Service d'Horodatage Universign

Politique d'Horodatage

OID: 1.3.6.1.4.1.15819.5.2.2

VERSION : **2.1**	DIFFUSION : ***PUBLIQUE***	Date d'entrée en vigueur : **01/07/2016**

Table des matières

1 Introduction

1.1 Présentation Générale

Universign a choisi de se positionner en tant qu'Autorité d'Horodatage (AH) et Prestataire de Service d'Horodatage Électronique (PSHE) et propose un Service d'Horodatage (SH) à ses clients se conformant notamment aux exigences de qualification du Référentiel Général de Sécurité (RGS) pour son SH.

Le présent document constitue la Politique d'Horodatage (PH) d'Universign. Il présente le SH d'Universign et définit les engagements pris par Universign en tant qu'AH vis-à-vis de ce service. La présente PH identifie aussi les obligations et exigences portant sur les Abonnés et les Utilisateurs.

Une contremarque (CT) émise par le SH d'Universign permet d'attester de la réalité, à une date et une heure donnée, de l'existence d'une empreinte numérique. Les CTs sont délivrées et signées électroniquement par l'AH à l'aide d'Unités d'Horodatage (UHs).

L'objectif de ce document est de définir les engagements qu'Universign, en tant qu'AH, respecte dans la délivrance et la gestion de CTs, ainsi que les obligations des autres participants.

Le présent document est complété, dans sa partie mise en œuvre, par une Déclaration des Pratiques d'Horodatage (DPH) et des Conditions Générales d'Utilisation (CGU) du SH. La DPH d'Universign expose les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la PH, en particulier les processus qu'une UH emploiera pour la création des CTs et le maintien de l'exactitude de ses horloges. Universign, en tant qu'AH, peut mettre en œuvre plusieurs UHs pour gérer son SH.

L'Autorité de Certification (AC) délivrant les certificats pour les UH de l'AH est également sous la tutelle d'Universign et est définie par la Politique de Certification (PC) de l'AC UNIVERSIGN : [**PCU**].

Cette PH n'impose pas d'exigences sur le lien entre l'empreinte numérique à horodater et le contenu de la donnée électronique qui en est à l'origine. Cette vérification est à la charge de l'Abonné.

Dans le cadre de la présente PH, le jour et l'heure de chaque CT sont synchronisés avec le temps universel (UTC) avec une précision inférieure à une se-

conde. La présente PH applique un format de CT standard défini par le standard [**ETSI 319 422**]. La gestion de la synchronisation de l'horloge du SH est détaillée au chapitre 6.1.

La présente PH est élaborée sur la base des documents [**ETSI 319 421**] (OID : 0.4.0.2023.1.1) et de la PH type [**RGS_A_12**] défini par le RGS (OID : 1.2.250.1.137.2.2.1.2.2.4).

Principes de l'horodatage tel que réalisé par Universign

L'horodatage permet d'attester qu'une donnée existe à un instant donné. Pour cela, il convient d'associer à une représentation sans équivoque d'une donnée, (i.e. sa valeur de hachage associée à un identifiant d'algorithme de hachage), à un instant dans le temps. La garantie de cette association est fournie au moyen d'une CT qui est une structure signée qui contient en particulier :

— la valeur de hachage et l'algorithme de hachage de la donnée qui a été horodatée ;
— la date et le temps universel (UTC) ;
— l'identifiant du certificat de l'UH qui a généré la CT ;
— l'identifiant d'Universign en tant qu'AH (inclus dans le certificat d'horodatage) ;
— l'identifiant de l'Autorité de Certification ayant signé les clés privées installées sur les UHs.

Le SH mis en place par Universign, bénéficie de l'Infrastructure de Gestion de Clés (IGC) déjà établie par Universign, dont le service de certification de l'AC UNIVERSIGN.

Ce service de certification permet à l'AC UNIVERSIGN d'émettre les certificats des UHs.

Le système de synchronisation de l'horloge du SH permet à Universign de garantir à l'Abonné d'obtenir une empreinte temporelle avec un écart par rapport au temps universel (UTC) de moins d'une seconde.

L'AH Universign fait fonctionner plusieurs UHs. Chaque UH signe les CTs pour le compte de l'AH à l'aide d'une clé privée qui lui est dédiée, et dont la clé publique correspondante a été certifiée au préalable par l'AC UNIVERSIGN. Chaque UH dispose donc de son propre certificat d'horodatage.

1.2 Identification du document

Ce document est la Politique d'Horodatage d'Universign. Cette PH est identifiée, au sein du référentiel documentaire de l'infrastructure de confiance d'Universign, par un numéro d'identification unique : **1.3.6.1.4.1.15819.5.2.2**

L'OID est composé comme suit :

1.3.6.1.4.1.15819	Branche CRYPTOLOG (enregistrée auprès de l'ETSI)
1.3.6.1.4.1.15819.5	Branche des politiques
1.3.6.1.4.1.15819.5.2	Branche des politique d'horodatage

Les CTs respectant la présente politique la référenceront en utilisant ce numéro d'identification unique (OID). Pour information, ce champ est intégré dans le champ "Policy" des CTs. D'autres éléments, plus explicites (nom, numéro de version, date de mise à jour) permettent également de l'identifier.

