



universign

powered by
Cryptolog

AC Primaires Universign

Politique de Certification
Déclaration des Pratiques de Certification

OID: 1.3.6.1.4.1.15819.5.1.2.1
1.3.6.1.4.1.15819.5.1.2.2

Table des matières

1	Introduction	10
1.1	Présentation Générale	10
1.2	Identification du document	11
1.3	Entités intervenant dans l'IGC	12
1.3.1	Autorité de certification	12
1.3.2	Autorité d'enregistrement	12
1.3.3	Porteurs de Certificats	12
1.3.4	Utilisateurs de certificats	13
1.3.5	Autres Participants	14
1.4	Usage des certificats	14
1.4.1	Domaines d'utilisation applicables	14
1.4.2	Domaines d'utilisation interdits	14
1.5	Gestion de la présente politique	14
1.5.1	Entité gérant la politique	14
1.5.2	Point de contact	14
1.5.3	Entité déterminant la conformité des pratiques de la PC	15
1.5.4	Procédure d'approbation de la conformité de la PC/DPC	15
1.6	Définitions et abréviations	15
2	Responsabilités concernant la mise à disposition des informations devant être publiées	16
2.1	Entités chargées de la mise à disposition des informations	16
2.2	Informations Publiées	17
2.3	Délais et fréquences de publication	17
2.4	Contrôle d'accès aux informations publiées	17
3	Identification et authentification	18
3.1	Nommage	18
3.1.1	Types de noms	18
3.1.2	Noms explicites	19
3.1.3	Anonymisation ou pseudonymisation des porteurs	19
3.1.4	Règles d'interprétation des différentes formes de noms	19
3.1.5	Unicité des noms	19
3.1.6	Identification, authentification et rôle des marques déposées	19
3.2	Validation initiale de l'identité	20
3.2.1	Méthode pour prouver la possession de la clé privée	20
3.2.2	Validation de l'identité d'un organisme	20
3.2.3	Validation de l'identité d'un individu	20
3.2.4	Informations non vérifiées du porteur	21

3.2.5	Validation de l'autorité du demandeur	21
3.2.6	Critères d'interopérabilité	21
3.3	Identification et validation d'une demande de renouvellement de clés	21
3.3.1	Identification et validation pour un renouvellement courant	21
3.3.2	Identification et validation pour un renouvellement après révocation	21
3.4	Identification et validation d'une demande de révocation	21
4	Exigences opérationnelles sur le cycle de vie des certificats	22
4.1	Demande de certificat	22
4.1.1	Origine d'une demande de certificat	22
4.1.2	Processus et responsabilités pour l'établissement d'une demande de certificat	22
4.2	Traitement d'une demande de certificat	23
4.2.1	Exécution des processus d'identification et de validation de la demande	23
4.2.2	Acceptation ou rejet de la demande	23
4.2.3	Durée d'établissement du certificat	23
4.3	Délivrance du certificat	23
4.3.1	Actions de l'AC concernant la délivrance du certificat	23
4.3.2	Notification par l'AC de la délivrance du certificat	24
4.4	Acceptation du certificat	24
4.4.1	Démarche d'acceptation du certificat	24
4.4.2	Publication du certificat	24
4.4.3	Notification par l'AC aux autres entités de la délivrance du certificat	24
4.5	Usage de la bi-clé et du certificat	24
4.6	Renouvellement d'un certificat	25
4.6.1	Causes possibles de renouvellement d'un certificat	25
4.6.2	Origine d'une demande de renouvellement	25
4.6.3	Procédure de traitement d'une demande de renouvellement	25
4.6.4	Notification à l'Abonné de l'établissement du certificat modifié	25
4.6.5	Démarche d'acceptation du nouveau certificat	25
4.6.6	Publication du nouveau certificat	26
4.6.7	Notification par l'AC aux autres entités de la délivrance du nouveau certificat	26
4.7	Délivrance d'un nouveau certificat suite à changement de la bi-clé	26
4.7.1	Causes possibles de changement d'une bi-clé	26
4.7.2	Origine d'une demande d'un nouveau certificat	26

