universign

Politique de Certification /
Déclaration des Pratiques de Certification

AC Matérielle Universign

Universign
OID: 1.3.6.1.4.1.15819.5.1.3.(1/2/3/4)
Version: 1.2 / Date d'entrée en vigueur: 25 April 2014
DISTRIBUTION PUBLIQUE

Table des matières

1 Introduction

1.1 Présentation Générale

Universign s'est positionné comme Prestataire de Service de Certification (PSC).

Pour cela, Universign crée et opère différentes Autorités de Certification (AC). L'ensemble de ces Autorités de Certification définit l'Architecture de Confiance d'Universign (ACU). Dans le cadre de cette architecture de confiance, Universign opère des Autorités de Certification Primaires (AC Primaires). Celles-ci certifient exclusivement des Autorités de Certification (AC) capables de délivrer des certificats à des porteurs dans des conditions conformes aux standards de sécurité reconnus par Universign.

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

Le présent document (noté PC/DPC tout au long du document) rassemble la politique de certification des AC Matérielles et la déclaration des pratiques de certification de ces AC. Ce document définit les engagements d'Universign, en terme de sécurité et d'organisation, dans le cadre de la fourniture de certificats par les AC Matérielles d'Universign.

Architecture de Confiance d'Universign L'Architecture de Confiance d'Universign (présentée [1] dans la Figure 1.) est composée

- d'AC Primaires ;
- d'AC émettrices de certificats de porteurs finaux, rattachée chacune à au moins une AC Primaire ;
- de porteurs de certificats finaux ;
- d'utilisateurs.

Une AC Primaire ne délivre des certificats qu'à des AC répondant aux critères définis dans sa PC/DPC. Cette version de la PC/DPC ne considère pas la possibilité pour une AC autre qu'une AC Primaire de délivrer des certificats à d'autres Autorités de Certification, mais les versions ultérieures pourront prendre en compte cette option.

La présente version de l'ACU présente deux types de hiérarchies d'AC :

- les hiérarchies ayant pour AC racine une AC Primaire Matérielle, visant à émettre des certificats d'utilisateurs finaux protégés par du matériel cryptographique et appelées *hiérarchies matérielles*.
- les hiérarchies ayant pour AC racine une AC Primaire Logicielle, n'imposant pas d'émettre des certificats d'utilisateurs finaux protégés par du matériel cryptographique et appelées *hiérarchies logicielles*.

1. Ce schéma est donné à titre explicatif. Les AC effectivement utilisées ne sont pas celles représentées sur le schéma.

Le périmètre de la présente PC/DPC se limite aux AC non-Primaires de la *hiérarchie matérielle* (notées AC Matérielles dans le reste de ce document) (Voir Fig.1). Ces AC Matérielles délivrent des certificats aux porteurs de certificats finaux qui sont des personnes physiques, des entités ou des organisations dans les conditions définies dans la présente PC/DPC.

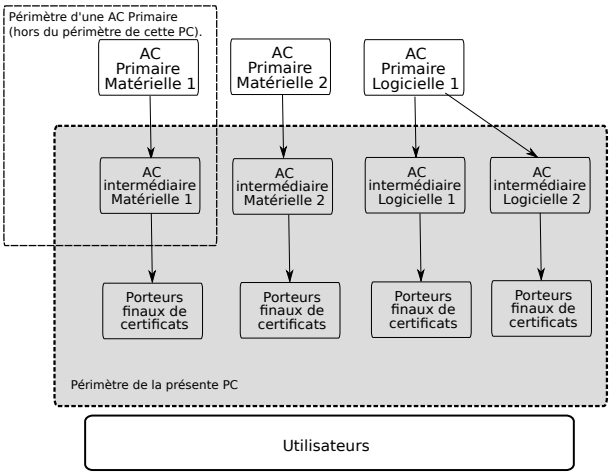

FIGURE 1: Principe de l'Architecture de Confiance d'Universign et périmètre de la présente PC

Cette version de la PC/DPC considère 4 familles de certificats conformément aux dispositions des Sections 1.2, 6.2.7 et 7.1.2 :

- Des certificats de personnes physiques, en conformité avec [**ETSI 101.456**] niveau QCP public, correspondant à l'OID 1.3.6.1.4.1.15819.5.1.3.1 ;
- Des certificats d'entité ou d'organisation, en conformité avec [**ETSI 102.042**] niveau NCP+, correspondant à l'OID 1.3.6.1.4.1.15819.5.1.3.2 ;
- Des certificats de personnes physiques, en conformité avec [**ETSI 102.042**] niveau LCP, correspondant à l'OID 1.3.6.1.4.1.15819.5.1.3.3 ;
- Des certificats d'entité ou d'organisation, en conformité avec [**ETSI 102.042**] niveau LCP, correspondant à l'OID 1.3.6.1.4.1.15819.5.1.3.4.

Périmètre de la présente PC Le périmètre de la présente PC/DPC se concentre sur les AC Matérielles et leur fonction de délivrance de certificats aux Porteurs de certificats finaux.

La présente PC/DPC définit les participants suivants :

- les AC Matérielles, qui délivrent des certificats à des Abonnés répondant aux exigences exprimées dans la présente PC/DPC ;
- des Abonnés, qui sont les porteurs de certificats délivrés par les AC Matérielles ;

– des utilisateurs, dont les opérations dépendent de l'architecture de confiance fournie par Universign.

1.2 Identification du document

Le présent document est la politique de certification des AC Matérielles d'Universign. Il contient également la déclaration des pratiques de certification de ces AC.

Universign, en tant qu'autorité éditrice de la présente PC/DPC, a assigné, au sein du référentiel documentaire de l'ACU, un identifiant pour chacune des familles de certificats délivrées par ses AC Matérielles et définies par la présente PC/DPC :

– 1.3.6.1.4.1.15819.5.1.3.1 pour les certificats délivrés à des personnes physiques avec enregistrement incluant un face-à-face ;
– 1.3.6.1.4.1.15819.5.1.3.2 pour les certificats délivrés à des entités ou organisations avec enregistrement incluant un face-à-face ;
– 1.3.6.1.4.1.15819.5.1.3.3 pour les certificats délivrés à des personnes physiques sans obligation d'enregistrement incluant un face-à-face ;
– 1.3.6.1.4.1.15819.5.1.3.4 pour les certificats délivrés à des entités ou organisations sans obligation d'enregistrement incluant un face-à-face ;

1.3 Entités intervenant dans l'IGC

1.3.1 Autorité de certification

Une Autorité de Certification est un terme générique désignant une autorité capable d'émettre des certificats à des porteurs de certificats.

Dans l'ACU d'Universign, deux types d'entités répondent à cette définition :

– les AC Primaires, qui délivrent des certificats à des AC Matérielles ;
– les AC Matérielles, qui délivrent des certificats à des porteurs de certificats finaux.

Le périmètre de cette PC/DPC traite des AC Matérielles et de la délivrance de certificats aux Abonnés (voir Section 1.1).

Gouvernance d'une AC Matérielle Une AC Matérielle 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 Matérielle.

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

– approuver le référentiel documentaire fourni par Universign ;

– approuver la PC/DPC ;
– définir le processus de mise à jour de la PC/DPC ;
– définir le processus garantissant que Universign intègre correctement les pratiques de la PC/DPC ;
– publier la PC/DPC et ses révisions à destination des Abonnés et Utilisateurs.

1.3.2 Autorité d'enregistrement

Dans le cadre de cette PC/DPC, l'AC Matérielle Universign opère sa propre Autorité d'Enregistrement. L'AC Matérielle peut confier certaines missions du processus d'enregistrement à des organisations tierces sous contrat avec Universign.

1.3.3 Porteurs de Certificats

Le terme de porteur de certificat est une notion générique pouvant recouvrir les entités suivantes :
– Le Sujet : une personne physique, une personne morale, une entité, une organisation, un composant ou une infrastructure qui est désignée par le champ `subject` du certificat ;
– L'Abonné : la personne physique ou morale qui contracte avec l'émetteur du certificat (elle peut être différente du sujet, une organisation peut contracter avec une AC pour émettre des certificats pour ses employés) ;
– Le Responsable du Certificat : les personnes physiques qui ont la responsabilité du certificat émis et de son cycle de vie (demande de certificat, révocation,...).

Selon les architectures mises en place, ces personnes et entités peuvent être confondues.

Dans le cadre de cette PC/DPC, on distingue deux types de certificats :
– les certificats désignant des personnes physiques ;
– les certificats des entités ou des organisations.

De ce fait, on fera, dans le cadre de cette version de la PC/DPC les distinctions suivantes :
– Le Sujet ne peut être que [2] :
  – une personne physique (attachée ou non à une entité ou organisation), ou
  – une entité ou organisation.

2. Les futurs versions de cette PC/DPC pourront considérer d'autres classes de sujet, tels que des AC, des composants (*e.g.* firewall) ou des infrastructures

Celui-ci est désigné par le champ `subject` du certificat émis par l'AC Matérielle.
- Pour le Responsable du Certificat, on distingue deux cas :
  - dans le cas ou le sujet est une personne physique, le responsable du certificat et le sujet sont confondus.
  - dans le cas d'un certificat d'entité ou d'organisation, un *Responsable de certificat* doit être nommé par l'Abonné (voir Section 1.3.5). Il sera responsable du cycle de vie du certificat.