1.3 Entités intervenants dans le SH

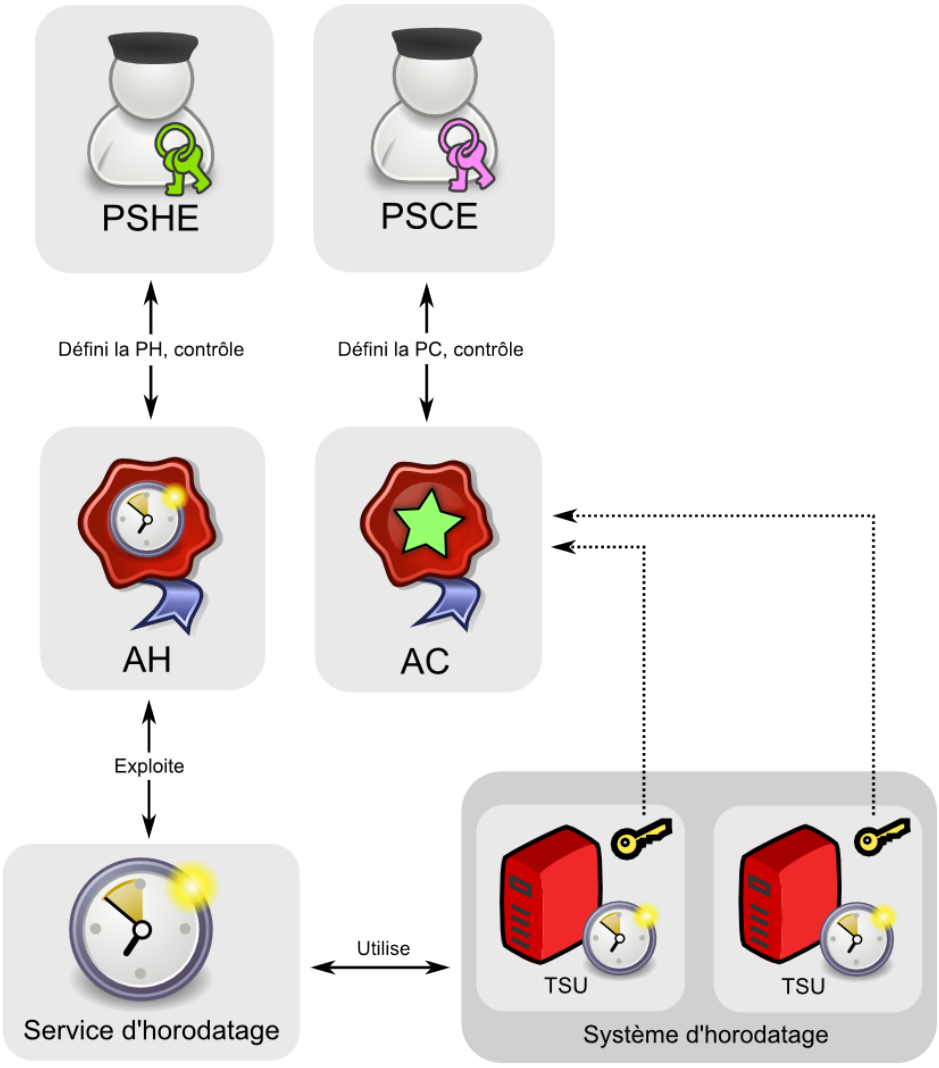

FIGURE 1: Organisation du SH d'Universign

1.3.1 Autorités de certification

Au sein d'un SH, les certificats des TSUs sont fournis par une AC. Ces certificats permettent aux Utilisateurs d'identifier l'AH.

1.3.2 Autorité d'horodatage

Dans le contexte réglementaire français, une Autorité d'Horodatage et un Prestataire de Services d'Horodatage Électronique sont deux notions allant naturellement ensemble.

L'ordonnance 2005-1516 [**ORD**] introduit et définit les prestataires de service de confiance (PSCO). Un PSHE est un type de PSCO particulier. Un PSHE se définit comme toute personne ou entité qui est responsable de la génération et de la gestion de contremarques de temps, vis-à-vis de ses Abonnés et des Utilisateurs. Un PSHE comporte au moins une AH mais peut en comporter plusieurs en fonction de son organisation. Un PSHE est identifié dans les certificats des UHs dont il a la responsabilité au travers de ses AHs.

Au sein d'un PSHE, une AH a en charge, au nom et sous la responsabilité de ce PSHE, l'application d'au moins une PH en s'appuyant sur une ou plusieurs UHs. Dans le cadre cette PH, le terme de PSHE n'est pas utilisé en dehors du présent chapitre et du chapitre 1.1 et le terme d'AH est le seul utilisé. Il désigne l'AH Universign chargée de l'application de cette PH, au sein du PSHE Universign.

L'AH est gérée par le Comité d'Approbation d'Universign. Le Comité d'Approbation est composé des instances dirigeantes d'Universign. Il est présidé par le Responsable de l'AH.

Ce dernier approuve la PH et les documents constituant le SH fourni par Universign.

Il s'agit d'une instance de la direction dotée de l'autorité et de la responsabilité finale pour :

- spécifier et approuver l'infrastructure et les pratiques du SH d'Universign ;
- approuver la PH et la DPH d'Universign ;
- garantir dans le temps les pratiques et politiques énoncées par l'AH dans le cadre d'exigences fonctionnelles, organisationnelles et techniques ;
- garantir dans le temps la mise en œuvre des UHs conformément à la DPH énoncée ;
- publier aux Abonnés et Utilisateurs la PH et les CGU et leurs révisions ;

1.3.3 Abonnés

Un Abonné est une entité ayant besoin de faire horodater des données auprès de l'AH Universign et qui a accepté les CGU.

1.3.4 Utilisateurs

Un Utilisateur est une entité (personne ou système) qui fait confiance à une CT émise sous cette PH par l'AH Universign. Un Utilisateur peut également être, ou non, un Abonné.

1.3.5 Autres participants

Sans objet.

1.4 Gestion de la PH

1.4.1 Entité gérant la PH

Universign
Cryptolog International
7, rue du Faubourg Poissonnière, 75009 Paris, France
contact@universign.eu

1.4.2 Point de contact

Les questions relatives à la présente PH sont à adresser à :

Le responsable de la Politique d'Horodatage
Universign
Cryptolog International
7, rue du Faubourg Poissonnière, 75009 Paris, France
contact@universign.eu

1.4.3 Entité déterminant la conformité des pratiques avec la PH

Le Comité d'Approbation d'Universign détermine l'adéquation et l'applicabilité de cette PH.

1.4.4 Procédures d'approbation de la conformité de la DPH

L'approbation de la conformité des pratiques documentées à la PH est prononcée par le Comité d'Approbation d'Universign, au vu des audits internes effectués.

1.5 Définitions et Abréviations

Définitions

Contremarque de temps (CT) :
Donnée qui lie une représentation d'une donnée à un temps particulier établissant ainsi la preuve que la donnée existait à cet instant-là.

Contrôleur :
Personne réalisant un contrôle des événements du SH.

Empreinte numérique :
Résultat d'une fonction de hachage caractérisant une donnée ; c'est une séquence de bits de longueur fixe pour une fonction de hachage donnée (par exemple 256 bits pour SHA-256).

Hébergeur :
Entité assurant l'hébergement d'une infrastructure technique, Web et informatique, dans un environnement sécurisé et de manière hautement connectée.

Liste de Certificats Révoqués (LCR) :
Liste signée numériquement par l'AC contenant les identifiants des certificats qui ont été révoqués avant leur date d'expiration.

Partenaires :
Universign désigne comme partenaire une personne, un groupe, une collectivité ou une entité avec laquelle elle s'associe dans le cadre de la fourniture de son SH à destination de ses Abonnés et Utilisateurs.

Service d'horodatage (SH) :
Ensemble des opérations nécessaires à la génération et à la gestion de CTs.