4.7.3	Procédure de traitement d'une demande d'un nouveau certificat	26
4.7.4	Notification à l'Abonné de l'établissement du nouveau certificat	26
4.7.5	Démarche d'acceptation du nouveau certificat	26
4.7.6	Publication du nouveau certificat	26
4.7.7	Notification par l'AC aux autres entités de la délivrance du nouveau certificat	26
4.8	Modification du certificat	27
4.8.1	Causes possibles de modification d'un certificat	27
4.8.2	Origine d'une demande de modification d'un certificat	27
4.8.3	Procédure de traitement d'une demande de modification d'un certificat	27
4.8.4	Notification à l'Abonné de l'établissement du certificat modifié	27
4.8.5	Démarche d'acceptation du certificat modifié	27
4.8.6	Publication du certificat modifié	27
4.8.7	Notification par l'AC aux autres entités de la délivrance du certificat modifié	27
4.9	Révocation et suspension des certificats	27
4.9.1	Causes possibles d'une révocation	27
4.9.2	Origine d'une demande de révocation	28
4.9.3	Procédure de traitement d'une demande de révocation	28
4.9.4	Délai accordé à une AC Intermédiaire pour formuler la demande de révocation	29
4.9.5	Délai de traitement par l'AC d'une demande de révocation	29
4.9.6	Exigences de vérification de la révocation par les utilisateurs de certificats	29
4.9.7	Fréquence d'établissement des LCR	29
4.9.8	Délai maximum de publication d'une LCR	29
4.9.9	Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats	29
4.9.10	Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats	29
4.9.11	Autres moyens disponibles d'information sur les révocations	29
4.9.12	Exigences spécifiques en cas de compromission de la clé privée	30
4.9.13	Causes possibles d'une suspension	30
4.9.14	Origine d'une demande de suspension	30
4.9.15	Procédure de traitement d'une demande de suspension	30
4.9.16	Limites de la période de suspension d'un certificat	30

4.10	Fonction d'information sur l'état des certificats	30
4.10.1	Caractéristiques opérationnelles	30
4.10.2	Disponibilité de la fonction	30
4.10.3	Dispositifs optionnels	31
4.11	Fin de la relation entre une AC Intermédiaire et une AC Primaire	31
4.12	Séquestre de clé et recouvrement	31
4.12.1	Politique et pratiques de recouvrement par séquestre des clés	31
4.12.2	Politique et pratiques de recouvrement par encapsulation des clés de session	31
5	Mesures de sécurité non techniques	31
5.1	Mesures de sécurité physique	31
5.1.1	Situation géographique et construction des sites	31
5.1.2	Accès physiques	32
5.1.3	Alimentation électrique et climatisation	33
5.1.4	Exposition aux dégâts des eaux	33
5.1.5	Prévention et protection incendie	33
5.1.6	Conservation des supports de données	33
5.1.7	Mise hors service des supports	33
5.1.8	Sauvegarde hors site	34
5.2	Mesures de sécurité procédurales	34
5.2.1	Rôles de confiance	34
5.2.2	Nombre de personnes requises par tâches	35
5.2.3	Identification et authentification pour chaque rôle	35
5.2.4	Rôles exigeant une séparation des attributions	35
5.2.5	Analyse de risque	35
5.3	Mesures de sécurité vis-à-vis du personnel	36
5.3.1	Qualifications, compétences et habilitations requises	36
5.3.2	Procédures de vérification des antécédents	36
5.3.3	Exigences en matière de formation initiale	36
5.3.4	Exigences et fréquence en matière de formation continue	36
5.3.5	Fréquence et séquence de rotation entre différentes attributions	37
5.3.6	Sanctions en cas d'actions non autorisées	37
5.3.7	Exigences vis-à-vis du personnel des prestataires externes	37
5.3.8	Documentation fournie au personnel	37
5.4	Procédures de constitution des données d'audit	37
5.4.1	Type d'évènements à enregistrer	37
5.4.2	Fréquence de traitement des journaux d'évènements	38
5.4.3	Période de conservation des journaux d'évènements	38