1.3.4 Utilisateurs de certificats

Les utilisateurs sont quiconque, personne physique ou morale, dont les activités vont dépendre de la validité du lien entre le nom du Sujet et de la clé publique associée. Les utilisateurs sont responsables de décider de la manière dont ils vérifieront la validité de ce lien, *a minima* ils devront vérifier les informations sur le statut de révocation de ce certificat. Un utilisateur peut utiliser les informations présentes dans le certificat (tel que l'identifiant de la présente PC/DPC) pour déterminer la validité du certificat pour une utilisation particulière.

1.3.5 Autres Participants

Toutes les composantes de l'IGC sont définies dans les sections précédentes et la présente section.

Mandataires de certification La présente politique de certification définit des mandataires de certification. La nomination d'un ou de plusieurs mandataires de certification (MC) ne s'applique qu'au cas de la délivrance de certificat d'entreprise ou d'administration. Dans le cas du recours à des MC, le MC doit être formellement désigné par un représentant légal de l'entité concernée. Le MC est en relation directe avec l'AE de l'AC Matérielle.

Le rôle du MC est le suivant :
- effectuer correctement et de façon indépendante les contrôles d'identité des futurs Sujets de l'entité pour laquelle il est MC ;
- respecter les parties de cette PC/DPC qui lui incombent. Il est de la responsabilité de l'entité contractant avec l'AC Matérielle de signaler à l'AC Matérielle, si possible préalablement mais au moins sans délai, le départ du MC de ses fonctions et, éventuellement, lui désigner un successeur.

Le MC ne doit en aucun cas avoir accès aux moyens qui lui permettraient d'activer et d'utiliser la clé privée associée à la clé publique contenue dans le certificat délivré au porteur.

Les engagements du MC à l'égard de l'AC Matérielle précisés ci-dessus doivent faire l'objet d'un contrat entre l'entité responsable du MC et Universign.

Responsable de certificat Dans le cadre de la présente PC/DPC, l'AC Matérielle émet des certificats d'entité ou d'organisation. Un Responsable de certificat est une personne physique qui est responsable :

- des démarches administrative liées à l'émission du certificat de l'entité ou organisation identifiée dans le certificat, ainsi que du cycle de vie du certificat ;
- de la clé privée correspondant à ce certificat.

Le Responsable de certificat doit donc avoir une délégation pour exercer ces responsabilités pour le compte de l'entité identifiée dans le certificat. De ce fait, le Responsable de certificat a un lien contractuel, hiérarchique ou réglementaire avec l'entité et doit être explicitement nommé par celle-ci. Le Responsable de certificat doit respecter les conditions qui lui incombent, telles que définies dans cette PC/DPC.

Il est à noter que le certificat d'entité ou d'organisation n'étant pas attaché à une personne physique, son Responsable de certificat peut être amené à changer en cours de validité du certificat : départ du Responsable de certificat de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc. L'entité doit signaler à l'AC Matérielle préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un Responsable de certificat de ses fonctions et lui désigner un successeur. Une AC Matérielle doit révoquer un certificat d'entité ou d'organisation pour lequel il n'y a plus de Responsable de certificat explicitement identifié, après plusieurs relances auprès de l'Abonné.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

Bi-clés et certificats émis par l'AC Matérielle Les bi-clés associées aux certificats émis sont destinées à être utilisées pour signer électroniquement des données dans le cadre d'échanges dématérialisés avec les utilisateurs de certificats.

Bi-clés et certificats d'AC Matérielle L'AC Matérielle dispose d'une seule bi-clé rattachée à au moins une AC Matérielle Primaire de niveau supérieur. Cette bi-clé peut être utilisée pour signer :

- les certificats des porteurs ;
- les LCR et/ou les réponses OCSP de l'AC Matérielle ;
- les certificats techniques des composantes de son infrastructure.

1.4.2 Domaines d'utilisation interdits

Tout autre usage que celui défini dans le paragraphe précédent est interdit par la présente PC/DPC. De plus, le certificat doit être utilisé dans la limite des lois et réglementations en vigueur.

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 certification
AC Matérielle Universign
Cryptolog International
6-8, Rue Basfroi, F-75011 Paris, France
contact@universign.eu

1.5.3 Entité déterminant la conformité des pratiques de la PC

Le comité d'approbation d'Universign détermine l'adéquation de l'applicabilité de cette PC.

1.5.4 Procédure d'approbation de la conformité de la DPC

L'approbation et la mise à jour de la conformité des pratiques documentées à la PC/DPC sont prononcées 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/DPC sont les suivants :

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

Universign : Pour le besoin des présentes et des documents régissant l'offre d'IGC, la société Cryptolog International, SAS au capital 318 513 euros, 6/8 rue Basfroi, 75011 Paris, enregistrée au RCS de Paris sous le numéro 439129164.

Abréviations

Les abréviations utilisées dans la présente PC/DPC sont les suivantes :

AC : Autorité de certification
PC : Politique de certification
LCR : Liste des certificats révoqués
CSP : Certification Service Provider
DN : Distinguished Name
HSM : Hardware Security Module (module cryptographique)
OID : Object Identifier
IGC : Infrastructure de Gestion de Clés
AE : Autorité d'enregistrement
RGS : Référentiel Général de Sécurité

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 Matérielle, met à disposition des utilisateurs de certificats la présente PC/DPC. La présente PC/DPC 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/DPC.

2.2 Informations Publiées

Les informations publiées par l'AC Matérielle Universign sont les suivantes :
– la présente PC/DPC [3] ;

3. une copie des versions précédentes de cette PC/DPC, ainsi que les dates de validité de chacune d'elles sont tenus à la disposition des utilisateurs sur demande.

- les LCRs publiées selon les exigences de cette PC/DPC ;
- les certificats des AC Matérielles Universign en cours de validité ;
- la Déclaration d'IGC ;
- l'Accord de Souscription ;
- l'Accord d'Utilisation.

Le site de publication est disponible 24h/24 et 7j/7 en conditions normales de fonctionnement.

2.3 Délais et fréquences de publication

La présente PC/DPC : La présente PC/DPC est publiée en conformité avec la section 9.12.

Les LCRs : Une AC Matérielle d'Universign émet des LCR permettant de diffuser le statut des certificats qu'elle a émis. Les LCR sont mises publiquement à disposition (voir Sect. 2.1). Elles sont publiées quotidiennement.

Les certificats des répondeurs OCSP : Les certificats des répondeurs OCSP sont inclus dans chaque réponse OCSP générée. De ce fait, ils ne sont pas obligatoirement diffusés sur le site de publication.

Les certificats des AC Matérielles Universign en cours de validité : Les certificats de l'AC Matérielle sont diffusés ou mis en ligne au maximum 24 heures après leur génération et obligatoirement avant leur utilisation effective.

L'Accord de Souscription, la Déclaration d'IGC et l'Accord d'Utilisation sont publiés dés que nécessaire.

2.4 Contrôle d'accès aux informations publiées

Universign s'interdit de mettre en œuvre des moyens techniques pour limiter l'accès aux informations publiées. Le fait pour un Utilisateur d'accéder aux informations publiées implique qu'il accepte préalablement l'Accord d'Utilisation. Universign met en place des contrôles d'accès afin de s'assurer que les personnes non autorisées ne puissent pas ajouter, modifier ou effacer des données publiées.

3 Identification et authentification

3.1 Nommage

3.1.1 Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500.

L'AC Matérielle et le Sujet sont identifiés par un nom explicite (appelé "DN" par la suite) de type X.501. Ce type de DN est défini dans le chapitre 7. Les détails du processus permettant à l'AC Matérielle Universign d'identifier l'Abonné sont décrits dans le chapitre 3.2.2 et le chapitre 3.2.3.

Certificats de personnes physiques Tous les certificats de personnes physiques émis par l'AC Matérielle Universign comportent les champs suivants dans le DN :

Champ	Obligatoire	Sémantique du champ	Vérifié par l'AE	Document utilisé pour la vérification
C	non	Nationalité de la personne physique.	oui	Pièce d'identité en cours de validité.
O	non	Nom légal de l'entité à laquelle est ratachée la personne physique	oui	Document d'identification officiel de la société et mandat signé.
OU	non	Cas 1 : Le champ commence par 4 chiffres. Il s'agit de l'identifiant unique légal de l'entité [4] structuré suivant l'ISO 6523	oui	Document d'identification de la société.
		Cas 2 : Le champ ne commence pas par 4 chiffres. Il s'agit d'un champ libre	non	
SERIALNUMBER	oui	Le numéro de série attribué par l'AE	oui [5]	
CN	oui	Nom et prénom de la personne physique	oui	Pièce d'identité en cours de validité.

4. Pour une société française, 0002 suivi d'un espace et du numéro de SIREN ou de SIRET
5. il sera uniquement vérifié que ce numéro est unique

Chaque DN émis doit être unique. Cette unicité est obtenue par un numéro de série unique (SERIALNUMBER) inclus dans chaque certificat.