Système d'horodatage :
Ensemble des UHs et des composants d'administration et de supervision utilisé pour fournir un SH.

Unité d'Horodatage (UH) :
Ensemble de matériel et de logiciel en charge de la création de CTs caractérisé par un identifiant de l'Unité d'Horodatage certifié par une AC, et une clé unique de signature de CTs.

Universign :
Pour les besoins des présentes et des documents régissant l'offre d'horodatage, la société Cryptolog International, SAS au capital de 504 932 euros, sise 7, rue du Faubourg Poissonnière, 75009 Paris, enregistrée au RCS de Paris sous le numéro 439129164.

Abréviations

AH : Autorité d'Horodatage
AC : Autorité de Certification
CGU : Conditions Générales d'Utilisation
CNIL : Commission Nationale de l'Informatique et des Libertés
CT : Contremarque de Temps
DPH : Déclaration des Pratiques d'Horodatage
LCR : Liste de Certificats Révoqués
NTP : Network Time Protocol
OID : Object IDentifier
PH : Politique d'Horodatage
PSHE : Prestataire de Service d'Horodatage Electronique
RGS : Référentiel Général de Sécurité
SH : Service d'Horodatage
UH : Unité d'Horodatage

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

2.1 Entités chargées de la mise à disposition des informations

Universign, en tant qu'AH, met à disposition des Utilisateurs la présente PH. La présente PH est disponible via Internet, sur le site web : http://docs.universign.eu.

Les informations relatives aux pratiques d'horodatage destinées à être publiquement diffusées se trouvent dans la présente PH et les CGU.

2.2 Informations publiées

Les informations publiées sont les suivantes :
— cette PH ;
— les Conditions Générales d'Utilisation ;

— l'Accord d'Utilisation ;
— les certificats des TSUs.

2.3 Délais et fréquences de publication

Une nouvelle PH sera publiée dans le cas où :
— des modifications notables de la DPH entraînent un impact sur la présente PH ;
— des évolutions réglementaires impactent la présente PH.

Les certificats des UHs sont diffusés ou mis en ligne au maximum 24 heures après leur génération et obligatoirement avant leur utilisation effective.

2.4 Contrôle d'accès aux informations publiées

Les informations publiées sont mises en ligne sur le site web d'Universign et accessibles en lecture à l'ensemble de la communauté. Les PH et CGU sont accessibles en lecture à toute personne souhaitant en prendre connaissance sur le site web d'Universign : http://docs.universign.eu.

Les ajouts, suppressions et modifications de ces informations sont limités aux personnes autorisées d'Universign, au travers d'un contrôle d'accès.

3 Dispositions générales

3.1 Obligations de l'AH

Universign doit assurer la conformité avec les exigences et les procédures prescrites dans cette politique.

Universign doit garantir l'adhésion aux obligations complémentaires indiquées dans la CT ou bien par référence.

Universign doit fournir un SH conforme à sa DPH.

Universign doit remplir tous ses engagements tels que stipulés dans ses CGU.

Universign doit garantir la délivrance technique des CTs.

Universign doit garantir l'application de sa DPH et la couverture des exigences exprimées dans la présente PH.

3.2 Obligations de l'Abonné

L'Abonné doit accepter et se conformer au CGU du SH d'Universign.

Il est également recommandé que l'Abonné vérifie que le certificat de l'UH délivrant une CT est valable au moment de la demande d'horodatage (voir chapitre 6.8).

3.3 Obligations de l'Utilisateur

L'Utilisateur doit vérifier que les CTs ont été correctement signéees et que le certificat de l'UH correspondant n'est pas révoqué à l'instant de cette vérification grâce aux LCRs publiées par l'AC UNIVERSIGN.

L'Utilisateur doit également vérifier que les demandes de CTs sont bien émises par une UH d'Universign. Pour cela l'Utilisateur doit vérifier que la référence à une UH Universign est bien présente dans la contremarque qu'il souhaite vérifier.

Enfin, l'Utilisateur doit tenir compte des limitations sur l'utilisation de la CT indiquées dans la présente PH et l'accord d'utilisation.

3.4 Obligations pour les AC fournissant les certificats des UHs

Les certificats doivent être délivrés par une AC qualifiée conforme à la fois
— au standard [**ETSI 319 411-2**] ;
— au standard [**RGS_A_10**] selon la Politique de Certification type "Cachet" de niveau au moins une étoile (*)

3.5 DPH

Universign garantit qu'elle possède la fiabilité nécessaire pour fournir un SH et décrit la mise en œuvre de son SH dans sa DPH. Ce document garantit que :

1. Universign effectue une évaluation de risques pour évaluer les actifs et les menaces pour ces actifs afin de déterminer les contrôles de sécurité nécessaires et les procédures opérationnelles ;
2. Universign possède une déclaration des pratiques et des procédures utilisées pour adresser toutes les exigences identifiées dans la présente PH ;

3. La DPH identifie les obligations et les exigences de mise en œuvre que doivent respecter l'AH, les Partenaires, les Abonnés et les Utilisateurs, dans le cadre du SH d'Universign ;
4. Universign met à la disposition des Abonnés et des Utilisateurs les parties publiques de sa DPH (incluses dans ses CGU) pour qu'ils puissent évaluer la conformité à la présente PH ;
5. Universign met en place une organisation adéquate pour l'approbation de sa DPH et la vérification de la concordance entre cette déclaration et la présente PH ;
6. Le Responsable de l'AH garantit que les pratiques sont correctement mises en œuvre ;
7. Une procédure de contrôle périodique est définie par Universign pour vérifier que ses pratiques sont conformes à sa DPH ;
8. Universign vise à être certifié comme étant conforme à la présente PH par un organisme évaluateur indépendant.

Par la suite, toute modification envisagée à l'initiative d'Universign qui pourrait entraîner une non-conformité avec sa PH ou avec sa DPH sera soumise de nouveau à un organisme évaluateur indépendant pour avis.

Note : La DPH n'a pas vocation à être publiquement diffusée. Pour la consulter, une demande formelle devra être faite auprès de l'AH UNIVERSIGN.

3.6 CGU

Universign met à disposition de l'Abonné ses CGU. L'Abonné doit respecter les différentes clauses établies dans les CGU.

Les CGU sont publiques et sont publiées sur le site Internet d'Universign : http://docs.universign.eu.

3.7 Conformité avec les exigences légales

3.7.1 Droit applicable

Le présent document est régi par la loi française.