5.4.4	Protection des journaux d'évènements	38
5.4.5	Procédure de sauvegarde des journaux d'évènements	38
5.4.6	Système de collecte des journaux d'évènements	38
5.4.7	Notification de l'enregistrement d'un évènement au responsable de l'évènement	39
5.4.8	Évaluation des vulnérabilités	39
5.5	Archivage des données	39
5.5.1	Types de données à archiver	39
5.5.2	Période de conservation des archives	40
5.5.3	Protection des archives	40
5.5.4	Procédure de sauvegarde des archives	40
5.5.5	Exigences d'horodatage des données	40
5.5.6	Système de collecte des archives	40
5.5.7	Procédures de récupération et de vérification des archives	40
5.6	Changement de clés d'AC	41
5.7	Reprise suite à compromission et sinistre	41
5.7.1	Procédures de remontée et de traitement des incidents et des compromissions	41
5.7.2	Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)	41
5.7.3	Procédures de reprise en cas de compromission de la clé privée d'une composante	41
5.7.4	Capacités de continuité d'activité suite à un sinistre	42
5.8	Fin de vie de l'IGC	42
6	Mesures de sécurité techniques	43
6.1	Génération et installation de bi-clés	43
6.1.1	Génération et installation de bi-clés	43
6.1.2	Transmission de la clé privée à une AC Intermédiaire	43
6.1.3	Transmission de la clé publique à une AC primaire	43
6.1.4	Transmission de la clé publique de l'AC aux utilisateurs de certificats	43
6.1.5	Tailles des clés	44
6.1.6	Vérification de la génération des paramètres des bi-clés et de leur qualité	44
6.1.7	Objectifs d'usage de la clé	44
6.2	Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques	44
6.2.1	Standards et mesures de sécurité pour les modules cryptographiques	44
6.2.2	Contrôle de la clé privée	45

6.2.3	Séquestre de la clé privée	45
6.2.4	Copie de secours de la clé privée	45
6.2.5	Archivage de la clé privée	45
6.2.6	Transfert de la clé privée vers / depuis le module cryptographique	45
6.2.7	Stockage de la clé privée dans un module cryptographique	46
6.2.8	Méthode d'activation de la clé privée	46
6.2.9	Méthode de désactivation de la clé privée	46
6.2.10	Méthode de destruction des clés privées	46
6.2.11	Niveau de qualification du module cryptographique et des dispositifs de protection de clés privées	46
6.3	Autres aspects de la gestion des bi-clés	47
6.3.1	Archivage des clés publiques	47
6.3.2	Durées de vie des bi-clés et des certificats	47
6.4	Données d'activation	47
6.4.1	Génération et installation des données d'activation	47
6.4.2	Protection des données d'activation	47
6.4.3	Autres aspects liés aux données d'activation	48
6.5	Mesures de sécurité des systèmes informatiques	48
6.5.1	Mesures de sécurité techniques spécifiques aux systèmes informatiques	48
6.5.2	Niveau de qualification des systèmes informatiques	50
6.6	Mesures de sécurité des systèmes durant leur cycle de vie	50
6.6.1	Mesures de sécurité liées au développement des systèmes	50
6.6.2	Mesures liées à la gestion de la sécurité	50
6.6.3	Niveau d'évaluation sécurité du cycle de vie des systèmes	51
6.7	Mesures de sécurité réseau	51
6.8	Horodatage / Système de datation	51
7	Profil des certificats, des OCSP et des LCR	52
7.1	Profil des certificats	52
7.1.1	Certificat de l'AC	52
7.1.2	Certificat de l'AC Intermédiaire	53
7.2	Profil des LCRs	55
7.3	Profil des OCSPs	55
8	Audit de conformité et autres évaluations	55
8.1	Fréquences et / ou circonstances des évaluations	55
8.2	Identités / qualifications des évaluateurs	56
8.3	Relations entre évaluateurs et entités évaluées	56
8.4	Sujets couverts par les évaluations	56

