Politique de Certification

Universign Timestamping CA

Universign
OID: 1.3.6.1.4.1.15819.5.1.1
Version: 1.4
DIFFUSION PUBLIQUE

1 Introduction

1.1 Présentation générale

UNIVERSIGN s'est positionnée comme Prestataire de Service de Certification Électronique (PSCE) pour ses propres besoins, et particulièrement pour ses besoins de son Service d'Horodatage (SH) pour lequel elle vise à être qualifiée.

L'organisation adoptée pour cela est présentée dans le chapitre 1.3

La présente Politique de Certification (PC) définit les engagements d'UNIVERSIGN dans le cadre de la fourniture de certificats pour son SH conformément à la PC type RGS "Cachet" pour laquelle elle vise à être référencée pour le niveau *.

1.2 Identification du document

Ce document est la Politique de Certification d'UNIVERSIGN. Cette PC est est identifiée, au sein du référentiel documentaire de l'infrastructure de confiance d'UNIVERSIGN, par un numéro d'identification unique : **1.3.6.1.4.1.15819.5.1.1**

1.3 Entités intervenants dans l'IGC

1.3.1 Autorités de certification

Dans le contexte règlementaire français, une Autorité de Certification (AC) et un Prestataire de Services de Certification Électronique (PSCE) sont deux notions allant naturellement ensemble.

L'ordonnance 2005-1516 [**ORD**] introduit et définit les prestataires de service de confiance (PSCO). Un PSCE est un type de PSCO particulier. Un PSCE se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des Responsables de Certificat Cachet (RCCs) et Utilisateurs. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

Au sein d'un PSCE, une AC a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une PC et est identifiée comme telle, en

tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette PC. Dans le cadre de cette PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre 1.1 et le terme d'AC est le seul utilisé. Il désigne l'AC UNIVERSIGN chargée de l'application de la PC au sein du PSCE UNIVERSIGN.

L'AC 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'AC.

Ce dernier approuve la PC et les documents constituant l'IGC fourni par UNIVERSIGN.

Il s'agit d'une instance de la direction dotée de l'autorité et de la responsabilité finale pour :
- définir et approuver l'IGC et les pratiques ;
- approuver la PC et la DPC ;
- définir le processus de mises à jour de la DPC et de la PC ;
- définir le processus garantissant que UNIVERSIGN intègre correctement les pratiques de la DPC ;
- définir les processus assurant que la PC est bien supportée par la DPC ;
- publier la PC et la partie publique de la DPC (incluse dans cette PC) et leurs révisions aux Abonnés et Utilisateurs.

1.3.2 Autorité d'enregistrement

Dans le cadre de la délivrance de certificat pour ses propres serveurs, UNIVERSIGN est sa propre Autorité d'Enregistrement (AE).

1.3.3 Abonnés (Responsables de Certificat Cachet)

Dans le cadre de cette PC, un Abonné, aussi appelé Responsable de Certificat Cachet (RCC) est une personne physique qui est responsable de l'utilisation du certificat de cachet du serveur identifié dans le certificat, pour le compte de l'entité également identifiée dans ce certificat. Le RCC appartient à cette entité.

En cas de changement de fonction ou de départ du RCC, un nouveau RCCS doit être nommé sans délai.

1.3.4 Utilisateurs de certificats

Les Utilisateurs sont l'ensemble de la population, entité ou personne physique, qui reàçoit des jetons d'horodatage et qui souhaite vérifier le certificat utilisé par

l'Autorité d'Horodatage les ayant émis.

1.3.5 Autres participants

Composantes de l'IGC Toutes les composantes de l'IGC sont gérées et exploitées par UNIVERSIGN.

Mandataires de Certification La présente politique de certification ne définit pas de mandataires de certification.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

Bi-clés et certificats du serveur informatique Cette PC traite des bi-clés et des certificats utilisés par les Unités d'Horodatage (UHs) d'UNIVERSIGN.

Les UHs utilisent les bi-clés pour signer les CTs qu'elles délivrent, afin que les Utilisateurs puissent en vérifier la signature.

Bi-clés et certificats d'AC et de composantes Les certificats de l'AC définis par la présente PC sont utilisés pour signer :

- les certificats des UHs du SH d'UNIVERSIGN ;
- les LCRs de l'AC.

L'AC dispose d'une seule bi-clé de signature de certificate active à un moment donnée et le certificat correspondant est un certificat racine. Ce certificat est autosigné et non rattaché à une AC de niveau supérieur.

1.4.2 Domaines d'utilisation interdits

Tout autre usage que celui défini dans le paragraphe précédent est interdit par la présente PC.

1.5 Gestion de la Politique de Certification

1.5.1 Entité gérant la PC

UNIVERSIGN
Cryptolog International
6-8, Rue Basfroi, F-75011 Paris, France
contact@universign.eu

1.5.2 Point de contact

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

Le responsable de la Politique de Cetification
UNIVERSIGN
Cryptolog International
6-8, Rue Basfroi, F-75011 Paris, France
contact@universign.eu

1.5.3 Entité déterminant la conformité des pratiques avec la PC

Le Comité d'Approbation d'UNIVERSIGN determine l'adéquation et l'applicabilité de cette PC.

1.5.4 Procédures d'approbation de la conformité de la DPC

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

1.6 Définitions et abréviations

Définitions

Les termes utilisés dans la présente PC sont les suivants :

Autorité d'horodatage (AH) : Désigne une entité qui a en charge l'application d'une politique d'horodatage en s'appuyant sur une ou plusieurs UHs. L'AH délivre des contremarques de temps avec une précision donnée et à partir de source de temps choisies.

Infrastructure de gestion de clés (IGC) : Ensemble de composantes fournissant des services de gestion de clés et de certificats au profit d'une communauté d'utilisateurs.

Unité d'Horodatage (UH) : Désigne l'ensemble des matériels et des logiciels utilisés pour la création de contremarques de temps. L'UH est caractérisée par un identifiant délivré par une AH et une clé unique de signature de contremarques de temps.

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 6-8, rue Basfroi, 75011 Paris, enregistrée au RCS de Paris sous le numéro 439129164.