3.7.2 Règlement des différends

EN CAS DE LITIGE ENTRE LES PARTIES DÉCOULANT DE L'INTERPRÉTATION, L'APPLICATION ET/OU L'EXÉCUTION DU CONTRAT ET À DÉFAUT D'ACCORD AMIABLE ENTRE LES PARTIES CI-AVANT, COMPÉTENCE EXCLUSIVE EST ATTRIBUÉE AU TRIBUNAL DE COMMERCE DE PARIS.

3.7.3 Propriété intellectuelle des infrastructures Universign

Sur le plan de la propriété intellectuelle, les produits mis en œuvre dans le SH sont la propriété d'Universign.

Les Abonnés et les Utilisateurs ne disposent d'aucun droit de propriété intellectuelle sur ces différents éléments. Toute utilisation ou reproduction, totale ou partielle, de ces éléments et/ou des informations qu'ils contiennent, par quelque procédé que ce soit, est strictement interdite et constitue une contrefaçon sanctionnée par le "code de la propriété intellectuelle", sauf accord préalable et écrit d'Universign.

3.7.4 Données nominatives

Les informations nominatives contenues sur les plates-formes d'Universign font l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL), conformément aux dispositions suivantes : [CNIL].
Les Abonnés sont informés que les données personnelles qu'ils communiquent pourront être transmises et exploitées par Universign et les différents partenaires intervenant dans les échanges concernés, conformément à l'article 32 de cette loi.

Les Abonnés sont informés qu'ils disposent d'un droit d'accès, de rectification et d'opposition portant sur les données les concernant en contactant Universign.

Universign prend toutes les mesures nécessaires pour que les données personnelles soient protégées et conservées confidentielles conformément aux termes de la loi n°78-17 du 6 janvier 1978.

Le personnel d'Universign est tenu de respecter les dispositions de la loi : [CNIL], dont la violation est passible de sanctions disciplinaires et pénales.

Ils doivent notamment s'abstenir, s'agissant des informations nominatives auxquelles ils accèdent, de toute collecte, de toute utilisation détournée et, d'une ma-

nière générale, de tout acte susceptible de porter atteinte à la vie privée ou à la réputation des personnes.

Universign s'engage, en tant qu'AH, à ne pas divulguer les informations fournies par les Abonnés, à moins de leur accord, d'une décision judiciaire ou d'une exigence légale.

3.8 Amendements à la PH

3.8.1 Procédures d'amendement

Universign, via son Comité d'Approbation, est responsable de la création, l'approbation, la maintenance et les modifications de cette PH.

Lorsqu'une nouvelle version de la PH est approuvée par le Comité d'Approbation d'Universign, elle sera publiée sur le site web d'Universign et remplacera les termes de la version précédente.

3.8.2 Mécanisme et période d'information sur les amendements

Les seules modifications que le Comité d'Approbation peut opérer sur la PH en vigueur sans notification sont les changements mineurs comme par exemple, les corrections rédactionnelles et typographiques, les clarifications ou les corrections d'erreurs manifestes. Le Comité d'Approbation est le seul juge pour déterminer si une modification est mineure ou non.

Pour une modification non mineure, la nouvelle PH sera mise en ligne pour commentaire, avec une indication de la date d'effet proposée.

Lorsqu'une nouvelle version de la PH est mise en ligne, tous les Abonnées et Utilisateurs du SH d'Universign sont informés de la nature, de la date et de l'heure du changement, par une publication sur le blog d'Universign.

À l'issue de la période de commentaires, le Comité d'Approbation peut décider de publier la nouvelle PH telle quelle, de redémmarer le processus d'amendement avec une version modifiée ou de retirer la version proposée.

Sauf indication contraire, la nouvelle version de la PH entre en vigueur 14 jours ouvrés après sa mise en ligne et reste valide jusqu'à l'entrée en vigueur d'une nouvelle version.

3.8.3 Circonstances selon lesquelles l'OID doit être changé

Si le Comité d'Approbation détermine qu'un changement d'OID est nécessaire, la nouvelle version indiquera le nouvel OID.

Le Comité d'Approbation reste seul juge pour déterminer si un changement d'OID est nécessaire. Un changement d'OID est principalement effectué lors d'un changement majeur pouvant affecter le niveau d'assurance des CTs déjà émises.

4 Exigences opérationnelles

4.1 Gestion des requêtes de CTs

Universign fournit un service de gestion des requêtes de CT. Les conditions particulières de fourniture de ce service font l'objet des CGU acceptées par l'Abonné.

4.2 Fichiers d'audit

Sauf indication contraire, Universign garantit que toutes les informations appropriées concernant le fonctionnement du SH sont enregistrées pendant une durée de cinq (5) ans après la mise hors service de l'UH correspondante, en particulier dans le but de fournir une preuve en cas d'enquêtes légales.

Les fichiers d'audit portent sur les événements relatifs :
— à la génération de CTs ;
— aux actes d'administration sur le service d'horodatage : gestion du contexte, import de certificat, état du service ;
— au fonctionnement de l'horloge interne et à sa synchronisation ;
— au cycle de vie des clés des UH ;
— au cycle de vie des certificats d'UH ;
— à tout type d'événements susceptibles d'avoir un impact sur le fonctionnement des UHs.

Chaque évènement d'audit contient la date et l'heure précise de l'événement.

La confidentialité des enregistrements d'audit est assurée par une gestion d'accès physique, système et réseau appropriée. L'intégrité est assurée cryptographiquement.

La gestion de ces enregistrements est conforme à la gestion des informations classifiées d'Universign.

4.3 Gestion de la durée de vie de la clé privée

Universign garantit que les clés privées de signature des UHs ne sont pas employées au-delà de la fin de leur cycle de vie.

L'UH détruit automatiquement la clé privée si la fin de la période d'utilisation de cette clé privée a été atteinte. Les clés des UHs ne sont pas renouvellées.

Universign s'assure que le nombre d'UHs en activité à tout moment est suffisant pour assurer la bonne marche du service.

4.4 Synchronisation de l'horloge

Universign 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. Universign garantit que la dérive de l'horloge interne d'une UH au delà de l'exactitude déclarée sera détectée. La détection d'une dérive de l'horloge du SH fera l'objet d'une publication sur le blog d'Universign de manière à en informer ses Abonnés et ses Utilisateurs ;
4. si l'horloge d'une UH est détectée comme étant en dehors de l'exactitude annoncée, alors les CTs ne sont plus générées ;
5. Universign 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.

4.5 CT

Universign garantit que les CTs sont générées en toute sécurité et incluent le temps correct. Universign émet uniquement des CTs qualifiées.