8.5	Actions prises suite aux conclusions des évaluations	56
8.6	Communication des résultats	57
9	Autres problématiques métiers et légales	57
9.1	Tarifs	57
9.1.1	Tarifs pour la fourniture ou le renouvellement de certificats	57
9.1.2	Tarif pour accéder aux certificats	57
9.1.3	Tarifs pour accéder aux informations d'état et de révocation des certificats	57
9.1.4	Tarifs pour d'autres services	57
9.1.5	Politique de remboursement	58
9.2	Responsabilité financière	58
9.2.1	Couverture par les assurances	58
9.2.2	Autres ressources	58
9.2.3	Couverture et garantie concernant les entités utilisatrices	58
9.3	Confidentialité des données professionnelles	58
9.3.1	Périmètre des informations confidentielles	58
9.3.2	Informations hors du périmètre des informations confidentielles	59
9.3.3	Responsabilités en terme de protection des informations confidentielles	59
9.4	Protection des données personnelles	59
9.4.1	Politique de protection des données personnelles	59
9.4.2	Informations à caractère personnel	59
9.4.3	Informations à caractère non personnel	59
9.4.4	Responsabilité en termes de protection des données personnelles	59
9.4.5	Notification et consentement d'utilisation des données personnelles	60
9.4.6	Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives	60
9.4.7	Autres circonstances de divulgation d'informations personnelles	60
9.5	Droits sur la propriété intellectuelle et industrielle	60
9.6	Interprétations contractuelles et garanties	61
9.6.1	Autorité de Certification	61
9.6.2	Service d'enregistrement	61
9.6.3	Abonné	62
9.6.4	Utilisateurs de certificats	62
9.6.5	Autres participants	62
9.7	Limite de garantie	62

9.8	Limite de responsabilité	62
9.9	Indemnités	63
9.10	Durée et fin anticipée de validité de la PC	63
9.10.1	Durée de validité	63
9.10.2	Fin anticipée de validité	63
9.10.3	Effets de la fin de validité et clauses restant applicables	63
9.11	Notifications individuelles et communications entre les participants	64
9.12	Amendements à la PC	64
9.12.1	Procédures d'amendement	64
9.12.2	Mécanisme et période d'information sur les amendements	64
9.12.3	Circonstances selon lesquelles l'OID doit être changé	65
9.13	Dispositions concernant la résolution de conflits	65
9.14	Juridictions compétentes	65
9.15	Conformité aux législations et réglementations	65
9.16	Dispositions diverses	65
9.16.1	Accord global	65
9.16.2	Transfert d'activités	65
9.16.3	Divisibilité	65
9.16.4	Application et renonciation	66
9.16.5	Force majeure	66
9.17	Autres dispositions	66
9.17.1	Obligation de loyauté	66
9.17.2	Accessibilité	66
A	Exigence de l'AC intermédiaire	67
B	Acteurs Essentiels de Confiance	68
B.1	Origine des Acteurs Essentiels de Confiance	69
B.2	Procédure pour devenir Acteur Essentiel de Confiance	69
B.3	Désinscription d'un Acteur Essentiel de Confiance	69
B.4	Évènements communiqués aux Acteurs Essentiels de Confiance	70

1 Introduction

1.1 Présentation Générale

Universign s'est positionné comme Prestataire de Service de Confiance (PSCo). 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 Intermédiaires (AC Intermédiaires) capables de délivrer des certificats à des porteurs dans des conditions conformes aux standards de sécurité reconnus par la Commission Européenne et l'ANSSI. Chaque AC Primaire vise à être certifiée en conformité avec la norme [ETSI 319 411-1] au niveau NCP+.

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

Le présent document (ci-après désigné PC/DPC tout au long du document) rassemble la politique de certification des AC Primaires 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 Primaires d'Universign.

Architecture de Confiance d'Universign L'Architecture de Confiance de Universign (présentée¹ dans la Figure 1.) est composée

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

Une AC Primaire ne délivre des certificats qu'à des AC Intermédiaires répondant aux critères définis dans l'Annexe A de la présente PC/DPC. Les AC Intermédiaires délivrent des certificats aux porteurs de certificats finaux qui sont des personnes physiques ou morales.

Cette version de la PC/DPC ne considère pas la possibilité pour une AC Intermédiaire de délivrer des certificats à d'autres AC, mais les versions ultérieures pourront prendre en compte cette option. Cette version de la PC/DPC considère deux familles de certificat conformément aux exigences de l'Annexe A.