Abréviations

Les abréviations utilisées dans la présente PC sont les suivantes :

AC : Autorité de Certification
AE : Autorité d'Enregistrement
AH : Autorité d'Horodatage
CT : Contremarque de Temps
DN : Distinguished Name
HSM : Hardware Security Module (module cryptographique)
IGC : Infrastructure de Gestion de Clés
LCR : Liste des Certificats Révoqués
OID : Object Identifier
PC : Politique de Certification
PSCE : Prestataire de Services de Certification Èlectronique
RCC : Responsable de Certificat Cachet
RGS : Référentiel Général de Sécurité
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'AC, met à disposition des utilisateurs de certificats la présente PC. La présente PC est disponible via Internet, sur le site web : http://docs.universign.eu.

Les informations relatives aux pratiques de certification destinées à être publiquement diffusées se trouvent dans la présente PC.

2.2 Informations publiées

Les informations publiées sont les suivantes :
– la présente PC ;

– les LCRs ;
– le certificat de l'AC UNIVERSIGN en cours de validité ;
– l'empreinte du certificat de l'AC UNIVERSIGN.

L'AC met à disposition des RCCs, qui sont des personnes internes à UNIVERSIGN, les exigences et les reponsabilités de chacun des acteurs à travers la présente politique de certification.

Du fait de cet usage, l'AC ne publie pas de Conditions Générales d'Utilisation pour son service d'émission de certificats.

2.3 Délais et fréquences de publication

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

Les certificats de l'AC sont diffusés ou mis en ligne au maximum 24 heures après leur génération et obligatoirement avant leur utilisation effective.

Les LCRs sont publiées au plus tard dans les 24 heures suivant la demande de révocation.

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 PC et LCRs 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 Identification et authentification

3.1 Nommage

3.1.1 Types de noms

L'AC et l'UH sont identifiées par un nom explicite (appelé "DN" par la suite) de type X.501. Ce type de DN est défini dans le chapitre 7.

3.1.2 Noms explicites

Le DN de l'AC est précisé dans le chapitre 7.
Le DN d'une UH d'UNIVERSIGN est précisé dans le chapitre 7.

3.1.3 Anonymisation ou pseudonymisation des porteurs

Sans objet.

3.1.4 Règles d'interprétation des différentes formes de noms

L'interprétation du champs `DN` des certificats de cachets émis est conforme à [RGS_A_14].

Plus particulièrement, l'interprétation des champs se fait comme suit :

Champ	Interprétation
C	Pays d'enregistrement de la société opérant l'unité d'horodatage
O	Nom de la société opérant l'unité d'horodatage
OU	ICD du pays d'enregistrement de la société opérant l'unité d'horodatage suivi de son numéro d'identification unique
CN	Identifiant unique de l'unité d'horodatage

UNIVERSIGN, en tant qu'AC, ne génère des certificats de cachet serveur qu'à destination de ses propres unités d'horodatage [1]. De ce fait, les champs doivent être interprétés comme suit.

champ `C` Le champ `C` contient la valeur `FR`, pays d'enregistrement d'UNIVERSIGN.

champ `O` Le champ `O` contient la valeur `Cryptolog International`, société française opérant le service UNIVERSIGN.

1. UNIVERSIGN ne s'interdit pas, pour les versions ultérieurs de cette PC, à générer des certificats pour des unités d'horoatage non opérées par Universign mais satisfaisant aux exigences réglementaires de la présente PC, de ce fait la valeur des différents champs est fixée

champ `OU` Le champ `OU` contient les éléments :
- `0002`, comme ICD de la France, suivi d'un espace, puis de
- `43912916400026`, numéro de SIRET de la société CRYPTOLOG INTERNATIONAL

champ `CN` Les unités d'horodatage étant identifiées par un numéro, le `CN` :

`Universign Timestamping Unit xxx`

doit être interprété comme *l'unité d'horodatage Universign numéro* `xxx` où `xxx` est un numéro à 3 chiffres [2]. Le numéro d'unité d'horodatage est incrémenté de 1 à chaque nouveau certificat généré.

3.1.5 Unicité des noms

UNIVERSIGN, en tant qu'AC, s'assure que l'identifiant de l'UH, positionné dans le champ CN du certificat, est incrémenté à chaque nouvelle installation d'un certificat d'UH. UNIVERSIGN prend à sa charge la responsabilité de vérifier et d'établir des noms uniques pour les certificats de ses UHs.

3.1.6 Identification, authentification et ràôle des marques déposées

Sans objet.

3.2 Validation initiale de l'identité

L'enregistrement d'une UH auquel un certificat doit être délivré se fait via l'enregistrement du RCC. Ce responsable est obligatoirement une personne interne d'UNIVERSIGN.

L'identité du RCC est établie clairement dans la DPC. Le RCC doit être préalablement identifié et enregistré auprès de l'AC pour que sa demande soit recevable.

Une fois enregistré auprès de l'AC, le RCC peut demander la création de certificat pour des UHs appartenant à UNIVERSIGN.

Le RCC est présent lors de la génération de la clé d'UH.

3.2.1 Méthode pour prouver la possession de la clé privée

Sans objet.

2. de `001` à `999`

3.2.2 Validation de l'identité d'un organisme

Voir ci-dessous.

3.2.3 Validation de l'identité d'un individu

Dans le cadre de la présente PC, il s'agit de l'enregistrement d'un RCC sans Mandataire de Certification. Il s'agit nécessairement d'une personne interne à UNIVERSIGN.

Pour pouvoir demander l'émission d'un certificat pour une UH, le RCC doit être enregistré auprès de l'AC en ayant :

- Rempli et soumis au Responsable de l'AC le formulaire d'enregistrement d'un RCC signé ;
- Obtenu un mandat signé par son représentant légal ;
- Communiqué dans son dossier une copie d'une pièce d'identité valide ;
- Pris connaissance de la présente PC et plus particulièrement des responsabilités d'un RCC. Après lecture, le RCC doit signer cette PC.

Tous ces éléments constituent le dossier d'enregistrement d'un RCC et sont conservés par l'AC dans un coffre fort.

L'enregistrement d'un RCC se traduit nécessairement par un face à face entre le responsable de l'AC et le RCC.

En cas de changement de RCC, l'AC exige la nommination d'un nouveau RCC qui deviendra responsable des certificats rattachés au précédent RCC. Le changement de RCC nécessite la constitution du dossier d'enregistrement complet comme indiqué ci-dessus.

3.2.4 Informations non vérifiées du porteur

Sans objet.

