNumber	Nombre aléatoire de 160 bits caractéristique de la présente requête.
genTime	Date de l'horodatage au format ASN.1 GeneralizedTime
accuracy	Précision de 1 seconde
ordering	Contenu mis à FAUX
nonce	Valeur renvoyée à l'identique si présente dans la requête
tsa	Le nom de l'UH
extensions	Sans objet.

8 Audit de conformité et autres évaluations

8.1 Fréquences et / ou circonstances des évaluations

Des audits sont effectués par l'AH :
— un audit interne réalisé
  — soit par des prestataires externes spécialistes du domaine ;
  — soit par un responsable d'audit interne à l'AH.
— un audit de certification à la norme [ETSI 319 411-1] et [ETSI 319 411-2], réalisé tous les 2 ans par un organisme accrédité.

Un contrôle de conformité à la PH en vigueur est effectué :
— lors de la mise en œuvre opérationnelle du système ;
— au moins une fois par année civile (audit interne) ;
— lors de la surveillance ou du renouvellement des certifications, conformément aux procédures réglementaires en vigueur ;
— lorsqu'une modification significative est effectuée.

8.2 Identités / qualifications des évaluateurs

Les évaluateurs doivent s'assurer que les politiques, déclarations et services sont correctement mis en œuvre par l'AH et détecter les cas de non-conformité qui pourraient compromettre la sécurité du service offert. L'AH s'engage à mandater des évaluateurs dont les compétences sont éprouvées en matière de sécurité des systèmes d'information et spécialisés dans le domaine d'activité de la composante contrôlée.

8.3 Relations entre évaluateurs et entités évaluées

Sauf accord particulier entre l'AH et l'UTN, l'AH désigne l'évaluateur autorisé à effectuer l'audit. L'AH garantit l'indépendance et l'impartialité de l'évaluateur.

8.4 Sujets couverts par les évaluations

L'évaluateur procède à des contrôles de conformité de la composante auditée, sur toute ou partie de la mise en œuvre :

— de la PH ;
— de la DPH ;
— des composants de l'AH.

Avant chaque audit, les évaluateurs proposeront au Comité d'Approbation de l'AH une liste de composantes et procédures qu'ils souhaiteront vérifier. Ils établiront ainsi le programme détaillé de l'audit.

8.5 Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'évaluateur et son équipe rendent au Comité d'Approbation de l'AH, un avis parmi les suivants : "réussite", "échec", "à confirmer".

Avis “échec” : L'équipe d'audit émet des recommandations à l'AH. Le choix de la mesure à appliquer appartient à l'AH.

Avis “à confirmer”, l'équipe d'audit identifie les non conformités, et les hiérarchisent. Il appartient à l'AH de proposer un calendrier de résolution des non conformités. Une vérification permettra de lever les non conformités identifiées.

Avis “réussite”, l'AH confirme à la composante contrôlée la conformité aux engagements de la PH et de ses pratiques annoncées.

8.6 Communication des résultats

Les résultats des audits de conformité sont transmis au Comité d'Approbation, à l'UTN et mis à la disposition des autorités en charge de la qualification et de la certification du service.

9 Autres problématiques commerciales et légales

9.1 Tarifs

Les membres de l'UTN fixent les conditions tarifaires de leurs services.

9.1.1 Tarifs pour d'autres services

Pas d'engagement spécifique.

9.1.2 Politique de remboursement

Les services de l'AH ne font l'objet d'aucun remboursement.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

Les membres de l'UTN souscrivent à une assurance responsabilité appropriée permettant de couvrir les risques financiers liés à l'utilisation du service qu'elle fournit et conforme à la réglementation applicable à son activité.

Il appartient à l'AH d'évaluer le risque financier devant être couvert.