Certificats d'entité et d'organisation Tous les certificats d'entité et d'organisation émis par l'AC Matérielle Universign comportent les champs suivants dans le DN :

Champ	Obligatoire	Sémantique du champ	Vérifié par l'AE	Document utilisé pour la vérification
C	oui	Pays	oui	Document d'identification de la société.
ST	non	Etat/Région de l'entité opérant l'Abonné	oui	Document d'identification de la société.
L	non	Ville de l'entité opérant l'Abonné	oui	Document d'identification de la société.
O	oui	Nom légal de l'entité propriétaire de l'Abonné	oui	Document d'identification de la société.
OU	oui	Cas 1 : Le champ commence par 4 chiffres. Il s'agit de l'identifiant unique légal de l'entité [6] structuré suivant l'ISO 6523	oui	Document d'identification de la société.
	non	Cas 2 : Le champ ne commence pas par 4 chiffres. Il s'agit d'un champ libre	non [7]	
CN	oui	Nom libre désignant le certificat	non [8]	

Chaque DN émis doit être unique. Cette unicité est obtenue par le numéro d'identifiant unique de la société (OU).

3.1.2 Noms explicites

Le DN de l'AC Matérielle Universign est précisé dans le chapitre 7. L'AC Matérielle Universign ne délivre des certificats que si le DN est explicite, c'est-à-dire qu'il permet de déterminer l'identité de l'individu ou de l'organisation qui est le sujet du certificat.

6. Pour une société française, 0002 suivi d'un espace et du numéro de SIREN ou de SIRET
7. Il sera uniquement vérifié que le nom est explicite (voir Sect. 3.1.2)
8. Il sera uniquement vérifié que le nom est explicite (voir Sect. 3.1.2)

3.1.3 Anonymisation ou pseudonymisation des porteurs

Universign interdit l'utilisation de ces pratiques.

3.1.4 Règles d'interprétation des différentes formes de noms

Les règles d'interprétation sont définies dans le chapitre 7.

3.1.5 Unicité des noms

L'identité du Sujet (voir 3.1.1) est unique pour l'ensemble des certificats générés par l'AC Matérielle. L'AE s'assure de cette unicité durant le processus d'enregistrement (voir 3.2.2)

Pour le certificat de personne physique, ceci est réalisé en générant un numéro de série unique pour chaque dossier d'enregistrement. Ce numéro de série unique sera inscrit dans le champ `SERIALNUMBER` du `DN` du certificat. Pour le certificat de personne d'entité ou d'organisation, ceci est réalisé en ajoutant un identifiant unique légal de la société dans le champ `OU` et en s'assurant que pour chaque société donné, le champ `CN` est unique.

3.1.6 Identification, authentification et rôle des marques déposées

Les Abonnés ne doivent pas utiliser des noms qui enfreignent la propriété intellectuelle d'un tiers. Universign et ses filiales ne pourront être tenus de déterminer si le porteur de certificat est bien le détenteur des contenus soumis à la propriété intellectuelle qu'il souhaite inclure dans son certificat. De même, Universign et ses filiales ne pourront être tenus d'effectuer les opérations d'arbitrage et de médiation, et de façon plus générale toute action de résolution de conflit concernant la propriété d'un nom de domaine, d'un nom déposé ou d'une marque déposée. Universign et ses filiales s'autorisent à rejeter une demande de certificat en cas de conflit, sans être tenu responsable d'aucun préjudice vis-à-vis du porteur de certificat.

3.2 Validation initiale de l'identité

3.2.1 Méthode pour prouver la possession de la clé privée

Un Abonné doit prouver à l'AC Matérielle à laquelle il veut être rattaché qu'il possède bien la clé privée correspondant à la clé publique à certifier.

La preuve de possession est obtenue

– soit en signant la demande de certificat au format PKCS#10 (ou un mécanisme apportant des assurances équivalentes accepté par Universign) à l'aide de la clé privée de l'Abonné ;
– soit en effectuant une requête depuis un service gérant la paire de clé reconnu et accepté par Universign.

3.2.2 Validation de l'identité d'un organisme

La validation de l'identité d'une entité ou organisation est réalisée de la façon suivante :

– le cas échéant, pour un certificat de personne physique rattaché à une entité ou une organisation, soit :
  – directement lors l'enregistrement de la personne physique se réclamant d'un rattachement ;
  – indirectement lors de la validation de l'identité du ou des Mandataires de Certification associés à l'entité ou l'organisation [9] ;
– pour un certificat d'entité ou d'organisation, lors de l'enregistrement de son Responsable de certificat [10].

3.2.3 Validation de l'identité d'un individu

Quel que soit le type de certificat émis, le futur porteur de certificat devra fournir un ensemble d'éléments pour justifier de son identité et des éléments contenus dans le certificat. Une copie de l'ensemble de ces éléments d'identité fait partie du dossier d'enregistrement et sera conservé par Universign de façon sûre.

Certificat de personnes physiques L'identité du futur sujet est vérifiée par l'AE.

Cette vérification est réalisée :

– durant une rencontre en face-à-face pour les certificats délivrés sous l'OID 1.3.6.1.4.1.15819.5.1.3.1.
– sans obligation d'une rencontre en face-à-face pour les certificats délivrés sous l'OID 1.3.6.1.4.1.15819.5.1.3.3.

La personne fournira les éléments suivants :

– une pièce d'identité nationale comportant une photographie d'identité ;
– une adresse email et/ou un numéro de téléphone portable permettant à l'AC Matérielle de contacter le porteur ;

9. Ceci est justifié par le fait que chaque entité ou organisation n'aura qu'un nombre limité de mandataire à un instant donné.

10. Ceci est justifié par le fait que chaque entité ou organisation n'aura qu'un Responsable de certificat à un instant donné.

- si le Sujet souhaite faire rattacher le certificat à une entité ou une organisation (*i.e.* faire figurer de son certificat le nom de l'entité dans le champ `O` et son numéro d'identification dans le champ `OU`), il lui faut apporter la preuve qu'il est bien rattaché à l'entité. Cela peut se faire :
  - Soit, un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité attestant que le demandeur auquel le certificat doit être délivré appartient bien à l'organisation et l'autorisant à faire figurer ce lien dans le certificat. Ce mandat doit être signé pour acceptation par le demandeur bénéficiaire. Ce dernier doit également fournir une pièce justificative de l'existence de l'organisation, valide lors de la demande de certificat (typiquement un extrait Kbis pour une entreprise française). Le document justificatif doit porter le numéro d'identifiant unique légal de l'entreprise en question (en France, numéro SIRET par exemple) ;
  - Soit, s'enregistrer directement auprès d'un mandataire de certification de l'organisation, qui vérifiera par des moyens internes l'appartenance du demandeur à l'organisation et attestera de son appartenance. Le champ `O` et éventuellement le champ `OU` sera celui qui a été fixé dans le cadre du mandat de certification.
  - Soit par tout autre moyen, accepté par Universign, permettant de s'assurer avec une certitude suffisante du rattachement de la personne à l'entité.

Certificat d'entité ou d'organisation L'identité du responsable du certificat de l'entité ou de l'organisation est vérifiée par l'AE.

- durant une rencontre en face-à-face pour les certificats délivrés sous l'OID 1.3.6.1.4.1.15819.5.1.3.2.
- sans obligation d'une rencontre en face-à-face pour les certificats délivrés sous l'OID 1.3.6.1.4.1.15819.5.1.3.4.

La personne fournira les éléments suivants :

- une pièce d'identité nationale en cours de validité du futur responsable de certificat comportant une photographie d'identité ;
- une adresse email et/ou un numéro de téléphone portable permettant à l'AC Matérielle de contacter le responsable ;
- un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité désignant le futur responsable auquel le certificat doit être délivré. Ce mandat doit être signé pour acceptation par le futur responsable. Il doit fournir une pièce justificative de l'existence de l'organisation, valide lors de la demande de certificat (typiquement un extrait Kbis pour une entreprise française). Le document justificatif doit porter le numéro d'identifiant unique légal de l'entité ou organisation en question (en France, numéro SIRET pour une entreprise par exemple).

Identification d'un mandataire de certification Pour s'enregistrer comme mandataire de certification auprès de l'AE, le demandeur devra :

- fournir une pièce d'identité nationale en cours de validité comportant une photographie d'identité ;
- présenter un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité, le désignant explicitement comme mandataire de certification de son organisation. Ce mandat doit être signé par le demandeur pour acceptation ;
- fournir une pièce justificative de l'existence de l'organisation, valide lors de la demande de certificat (typiquement un extrait Kbis pour une entreprise française). Le document justificatif doit porter le numéro d'identifiant unique légal de l'entreprise en question (en France, numéro SIRET par exemple).

Cette vérification est réalisée durant une rencontre en face-à-face.

3.2.4 Informations non vérifiées du porteur

Il n'est pas opéré de vérification sur les champs qui ne sont pas explicitement définis comme vérifiés dans la section 3.1.1.

3.2.5 Validation de l'autorité du demandeur

L'AE d'une AC Matérielle identifie l'autorité d'une personne physique pour représenter une entité ou une organisation avec un mandat signé du représentant légal de l'entité ou de l'organisation. Ce dernier est fourni lors de l'enregistrement (voir Section 3.2.3).

3.2.6 Critères d'interopérabilité

Sans objet.

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

Dans le cadre de l'AC Matérielle 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

Certificat de personne physique Une demande de révocation peut être réalisée de la façon suivante :

- soit par l'interface utilisateur du service de révocation d'Universign, après authentification de l'utilisateur ;
- soit, en cas de perte de son mot de passe, via un service spécifique accessible à tous les porteurs de certificats. Universign réalise une authentification du demandeur et en cas de succès de l'authentification, révoque automatiquement le certificat.
- soit en envoyant un email précisant la demande de révocation à l'adresse revocation@universign.eu. L'utilisateur sera alors contacté par un personnel d'Universign occupant un rôle de confiance qui tentera d'authentifier la personne par les différents moyens à sa disposition.