3.2.5 Validation de l'autorité du demandeur

Le demandeur est obligatoirement un RCC enregistré auprès de l'AC comme identifié ci-dessus.

3.2.6 Critères d'interopérabilité

La présente PC est destinée à une AC interne d'UNIVERSIGN et ne définit aucun critère particulier d'intéropérabilité.

3.3 Identification et validation d'une demande de renouvellement de clés

Dans le cadre de l'AC UNIVERSIGN, il n'est pas procédé à des phases de renouvellement.

3.3.1 Identification et validation pour un renouvellement courant

Sans objet.

3.3.2 Identification et validation pour un renouvellement après révocation

Sans objet.

3.4 Identification et validation d'une demande de révocation

La demande de révocation est faite par le RCC en remplissant le formulaire de demande de révocation. Ce formulaire comporte les données nominatives du RCC et est transmis signé au Reponsable de l'AC.

Pour valider la demande, l'AC s'assure que :
- le RCC est correctement enregistré au sein de l'AC ;
- la demande est signée par le RCC. L'AC vérifie la signature par rapport à celle établie dans le dossier d'enregistrement du RCC ;
- valide l'identification de l'UH établie dans la demande de révocation.

Si ces conditions sont remplies, l'AC signe la demande de révocation et la transmet aux équipes d'administration systèmes et réseaux d'UNIVERSIGN qui procèdent aux étapes techniques de révocation.

4 Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Le RCC en charge d'une UH au sein d'UNIVERSIGN opère la demande de certificat de cette UH en remplissant le formulaire de demande d'enregistrement d'une UH.

4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificats

La demande d'enregistrement d'une UH nécessite que le RCC précise :
- la location géographique d'intégration de l'UH ;
- le DN identifiant l'UH ;
- les informations techniques du certificat : taille des clés, algorithmes.

Pour être recevable la demande doit être signée par le RCC et son représentant légal.

4.2 Traitement d'une demande de certificat

4.2.1 Exécution des processus d'identification et de validation de la demande

Les demandes de certificat pour l'UH sont validées par l'AC qui assure elle-même la fonction d'AE.

4.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, le RCC est immédiatement informé de la cause.

4.2.3 Durée d'établissement du certificat

L'AC commence à traiter la requête dans un délai raisonnable suivant sa réception. Une demande de certificat reste active tant qu'elle n'est pas rejetée.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

L'AC UNIVERSIGN est une AC hors-ligne et non connectée au réseau.

L'AC UNIVERSIGN reàçoit une demande de certificat au format PKCS#10 qu'elle signe pour délivrer le certificat correspondant.

4.3.2 Notification par l'AC de la délivrance du certificat

Cf. ci-dessus.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Une fois l'installation faite sur l'UH, le RCC vérifie les données présentes dans le certificat et valide l'exactitude du contenu. Les vérifications concernant le certificat installé sont également réalisées techniquement par l'UH.

Dans le cas où le certificat généré comporterait des erreurs, il serait immédiatement révoqué et une nouvelle procédure de génération du certificat serait alors déclenchée.

4.4.2 Publication du certificat

UNIVERSIGN publie le certificat d'UH sur l'url suivante : http://docs.universign.eu

4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat

Sans objet.

4.5 Usage de la bi-clé et du certificat

Pour les UHs, l'utilisation des clés privées est limitée à la signature de données.

Cet usage est indiqué explicitement dans les extensions des certificats d'UH.

4.6 Renouvellement d'un certificat

Aucun renouvellement n'est autorisé par l'AC UNIVERSIGN.

4.6.1 Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification au RCC de l'établissement du nouveau certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6 Publication du nouveau certificat

Sans objet.

4.6.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Sans objet.

4.7 Délivrance d'un nouveau certificat suite à changement de la bi-clé

Aucune délivrance de nouveau certificat n'est autorisée pour l'AC UNIVERSIGN.

4.7.1 Causes possibles de changement d'une bi-clé

Sans objet.

4.7.2 Origine d'une demande d'un nouveau certificat

Sans objet.

4.7.3 Procédure de traitement d'une demande d'un nouveau certificat

Sans objet.

4.7.4 Notification au RCC de l'établissement du nouveau certificat

Sans objet.

4.7.5 Démarche d'acceptation du nouveau certificat

Sans objet.

4.7.6 Publication du nouveau certificat

Sans objet.

4.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Sans objet.

4.8 Modification du certificat

La modification d'un certificat se traduit par sa révocation puis la formulation d'une nouvelle demande initiale.

4.8.1 Causes possibles de modification d'un certificat

Sans objet.

4.8.2 Origine d'une demande de modification d'un certificat

Sans objet.

4.8.3 Procédure de traitement d'une demande de modification d'un certificat

Sans objet.

4.8.4 Notification au RCC de l'établissement du certificat modifié

Sans objet.

4.8.5 Démarche d'acceptation du certificat modifié

Sans objet.

4.8.6 Publication du certificat modifié

Sans objet.

4.8.7 Notification par l'AC aux autres entités de la délivrance du certificat modifié

Sans objet.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

Les causes de révocation d'un certificat d'UH sont les suivantes :
- les informations de l'UH présentes dans le certificat ne sont plus exactes ;
- le RCC a dérogé à ses engagements vis-à-vis de la présente PC et des conditions d'usage du certificat ;
- suspicion de compromission, perte ou vol d'une clé privée ;
- erreur dans la procédure d'enregistrement ;
- arrêt d'activité de l'AC.

4.9.2 Origine d'une demande de révocation

Les personnes pouvant demander une révocation de certificat d'UH sont les suivantes :
- le responsable de l'AC ;
- le RCC.

4.9.3 Procédure de traitement d'une demande de révocation

La demande de révocation est validée par le responsable de l'AC.

Cette demande est soumise par le RCC et contient les informations suivantes :
- le DN du certificat de l'UH à révoquer ;
- les données nominatives du RCC ;

– éventuellement la cause de révocation. Cette donnée est à titre informatif et n'apparaît pas dans la LCR.

Le traitement d'une demande de révocation est effectuée par une personne autorisée au sein de l'AC.

4.9.4 Délai accordé au RCC pour formuler la demande de révocation

La demande de révocation est formulée au plus tàôt.

4.9.5 Délai de traitement par l'AC d'une demande de révocation

Le délai maximum de traitement est de 72 heures, même si les requêtes sont généralement traitées immédiatement.