Périmètre de la présente PC/DPC Le périmètre de la présente PC/DPC est restreint aux AC Primaires et à leur fonction de délivrance de certificats aux AC

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

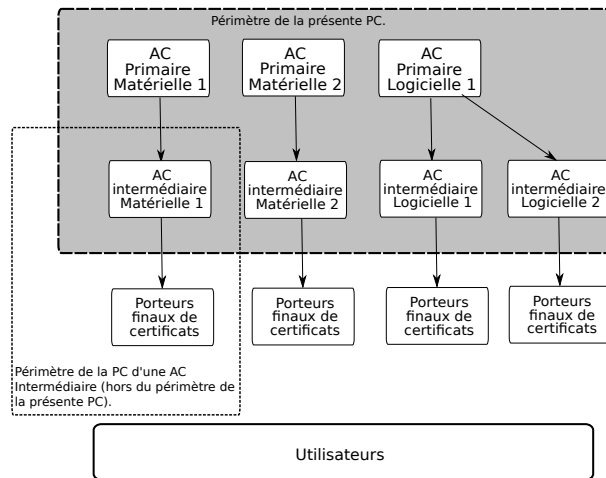


FIGURE 1: Principe de l'Architecture de Confiance Universign et périmètre de la présente PC

Intermédiaires. Chaque AC Intermédiaire doit fournir sa propre PC et sa propre DPC en conformité avec les exigences définies dans l'Annexe A de la présente PC/DPC. La délivrance de certificats aux porteurs de certificats finaux par les AC Intermédiaires sera décrite dans les PC et DPC des AC Intermédiaires. Elle est, de ce fait, hors du périmètre de la présente PC/DPC.

La présente PC/DPC définit les participants suivants :

- les AC Primaires, qui délivrent des certificats à des AC Intermédiaires répondant aux exigences exprimées dans la présente PC/DPC (voir Annexe A) ;
- des AC Intermédiaires, qui sont les porteurs de certificats des AC Primaires ;
- des utilisateurs, dont les opérations dépendent de l'ACU.

1.2 Identification du document

Le présent document est la Politique de Certification des AC Primaires 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 certificat délivrées par ses AC Primaires et définies par la présente PC/DPC :

- 1.3.6.1.4.1.15819.5.1.2.1 pour les AC Primaires Matérielles ;
- 1.3.6.1.4.1.15819.5.1.2.2 pour les AC Primaires Logicielles.

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, deux types d'entités répondent à cette définition :

- les AC Primaires d'Universign, qui délivrent des certificats à des AC Intermédiaires.
- les AC Intermédiaires, qui délivrent des certificats à des porteurs de certificats finaux.

Dans le périmètre de cette PC/DPC, qui concerne les AC Primaires et la délivrance de certificats aux AC Intermédiaires (voir Section 1.1), les AC Intermédiaires sont les porteurs de certificats. De ce fait, le terme d'AC fait référence, dans le cadre de cette PC/DPC, uniquement aux AC Primaires.

Gouvernance d'une AC Primaire Une AC Primaire 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 Primaire.

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 qu'Universign intègre correctement les pratiques de la PC/DPC ;
- publier la PC/DPC et leurs révisions aux AC Intermédiaires et Utilisateurs.

1.3.2 Autorité d'enregistrement

Une Autorité d'Enregistrement (AE) est une entité qui délivre les services d'identification et d'authentification des futurs porteurs de certificats.

Dans le cadre de cette PC/DPC, chacune des AC Primaires opère elle-même sa propre Autorité d'Enregistrement. La présente PC/DPC définit l'ensemble des responsabilités d'Universign, en tant qu'Autorité d'Enregistrement.

1.3.3 Porteurs de Certificats

Le terme de porteur de certificat est une notion générique pouvant recouvrir les entités suivantes :

- Le Sujet : la personne physique ou morale qui est désignée par le champ subject du certificat ;
- Le Contractant : la personne physique ou morale qui contracte avec l'émetteur du certificat ;
- Les Contacts Administratifs : 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, nous ferons les distinctions suivantes :

- Le Sujet ne peut être qu'une Autorité de Certification, nommée *AC Intermédiaire* dans le présent document. Celle-ci est désignée par le champ subject du certificat émis par l'AC Primaire.
- Le Contractant est l'organisation qui opère cette AC Intermédiaire. Cette organisation peut être :
 - soit Universign ou l'une de ses filiales ;
 - soit une organisation tierce ayant contracté avec Universign ou l'une de ses filiales.
- L'organisation opérant une AC Intermédiaire doit obligatoirement désigner un contact administratif. Cette personne est appelée *Contact Principal* dans ce document.