Certificat d'entité ou d'organisation Une demande de révocation se fait en envoyant un email à l'adresse revocation@universign.eu. L'utilisateur sera alors directement contacté par un personnel d'Universign occupant un rôle de confiance.

La personne en rôle de confiance exécute une procédure d'authentification de l'utilisateur, basée en partie sur les informations du dossier d'enregistrement.

4 Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Certificat de Personne Physique Le demandeur opère la demande de certificat en remplissant un formulaire de demande d'enregistrement. Le demandeur est l'Abonné. Si l'Abonné et le Sujet ne sont pas la même personne, l'Abonné doit apporter une preuve qu'il est autorisé à réaliser cette demande pour le Sujet.

Certificat d'entité ou d'organisation Le demandeur opère la demande de certificat en remplissant le formulaire de demande d'enregistrement. Le deman-

deur doit être le Responsable de certificat, nommé par le Responsable légal de l'entité ou organisation.

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

Certificat de personne physique, d'entité ou d'organisation.
Le processus d'enregistrement à l'AC Matérielle nécessite les étapes suivantes :

- Le demandeur doit lire et accepter l'Accord de Souscription de l'AC Matérielle.
- Le demandeur doit remplir avec des informations correctes la demande d'enregistrement et fournir à l'AE ou le cas échéant à un MC l'ensemble des éléments nécessaires du dossier d'enregistrement
- L'AE ou le MC valide les éléments du dossier d'enregistrement (voir Section 3.2.3) et les transmet de façon sécurisée à l'AC Matérielle.
- Dans le cas d'un enregistrement réalisé par un MC, le dossier est revalidé par l'AE après réception du dossier. Si le dossier est invalide ou incomplet, le certificat est alors révoqué. Sinon, il est définitivement validé.
- Le demandeur doit générer sa bi-clé dans un dispositif cryptographique satisfaisant aux exigences de la Section 6.2.11.
- Le demandeur doit fournir la clé publique à l'AC Matérielle.
- Le demandeur doit fournir une preuve que la clé privée associée à la clé publique lui appartient conformément aux exigences de la Section 3.2.1.

Universign s'assure que le processus d'enregistrement est réalisé en conformité avec la réglementation en vigueur.

Enregistrement d'un mandataire de certification
Le processus d'enregistrement d'un mandataire de certification est le suivant :
- l'organisation du futur mandataire doit contracter préalablement avec Universign ;
- le futur mandataire doit faire une demande d'enregistrement auprès de l'AE et fournir l'ensemble des éléments nécessaire au dossier d'enregistrement en Section 3.2.3 ;
- l'AE valide la demande et ajoute le MC à la liste de MC de l'AE.

4.2 Traitement d'une demande de certificat

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

Une AC Matérielle d'Universign assure elle-même la fonction d'AE. L'AE valide les demandes de certificats des demandeurs. L'AE identifie et valide les informations fournies par les demandeurs conformément aux dispositions de la section 3.2.

4.2.2 Acceptation ou rejet de la demande

La procédure de validation d'une demande de certificat par l'AE est la suivante :

- l'AE, ou le cas échéant le MC, vérifie que le dossier d'enregistrement est complet et valide. En particulier, l'AE ou le MC vérifie la conformité des informations contenues dans la demande d'enregistrement avec les documents justificatifs fournis par le demandeur ;
- l'AE ou le cas échéant le MC identifie avec succès le demandeur et les informations fournies conformément à la section 3.2 ;

En cas de rejet de la demande lors de l'une de ces étapes, le demandeur est immédiatement informé.

4.2.3 Durée d'établissement du certificat

L'AC Matérielle traite la requête de façon automatique dès 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

Une AC Matérielle crée un certificat à l'issue du processus de validation de la demande de certificat défini dans la section 4.2. La clé publique du Sujet doit être remise à l'AC Matérielle de façon à en assurer l'intégrité. Le certificat émis est conforme aux informations contenues dans la demande de certificat et au profil défini dans la section 7.1. Le certificat est généré dans des locaux sécurisés.

4.3.2 Notification par l'AC de la délivrance du certificat

Universign notifie dans un délai raisonnable le Demandeur de l'émission du certificat et le lui transmet de façon appropriée.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Les faits suivants sont considérés comme une acceptation implicite par un Abonné de son certificat émis par l'AC Matérielle :

- téléchargement du certificat par l'Abonné ou téléchargement d'un message contenant le certificat constitue une acceptation implicite du certificat ;
- l'absence d'objection sur le contenu du certificat dans un délai de 48h à compter de l'émission du certificat.

4.4.2 Publication du certificat

Une AC Matérielle ne publie pas les certificats émis sans l'accord préalable de l'Abonné.

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

Abonné :

Le certificat doit être utilisé en conformité avec :

- les exigences définies dans cette PC/DPC, en particulier les usages définis en section 1.4 ;
- l'Accord de Souscription ;
- toutes les conditions supplémentaires fixées par le contrat entre l'AC Matérielle et l'Abonné, le cas échéant ;
- l'extension `KeyUsage` ou tout autre extension contraignant l'utilisation de la clé, définie dans le certificat émis.

Les engagements de l'Abonné sont les suivants :

- l'Abonné s'engage à protéger sa ou ses clé privées dans un dispositif cryptographique tel que décrit dans la Section 6.2.11
- en cas de compromission de sa clé privée, l'Abonné s'engage à ne plus l'utiliser et notifier l'AC Matérielle de la compromission.
- en cas de compromission de la clé privée de l'AC Matérielle qui a émis le certificat, l'Abonné s'engage à ne plus utiliser son certificat.

Utilisateurs :

Les Utilisateurs doivent accepter l'Accord d'Utilisation avant d'utiliser tout certificat émis par une AC Matérielle. Les Utilisateurs sont responsables :

- de déterminer que l'utilisation du certificat est bien conforme aux utilisations autorisées et interdites par cette PC/DPC (voir section 1.4) ;
- de déterminer que le certificat est bien utilisé en conformité avec l'extension `KeyUsage` définie dans celui-ci ;
- de vérifier le statut du certificat.

4.6 Renouvellement d'un certificat

Aucun renouvellement n'est autorisé par l'AC Matérielle 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 à l'Abonné de l'établissement du certificat modifié

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 par l'AC Matérielle 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 à l'Abonné 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 à l'Abonné 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 émis par l'AC Matérielle sont les suivantes :

- demande de l'Abonné ;
- un Abonné n'a pas respecté ses engagements vis-à-vis d'une AC Matérielle, en particulier les exigences définies dans l'Accord de Souscription ;
- les informations présentes dans le certificat ne sont plus exactes ;
- forts soupçons de compromission, perte ou vol d'une clé privée ;
- une erreur dans la procédure d'enregistrement a été découverte ;
- un Abonné n'a pas versé le paiement relatif à l'émission du certificat, le cas échéant ;
- arrêt définitif d'activité de l'AC Matérielle Universign ;
- perte du contrôle de la clé privée associée au certificat, par le vol ou la perte des données d'activation de la clé privée ;

– l'utilisation du certificat en question porte préjudice à Universign.

4.9.2 Origine d'une demande de révocation

Certificat de personne physique Les personnes pouvant demander une révocation de certificat de personne physique sont les suivantes :
– le responsable de l'AC Matérielle, en son absence et en cas d'urgence, le Comité d'approbation d'Universign ;
– l'Abonné ;
– le Sujet, s'il diffère de l'Abonné.

Certificat d'entité ou d'organisation Les personnes pouvant demander une révocation de certificat d'entité ou d'organisation sont les suivantes :
– le responsable de l'AC Matérielle, en son absence et en cas d'urgence, le Comité d'approbation d'Universign ;
– le Responsable de certificat ;
– le représentant légal de l'entité ou de l'organisation.

4.9.3 Procédure de traitement d'une demande de révocation

Le Demandeur transmet une demande de révocation qui doit *a minima* contenir les informations suffisantes à la révocation :
– son nom complet ;
– l'identifiant de l'Abonné (voir la Sect. 3.1.1) ;
– les informations permettant à l'AC d'identifier de façon sûre le certificat à révoquer (par exemple, le numéro de série du certificat ou le `DN` complet du certificat) ;
– éventuellement la cause de la révocation. Cette information est donnée est à titre informatif et n'apparaît pas dans la LCR.

Certificat de personne physique Cette demande peut se faire de trois façons différentes, comme indiqué dans la section 3.4 :
– via l'interface utilisateur du service ;
– via un service spécifique accessible à tous les porteurs ;
– via messagerie électronique.

Certificat d'entité ou d'organisation La demande se fait par messagerie électronique, comme indiqué dans la section 3.4.

L'AC Matérielle Universign authentifie la demande de révocation conformément aux dispositions de la section 3.4 et révoque le certificat. Toutes les opéra-

tions sont réalisées de façon à garantir l'intégrité, la confidentialité (si nécessaire) et l'authenticité des données transmises tout au long du processus.

L'AC Matérielle Universign informe le Demandeur et le Abonné (s'il ne sont pas confondus) de la révocation effective du certificat et du changement de statut. Toute révocation est définitive.

4.9.4 Délai accordé à l'abonné pour formuler la demande de révocation

La demande de révocation doit être formulée au plus tôt.