4.9.6 Exigences de vérification de la révocation par les utilisateurs de certificats

L'Utilisateur est tenu de vérifier l'état des certificats et de la chaîne correspondante.

4.9.7 Fréquence d'établissement des LCR

La fréquence de publication des LCRs est de 24h.

4.9.8 Délai maximum de publication d'une LCR

Les LCRs sont publiées dans un délai maximum de 30 minutes suivant leur génération.

4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Sans objet.

4.9.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Sans objet.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

UNIVERSIGN préviendra directement et sans délai le point de contact de la DGME identifié sur le site : http://www.references.modernisation.gouv.fr.

4.9.13 Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

Les LCRs sont au format v2, publiées sur un site de publication accessible au sein de la société UNIVERSIGN.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible sur plusieurs serveurs de publication assurant une disponibilité en fonctionnement normal de 24h/24 et 7j/7.

En tout état de cause, l'AC assure que la LCR ne sera pas indisponible :
- plus de 4 heures durant les jours ouvrés par indisponibilité ;
- plus de 32 heures durant les jours ouvrés par mois.

4.10.3 Dispositifs optionnels

Sans objet.

4.11 Fin de la relation entre le RCCS et l'AC

En cas de fin de relation entre le RCC serveur et l'AC, la responsabilité des certificats correspondants est transférée vers un nouveau RCC.

4.12 Séquestre de clé et recouvrement

Il n'est pas procédé au séquestre de clé.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

4.12.2 Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

UNIVERSIGN s'appuie sur des locaux sécurisés pour héberger ses services de certification. Ces locaux disposent de zones verrouillées, de cages et d'armoires.

5.1.2 Accès physiques

L'accès aux zones des services de certification 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 de l'AC. Ce cahier de suivi établit notamment les informations suivantes :

- La date et l'heure de l'intervention ;
- Le nom et le prénom des intervenants ;
- Le détail de l'opération de maintenance réalisée ;
- La date et l'heure de la fin d'intervention ;
- La signature des intervenants.

L'accès physique est de plus restreint par la mise en œuvre des mécanismes de contrôle d'accès aux zones hautement sécurisées de l'hebergeur. Ces mécanismes se matérialisent par la possession de cartes à puce d'accès. Il est nécessaire de

réunir deux administrateurs, avec leur carte à puce, pour pouvoir accéder à ces zones.

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

Les profils d'accès à une zone sont définis et maintenus par l'AC 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 dégats des eaux

La définition du périmètre de sécurité prend en considération les risques inhérents aux dégàts 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 faàçon 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'AC 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'AC 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 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

L'AC opère en interne son IGC. Les Ràôles de Confiance définis dans ce présent chapitre sont applicables à l'ensemble des composantes de l'IGC.

Les ràôles de confiance suivants sont définis :

Reponsable de sécurité : il est responsable de tous les aspects sécurité du système d'information et de la mise en oeuvre opérationnelle de l'IGC.

Responsable d'application : il est en charge de la mise en oeuvre de la PC et de sa correspondance à la DPC, au sein de la composante dont il est responsable.

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

Administrateur Système : il est en charge de l'administration et de la configuration de l'ensemble des composants techniques de l'IGC.

Opérateur : il est en charge de l'exploitation des applications mise en oeuvre dans l'IGC.

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

En plus de ces ràôles opérationnels, l'AC a établi des porteurs de secrets. Ces porteurs assurent la confidentialité, l'intégrité et la disponibilité des parts de secrets qui leurs sont confiées.

5.2.2 Nombre de personnes requises par tàches

L'AC répartit les fonctions sensibles sur plusieurs personnes ayant un Ràôle de Confiance.

5.2.3 Identification et authentification pour chaque ràôle

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 traàçabilité des opérations ; la politique de contrôle d'accès limite l'accès aux seules personnes autorisées conformément à leur besoin d'en connaître. Les ràôles attribués sont notifiés par écrit aux personnes concernées.

5.2.4 Ràôles exigeant une séparation des attributions

L'AC garantit que les ràôles de Responsable de Sécurité et d'Administrateur Système ne peuvent être cumulés par la même personne physique.

L'AC 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 Ràôle de Confiance.

5.3 Mesures de sécurité vis à vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Tout intervenant amené à occuper un ràôle identifié comme sensible 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 possède l'expertise appropriée, et est familier des procédures de sécurité. Toute personne intervenant dans des ràôles de confiance est informée de ses responsabilités (des-

cription de poste) et des procédures liées à la sécurité du système et au contrôle du personnel.

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 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 le travail de ces intervenants.

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 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 ràôle affecté à l'intervenant. Les personnes appelées à occuper un ràôle opérationnel dans l'IGC disposent des procédures correspondantes.

5.4 Procédures de constitution des données d'audit

5.4.1 Type d'événements à enregistrer

UNIVERSIGN prend les mesures nécessaires pour enregistrer les événements suivants :

- événements systèmes des différentes composantes de l'IGC (démarrage des serveurs, accès réseau, ...) ;
- événements techniques des applications composant l'IGC ;
- événements fonctionnels des applications composant l'IGC (demande de certificats, validation, révocation, ...) ;
- opérations effectuées, intégrant entre autre les actions d'authentification des personnes ayant un ràôle de confiance.

L'AC UNIVERSIGN est une AC hors-ligne dont les événements sont enregistrés sur un support externe, après chaque opération. Ce support est conservé dans des conditions de sécurité suffisante.

Ces journaux permettent d'assurer la traàçabilité et l'imputabilité des actions effectuées (horodatage, affectation à l'intervenant).

Des enregistrements d'événements non informatiques sont réalisés pour :

- l'accès au site de production ;
- les actions de maintenance et de changement de configuration ;
- les changements de personnels ;
- les actions sur les supports contenant des informations confidentielles.

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'événements sont externalisés tous les mois puis sauvegardés sur un serveur de sauvegarde dans les locaux d'UNIVERSIGN. Ces archives sont

conservées jusqu'à l'expiration du dernier certificat émis par l'AC UNIVERSIGN.

5.4.4 Protection des journaux d'événements

Les journaux d'événements sont rendus accessibles uniquement au personnel autorisé d'UNIVERSIGN. Ils ne sont pas modifiables de manière non autorisée.

5.4.5 Procédure de sauvegarde des journaux d'événements

Les journaux sont sauvegardés régulièrement sur un support externe.