4.5.1 Contenu d'une CT

En réponse à une requête d'un Abonné, Universign fournit une CT conforme au standard [ETSI 319 422] et contenant les champs suivants :

version	Version 1
policy	OID : 1.3.6.1.4.1.15819.5.2.2
messageImprint	OID de l'algorithme de hash et l'empreinte numérique données à horodater. NB : Ces informations sont fournies dans la requête de l'Abonné.
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 FALSE
nonce	Valeur renvoyée à l'identique si présente dans la requête
tsa	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Timestamping Unit xxx] où "xxx" est le numéro de l'UH concernée. NB : Ce champ est égal au champ "subject" du certificat de l'UH signant la CT.
extensions	Sans objet.

4.5.2 Signature d'une CT

Conformément au chapitre 6.7 du présent document, le contenu de la CT est signé en employant une clé privée de type RSA d'une taille de 2048 bits

4.6 Compromission de l'Autorité d'Horodatage

Dans le cas d'évènements qui affectent la sécurité du SH et qui pourrait affecter des CTs émises, Universign garantit qu'une information appropriée est mise à la disposition des Abonnés et des Utilisateurs.

La compromission de l'AH peut être due à :
— la compromission des clés privées des UH ;
— la compromission de la clé privée de l'AC UNIVERSIGN ayant servi à générer les certificats des UH ;

— un problème d'exploitation.

Universign a intégré dans son Plan de Continuité d'Activité les compromissions pouvant intervenir sur son SH.

4.6.1 Plan de continuité

Le Plan de Continuité d'Activité d'Universign traite le cas de la compromission réelle ou suspectée de la clé privée de signature d'une UH ou la perte de calibrage de l'horloge d'une UH, qui pourrait affecter des CTs émises.

Universign a établi un contrat avec l'hébergeur de son système d'horodatage qui garantit que toutes les mesures nécessaires sont prises par l'hébergeur pour éviter les incidents d'exploitation.

Universign maintient son Plan de Continuité d'Activité à jour afin de couvrir et d'assurer le meilleur service possible vis-à-vis des risques suivants :

— compromission des clés privées ;
— indisponibilité du réseau ;
— indisponibilité du personnel qualifié ;
— problème de calibrage de l'horloge ;
— pannes de matériels informatiques.

Plus généralement, les incidents liés au SH sont traités selon la procédure de gestion des incidents en vigueur chez Universign.

4.6.2 Communication

Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une UH, qui pourrait affecter des CTs émises, Universign mettra à la disposition de tous les Abonnés et Utilisateurs une description de l'incident qui est survenu, conformément à son Plan de Communication. Ces informations sont publiées sur le site web : http://blogs.universign.eu

4.6.3 Arrêt de la génération de CTs

Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une UH, qui pourrait affecter des CTs émises, Universign prend les mesures nécessaires pour que les CTs de cette UH ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.

4.6.4 Information de validation des CTs

En cas d'un évènement majeur dans le fonctionnement d'Universign ou d'une perte de calibrage, qui pourrait affecter des CTs émises, chaque fois que cela sera possible, Universign mettra à la disposition de tous ses Abonnés et des Utilisateurs toute information pouvant être utilisée pour identifier les CTs qui pourraient avoir été affectées, à moins que cela ne contrevienne à la sécurité du SH.

4.6.5 Alerte ANSSI

Dans le cas d'une compromission, réelle ou suspectée de son SH, Universign préviendra directement et sans délai le point de contact de l'ANSSI, en sa qualité de Supervisory Body.

4.7 Fin d'activité

Des procédures de fin d'activité sont définies par Universign. Dans ce cadre, Universign garantit que les dérangements potentiels aux Abonnés et aux Utilisateurs seront réduits au minimum suite à la cessation d'activité du SH et assure en particulier la maintenance continue des informations nécessaires pour vérifier la justesse des CTs, même après l'arrêt de son SH.

Avant qu'Universign ne termine son SH les procédures suivantes seront exécutées :

- Universign rendra disponible à tous ses Abonnés et aux Utilisateurs l'information concernant sa fin d'activité en la publiant sur son site Internet ;
- Universign 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 CTs ;
- Universign 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 ;
- Universign maintiendra ses obligations de rendre disponible aux Utilisateurs pendant une période raisonnable ses clés publiques ainsi que ses certificats ;
- les clés privées des UH seront détruites de telle façon que les clés privées ne puissent pas être recouvrées, suivant la procédure décrite dans le chapitre 4.3.

Universign prend les mesures nécessaires pour couvrir les dépenses pour accomplir ces exigences minimales dans le cas où Universign tomberait en faillite

ou pour d'autres raisons serait incapable de couvrir les dépenses par elle-même.

Les dispositions prises pour la fin du service incluent :
— un avis aux Abonnés et aux Utilisateurs ;
— un transfert des obligations d'Universign à d'autres organismes.

Universign préviendra directement et sans délai l'ANSSI, en sa qualité de Supervisory Body.

5 Exigences physiques et environnementales, procédurales et organisationnelles

5.1 Exigences physiques et environnementales

5.1.1 Situation géographique et construction des sites

Universign héberge son SH dans des locaux sécurisés. Ces sites et locaux disposent de mécanismes de sécurité physique décrits dans ce chapitre (tels que des zones verrouillées, un service de gardiennage, des mécanismes de détection d'intrusion) permettant d'assurer une forte protection contre les accès non autorisés.

Les locaux sont composés de plusieurs zones de sécurité physique successives. Le passage d'une zone à la suivante se fait via un accès sécurisé, tel qu'une porte verrouillée par badge d'accès ou des sas à identification biométrique, qui assure un strict contrôle d'accès aux seules personnes autorisées. 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.

5.1.2 Accès physiques

L'accès aux zones des services d'horodatage d'Universign est restreint aux seules personnes nommément autorisées. Ces habilitations sont déclarées auprès de l'hébergeur d'Universign et un cahier de suivi est complété à chaque opération de maintenance réalisée sur les équipements du SH. Ce cahier de suivi établi notamment les informations suivantes :
— la date et l'heure de l'intervention ;
— le nom et le prénom des personnes présentes ;
— le détail de l'opération de maintenance réalisée ;
— la date et l'heure de la fin d'intervention ;
— la signature des personnes présentes.

L'accès physique est de plus restreint par la mise en œuvre de mécanismes de contrôle d'accès aux zones hautement sécurisées de l'hebergeur. Ces mécanismes

se matérialisent par la possession de cartes d'accès.

L'accès à ces salles est renforcée par un contrôle d'accès biométrique.

Les profils d'accès à une zone sont définis et maintenus par l'AH et transmis à l'hébergeur.