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

Le délai maximum de traitement est de 24 heures, à partir de l'authentification effective du demandeur et de l'acceptation de la demande, 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

Les LCRs sont émises au moins une fois par jour.

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

Le service de révocation et les statuts des certificats sont disponibles sur un site internet de publication. Le service d'information sur l'état des certificats inclut un ou plusieurs répondeurs OCSP. Universign fournit sur son site de publication un lien vers le répondeur OCSP à utiliser pour vérifier le statut du certificat. Les OCSPs sont disponibles, en fonctionnement normal, 24h/24 et 7J/7.

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

Un utilisateur a l'obligation de vérifier le statut d'un certificat avant de l'utiliser pour vérifier une signature électronique. L'Utilisateur peut soit consulter la LCR publiée la plus récente, soit effectuer une demande de statut du certificat auprès du répondeur OCSP.

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 s'engage à notifier, dans la mesure du possible, l'ensemble des participants de l'ACU en cas de compromission ou de soupçon de compromission de la clé privée d'une AC Matérielle.

4.9.13 Causes possibles d'une suspension

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

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 LCR et les liens vers le ou les répondeurs OCSP sont publiés sur un site de publication spécifique accessible publiquement :

- depuis l'adresse définie dans la Section 2.1 ;
- depuis l'adresse spécifiée dans les certificats émis.

Universign assure l'intégrité et l'authenticité des LCR publiées et des réponses OCSP. Les LCR et les réponses OCSP contiennent les informations sur le statut des certificats au moins jusqu'à ce que ceux-ci expirent.

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.

4.10.3 Dispositifs optionnels

Sans objet.

4.11 Fin de la relation entre l'abonné et l'AC

Ce point est régi par le contrat entre une AC Matérielle et l'Abonné, qui peut définir des obligations se poursuivant après l'expiration ou la révocation du certificat. En l'absence d'une telle clause, l'Abonné met fin à sa relation avec une AC Matérielle en laissant son certificat expirer sans faire de nouvelle demande de certificat ou en révoquant son certificat sans faire de demande de nouveau certificat.

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 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 de certification d'Universign est restreint aux seules personnes nommément autorisées. 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 ;
- la description 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'hébergeur. Ces mécanismes se matérialisent par la possession de badges d'accès.

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

Les profils d'accès à chaque zone sont définis et maintenus par Universign.

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 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 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. Ces mesures sont en conformités avec les lois et règlements en vigueur.

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'AC Matérielle 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 Matérielle et des personnels habilités.

Les AC Matérielles prennent des mesures pour se protéger contre l'obsolescence et la détérioration des médias durant la période de rétention des enregistrements.

5.1.7 Mise hors service des supports

Les supports recensés comme sensibles en 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. En particulier, les mesures de destruction suivantes s'appliquent.

- Support papier/ CD / cartes à puces : ces supports sont passés à la broyeuse avant d'être jetés.
- HSM : les HSM sont désinstallés (zeroization) puis le cas échéant rendus inutilisables suivant les recommandations du fabriquant.
- Média de stockage : ils sont rendus illisibles par des méthodes adéquates avant d'être jetés.

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 réalisées par des personnes ayant des rôles de confiance.

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.

Universign garantit que les sauvegardes sont testées de façon régulière pour s'assurer que les mesures du plan de continuité d'activité sont respectés.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

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

Les rôles de confiance suivants sont définis :

Responsable de sécurité : il possède la responsabilité globale de tous les aspects sécurité du système d'information et de la mise en œuvre opérationnelle de l'IGC. En tant que membre du Comité d'approbation, il est chargé de l'approbation des opérations de génération et révocation de certificats.

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 des opérations d'exploitation quotidienne de l'IGC. Il est autorisé à réaliser des sauvegardes et des restaurations.

Auditeur : il est autorisé à voir les archives et l'ensemble des données d'audits de l'AC Matérielle.

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

L'AC Matérielle a établi des opérateurs d'enregistrement. Ces opérateurs assurent l'ensemble des opérations d'enregistrement des futurs porteurs.

A l'instar de l'ensemble des employés de l'AC Matérielle, 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 de l'AC Matérielle.

5.2.2 Nombre de personnes requises par tâches

L'AC Matérielle met en place des procédures de façon à ce que plusieurs personnes ayant un Rôle de Confiance soient nécessaires pour chaque opération sur les fonctions sensibles (redémarrage de l'IGC, restauration des clés,...) .

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.

5.2.4 Rôles exigeant une séparation des attributions

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

Chaque AC Matérielle 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 risque

Universign réalise une analyse de risque afin d'identifier les menaces sur les AC Matérielles. Cette analyse de risque est revue périodiquement et lors de changements structurels significatifs d'une AC Matérielle.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

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

5.3.2 Procédures de vérification des antécédents

Universign (ou le cas échéant l'organisation tierce employant les opérateurs d'enregistrement) procède avant la nomination d'une personne à un Rôle de Confiance à la vérification des antécédents de cette dernière, de manière à valider son adéquation vis-à-vis du poste à pourvoir. Il est vérifié que :

- la personne n'a pas de conflit d'intérêt incompatible avec le rôle à pourvoir ;
- la personne n'a pas commis de crime ou de délit mettant en cause sa correspondance avec le rôle à pourvoir.

Universign (ou le cas échéant l'organisation tierce employant les opérateurs d'enregistrement) sélectionne les personnes remplissant les rôles de confiance en tenant compte de leur loyauté, leur sérieux et leur intégrité. Les vérifications sont réalisées dans le cadre de la loi et des réglementations en vigueur.

5.3.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement. Ce matériel de formation est maintenu en conformité avec les pratiques.

5.3.4 Exigences et fréquence en matière de formation continue

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information et/ou de formation des 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

Un prestataire externe ne peut se voir confier un Rôle de Confiance au sein d'une AC Matérielle, à l'exception du rôle d'opérateur d'enregistrement.

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

L'ensemble des règles et procédures de sécurité documentées sont soumis à l'approbation du Comité d'approbation d'Universign. 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 l'IGC disposent d'un accès aux procédures correspondantes et sont tenus de les respecter.

5.4 Procédures de constitution des données d'audit

5.4.1 Type d'évènements à enregistrer

Universign prend les mesures nécessaires pour enregistrer les évènements suivants :

- l'ensembles des évènements liés à l'enregistrement ;
- l'ensembles des évènements liés au cycle de vie des clés des AC Matérielles ;
- l'ensembles des évènements liés au cycle de vie des certificats émis par les AC Matérielles, y compris les évènements liés à la révocation ;

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

Une AC Matérielle décrit dans ces procédures internes le détail des évènements et des données enregistrées.

Ces procédure de traçabilité mises en place par l'AC Matérielle sont robustes et permettent l'agrégation des traces issues de différentes sources, la détection d'intrusion et un plan de monitoring

5.4.2 Fréquence de traitement des journaux d'évènements

Les journaux d'évènements sont exploités systématiquement en cas de remontée d'un évènement anormal.

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pour une durée minimum d'un mois. Les journaux d'évènements sont externalisés tous les mois pour être archivés dans les locaux d'Universign.

5.4.4 Protection des journaux d'évènements

Les journaux d'évènements 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'évènements

Les journaux sont sauvegardés régulièrement sur un système externe.

5.4.6 Système de collecte des journaux d'évènements

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

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

Il n'y a pas de notification des évènements.

5.4.8 Évaluation des vulnérabilités

L'AC Matérielle Universign met en place les contrôles suivants :
- contrôle quotidien des accès physiques au sein de la salle ;
- contrôle des publications de LCR quotidien ;
- analyse quotidienne des évènements de l'AC par des personnels occupant des rôles de confiance.

Ces contrôles permettent à l'AC de détecter :
- les accès non autorisés ;
- les anomalies techniques ;
- les incohérences entre les différents évènements de l'AC.

5.5 Archivage des données

5.5.1 Types de données à archiver

Les données archivées sont les suivantes :
- les données d'enregistrement des Abonnés et des Responsables de certificats :
  - la preuve de l'acceptation des conditions générales d'utilisation par les Abonnés (voir Section 4.1.2) ;
  - les demandes d'enregistrement des Abonnés
  - une copie des éléments ayant permis de vérifier l'identité d'une personne physique
  - le cas échéant, pour les certificats de personne physique rattachée à une entité or organisation, une copie des éléments ayant permis de vérifier le lien entre la personne physique et l'entité ou organisation, ainsi que la preuve d'existence de celle-ci (voir Section 3.2.2) ;
  - le cas échéant, pour les certificats d'entité et d'organisation, une copie des éléments ayant permis de vérifier le lien entre le Responsable de certificat et l'entité ou l'organisation, ainsi que les documents ayant permit d'établir l'existence de l'organisation (voir Section 3.2.2) ;
- les journaux d'évènements. Ceux-ci contiennent en particulier :
  - les évènements relatifs à un changement significatif de l'environnement de l'AC Matérielle et la date/heure précise d'occurrence de l'évènement.
  - les évènements relatifs au opérations sur les clés et les certificats émis par l'AC Matérielle et la date/heure précise d'occurrence de l'évènement.

Une AC Matérielle décrit dans ses procédures interne le détail des données et évènements qui sont conservés.

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 Matérielle.

Journaux d'évènements :
Les journaux d'évènements sont archivés et conservés jusqu'à l'expiration du der-

nier certificat émis par l'AC.