9.2.2 Autres ressources

L'AH met en œuvre une politique administrative et financière visant à maintenir pendant toute la durée de son activité les ressources financières nécessaires pour remplir les obligations définies par la PH.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Pas d'engagement spécifique.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations suivantes sont considérées comme confidentielles :
— les clés privées de l'AH,
— les données d'activation associées aux clés privées de l'AH,
— les journaux d'événements,
— les rapports d'audit,
— les plans de continuité, de reprise et d'arrêt d'activité.

D'autres informations peuvent être considérées comme confidentielles par l'AH.

9.3.2 Informations hors du périmètre des informations confidentielles

Le site de publication de l'AH et son contenu sont considérés comme public.

9.3.3 Responsabilités en termes de protection des informations confidentielles

L'AH s'engage à traiter les informations confidentielles conformément aux obligations qui lui sont applicables.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

L'AH collecte et traite les données à caractère personnel conformément aux réglementations relatives à la protection des données à caractère personnel qui lui sont applicables.

9.4.2 Informations à caractère personnel

Sans objet.

9.4.3 Informations à caractère non personnel

Des accords entre l'AH et les utilisateurs de ses services peuvent prévoir un traitement particulier des informations à caractère non personnel et non confidentiel au sens de l'article 9.3.1.

9.4.4 Responsabilité en termes de protection des données personnelles

L'AH est responsable du traitement des données à caractère personnel des utilisateurs de son service.

9.4.5 Notification et consentement d'utilisation des données personnelles

L'AH informe les personnes dont elle collecte les données à caractère personnel du traitement de ces données et des finalités de ces traitements.

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

Sans objet.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Des accords entre l'AH et les utilisateurs de ses services peuvent prévoir la divulgation d'informations personnelles dans les limites prévues par la réglementation française.

9.5 Droits sur la propriété intellectuelle et industrielle

Dans le cadre de son activité, l'AH peut être amenée à délivrer ou permettre l'utilisation d'éléments protégés par la propriété intellectuelle et industrielle.

Ces éléments et les droits d'auteur y afférents resteront la propriété du détenteur de ces droits. Les Parties Utilisatrices peuvent reproduire ces éléments pour leurs usages internes. Une autorisation préalable du détenteur des droits d'auteur est nécessaire pour la mise à la disposition de tiers, extraction ou réutilisation en tout ou en partie, ces éléments ou des œuvres dérivées ou copies de ceux-ci en dehors des nécessités du service de l'AH.

Toute utilisation ou reproduction, totale ou partielle, de ces éléments et/ou des informations qu'ils contiennent, non autorisées par l'autre partie, à d'autres fins que le fonctionnement du service, est strictement interdite et constitue une contrefaçon qui pourra faire l'objet de poursuites judiciaires.

L'utilisation des informations contenues dans les Contremarques ou afférentes à leur statut est autorisée dans le strict respect de l'Accord d'Utilisation.

9.6 Interprétations contractuelles et garanties

Les obligations communes des AH de l'UTN sont les suivantes :
— protéger et garantir l'intégrité et la confidentialité de leurs clés cryptographiques privées ;
— utiliser leurs clés cryptographiques privées uniquement dans les conditions et avec les outils spécifiés dans la PH ;
— appliquer et respecter les exigences de la PH et de la DPH leur incombant ;
— se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'UTN ;
— accepter les conséquences de ces contrôles et en particulier, remédier aux non-confirmités qui pourraient être révélées ;

— documenter leurs processus internes de fonctionnement ;
— mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des opérations dont elle est en charge en garantissant la qualité et la sécurité de ces opérations.

9.6.1 Autorité d'Horodatage

L'AH est responsable :
— de la conformité de la DPH vis-à-vis de la PH ;
— de la conformité des Contremarques à la PH ;
— du respect de tous les principes de sécurité par les différentes composantes de l'AH et des contrôles afférents.

L'AH est responsable des préjudices causés aux Parties Utilisatrices si la date et de l'heure qu'indique la Contremarque de temps et l'intégrité des données auxquelles se rapportent cette date et cette heure sont erronées.