Les zones sécurisées des sites et locaux sécurisés d'Universign sont régulièrement inspectées pour vérifier que les systèmes de contrôle d'accès sont toujours opérationnels. Les systèmes de supervision et d'historisation sont mis en œuvre sur tous les sites pour les zones sécurisées.

Les contrôles d'accès sont appliqués à toutes les zones sécurisées.

5.1.3 Alimentation électrique et climatisation

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

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 (rupture de canalisation par exemple).

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.

5.1.7 Mise hors service des supports

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

5.1.8 Sauvegarde hors site

Afin de permettre une reprise après incident conforme à ses engagements, Universign met en place des sauvegardes hors site des informations et fonctions critiques.

Universign 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.

5.2 Exigences procédurales

5.2.1 Rôles de Confiance

Les rôles de confiance suivants sont définis :
- Responsable Sécurité de l'AH : il est responsable de tous les aspects sécurité du SH ;
- Administrateur système de l'AH : il installe, configure et maintient à jour l'ensemble de la plate-forme technique du SH ;
- Opérateur de l'AH : il a la responsabilité du fonctionnement quotidien des UHs ;
- Contrôleur de l'AH : il est en charge de l'analyse récurrente des événements intervenant sur les composantes de l'AH.

Pour pouvoir réaliser les opérations d'exploitation et de supervision, Universign s'appuie sur ses équipes internes.

A l'instar de l'ensemble des employés Universign, les personnels en rôle de confiance doivent être libres de tous conflits d'intérêt incompatibles avec leurs missions. Les rôles de confiance attribués sont notifiés par écrit aux personnes concernées par la direction d'Universign. Universign s'assure régulièrement que l'ensemble des rôles de confiance sont pourvus afin d'assurer une continuité de l'activité.

5.2.2 Nombre de personnes requises par tâches

L'AH répartit les fonctions sensibles sur plusieurs personnes ayant un Rôle de Confiance.

5.2.3 Identification et authentification pour chaque rôle

Des mesures d'identification et d'authentification sont mises en place afin de supporter la mise en œuvre de la politique de contrôle d'accès et la traçabilité des opérations. La politique de contrôle d'accès limite l'accès aux seules personnes autorisées conformément à leur besoin d'en connaître.

Les rôles de confiance sont notifiés par écrit aux personnes concernées.

5.2.4 Rôles exigeant une séparation des attributions

L'AH UNIVERSIGN garantit que les opérations de sécurité sont séparées des opérations d'exploitation classiques et qu'elles sont réalisées systématiquement sous couvert d'une personne ayant un rôle de confiance.

5.2.5 Analyse de risques

Une analyse de risque est menée par Universign pour identifier les menaces qui pèsent sur les UH. Cette analyse de risque est revue périodiquement et lors de changements structurels significatifs du SH. De plus, la méthodologie utilisée pour effectuer l'analyse de risque permet de s'assurer que l'inventaire Universign est maintenu à jour.

5.2.6 Gestion des accès aux systèmes informatiques

Identification et authentification :
Les systèmes, applications et bases de données identifient et authentifient de façon unique les opérateurs et administrateurs. Toute interaction entre le système et un opérateur n'est possible qu'après une identification et une authentification réussies. Pour chaque interaction, le système établit l'identité du personnel intervenant.

Les informations d'authentification sont stockées de façon telle qu'elles sont seulement accessibles par des utilisateurs autorisés.

Contrôle d'accès :
Les profils et droits d'accès aux équipements de l'AH sont définis et documentés, ainsi que les procédures d'enregistrement et de désenregistrement des personnels intervenants.

Les systèmes, applications et bases de données peuvent distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux. Il est possible de :

— refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un objet ;
— limiter l'accès d'un utilisateur à un objet aux seules opérations qui ne modifient pas cet objet ;
— accorder les droits d'accès à un objet en descendant jusqu'au niveau de granularité de l'utilisateur individuel.

Quelqu'un qui n'est pas un utilisateur autorisé ne peut pas accorder ou retirer des droits d'accès à un objet. De même, seuls des utilisateurs autorisés peuvent créer de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants.

Administration et exploitation :
L'utilisation de programmes utilitaires est restreinte et contrôlée.

5.2.7 Gestion de l'exploitation

Plannification et dimensionnement du 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.

Protection contre les codes malveillants :
Des mesures de maîtrise de détection et de prévention sont mises en œuvre sur l'ensemble des composants du SH afin de fournir une protection contre les logiciels malveillants.

Gestion de la sécurité des réseaux :
Les mesures mises en place répondent à la stratégie de gestion des risques d'Universign pour les systèmes d'information.

Les services de l'AH sont implantés sur un réseau protégé par des passerelles de type "coupe-feu" segmentant les réseaux en fonction de leur sensibilité. Ces passerelles sont configurées de façon à n'accepter que les flux strictement nécessaires. Les flux réseaux sont redondés de manière à assurer la disponibilité des services. De plus, les composants critiques sont placés dans les zones les plus sécurisées.

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. Universign configure l'ensemble des systèmes en s'appuyant sur un master durci (suppression ou désactivation de tous les comptes, applications, services, protocoles et ports non utilisés).

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.

Universign 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 type VPN ainsi que la possibilité de modifier à tout instant les droits d'accès. Universign met également en place un réseau d'administration déconnecté du réseau nominal.

Universign met en place des procédures de contrôle d'accès pour séparer les fonctions d'administration et les fonctions opérationnelles. L'ensemble des applications nécessite une authentification. Une politique de contrôle d'accès est mise en place pour limiter l'accès de ces applications aux seules personnes de confiance autorisées.

Manipulation et sécurité des supports :

L'ensemble des matériels sensibles des composantes du SH fait l'objet de procédure de maintenance afin de garantir la disponibilité des fonctions et des informations.

Les conditions de fin de vie (destruction et mise au rebut) des équipements sont documentées afin de garantir la non divulgation des informations sensibles qu'ils peuvent détenir.

Echange des informations :

Des mesures de sécurité sont mises en œuvre de manière à garantir l'authentification d'origine, l'intégrité et la confidentialité le cas échéant des données échangées entre entités intervenant dans le processus.

5.2.8 Développement, déploiement et maintenance

Le SH utilise des componsants de confiance. En particulier, les UHs répondent aux exigences réglementaires. Le comité d'approbation de l'AH est avertie de toute modification significative du système.

Les évolutions des composantes font l'objet d'une remise à jour des procédures opérationnelles. Des mesures de contrôles des actions de maintenance sont mises en application.