L'ensemble des archives est conservé en conformité avec la législation en vigueur (voir Sect. 9.4.1)

5.5.3 Protection des archives

Quels que soient leurs supports, 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

Des sauvegardes régulières des archives sous forme électroniques sont réalisées par les personnels de confiance d'Universign. Ces sauvegardes sont exportées hors du site de production et bénéficient de mesures de protection de la confidentialité et de l'intégrité.

5.5.5 Exigences d'horodatage des données

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

5.5.6 Système de collecte des archives

Les systèmes de collecte des archives d'Universign sont internes.

5.5.7 Procédures de récupération et de vérification des archives

Les archives (papiers 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

Universign n'a pas de procédure automatique de renouvellement de clé, cependant, une AC Matérielle doit générer une nouvelle bi-clé et le certificat associé dans un temps raisonnable avant l'expiration du certificat en cours de validité, afin de permettre une transition en douceur vers le ou les nouveaux certificats. L'AC Matérielle doit appliquer toutes les actions nécessaires pour éviter tout arrêt des

opérations des utilisateurs du certificat de l'AC Matérielle. La nouvelle clé et son certificat doivent être générés et publiés en accord avec cette PC/DPC.

5.7 Reprise suite à compromission et sinistre

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

Chaque AC Matérielle met en place des procédures et des moyens de remontée et de traitement des incidents (sensibilisation, formation des personnels, analyse des différents journaux d'évènements, ...). Ces moyens permettent de minimiser les dommages en cas d'incidents.

L'AC Matérielle a mis en place un plan de réponse en cas d'incident majeur, tels qu'une compromission de ses mécanismes de publication ou de son mécanisme d'émission de certificat.

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

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.

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

Ce point est couvert par les plans de continuité et de reprise d'activité. La compromission d'une clé de l'AC Matérielle entraîne immédiatement la révocation des certificats délivrés. Dans ce cas, les différents acteurs et entités concernés seront avertis du caractère non sûr de la LCR signée par la clé compromise de l'AC Matérielle. Des mesures similaires sont prises si l'algorithme utilisé ou les paramètres utilisés par l'AC Matérielle ou les Abonnés deviennent d'une robustesse insuffisante pour les usages de l'AC Matérielle.

5.7.4 Capacités de continuité d'activité suite à un sinistre

La capacité de continuité de l'activité suite à un sinistre est traitée par le plan de reprise et le plan de continuité d'activité d'Universign. Suite à un sinistre, l'AC

Matérielle met en place ce plan afin de restaurer les services touchés. En particulier, chaque AC Matérielle a une architecture redondée pour ses services les plus critiques. De plus, Universign gère un stock de matériel de rechange afin de palier toute panne matérielle. En cas d'incident majeur, Universign possède un plan de reprise d'activité lui permettant de remettre en place une AC Matérielle dans une durée raisonnable. Ce plan s'appuie sur une salle d'hébergement secondaire susceptible d'accueillir les activités en cas de nécessité.

Suite à la reprise d'activité, Universign met en œuvre, dans la mesure du possible, l'ensemble des mesures nécessaires pour éviter qu'un sinistre similaire se reproduise. Les opérations de restauration sont réalisées par des personnels occupant des Rôles de Confiance.

5.8 Fin de vie de l'IGC

En cas d'arrêt définitif de service d'une AC Matérielle, Universign met en place un plan de fin de vie de cette AC Matérielle. Ce plan de fin de vie pourra entre autre adresser les points suivant :

1. information directe à l'ensemble des Abonnés, à l'ensemble des entités avec lesquels l'AC Matérielle est sous contrat ;
2. mise à disposition des informations pour les Utilisateurs ;
3. notification de l'arrêt à l'ensemble des AC de niveau supérieur ;
4. potentielle révocation de tous les certificats émis encore en cours de validité ;
5. sort de la clé privée de l'AC Matérielle, qui devra être détruite ou rendue inutilisable ;
6. dispositions nécessaires pour transférer ses obligations relatives aux dossiers d'enregistrement, aux listes de révocations et aux archives des données d'audit pour les durées respectives pour lesquelles elle s'est engagée vis-à-vis des utilisateurs et des Abonnés.

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération et installation de bi-clés

Clés d'AC Matérielle :

Les clés de l'AC Matérielle sont générées :

– lors d'une cérémonie des clés devant témoins (dont un huissier de justice) ;

– sous le contrôle d'au moins deux personnes ayant des rôle de confiance (voir Sect. 5.2.1) ;
– dans les locaux sécurisés (voir Sect. 5.1) ;
– au sein d'un HSM répondant aux exigences définies dans la section 6.2.11.

Clés d'Abonné :

Les clés de l'Abonné sont générées :

– dans les locaux sécurisés (voir Sect. 5.1) ;
– au sein d'un HSM répondant aux exigences définies dans la section 6.2.11.

6.1.2 Transmission de la clé privée au serveur

Sans objet. Les Abonnés possèdent leur propre HSM générateur de bi-clé.

6.1.3 Transmission de la clé publique à l'AC

La clé publique d'une Abonné est transmise électroniquement par l'Abonné à l'AC Matérielle d'une façon apportant des garanties suffisantes quant à l'intégrité et l'origine de la clé publique.

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

Les certificats des AC Matérielles d'Universign sont publiés sur le site : http://docs.universign.eu.

Les certificats doivent contenir les informations conformes à la politique de certification de l'AC ayant émis le certificat.

Les Utilisateurs peuvent également adresser un email au point de contact identifié au paragraphe 1.5.2 une demande de confirmation des certificats d'AC Matérielle. L'en-tête du mail doit contenir l'information suivante "Demande des certificats des AC Matérielles d'Universign ".

6.1.5 Tailles des clés

Les clés des AC Matérielles d'Universign doivent être conformes (ou être cryptographiquement supérieures ou égales) aux caractéristiques suivantes :

Certificat	Taille des clés	Format
AC Matérielle	2048	RSA

Les clés des Abonnés doivent être conformes (ou être cryptographiquement

supérieures ou égales) aux caractéristiques suivantes :

Certificat	Taille des clés	Format
Abonné	2048	RSA

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

Les AC Matérielles et les Abonnés doivent utiliser des algorithmes et du matériel certifié (voir Sect. 6.2.11), avec 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

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 6.2.11. L'AC Matérielle s'assure de la sécurité des HSM utilisés tout au long de leur cycle de vie. En particulier, l'AC Matérielle 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 décommissionné.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Les clés privées des AC Matérielles Universign sont contrôlées 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 œuvre par l'AC Matérielle par une méthode de partage à seuil.

6.2.3 Séquestre de la clé privée

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

6.2.4 Copie de secours de la clé privée

Les clés privées d'AC Matérielle font l'objet de copies de sauvegarde :

– soit hors d'un module cryptographique mais sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. 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. Ces copies de sauvegarde de clé privée de l'AC Matérielle sont stockées dans un coffre fort sécurisé, accessible uniquement par des personnels de confiance.
– soit dans un module cryptographique équivalent opéré dans des conditions de sécurité similaires ou supérieures.

Les sauvegardes sont réalisées sous le contrôle de deux personnels de confiance.

6.2.5 Archivage de la clé privée

Les clés privées de l'AC Matérielle ne sont pas archivées.

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

Les clés privées de l'AC Matérielle sont générées dans son module cryptographique et ne sont transférées que pour la réalisation de copies de secours (voir Section 6.2.4). 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. Chaque génération de copie de secours ou de restauration dans un HSM est réalisée par au moins deux personnels de confiance dans des locaux sécurisés.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées des AC Matérielles sont protégées par leurs modules cryptographiques.

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

L'activation des clés privées d'AC Matérielle est contrôlée par des données d'activation et est réalisée au sein d'un module cryptographique répondant aux exigences de la Section 6.2.11, sous le contrôle de deux personnes dans des Rôles de Confiance.

6.2.9 Méthode de désactivation de la clé privée

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

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

Module cryptographique de l'AC Matérielle : Le HSM utilisé par l'AC Matérielle doit satisfaire les exigences de certification suivantes :

- EAL 4+ aux Critères Communs ISO/CEI 15408 (conforme au Profil de protection CWA 14167-2 ou CWA 14167-3) ; ou
- FIPS 140-2 level 3 ou équivalent ou supérieur.

Module cryptographique des Abonnés : L'AC Matérielle ne fournit pas les HSM des Abonnés. Les HSM des Abonnés doivent satisfaire au minimum aux certifications suivantes :

- EAL 4+ aux Critères Communs ISO/CEI 15408 (conforme au Profil de protection CWA 14169 ou certifié conforme au Profil de protection Secure

Signature Creation Device (SSCD) par une entité gouvernementale européenne). ; ou
– FIPS 140-2 level 2 ou équivalent ou supérieur.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

L'AC Matérielle archive sa ou ses clés publiques, en conformité avec les exigences de la section 5.5.

6.3.2 Durées de vie des bi-clés et des certificats

Une AC Matérielle ne délivre pas aux Abonnés de certificats dont la date de validité dépasserait la durée de vie de la clé privée de l'AC Matérielle.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

La génération et l'installation des données d'activation du HSM de l'AC Matérielle sont réalisées durant la cérémonie des clés devant témoins dont un huissier de justice dans des locaux sécurisés. Ces données d'activation sont stockées sur des cartes à puce et remises à des porteurs de secrets. Chaque porteur de secret prend les mesures nécessaires pour se prémunir contre la perte, le vol, l'utilisation non autorisée ou la destruction non autorisée des cartes à puce et des données d'activation qu'elles contiennent.