Pour faire partie de l'ACU, les AC Intermédiaires doivent se conformer au processus d'enregistrement défini dans cette PC/DPC (voir Section 4.1). En particulier, elles doivent se conformer à l'ensemble des exigences définies dans l'annexe A.

1.3.4 Utilisateurs de certificats

Les utilisateurs sont toutes personnes physiques ou morales, dont les activités vont dépendre de la validité du lien entre le nom de l'AC Intermédiaire et de la clé publique associée. Il appartient aux utilisateurs de vérifier, selon les moyens qu'ils estiment adéquats, la validité de ce lien ; *a minima* ils devront vérifier les informations sur le statut de révocation du 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

Les Acteurs Essentiels de Confiance sont des individus ou entités ayant une forte implication dans l'ACU ou du fait de leur statut ont un lien privilégié avec Universign. Un Acteur Essentiel de Confiance peut être (liste non exhaustive) :

- un éditeurs de logiciel contenant un magasin de certificats de confiance ;
- un responsable de Trust-Service Statut List (TSL) ;
- un organisme gouvernemental.

Universign maintient une liste de ces Acteurs Essentiels de Confiance et les notifie lorsque certains évènements majeurs du cycle de vie d'une AC Primaire se produisent (voir Annexe B).

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

Les bi-clés d'une AC Intermédiaire peuvent être utilisées pour signer :

- les certificats des porteurs ;
- ses LCR et/ou ses réponses OCSP ;
- 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. En particulier, la présente version de la PC/DPC interdit la signature de certificats d'Autorité de Certification par des AC Intermédiaires. De plus, le certificat doit être utilisé dans la limite des lois et réglementations en vigueur.

1.5 Gestion de la présente politique

1.5.1 Entité gérant la politique

Universign
5-7, Rue du Faubourg Poissonnière, 75009 Paris, France
contact@universign.eu

1.5.2 Point de contact

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

Universign
AC Primaire
A l'attention du Responsable des Politiques
5-7, Rue du Faubourg Poissonnière, 75009 Paris, France
contact@universign.eu

1.5.3 Entité déterminant la conformité des pratiques de la PC

Le Comité d'Approbation d'Universign détermine la pertinence et l'applicabilité de cette PC/DPC.

1.5.4 Procédure d'approbation de la conformité de la PC/DPC

Le Comité d'Approbation d'Universign prononce l'approbation (et les éventuelles mises à jour) de la conformité des pratiques documentées de la PC/DPC, au vu des résultats d'audits internes effectués.

1.6 Définitions et abréviations

Définitions

Les termes utilisés dans la présente politique sont les suivants :

Autorité de Certification

Autorité qui a en charge l'application de la Politique de Certification, l'émission et la bonne gestion des Certificats. Dans le cadre de cette PC/DPC, l'Autorité de Certification est Universign.

Certificat

Document électronique délivré par Universign comportant l'identité du porteur du Certificat et une clé mathématique dite publique, utilisée pour contrôler l'identité du porteur du certificat.

Infrastructure de gestion des clés

Ensemble des composantes (physiques, procédurales et logicielles) fournissant des services de gestion des clés et de certificats au profit d'une communauté d'utilisateurs.

Liste des Certificats Révoqués

Liste contenant l'ensemble des Certificats qui ne sont plus valables et qui ne sont plus dignes de confiance.

Object Identifier

Identifiant unique attribué par une entité de standardisation reconnue (l'AFNOR

en France). Il est ensuite décliné par Universign pour identifier ses documents de façons uniques.

Politique de Certification

Le présent document, comportant l'ensemble des engagements pris par Universign en termes de sécurité et d'organisation dans le cadre de la fourniture de Certificats.

Universign

Nom commercial de la société Cryptolog International, SAS au capital de 504 932 euros dont le siège social est situé 7 rue du Faubourg Poissonnière, 75009 Paris, immatriculée au Registre du Commerce et des Sociétés de Paris sous le numéro 439 129 164.