Bon fonctionnement des applications :
Les infrastructures de développement et d'essai sont séparées des infrastructures opérationnelles du service d'horodatage.

Les critères de recette et validation de nouveaux systèmes d'information, de mises à niveau et nouvelles versions sont documentés et des essais adéquats du système sont effectués avant sa recette et mise en production.

5.2.9 Historiques, alertes et gestion des incidents

Un suivi d'activité est possible au travers des journaux d'événements.

Tout dysfonctionnement des UHs est notifié immédiatement au superviseur et exploitant des plate-formes de services d'Universign. Ces notifications concernent notamment :
— les arrêts / relances des services ;
— les désynchronisations des horloges du SH ;
— les perturbations réseaux du SH.

Tous les événements sont stockés dans une base de données qui permet d'historiser l'ensemble des événements du service, dont les incidents.

En cas d'incidents, Universign agira d'une façon opportune et coordonnée pour répondre rapidement, limiter l'impact des infractions à la sécurité et rétablir au plus tôt le service nominal.

5.3 Mesures de sécurité vis à vis du personnel

Universign a établi sa Politique de Sécurité de l'information. Ce document adresse, entre autre, la sécurité de l'information appliquée aux ressources humaines. Universign établit à travers ce document que les personnes ayant un Rôle

de Confiance sont sélectionnées avec soin et sont mises au courant de manière non ambiguë des opérations et des règles qu'ils devront suivre.

5.3.1 Qualifications, compétences, et habilitations requises

Tout intervenant amené à occuper un Rôle de Confiance est soumis à une clause de confidentialité, gérée par l'employeur. Universign s'assure que les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles. Le personnel d'encadrement d'Universign possède l'expertise appropriée, et est familier des procédures de sécurité. Toute personne intervenant dans des rôles de confiance est informée de ses responsabilités via sa fiche de poste et par des procédures liées à la sécurité du système et au contrôle du personnel.

Les personnels employés sur le service d'horodatage d'Universign possèdent des connaissances suffisantes :

- sur la technologie de l'horodatage ;
- sur la technologie de la signature numérique ;
- sur les mécanismes pour le calibrage ou la synchronisation des horloges des UH avec le temps UTC ;
- pour le personnel avec des responsabilités de sécurité, sur les procédures de sécurité ;
- sur la sécurité de l'information et l'évaluation des risques.

5.3.2 Procédures de vérification des antécédents

Universign procède avant le recrutement d'une personne à la vérification des antécédents de cette dernière, de manière à valider sa correspondance vis-à-vis du poste à pourvoir.

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 en matière de formation continue et fréquences des formations

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

Les intervenants sont formés à la gestion des incidents et sont au fait de l'organisation de remontée d'incidents.

5.3.5 Fréquence et séquence de rotations entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont énoncées dans une charte d'utilisation des moyens informatiques et à travers le document définissant la sécurité de l'information appliquées aux ressources humaines. Ces sanctions sont énoncées à tous les employés d'Universign.

5.3.7 Exigences vis à vis du personnel des prestataires externes

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

Les types d'engagement sont des contrats relatifs à la réalisation d'une prestation, des engagements de confidentialité et une charte d'utilisation des moyens informatiques.

5.3.8 Documentation fournie au personnel

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 dans le service d'horodatage disposent des procédures correspondantes.

6 Exigences de sécurité techniques

6.1 Exactitude du temps

Les horloges des UH sont supervisées localement par des serveurs de temps de référence. Ces derniers 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.

Universign garantit que les CTs générées par son SH ont un décalage de temps inférieur à une seconde par rapport à UTC.

6.2 Génération de clé

Universign garantit que toutes les clés cryptographiques sont produites dans des circonstances contrôlées. En particulier, la génération des clés de signature des UH est effectuée

- dans les locaux sécurisés ;
- au sein d'un HSM répondant aux exigences de certification suivantes :
  - EAL 4 aux Critères Communs ISO/CEI 15408 ou équivalent ; ou
  - FIPS 140-2 level 3.

À aucun moment les clés privées d'UH ne sont exportées hors des ressources cryptographiques. Les clés sont stockées au sein d'un unique module cryptographique. Les clés sont générées uniquement dans le but d'être utilisées au sein du SH.

Les clés privées d'UH sont de type RSA et ont une longueur de 2048 bits.

6.3 Certification des clés de l'UH

La demande de certificat d'UH est réalisée auprès de l'AC UNIVERSIGN, conformément aux engagements énoncés dans la politique de certification correspondante [**PCU**].

Les certificats délivrés par l'AC ont un format conforme à ce qui est présenté dans la politique de certification.

L'AH respecte les obligations qui lui incombent et qui découlent de la politique de certification de l'AC.

L'AH vérifie, lors de l'import du certificat de l'UH, qu'il provient bien de l'AC UNIVERSIGN.

Chaque UH possède une unique clé active à un instant donné.

Universign s'assure que les clés des UH sont chargées au sein du module cryptographique avant d'émettre le premier jeton.

6.4 Protection des clés privées des UHs

Universign garantit que des clés privées des UHs restent confidentielles et conservent leur intégrité. En particulier, les clés de signature des UHs sont gardées et utilisées à l'intérieur d'un module d'horodatage répondant aux exigences de l'état de l'art en la matière.

Les modules cryptographiques utilisés par Universign 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.

Universign s'assure de la sécurité des HSM utilisés tout au long de leur cycle de vie.

En particulier, Universign met en place les procédures nécessaires pour :
— s'assurer de l'intégrité des HSM 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, de sauvegarde et de restauration des clés de signature sont réalisées sous le contrôle de deux personnels ayant des Rôles de Confiance ;
— s'assurer que le HSM fonctionne correctement ;
— s'assurer que les clés contenues dans le HSM sont bien détruites lorsque celui-ci est dé-commissionné.

6.5 Sauvegarde des clés des UHs

Universign interdit l'archivage et la sauvegarde des clés des UHs.

6.6 Destruction des clés des UHs

Universign garantit que les clés de signature des UHs sont détruites à la fin de leur cycle de vie.

6.7 Algorithmes obligatoires

L'AH Universign :

1. accepte des empreintes numériques générées par des Abonnés et employant les algorithmes de hachage conformes aux exigences des autorités compétentes en la matière. Les algorithmes de calcul d'empreinte numérique acceptés sont les suivants :
   — SHA-1 [1]
   — SHA-256
   — SHA-384
   — SHA-512
2. génére des CTs signées selon les algorithmes et les longueurs de clé conformes aux exigences des autorités compétentes en la matière. La bi-clé de l'UH

1. L'utilisation de cet algorithme est encore accepté pour des raisons de compatibilité. Bien qu'aucune attaque pratique n'ait pour l'instant été exposée, il est aujourd'hui considéré comme faible. Il est recommandé d'utiliser un des autres algorithmes de la liste.

est une bi-clé RSA de 2048 bits. L'algorithme de signature utilise une fonction de hachage de la famille SHA-2.