5.4.6 Système de collecte des journaux d'évènements

Les systèmes de collecte des journaux d'évènements d'UNIVERSIGN sont internes.

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

Sans objet.

5.4.8 Èvaluation des vulnérabilités

L'AC UNIVERSIGN n'est pas accessible en termes de réseau et met en place les contrôles suivants :

- Contrôle des accès physiques au sein de la salle "off-line" quotidien ;
- Contrôle des publications de LCR quotidien ;
- Récupération des événements et sauvegarde de l'AC mensuelle. L'ensemble des événements est ensuite analysé par le Contrôleur de l'AC.

Ces contrôles permettent à l'AC de détecter :

- Les accès non autorisés ;
- Les anomalies techniques ;
- Les incohérences entre les différents événements de l'AC.

5.5 Archivage des données

5.5.1 Types de données à archiver

Les données archivées sont les suivantes :

- les logiciels exécutables et les fichiers de configuration des équipements informatiques ;
- la PC et la DPC ;
- les certificats et LCRs publiés ;
- les données d'enregistrement des RCCs ;
- les formulaires d'établissement d'une UH ;
- les formulaires de révocation d'un certificat d'UH ;
- les journaux d'événements.

5.5.2 Période de conservation des archives

Dossiers de demande de certificat :
Les formulaires de demande de certificat sont conservés durant toute la durée de vie de l'AC.

Certificats et LCR émis par l'AC :
Les certificats des UHs et d'AC, ainsi que les LCR produites, sont archivés pendant au moins cinq ans après l'expiration de ces certificats.

Journaux d'événements :
Les journaux d'événements sont archivés et conservés jusqu'à l'expiration du dernier certificat émis par l'AC.

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 lisibles et exploitables sur l'ensemble de leur cycle de vie et sont conservées dans un environnement sécurisé.

5.5.4 Procédure de sauvegarde des archives

Sans objet.

5.5.5 Exigences d'horodatage des données

L'AC UNIVERSIGN est une AC hors-ligne, cependant, lors d'une opération de l'AC, une vérification de l'horloge est opérée pour garantir que les serveurs de l'IGC sont correctement synchronisés.

5.5.6 Système de collecte des archives

Les systèmes de collecte des archives d'UNIVERSIGN 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 internes d'UNIVERSIGN.

5.6 Changement de clés d'AC

Les certificats d'AC sont renouvelés au plus tous les quatre ans.
La durée de vie des certificats d'AC étant de dix ans, UNIVERSIGN sera donc amené à utiliser plusieurs clés et certificats d'AC simultanément.

5.7 Reprise suite à compromission et sinistre

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

Des procédures et des moyens de remontée et de traitement des incidents (sensibilisation, formation des personnels, analyse des différents journaux d'événements, ...) sont mis en œuvre.

Un incident majeur, une perte, une suspicion de compromission ou un vol de la clé privée de l'AC par exemple est immédiatement notifié au Comité d'Approbation, qui, si cela s'avère nécessaire, peut décider de mettre fin à l'AC.

Dans tous ces cas, UNIVERSIGN s'engage à prévenir directement et sans délai le point de contact de la DGME identifié sur le site : http://www.references.modernisation.gouv.fr.

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'IGC. Ce plan est testé au moins une fois tous les trois ans.

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

La compromission d'une clé de l'AC entraîne immédiatement la révocation des certificat délivrés. Dans ce cas les différents acteurs et entités concernées seront avertis du caractère non sûr de la LCR signée par la clé compromise de l'AC.

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 d'activité d'UNIVERSIGN. Le Plan de Reprise d'Activité est testé au moins une fois tous les trois ans.

5.8 Fin de vie de l'IGC

En cas d'arrêt de service, les exigences suivantes seront prises en compte :

1. la clé privée d'émission des certificats ne sera transmise en aucun cas ;
2. tous les certificats émis encore en cours de validité seront révoqués ;
3. la clé privée de l'AC sera détruire.

En cas de cessation d'activité, UNIVERSIGN s'engage à prévenir directement et sans délai le point de contact de la DGME identifié sur le site : http://www.references.modernisation.gouv.fr.

UNIVERSIGN mettra à disposition ces informations à travers le blog UNIVERSIGN.

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

Clés d'AC :
Les clés de l'AC sont générées lors d'une cérémonie des clés au sein d'un HSM répondant aux exigences de l'annexe A.

Clés d'UHs :
Les clés des UHs sont générées au sein de HSM répondant aux exigences de l'annexe B.

6.1.2 Transmission de la clé privée au serveur

Sans objet. Les serveurs d'horodatage possèdent leur propre HSM générateur de bi-clé.

6.1.3 Transmission de la clé publique à l'AC

L'opération visant à faire signer par l'AC un certificat d'UH est une opération réalisée sur site par les personnels habilités. La clé publique d'une UH est transmise sur site à l'AC.

6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

Le certificat de l'AC UNIVERSIGN et son empreinte sont publiés sur le site : http://docs.universign.eu.

Le certificat doit contenir les informations présentées dans le chapitre 7 de la présente politique de certification.

Les Utilisateurs peuvent également adresser un email au point de contact identifié au paragraphe 1.5.2 une demande de confirmation du certificat d'AC. L'entête du mail doit contenir l'information suivante "Demande du certificat AC UNIVERSIGN ".

6.1.5 Tailles des clés

Les clés utilisées par l'AC UNIVERSIGN ont les caractéristiques suivantes :

Certificat	Taille des clés	Format
AC UNIVERSIGN	2048	RSA
UH UNIVERSIGN	2048	RSA

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

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

Les paramètres et les algorithmes utilisés sont documentés dans le chapitre 7 de cette présente PC.

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

Modules cryptographiques de l'AC :
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 CC EAL4+ et qualifiés au niveau renforcé par l'ANSSI. Ils répondent aux exigences de l'annexe A.

Modules cryptographiques des UHs :
Les UHs utilisent des modules cryptographiques répondant aux exigences de l'annexe B.

6.2.2 Contrôle de la clé privée par plusieurs personnes

La clé privée de l'AC UNIVERSIGN est contrôlée par des données d'activation stockées sur des cartes à puce et remises à des porteurs de secrets lors de la cérémonie des clés.

Un partage de secret du HSM est mis en oeuvre par l'AC selon la méthode de partage à seuil de Shamir.