9.6.2 Service d'enregistrement

Cf. ci-dessus.

9.6.3 Porteur

Le Porteur :
— communique des informations exactes et à jour lors d'une demande d'établissement d'un Certificat ;
— est responsable de l'accès à sa clé privée et le cas échéant, des moyens d'activation de sa clé ;
— respecte les conditions d'utilisation de sa clé privée ;
— informe l'AC de toute modification des informations contenues dans son Certificat ;
— adresse sans délai une demande de révocation de son Certificat en cas de suspicion de compromission de la clé privée correspondante ou des moyens d'activation de cette clé.

9.6.4 Parties Utilisatrices

Les Parties Utilisatrices s'engagent à respecter les obligations prévues par l'Accord d'Utilisation et à prendre connaissance des termes et conditions de la PH applicable au service qu'elles utilisent en particulier des limites d'utilisations et de garanties associées au service.

9.6.5 Autres participants

Pas d'engagement spécifique.

9.7 Limite de garantie

Les limites de garantie de l'AH sont prévues par les conditions d'utilisation du service d'horodatage et l'Accord d'Utilisation.

9.8 Limite de responsabilité

L'AH n'est pas responsable d'une utilisation des Contremarques non autorisée ou non conforme à la PH, à l'Accord de Souscription ou à l'Accord d'Utilisation.

L'AH ne saurait être tenue responsable des dommages indirects liés à l'utilisation d'une Contremarque.

L'AH n'est pas responsable de l'utilisation non autorisée ou non conforme à leur documentation des équipements et/ou logiciels mis à la disposition des utilisateurs du service d'horodatage.

9.9 Indemnités

Les conditions d'indemnisation des préjudices causés aux Porteurs et aux Parties Utilisatrices sont prévues contractuellement.

9.10 Durée et fin anticipée

9.10.1 Durée de validité

La PH entre en vigueur à compter de sa publication sur le site de publication de l'UTN.

9.10.2 Fin anticipée de validité

La PH reste en vigueur jusqu'à son remplacement par une nouvelle version.

9.10.3 Effets de la fin de validité et clauses restant applicables

Sauf dispositions contraires prévues par la présente PH ou par la PH qui viendrait la remplacer, la fin de validité de la PH entraîne l'extinction de toutes les obligations de l'AH applicables aux Contremarques émises conformément aux présentes.

9.11 Notifications individuelles et communications entre les participants

Sauf en cas d'accord entre les parties concernées, toutes les notifications individuelles et les communications prévues par la PH doivent être adressées par des moyens garantissant leur origine et leur réception.

9.12 Amendements

9.12.1 Procédures d'amendements

L'UTN peut amender la PH. Ces amendements prennent la forme de nouvelles versions de la PH. Ils sont publiés sur le site de publication de l'UTN. L'UTN détermine si les modifications à la PH nécessitent un changement des OID pour les Contremarques émises.

9.12.2 Mécanisme et période d'information sur les amendements

L'UTN peut effectuer des modifications sans notifications sur la PH en vigueur en cas de changement mineur, comme par exemple des corrections typographiques ou d'URL. L'UTN est la seule entité autorisée à apprécier si une modification est mineure ou non.

L'UTN informe ses membres de son intention de modifier la PH, en précisant les modifications proposées et la période de commentaire. Ces propositions de modifications sont également publiées sur le site du l'UTN. Les membres administrant leur propre site de publication doivent y publier les propositions de modifications dès leur réception.

Période de commentaires Sauf en cas d'indication contraire, la période de commentaire est fixée à un (1) mois à compter de la publication de la proposition de modification non-mineures sur le site de publication de l'UTN. Toutes les entités intervenant dans l'UTN peuvent soumettre des commentaires durant cette période.

Traitement des commentaires À l'issue de la période de commentaires, l'UTN peut décider de publier la nouvelle PH ou de procéder à un nouveau processus d'amendement avec une version modifiée ou de retirer la version proposée.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

En cas de modification substantielle de la PH, le Comité d'Approbation de l'UTN peut décider qu'un changement d'OID est nécessaire.