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 sous 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 individuel. Chaque porteur de secret est responsable de sa part de secret d'activation et donne son accord en signant un formulaire définissant ses responsabilités.

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 techniques spécifiques aux systèmes informatiques

Identification et authentification

Les systèmes, applications et bases de données identifient et authentifient de façon 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 façon 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 utilisateur, 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 rebut) des équipements sont documentées 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 procédures de suivi de cycle de vie afin de garantir la traçabilité et de procédures 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.

Un suivi de la capacité et des projections sont réalisés afin de s'assurer que les AC Matérielles ont les capacités de stockage et de production suffisantes.

Intégrité des composantes :

Les composantes du réseau local sont maintenues dans un environnement physiquement 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 différentes composantes.

Journalisation et audit :

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

Supervision et contrôle :

Une surveillance permanente est mise en place et des systèmes d'alarme 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

Tous les composants logiciels de l'IGC développés par Universign sont développés dans des conditions et suivant un processus de développement donnant des assurances sur leur sécurité. Universign met en œuvre des processus qualité au cours du design et du développement de ses logiciels. Universign s'assure, lors de la mise en production d'un élément logiciel, de son origine et de son intégrité. Les infrastructures de développement et d'essai sont séparées des infrastructures opérationnelles de l'IGC.

6.6.2 Mesures liées à la gestion de la sécurité

Universign s'assure que la mise à jour des logiciels est réalisée de façon à assurer la sécurité du système. Les mises à jour sont réalisées par des personnels de confiance d'Universign.

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

Sans objet.

6.7 Mesures de sécurité réseau

Les services de l'AC Matérielle sont implantés sur un réseau protégé par des passerelles de type "coupe-feu". Ces passerelles sont configurées de façon à n'accepter que les flux strictement nécessaires.

Les communications réseaux véhiculant des informations confidentielles font l'objet de mesures de protection contre l'écoute des informations.

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

L'AC Matérielle met en place des procédures de gestion des accès d'administration de la plate-forme afin de maintenir la sécurité. Ces mesures incluent l'authentification des administrateurs, la production de traces pour les audits ainsi que la possibilité de modifier à tout instant les droits d'accès.

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

6.8 Horodatage / Système de datation

L'ensemble des serveurs de l'AC Matérielle d'Universign est synchronisé avec la même source de temps pour garantir que les serveurs de l'IGC sont correctement synchronisés.

7 Profil des certificats, des OCSP et des LCR

7.1 Profil des certificats

7.1.1 Certificat de l'AC

Champs de base

Champs	Valeur
Version	v3
Numéro de série	défini par l'outil
Signature	RSA/SHA-256
Issuer DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=`Universign Primary CA hardware`
Validité	10 ans
Subject DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=`Universign CA hardware`
Clé publique	RSA 2048 bits

Extensions du certificat

Champ	OID	Critique	Valeur
Authority Key Identifier	2.5.29.35	Non	
KeyIdentifier			RFC 5280 - Méthod 0
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
Basic Constraint	2.5.29.19	Oui	
CA			Vrai
Maximum Path Length			0 [11]
CRL Distribution Points	2.5.29.31	Non	
fullName			http://crl.universign.eu/universign_primary_ca_hardware.crl [12]
reasons			Absent
cRLIssuer			Absent
Certificate Policies	2.5.29.32	Non	
policyIdentifier			2.5.29.32.0
policyQualifierId			1.3.6.1.5.5.7.2.1
qualifier			http://docs.universign.eu/

11. Cette version de la PC/DPC limite le paramètre `Maximum Path Length` à 0.
12. Cette URL est donnée à titre indicatif et est sujette à des changements potentiels. Seul l'URL présente dans le certificat fait foi.

7.1.2 Certificat de l'Abonné

Champs de base

Certificat de Personne Physique

Champ	Valeur
Version	v3
Numéro de série	défini par l'outil
Signature	RSA/SHA-256
Issuer DN	C=FR O=Cryptolog International OU=0002 43912916400026 CN=`Universign CA hardware`
validité	5 ans
Subject DN	C=Code du Pays d'origine du porteur O= Nom de l'organisation de rattachement, si applicable. OU= Numéro de l'organisation de rattachement, si applicable. SERIALNUMBER= défini par l'outil. CN= Nom et Prénom de la Personne.
Clé publique	RSA 2048 bits

Certificat d'entité ou d'organisation

Champ	Valeur
Version	v3
Numéro de série	défini par l'outil
Signature	RSA/SHA-256
Issuer DN	C=FR O=Cryptolog International OU=0002 43912916400026 CN=`Universign CA hardware`
validité	5 ans
Subject DN	C=Pays de l'entité ou de l'organisation O= Nom de l'entité ou de l'organisation OU= Numéro d'identification CN= Champ libre
Clé publique	RSA 2048 bits

Extensions du certificat

Certificat de Personne Physique

Champ	OID	Critique	Valeur
Authority Key Identifier	2.5.29.35	Non	
KeyIdentifier			RFC 5280 - Méthode 0
Subject Key Identifier	2.5.29.14	Non	
KeyIdentifier			RFC 5280 - Méthode 1
Key Usage	2.5.29.15	Oui	
digitalSignature			Faux
nonRepudiation			Vrai
keyEncipherment			Faux
dataEncipherment			Faux
keyAgreement			Faux
keyCertSign			Faux
cRLSign			Faux
encipherOnly			Faux
decipherOnly			Faux
Basic Constraint	2.5.29.19	Oui	
CA			Faux
CRL Distribution Points	2.5.29.31	Non	
fullName			http://crl.universign.eu/universign_subordinate_ca_hardware.crl [13]
reasons			Absent
cRLIssuer			Absent
Certificate Policies	2.5.29.32	Non	
policyIdentifier			1.3.6.1.4.1.15819.5.1.3.1 ou 1.3.6.1.4.1.15819.5.1.3.3 [14]
policyQualifierId			1.3.6.1.5.5.7.2.1
qualifier			http ://docs.universign.eu/
Qualified Certificate Statements [15]	1.3.6.1.5.5.7.1.3	Non	
Qualified Certificate Statment			0.4.0.1862.1.1
Authority Info Access	1.3.6.1.5.5.7.1.1	Non	
fullName			http://scah.ocsp.universign.eu/ [16]

13. Cette URL est donnée à titre indicatif et est sujette à des changements potentiels. Seul l'URL présente dans le certificat fait foi.
14. Selon la méthode d'enregistrement mise-en-oeuvre.
15. Seulement pour les certificats 1.3.6.1.4.1.15819.5.1.3.1 (Enregistrement en face-à-face))
16. Cette URL est donnée à titre indicatif et est sujette à des changements potentiels. Seul l'URL

Certificat d'entité ou d'organisation

Champ	OID	Critique	Valeur
Authority Key Identifier	2.5.29.35	Non	
KeyIdentifier			RFC 5280 - Méthod 0
Subject Key Identifier	2.5.29.14	Non	
KeyIdentifier			RFC 5280 - Méthode 1
Key Usage	2.5.29.15	Oui	
digitalSignature			Faux
nonRepudiation			Vrai
keyEncipherment			Faux
dataEncipherment			Faux
keyAgreement			Faux
keyCertSign			Faux
cRLSign			Faux
encipherOnly			Faux
decipherOnly			Faux
Basic Constraint	2.5.29.19	Oui	
CA			Faux
CRL Distribution Points	2.5.29.31	Non	
fullName			http://crl.universign.eu/universign_subordinate_ca_hardware.crl [17]
reasons			Absent
cRLIssuer			Absent
Certificate Policies	2.5.29.32	Non	
policyIdentifier			1.3.6.1.4.1.15819.5.1.3.2 ou 1.3.6.1.4.1.15819.5.1.3.4 [18]
policyQualifierId			1.3.6.1.5.5.7.2.1
qualifier			http ://docs.universign.eu/
Authority Info Access	1.3.6.1.5.5.7.1.1	Non	
fullName			http://scah.ocsp.universign.eu/ [19]

présente dans le certificat fait foi.

17. Cette URL est donnée à titre indicatif et est sujette à des changements potentiels. Seul l'URL présente dans le certificat fait foi.

18. Selon la méthode d'enregistrement mise-en-oeuvre.

19. Cette URL est donnée à titre indicatif et est sujette à des changements potentiels. Seul l'URL présente dans le certificat fait foi.

7.2 Profil des LCRs

Champs de base

Champ	Valeur
Version	1
Signature	RSA/SHA-256
Issuer DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=`Universign CA hardware`
Next Update	This Update + 7 jour

Extensions de LCR

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

7.3 Profil des OCSPs

Universign propose la vérification du statut des certificats émis via des répondeurs OCSP (Online Certificate Status Protocol). Le répondeur OCSP permet de répondre en temps réel à des requêtes demandant le statut d'un certificat particulier sans avoir besoin de télécharger la LCR. L'OCSP d'Universign supporte le standard RFC 5019.

Extension des OCSP Les réponses OCSP contiennent des dates de validité permettant à l'utilisateur d'établir si la réponses OCSP est assez récente pour l'usage qu'il souhaite en faire. Universign OCSP n'utilise pas de *nonce* dans ces réponses OCSP. L'utilisateur, de ce fait, ne doit pas s'attendre à recevoir un nonce dans ces réponses si sa requête en contenait un.