6.2.3 Séquestre de la clé privée

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

6.2.4 Copie de secours de la clé privée

Les clés privées d'AC font l'objet de copies de secours, hors d'un module cryptographique mais sous forme chiffrée et avec un mécanisme de contrôle d'intégrité.

Toute copie de sauvegarde de clé privée de l'AC est stockée dans un coffre fort sécurisé.

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

6.2.5 Archivage de la clé privée

Les clés privées de l'AC et des UHs ne sont pas archivées.

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

Les clés privées de l'AC sont générées dans son module cryptographique et ne sont donc pas transférées hormis pour la copie de secours. Lors de la génération d'une copie de secours, le transfert opéré met en place un mécanisme de chiffrement permettant de garantir qu'aucune information sensible ne transite de manière non sécurisée.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées de l'AC sont stockées dans leur module cryptographique.

À des fins de copie de secours, le stockage est effectué en dehors d'un module cryptographique moyennant le respect des mesures du chapitre 6.2.4.

6.2.8 Méthode d'activation de la clé privée

Clés privées d'AC :
L'activation des clés privées est contrôlée par des données d'activation et est réalisé au sein d'un module cryptographique répondant aux exigences de l'annexe A, sous le contrôle de deux personnes dans des Ràôles de Confiance.

Clés privées des UHs :
L'activation des clés privées d'une UH est contrôlée via des données d'activation et est réalisée sur un module cryptographique répondant aux exigences de l'annexe B.

6.2.9 Méthode de désactivation de la clé privée

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

Clés privées des UHs :
La désactivation de la clé privée s'opère lors de l'arrêt du module cryptographique.

6.2.10 Méthode de destruction des clés privées

Clés privées de l'AC :
La destruction de la clé privée de l'AC est effectuée à partir de son module cryptographique. En cas de destruction, l'AC s'assure que toute les copies de secours correspondantes sont également détruites.

Clés privées des UHs :
La destruction de la clé privée d'une UH est effectuée à partir de son module cryptographique.

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

Module cryptographique de l'AC :
Le HSM de l'AC est évalué :
- EAL 4+ aux Critères Communs ;
- Qualifié au niveau renforcé par l'ANSSI (référence 2010/09).

Module cryptographique des serveurs :
L'AC ne fournit pas les UHs.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques de l'AC sont archivées 5 ans après l'expiration du certificat d'AC correspondant.

6.3.2 Durées de vie des bi-clés et des certificats

UH :
La clé privée d'une UH a une durée de vie de 1 an. Le certificat d'une UH a une durée de vie de 6 ans.

AC UNIVERSIGN :
Les clés privées et les certificats de l'AC ont une durée de vie de 10 ans.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Génération et installation des données d'activation correspondant à la clé privée de l'AC

La génération et l'installation des données d'activation du HSM de l'AC sont réalisées durant la cérémonie des clés. Ces données d'activation sont stockées sur des cartes à puce et remise à des porteurs de secrets.

6.4.2 Protection des données d'activation

Les données d'activation sont stockées sur une carte à puce nominative et personnelle. Cette carte à puce est de la responsabilité de la personne à qui la carte est remise et est protégée par un code PIN qui est personnel au porteur de secret. Les cartes à puce sont ensuite stockées dans un coffre fort sécurisé.

6.4.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Mesures de sécurité technique spécifiques aux systèmes informatiques

Identification et authentification

Les systèmes, applications et bases de données identifient et authentifient de faàçon unique les utilisateurs. Toute interaction entre le système et un utilisateur n'est possible qu'après une identification et une authentification réussies. Pour chaque interaction, le système peut établir l'identité de l'entité.

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

Contrôle d'accès :

Les profils et droits d'accès aux équipements d'UNIVERSIGN sont définis et documentés, comprenant également les procédures d'enregistrement et de désenregistrement des utilisateurs.

Les systèmes, applications et bases de données sont tels que l'on peut distinguer et administrer les droits d'accès de chaque utilisateur, au niveau d'un utilisa-

teur, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux. Il est ainsi 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 accorder ou retirer des droits d'accès à un objet. De même, seuls des utilisateurs autorisés peuvent introduire de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants.

Administration et exploitation :
L'utilisation de programmes utilitaires est restreinte et contrôlée sur les infrastructure de l'IGC.

Les procédures opérationnelles d'administration et exploitation de l'IGC sont documentées, suivies et régulièrement mises à jour.

Les conditions de mise en service (paramétrage initial de sécurité des serveurs) sont documentées.

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

L'ensemble des matériels sensibles de l'IGC fait l'objet de procédure de maintenance afin de garantir la disponibilité des fonctions et des informations. Les procédures associées sont documentées.

Les personnels concernés par ces procédures sont nommés par la direction d'UNIVERSIGN.

Des mesures de contrôles des actions de maintenance sont mises en application.

Intégrité des composantes :
Les composantes du réseau local sont maintenues dans un environnement phy-

siquement sécurisé. Des vérifications périodiques de conformité de leur configuration sont effectuées.

Sécurité des flux :
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 les differentes composantes.

Journalisation et audit :
Un suivi d'activité est possible au travers des journaux d'événements.

Supervision et contrôle :
Une surveillance permanente est mise en place et des systèmes d'alarmes sont installés pour détecter, enregistrer et permettre de réagir rapidement face à toute tentative non autorisée et / ou irrégulière d'accès aux ressources (physique et / ou logique).

Sensibilisation :
Des procédures appropriées de sensibilisation des personnels sont mises en œuvre.

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

Les infrastructures de développement et d'essai sont séparées des infrastructures opérationnelles de l'IGC.

Toute mise à jour d'une des composantes de l'IGC bénéficie d'une procédure de recette. Pour être mis en production, un Procès Verbal de recette doit être signé par le responsable de l'AC.

6.6.2 Mesures liées à la gestion de la sécurité

Les évolutions des composantes font l'objet d'une remise à jour des procédures opérationnelles.

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

Sans objet.

6.7 Mesures de sécurité réseau

L'AC UNIVERSIGN est une AC hors-ligne non connectée au réseau. La propagation d'information comme la mise à disposition des LCR se fait à travers un canal de communication mono-directionel.

6.8 Horodatage / Système de datation

cf. chapitre 5.5.5.