Un changement d'OID pourra être effectué si la modification de la PH est susceptible d'affecter le niveau d'assurance des Contremarques déjà émises.

9.13 Dispositions concernant la résolution de conflits

L'AH met en place une procédure adéquate pour permettre le règlement amiable des différents qui l'opposent aux utilisateurs de ses services.

9.14 Juridictions compétentes

En cas de litige entre l'AH et l'UTN découlant de l'interprétation, l'application et/ou l'exécution de la PC et à défaut d'accord amiable entre les parties ci-avant, la compétence exclusive est attribuée aux juridictions compétentes du ressort de la Cour d'appel de Paris.

9.15 Conformité aux législations et réglementations

Les dispositions de la PH sont conformes aux exigences du droit français applicables.

Les textes législatifs et réglementaires applicables à la PH sont, notamment, ceux indiqués en référence de la présente politique.

9.16 Dispositions diverses

9.16.1 Accord global

L'AH pourra préciser des exigences spécifiques dans la DPH.

9.16.2 Transfert d'activités

Pas d'engagement spécifique.

9.16.3 Conséquences d'une clause non valide

Dans le cas où une clause de la PH s'avérerait être nulle ou réputée non-écrite de l'avis de la juridiction compétente, la validité, la légalité et le caractère exécutoire des autres clauses ne serait en aucun cas affectées ou réduites.

9.16.4 Application et renonciation

Les exigences définies dans la PH doivent être appliquées selon les dispositions de la PH et de la DPH associée sans qu'aucune exonération des droits, dans l'intention de modifier tout droit ou obligation prescrit, ne soit possible.

9.16.5 Force majeure

L'AH ne saurait être tenue pour responsable des dommages indirects et interruption de ses services relevant de la force majeure, laquelle aurait causé des dommages directs à leurs utilisateurs.

9.17 Autres dispositions

9.17.1 Impartialité

Pour garantir l'impartialité de ses opérations, l'AH s'assure que les personnes qui occupent des Rôles de Confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs missions.

9.17.2 Accessibilité

Dans la mesure du possible, l'AH permet aux personnes handicapées d'accéder aux services qu'elle fournit.

Références

[**RFC 3647**]
Network Working Group - Request for Comments : 3647 - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework - November 2003.

[**ETSI 319 401**]
ETSI EN 319 401 V2.1.1 - Electronic Signatures and Infrastructures (ESI) ; General Policy Requirements for Trust Service Providers (2016-02)

[**ETSI 319 411-1**]
ETSI EN 319 411-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI) ; Policy and security requirements for Trust Service Providers issuing certificates ; Part 1 : General requirements (2016-02)

[**ETSI 319 411-2**]
ETSI EN 319 411-2 V2.1.1 - Electronic Signatures and Infrastructures (ESI) ; Policy and security requirements for Trust Service Providers issuing certificates ; Part 2 : Requirements for trust service providers issuing EU qualified certificates (2016-02)

[**ETSI 319 412-2**]
ETSI EN 319 412-2 V2.1.1 - Electronic Signatures and Infrastructures (ESI) ; Certificate Profiles ; Part 2 : Certificate profile for certificates issued to natural persons (2016-02)

[**ETSI 319 412-3**]
ETSI EN 319 412-3 V1.1.1 - Electronic Signatures and Infrastructures (ESI) ; Certificate Profiles ; Part 3 : Certificate profile for certificates issued to legal persons (2016-02)

[**ETSI 319 412-5**]
ETSI EN 319 412-5 V2.1.1 - Electronic Signatures and Infrastructures (ESI) ; Certificate Profiles ; Part 5 : QC Statements (2016-02)

[**ETSI 319 421**]
ETSI EN 319 421 V1.1.1 - Electronic Signatures and Infrastructures (ESI) ; Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (2016-03)