Abréviations

Les abréviations utilisées dans la présente politique sont les suivantes :

AC : Autorité de Certification

AE : Autorité d'Enregistrement

DN : Distinguished Name

DPC : Déclaration des Pratiques de Certification

HSM : Hardware Security Module (module cryptographique)

IGC : Infrastructure de Gestion de Clés

LCR : Liste des Certificats Révoqués

OID : Object Identifier

PC : Politique de Certification

PSCo : Prestataire de Services de Confiance

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 Primaire, 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 les AC Primaires d'Universign sont les suivantes :

- la présente PC/DPC² ;
- Les LCRs publiées selon les exigences de cette PC/DPC ;
- les certificats des AC Primaires Universign en cours de validité ainsi que leurs empreintes ;
- la Déclaration d'IGC ;
- 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 Primaire 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 AC Primaires Universign en cours de validité ainsi que leurs empreintes : Les certificats de l'AC Primaire ainsi que leurs empreintes 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 dès que nécessaire, lors de leurs mises à jour.

Les exigences sur les délais et fréquence de publication des informations des AC Intermédiaires sont définies dans l'Annexe A.

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.

2. une copie des versions précédentes de cette PC/DPC, ainsi que les dates de validité associée est disponible sur demande.

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.

Chaque AC Primaire et chaque AC Intermédiaire est identifiée par un nom explicite (appelé "DN" par la suite) de type X.501. Ce type de DN est défini dans le chapitre 7. Tous les certificats émis par une AC Primaire d'Universign comportera des champs conformément au tableau suivant :

Champ	Obligatoire	Sémantique du champ	Vérifié par l'AE	Document utilisé pour la vérification
C	Oui	Pays	Oui	Document légal d'identification de la société
ST	Non	Etat/Région de l'entité opérant l'AC Intermédiaire	Oui	Document légal d'identification de la société
L	Non	Ville de l'entité opérant l'AC Intermédiaire	Oui	Document légal d'identification de la société
O	Oui	Nom légal de l'entité propriétaire de l'AC Intermédiaire	Oui	Document légal d'identification de la société
OU	Oui	Identifiant unique légal de l'entité ³ structuré suivant l'ISO 6523	Oui	Document légal d'identification de la société
CN	Oui	Nom libre désignant l'AC Intermédiaire	Oui ⁴	

Les détails du processus permettant à l'AC Primaire Universign d'identifier l'AC Intermédiaire sont décrits dans le chapitre 3.2.2 et le chapitre 3.2.3.

3. Pour une société française, 0002 suivi d'un espace et du numéro de SIREN ou de SIRET

4. Il sera uniquement vérifié que le nom est explicite (voir Sect. 3.1.2)

3.1.2 Noms explicites

Une AC Primaire d'Universign ne délivre des certificats que si le DN du certificat est explicite, c'est-à-dire que le DN a une interprétation sémantique naturelle permettant de déterminer l'identité de l'organisation qui est le sujet du certificat. En dernier recours, il revient au Comité d'Approbation d'Universign de décider si le nom est bien explicite.

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

Pas de conditions particulières.

3.1.5 Unicité des noms

Les noms des AC Intermédiaires doivent être uniques pour les certificats émis par une AC Primaire donnée. Cette vérification est réalisée par l'AE au moment de l'enregistrement⁵. Il est possible pour une AC Intermédiaire d'avoir plusieurs certificats avec le même Subject Distinguished Name (DN) à l'intérieur de l'ACU.

3.1.6 Identification, authentification et rôle des marques déposées

Les AC Intermédiaires 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.

5. Une AC Primaire ne délivrant des certificats qu'à des AC Intermédiaires, une vérification manuelle par l'AE est raisonnable.

3.2 Validation initiale de l'identité

3.2.1 Méthode pour prouver la possession de la clé privée

Une AC Intermédiaire doit prouver à l'AC Primaire à laquelle elle veut être rattachée qu'elle possède bien la clé privée correspondant à la clé publique à certifier.

La preuve de possession est obtenue en signant la demande de certificat au format PKCS#10 à l'aide de la clé privée de l'AC Intermédiaire (ou un mécanisme cryptographique équivalent accepté par Universign).

3.2.2 Validation de l'identité d'un organisme

La validation de l'identité de l'entité opérant une AC Intermédiaire est réalisée à travers la validation de l'identité de son Contact Principal. Ceci est justifié par le fait que chaque AC Intermédiaire n'aura qu'un seul Contact Principal à un instant donné.