8 Audit de conformité et autres évaluations

8.1 Fréquences et / ou circonstances des évaluations

Un audit de conformité à la PC en vigueur est effectué lors de la mise en œuvre opérationnelle d'une AC Matérielle, et lors de toute modification significative.

Universign bénéficie de plusieurs types d'audit :
- un audit interne ;
- un audit de certification à la norme [ETSI 102.042], réalisé annuellement par un organisme accrédité.
- un audit de certification à la norme [ETSI 101.456], réalisé annuellement par un organisme accrédité.

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 conformité qui pourraient compromettre la sécurité du service offert. Une AC Matérielle 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

Pour l'audit interne, 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'AC Matérielle auditée. Pour l'audit de certification, l'évaluateur doit être indépendant et exempt de tout conflit d'intérêt.

8.4 Sujets couverts par les évaluations

L'évaluateur procède à des contrôles de conformité de l'AC Matérielle auditée, sur toute ou partie de la mise en œuvre :
- de la PC/DPC ;
- des composantes de l'AC Matérielle.

Avant chaque audit, les évaluateurs proposeront au Comité d'approbation de l'AC Matérielle 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 Comité d'approbation de l'AC Matérielle auditée, un avis parmi les suivants : "réussite", "échec",

"à confirmer".

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

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

8.6 Communication des résultats

Les résultats des audits de conformité de chaque AC Matérielle sont tenus à la disposition des organismes de certification en charge de chacune des AC Matérielles .

9 Autres problématiques métiers et légales

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Une AC Matérielle est autorisée à tarifer ses services de génération de certificats.

9.1.2 Tarifs pour accéder aux certificat

Une AC Matérielle offre un accès gratuit à son site de publication.

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

Une AC Matérielle offre un accès gratuit au service de publication des LCR et au service de révocation. Cependant, dans le cas ou une AC Matérielle mettrait en place en parallèle des services avancés supplémentaires de publication et de révocation, alors elle pourrait être autorisée à tarifier ces services spécifiques.

9.1.4 Tarifs pour d'autres services

Une AC Matérielle offre l'accès à cette PC/DPC gratuitement. Toute utilisation autre que la consultation, telles que la reproduction, la distribution, la modification, la création de produits dérivées de cette PC/DPC devra se faire avec l'accord d'Universign et sera éventuellement soumise à un accord de licence.

9.1.5 Politique de remboursement

Dans la limite de la réglementation applicable, Universign ne pratique pas de politique de remboursement.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

Universign a souscrit à une assurance professionnelle. Universign encourage ses clients, en particulier les Abonnés, à des souscriptions similaires, mais ne l'impose pas.

9.2.2 Autres ressources

Universign met en œuvre une politique financière visant, dans la mesure du possible, à avoir en permanence les ressources financières nécessaires pour remplir les obligations et opérations définies dans cette PC/DPC.

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 des AC Matérielles,
- les données d'activation associées aux clés privées des AC Matérielles d'Universign,
- les journaux d'évènements,
- les dossiers d'enregistrement (acceptés et refusés),
- les rapports d'audit,
- les plans de continuité, de reprise et d'arrêt d'activité,
- les causes de révocation des certificats.

D'autre informations peuvent être classées confidentielles, en particulier si elles ont été démontrées sensibles suite à une analyse de risque (Voir Section 5.2.5).

9.3.2 Informations hors du périmètre des informations confidentielles

Le site de publication d'Universign et son contenu (certificat, LCR, information de statut des certificats, etc) est considéré comme public, donc non confidentiel.

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 en confidentialité et conservées conformément aux termes de la loi N° 78-17 du 6 janvier 1978.

9.4.2 Informations à caractère personnel

Les données des dossiers d'enregistrement non publiées dans les certificats ou les LCR sont considérées comme privées.

9.4.3 Informations à caractère non personnel

Pas d'engagement spécifique.

9.4.4 Responsabilité en termes de protection des données personnelles

Toute information personnelle sera protégée par Universign contre la compromission dans le cadre de la réglementation en vigueur.

9.4.5 Notification et consentement d'utilisation des données personnelles

Sauf cas défini dans la présente PC/DPC, dans l'Accord de Souscription ou dans un accord formel entre l'AC Matérielle et l'Abonné, Universign n'utilisera pas les informations privées sans autorisation, dans les limites de la réglementation en vigueur.

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 dans le cadre d'une procédure judiciaire.

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 par Universign 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.

Propriété intellectuelle des informations des Certificats et des Révocations Universign garde l'entière propriété intellectuelle des certificats et des informations de révocation émis par Universign. Universign accorde la permission de reproduire et de redistribuer les certificats émis si :

- il n'en est pas fait d'usage commercial ;
- les certificats ne sont modifiés d'aucune manière ;
- l'Accord d'Utilisation s'applique à leur utilisation.

Universign accorde la permission d'utiliser les informations de statut des certificats dans le cadre défini par l'Accord d'Utilisation.

Propriété intellectuelle de cette PC/DPC Universign possède la propriété intellectuelle de cette PC/DPC.

Propriété intellectuelle des noms Un Abonné garde la propriété intellectuelle, le cas échéant, des marques et noms déposés contenus dans le dossier d'enregistrement ou dans le `DN` du certificat émis.

Propriété intellectuelle sur les clés

Les bi-clés des AC Matérielles sont la propriété intellectuelle d'Universign. Les bi-clés des Abonnés sont la propriété de chaque Abonné. Les données d'acti-

vation des bi-clés des AC Matérielles sont la propriété 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/DPC de l'AC Matérielle et les documents qui en découlent ;
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC Matérielle ;
- 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/DPC ;
- de la conformité des certificats émis vis-à-vis de la présente PC/DPC ;
- 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 Matérielle 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 Matérielle 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

L' Abonné :
- communique des informations exactes et à jour lors d'une demande d'établissement d'un Abonné ;
- protège la clé privée dont il a la responsabilité ;
- respecte les conditions d'utilisation de la clé privée conformément à ce qui est établi dans la présente PC/DPC ;
- informe l'AC Matérielle de toute modification concernant les informations contenues dans le certificat de l'Abonné ;
- fait sans délai une demande de révocation du certificat d'Abonné en cas de suspicion de compromission de la clé privée correspondante.

L' Abonné est enregistré auprès de l'AC Matérielle Universign conformément à la procédure définie dans la présente PC/DPC.

9.6.4 Utilisateurs de certificats

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

9.6.5 Autres participants

Mandataires de certification Le Mandataires de certification est responsable de :
- l'identification des individus et de la validation de leur lien avec l'entité d'appartenance ;
- du respect du processus d'enregistrement des dossiers dont il est responsable.

9.7 Limite de garantie

Les limites des garanties offertes par les AC Matérielles sont décrites dans l'Accord de Souscription et dans l'Accord d'Utilisation, dans la limite des lois et règlements applicables.

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, des informations de révocation, 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 française, 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

L'AC Matérielle s'autorise à demander des indemnités à l'Abonné si celui-ci ne respecte pas les conditions contractuelles liant les deux entités.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

La présente PC/DPC est mise en application lors de sa publication sur le site de publication de Universign à la fin de la période de commentaire. La présente PC/DPC reste en application jusqu'à la fin de vie du dernier certificat émis au titre de cette PC/DPC.

9.10.2 Fin anticipée de validité

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

9.10.3 Effets de la fin de validité et clauses restant applicables

En fin de validité de cette PC/DPC, les participants de l'IGC restent liés par cette PC/DPC pour tous les certificats émis lorsqu'elle était valide, jusqu'à l'expiration du dernier certificat.

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/DPC 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'amendement

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

Lorsqu'une nouvelle version de la PC/DPC est approuvée le Comité d'approbation d'Universign, elle est publiée sur le site web d'Universign et remplace les termes de la version précédente à l'issue de la période de commentaires.

9.12.2 Mécanisme et période d'information sur les amendements

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

Lorsqu'une nouvelle version de la PC/DPC 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/DPC telle quelle, de redémarrer le processus

d'amendement avec une version modifiée ou de retirer la version proposée.

Sauf indication contraire, la nouvelle version de la PC/DPC 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 DÉCOULANT DE L'INTERPRÉTATION, L'APPLICATION ET/OU L'EXÉCUTION DU CONTRAT ET À DÉFAUT D'ACCORD AMIABLE ENTRE LES PARTIES CI-AVANT, LA COMPETENCE EXCLUSIVE EST ATTRIBUÉE 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 français et notamment aux documents [CNIL].

9.16 Dispositions diverses

9.16.1 Accord global

Sans objet.

9.16.2 Transfert d'activités

Sans objet.

9.16.3 Divisibilité

Dans le cas où une disposition de la PC/DPC s'avérerait être invalide, illégale ou non exécutoire de l'avis d'un tribunal de la juridiction compétent, la validité, la légalité et le caractère exécutoire des autres clauses ne seront en aucun cas affectées ou réduites.

9.16.4 Application et renonciation

Sans objet.

9.16.5 Force majeure

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

9.17 Autres dispositions

Sans objet.

Références

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

[**RFC 5280**]
Network Working Group - Request for Comments : 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile - May 2008

[**ETSI 102.042**]
ETSI TS 102 042 V2.2.1 - Policy requirements for certification authorities issuing public key certificates (2011-12)

[**ETSI 101.456**]
ETSI TS 101 456 V1.4.3 - Policy requirements for certification authorities issuing qualified certificates (2007-5)

[**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.