7 Profil des certificats, des OCSP et des LCR

7.1 Profile des certificats

7.1.1 Certificats de l'AC

Champs de base

Champs	Valeur
Version	2
Numéro de série	défini par l'outil
Signature	RSA/SHA-256
Issuer DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Timestamping CA (ou Universign Timestamping CA 2015)
Validité	10 ans
Subject DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Timestamping CA (ou Universign Timestamping CA 2015)
Clé publique	RSA 2048 bits

Extension du certificat

Champ	OID	Critique	Valeur
Subject Key Identifier	2.5.29.14	Non	
KeyIdentifier			RFC 5280 - Méthode 1
Key Usage	2.5.29.15	Oui	
digitalSignature			Faux
nonRepudiation			Faux
keyEncipherment			Faux
dataEncipherment			Faux
keyAgreement			Faux
keyCertSign			Vrai
cRLSign			Vrai
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	
CA			Vrai
Maximum Path Length			Absent

7.1.2 Certificat d'une UH

Champs de base

Champs	Valeur
Version	2
Numéro de série	défini par l'outil
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[3]	
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

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

7.2 Profil des LCRs

Champs de base

Champs	Valeur
Version	1
Signature	RSA/SHA-256
Issuer DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Timestamping CA (ou Universign Timestamping CA 2015)
Validité	7 jours
Next Update	This Update + 1 jour

Extension de LCR

Champ	OID	Critique	Valeur
Authority Key Identifier	2.5.29.35	Non	
KeyIdentifier			RFC 5280 - Méthode 0
CRL Number	2.5.29.20	Non	
CRLNumber			défini par l'outil

7.3 Profil des OCSPs

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
  - soit par des prestataires externes spécialistes du domaine de l'IGC ;
  - soit par un responsable d'audit interne à Cryptolog.
- un audit de qualification réalisé par un organisme accrédité au moins une fois par an.

Un contrôle de conformité à la PC 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.

A l'occasion du référencement RGS de l'AC UNIVERSIGN, un premier audit a été effectué par la société LSTI, conformément aux procédures règlementaires en vigueur.

8.2 Identités / qualifications des évaluateurs

Le contrôleur 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 conformité qui pourraient compromettre la sécurité du service offert.

L'AC 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 PC ;
- de la DPC ;
- des composants de l'IGC.

Avant chaque audit, les évaluateurs proposeront au Comité d'Approbation de l'AC 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 au responsable légal d'UNIVERSIGN (AC), un avis parmi les suivants : "réussite", "échec", "à confirmer".

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

En cas de résultat "à confirmer", l'équipe d'audit identifie les non conformités, et les hiérarchisent. Il appartient à l'AC 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'AC confirme à la composante contrôlée la conformité aux engagements de la PC et de ses pratiques annoncées.

8.6 Communication des résultats

Les résultats des audits de conformité sont tenus à la disposition de l'organisme de qualification intéressé.

9 Autres problématiques métiers et légales

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Sans objet.

9.1.2 Tarifs pour accéder aux certificat

Sans objet.

9.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats

Sans objet.

9.1.4 Tarifs pour d'autres services

Sans objet.

9.1.5 Politique de remboursement

Sans objet.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

Sans objet.

9.2.2 Autres ressources

Sans objet.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Sans objet.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations suivantes sont traitées comme confidentielles :
- les clés privées de l'AC UNIVERSIGN et des UH,
- la partie non publique de la DPC,
- les données d'activation associées aux clés privées de l'AC Racine UNIVERSIGN et des UH,
- les journaux d'événements,
- les causes de révocations des certificats.

9.3.2 Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3 Responsabilités en terme de protection des informations confidentielles

UNIVERSIGN s'engage à traiter les informations confidentielles recueillies dans le respect des lois et règlements en vigueur.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

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.

9.4.2 Informations à caractère personnel

Aucune information personnelle n'est enregistrée dans le cadre de l'AC UNIVERSIGN.

9.4.3 Informations à caractère non personnel

Pas d'engagement spécifique.

9.4.4 Responsabilité en termes de protection des données personnelles

Sans objet.

9.4.5 Notification et consentement d'utilisation des données personnelles

Sans objet.

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

Les enregistrements peuvent être mis à disposition en cas de besoin pour servir de preuve en justice.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Pas d'engagement spécifique.

9.5 Droits sur la propriété intellectuelle et industrielle

Sur le plan de la propriété intellectuelle, les produits mis en œuvre dans l'IGC 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 contrefaàçon sanctionnée par le "code de la propriété intellectuelle", sauf accord préalable et écrit d'UNIVERSIGN.

9.6 Interprétations contractuelles et garanties

Les obligations communes aux composantes de l'IGC sont les suivantes :
- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ;
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent ;
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante) ;
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1 Autorité de Certification

UNIVERSIGN est responsable :
- de la validation et de la publication de la PC ;
- de la validation de la DPC, et de leur conformité à la PC ;
- de la conformité des certificats émis vis-à-vis de la présente PC ;
- du respect de tous les principes de sécurité par les différentes composantes de l'IGC, et des contrôles afférents.

Sauf à démontrer qu'elle n'a commis aucune faute intentionnelle ou de négligence, l'AC UNIVERSIGN est responsable de tout préjudice causé aux Utilisateurs si :
- les informations contenues dans le certificat ne correspondent pas aux informations d'enregistrement ;
- l'AC n'a pas fait procéder à l'enregistrement de la révocation d'un certificat, et n'a pas publié cette information conformément à ses engagements.

9.6.2 Service d'enregistrement

Cf. ci-dessus.

9.6.3 Abonné

Le RCC :
- Communique des informations exactes et à jour lors d'une demande d'établissement d'une UH ;
- Protège la clé privée du serveur dont il a la responsabilité ;
- Protège l'accès à la base de certificats du serveur ;
- Respecte les conditions d'utilisation de la clé privée du serveur conformément à ce qui est établi dans la présente PC ;
- Informe l'AC de toute modification concernant les informations contenues dans le certificat de l'UH ;
- Fait sans délai une demande de révocation du certificat d'une UH en cas de suspicion de compromission de la clé privée correspondante.

Le RCC est enregistré auprès de l'AC UNIVERSIGN conformément à la procédure définie dans la présente politique de certification.

9.6.4 Utilisateurs de certificats

Les utilisateurs utilisant les certificats de l'AC doivent :
- vérifier et respecter l'usage pour lequel le certificat a été émis ;
- vérifier l'état de révocation du certificat ;
- vérifier et repecter les obligations exprimées dans la présente PC.