6.8 Vérification des CTs

Universign garantit que les Utilisateurs peuvent avoir accès à l'information nécessaire pour vérifier la signature numérique des CTs. Universign assure notamment que les certificats des UH sont disponibles, soit joints à la CT, soit disponibles sur le site web d'Universign : http://docs.universign.eu.

6.9 Durée de validité des certificats de clé publique des UHs

Un certificat d'UH a une durée de vie de six (6) ans. Universign s'assure que l'algorithme choisi et la longueur des clés sont reconnus comme adéquats pour cette durée de validité.

6.10 Durée d'utilisation des clés privées des UHs

La clé privée liée à ce certificat et permettant la signature des CTs a une durée d'utilisation de un an.

Sachant que la durée de vie d'un certificat d'UH est de 6 ans, cela permet aux Abonnés et Utilisateurs de pouvoir vérifier la validité de leur CT pendant au moins cinq (5) ans après que celle-ci ait été émise.

7 Profile des certificats et des CTs

7.1 Profils des certificats

Champs de base

Champ	Valeur
Version	2
Numéro de série	défini par l'AC
Signature	RSA/SHA-256
Issuer DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Timestamping CA (ou Universign Timestamping CA 2015)
Validité	6 ans
Subject DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Timestamping Unit xxx
Clé publique	RSA 2048 bits

Extension du certificat

Champ	OID	Critique	Valeur
Authority Key Identifier	2.5.29.35	Non	
KeyIdentifier			RFC 5280 - Méthode 0
Key Usage	2.5.29.15	Oui	
digitalSignature			Vrai
nonRepudiation			Faux
keyEncipherment			Faux
dataEncipherment			Faux
keyAgreement			Faux
keyCertSign			Faux
cRLSign			Faux
encipherOnly			Faux
decipherOnly			Faux
Certificate Policies	2.5.29.32	Non	
policyIdentifier			1.3.6.1.4.1.15819.5.1.1
policyQualifierId			1.3.6.1.5.5.7.2.1
qualifier			http ://docs.universign.eu/
Basic Constraint	2.5.29.19	Oui[2]	
CA			Faux
Maximum Path Length			Absent
Extended Key Usage	2.5.29.37	Oui	
KeyPurposeId			id-kp-timeStamping
CRL Distribution Points	2.5.29.31	Non	
fullName			http ://crl.universign.eu/tsa_root.crl
reasons			Absent
cRLIssuer			Absent

7.2 Profils des CTs

version	Version 1
policy	OID : 1.3.6.1.4.1.15819.5.2.2
messageImprint	OID de l'algorithme de hash et l'empreinte numérique données à horodater. NB : Ces informations sont fournies dans la requête de l'Abonné.
serialNumber	Nombre aléatoire de 160 bits caractéristique de la présente requête.

2. La PC autorise de fixer le paramètre de criticité à `Non` afin d'assurer la conformité avec les exigences du référentiel RGS.

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	DN=[C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Timestamping Unit xxx] où "xxx" est le numéro de l'UH concernée. NB : Ce champ est égal au champ "subject" du certificat de l'UH signant la CT.
extensions	Sans objet.

8 Audit de conformité et autres évaluations

8.1 Fréquences et / ou circonstances des évaluations

Universign bénéficie de plusieurs types d'audit :
- un audit interne réalisé au moins une fois par an
  - soit par des prestataires externes spécialistes du domaine du SH ;
  - soit par un responsable d'audit interne à Cryptolog.
- un audit de qualification réalisé par un organisme accrédité au moins une fois tous les 2 ans.

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 ;
- lors de toute modification significative est effectué.

8.2 Identités / qualifications des évaluateurs

L'évaluateur se doit d'être rigoureux pour s'assurer que les politiques, déclarations et services sont correctement mis en œuvre et détecter les cas de non conformités qui pourraient compromettre la sécurité du service offert.

L'AH s'engage à mandater des évaluateurs qui sont compétents en sécurité des systèmes d'information, en particulier dans le domaine d'activité de la composante contrôlée.

8.3 Relations entre évaluateurs et entités évaluées

L'évaluateur est désigné par Universign, qui l'autorise à contrôler les pratiques de la composante cible de l'audit. Il peut être interne à Universign mais sera indépendant de l'AH.

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 ;
— du SH.

Avant chaque audit, les évaluateurs proposeront au Comité d'Approbation de l'AH une liste de composantes, et procédures qu'ils souhaiteront vérifier, et 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'équipe d'audit rend à l'AH un avis qui peut être « réussite », « échec », ou « à confirmer ».

En cas d'échec, l'équipe d'audit émet des recommandations à l'AH. Le choix de la mesure à appliquer appartient à l'AH.

En cas de résultat « 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. Un contrôle de vérification permettra de lever les non conformités identifiées.

En cas de réussite, l'AH confirme à la composante contrôlée la conformité aux exigences de la PH.

8.6 Communication des résultats

Les résultats de l'audit seront tenus à la disposition du Comité d'Approbation de l'Autorité d'Horodatage, et de l'organisme de qualification en charge de la qualification de l'AH.

Références

[**ORD**]
Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

[**PCU**]
Politique de Certification de l'AC UNIVERSIGN
OID :1.3.6.1.4.1.15819.5.1.2

[**RGS_A_10**]
Référentiel Général de Sécurité - Politique de Certification Type Cachet V2.3 (2010/02). OID : 1.2.250.1.137.2.2.1.2.2.6

[**ETSI 319 411-2**]
ETSI EN 319 411-2 V2.1.1 (2016-02) - 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.

[**ETSI 319 421**]
ETSI EN 319 421 V1.1.1 (2016-03) - Electronic Signatures and Infrastructures (ESI) ; Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. OID : 0.4.0.2023.1.1

[**RGS_A_12**]
Référentiel Général de Sécurité - Politique d'Horodatage Type V2.3 (2010/02). OID : 1.2.250.1.137.2.2.1.2.2.4

[**ETSI 319 422**]
ETSI EN 319 422 V1.1.1 (2016-03) - Electronic Signatures and Infrastructures (ESI) ; Time-stamping protocol and time-stamp token profiles.

[**CNIL**]
Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.