9.6.5 Autres participants

Sans objet.

9.7 Limite de garantie

Sans objet.

9.8 Limite de responsabilité

UNIVERSIGN ne pourra pas être tenu pour responsable d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées et des données d'activation, des LCR, ainsi que de tout autre équipement ou logiciel mis à disposition.

UNIVERSIGN décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par l'Abonné.

De plus, dans la mesure des limitations de la loi franàçaise, UNIVERSIGN ne saurait être tenu responsable :
- d'aucune perte financière ;
- d'aucune perte de données ;
- d'aucun dommage indirect lié à l'utilisation d'un certificat ;
- d'aucun autre dommage.

En toute hypothèse, la responsabilité d'UNIVERSIGN sera limitée, tous faits générateurs confondus et pour tous préjudices confondus, au montant payé à UNIVERSIGN par l'Abonné concernant le fait générateur et ce, dans le respect et les limites de la loi applicable. Sauf prescription légale contraire, toute action de l'Abonné au titre des présentes devra intervenir au plus tard dans un délai de six mois à compter de la survenance du fait générateur fondant l'action.

9.9 Indemnités

Sans objet.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

La présente PC reste en application jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 Fin anticipée de validité

Cette PC reste en vigueur jusqu'à son remplacement par une nouvelle version.

9.10.3 Effets de la fin de validité et clauses restant applicables

Sans objet.

9.11 Notifications individuelles et communications entre les participants

Sauf en cas d'accord entre les parties concernées, tous les avis et autres communications qui doivent être fournis, délivrés ou envoyés conformément à la PC en vigueur doivent être écrits et envoyés par des moyens offrant une confiance raisonnable sur leur origine et leur réception.

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

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

Lorsqu'une nouvelle version de la PC est approuvée la le Comité d'approbation d'UNIVERSIGN, elle sera publiée sur le site web d'UNIVERSIGN et remplacera les termes de la version précédente.

9.12.2 Mécanisme et période d'information sur les amendements

Les seules modifications que le Comité d'Approbation peut opérer sur la PC 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 PC sera mise en ligne pour commentaire, avec une indication de la date d'effet.

Lorsqu'une nouvelle version de la PC est mise en ligne, tous les Abonnées et Utilisateurs de l'IGC d'UNIVERSIGN sont informés de la nature, de la date et de l'heure du changement, par une publication sur le site web d'UNIVERSIGN.

À l'issue de la période de commentaires, le Comité d'Approbation peut décider de publier la nouvelle PC 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 PC entre en vigueur 14 jours ouvrés après sa mise en ligne et reste valide jusqu'à l'entrée en vigueur d'une nouvelle version.

9.12.3 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 certificats déjà émis.

9.13 Dispositions concernant la résolution de conflits

EN CAS DE LITIGE ENTRE LES PARTIES DECOULANT DE L'INTERPRETATION, L'APPLICATION ET/OU L'EXECUTION DU CONTRAT ET A DEFAUT D'ACCORD AMIABLE ENTRE LES PARTIES CI-AVANT, LA COMPETENCE EXCLUSIVE EST ATTRIBUEE AU TRIBUNAL DE COMMERCE DE PARIS.

9.14 Juridictions compétentes

Voir ci-dessus.

9.15 Conformité aux législations et réglementations

Cette PC est conforme au droit franàçais et notamment aux documents [**CNIL**], [**ORD**], [**DRGS**] et [**ARGS**].

9.16 Dispositions diverses

9.16.1 Accord global

Pas d'engagement spécifique.

9.16.2 Transfert d'activités

Sans objet.

9.16.3 Conséquences d'une clause non valide

Pas d'engagement spécifique.

9.16.4 Application et renonciation

Pas d'engagement spécifique.

9.16.5 Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux franàçais, notamment le cas d'un événement irrésistible, insurmontable et imprévisible.

9.17 Autres dispositions

Sans objet.

A Exigences de sécurité du module cryptographique de l'AC

A.1 Exigences sur les objectifs de sécurité

Le module cryptographique utilisé pour la génération des certificats et des LCRs doit répondre aux exigences de sécurité suivantes :

- Assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et leur destruction sûre en fin de vie ;
- Être capable d'identifier et d'authentifier ses utilisateurs ;
- Limiter l'accès à ses services en fonction de l'utilisateur et du ràôle qui lui a été assigné ;
- Etre capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Permettre de créer une signature numérique pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance des clés privées ;
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- Si une fonction de sauvegarde et de restauration des clés privées de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration ;
- Détecter les tentatives d'altération physique et entrer dans un état sûr quand une tentative d'altération est détectée.

A.2 Exigences sur la certification

Le module cryptographique utilisé par UNIVERSIGN est qualifié au niveau renforcé, selon le processus décrit dans le [**RGS**], et est conforme aux exigences du chapitre ci-dessus.

B Exigences de sécurité du module cryptographique du serveur

B.1 Exigences sur les objectifs de sécurité

Le module cryptographique utilisé par le serveur pour générer, stocker et utiliser sa bi-cle doit répondre aux exigences de sécurité suivantes :

- garantir que la génération de bi-clé est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;

- assurer la correspondance entre la clé privée et la clé publique ;
- générer une signature numérique qui ne peut être falsifiée sans la connaissance de la clé privée ;
- assurer pour le serveur légitime uniquement la fonction de génération des signature numérique et protéger la clé privée contre toute utilisation par des tiers ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

Références

[**ARGS**] Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en oeuvre de la procédure de validation des certificats électroniques.

[**DRGS**] Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

[**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.

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

[**RGS**]
Référentiel Général de Sécurité - Version 1.0 - 06/05/2010.

[**RGS_A_10**]
Référentiel Général de Sécurité - Politique de Certification Type Cachet - Version 2.3 - 11/02/2010. OID : 1.2.250.1.137.2.2.1.2.2.6

[**RGS_A_12**]
Référentiel Général de Sécurité - Politique d'Horodatage Type - Version 2.3 - 18/02/2010. OID : 1.2.250.1.137.2.2.1.2.2.4

[**RGS_A_14**]
Référentiel Général de Sécurité - Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques - Version 2.3 - 11/02/2010. OID : 1.2.250.1.137.2.2.1.2.1.4

[**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.