3.2.3 Validation de l'identité d'un individu

L'identité de la personne physique représentant l'AC Intermédiaire est vérifiée par l'AE durant une rencontre en face-à-face. Seuls les éléments nécessaires à l'établissement du certificat seront demandés par Universign. La personne fournira les éléments suivants :

- un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité désignant le futur porteur auquel le certificat doit être délivré. Ce mandat doit être signé pour acceptation par le futur porteur bénéficiaire,
- une pièce justificative à valeur légale de l'existence de l'entité de rattachement, 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).
- une pièce d'identité nationale comportant une photographie d'identité récente et précisant la date et le lieu de naissance ;
- l'adresse postale et l'adresse mail permettant à l'AC Primaire de contacter le porteur.

Une copie de ces éléments d'identité fait partie du dossier d'enregistrement et sera conservée par Universign de façon sûre.

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 Primaire identifie l'autorité du représentant d'une AC Intermédiaire avec un mandat signé du représentant légal de l'entité ou de l'organisation. Le mandat est fourni lors de l'enregistrement (voir Section [3.2.3](#)).

3.2.6 Critères d'interopérabilité

Une AC Intermédiaire certifiée par l'AC Primaire Universign doit s'engager aux dispositions de l'Annexe [A](#).

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

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

3.3.1 Identification et validation pour un renouvellement courant

Sans objet.

3.3.2 Identification et validation pour un renouvellement après révocation

Sans objet.

3.4 Identification et validation d'une demande de révocation

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

Pour valider la demande, l'AC Primaire s'assure que :

- le Contact Principal est correctement enregistré au sein de l'AC Primaire ;
- la demande est signée par le Contact Principal. L'AC Primaire vérifie la signature par rapport à celle établie dans le dossier d'enregistrement du Contact Principal ;

- l'identification de l'AC Intermédiaire est établie dans la demande de révocation.

Si ces conditions sont remplies, le responsable de l'AC Primaire signe la demande de révocation et la transmet aux équipes d'Universign qui procèdent aux étapes techniques de révocation.

4 Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Pour une AC Intermédiaire donnée, le Contact Principal opère la demande de certificat auprès d'une AC Primaire.

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

Le processus d'enregistrement d'une AC Intermédiaire à une AC Primaire nécessite les étapes suivantes :

- Dans le cas où l'AC Intermédiaire n'est pas opérée par Universign ou l'une de ses filiales, l'AC Intermédiaire doit établir un accord formel (contrat) avec l'AC Primaire.
- Le Contact Principal doit fournir les informations requises lors de la demande d'enregistrement d'une AC Intermédiaire. A ce titre, il est garant de l'exactitude des informations fournies et doit fournir l'ensemble des éléments nécessaires au dossier d'enregistrement, en particulier les preuves que l'AC Intermédiaire satisfait aux exigences de l'annexe A ;
- L'AC Intermédiaire doit générer sa bi-clé ;
- Le Contact Principal doit fournir la clé publique de l'AC Intermédiaire à l'AC Primaire ;
- Le Contact Principal doit fournir une preuve que la clé privée associée à la clé publique lui appartient.

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

4.2 Traitement d'une demande de certificat

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

L'AC Primaire d'Universign assure elle-même la fonction d'AE. Elle peut sous-traiter une partie des missions d'enregistrement à des sociétés tierces liée de manière contractuelle avec Universign. L'AE valide les demandes de certificats des AC Intermédiaires. L'AE identifie et valide les informations fournies par les AC Intermédiaires 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 d'une AC Intermédiaire par une AC Primaire est la suivante :

- l'AC Primaire, en tant qu'autorité d'enregistrement, vérifie que le dossier d'enregistrement est complet et valide. En particulier, l'AC Primaire vérifie les preuves de conformité aux exigences de l'annexe A fournies par l'AC Intermédiaire ;
- l'AC Primaire identifie avec succès le demandeur et les informations fournies conformément à la section 3.2 ;
- le Comité d'Approbation d'Universign accepte la demande de certificat⁶.

En cas de rejet de la demande lors de l'une de ses étapes, le Contact Principal de l'AC Intermédiaire est immédiatement informé du motif. À tout moment durant le processus, l'AC Primaire peut demander à l'AC Intermédiaire des éléments complémentaires ou de justifier sa conformité aux exigences de cette PC/DPC.

4.2.3 Durée d'établissement du certificat

Une AC Primaire commence à traiter la requête dans un délai raisonnable suivant sa réception. Sauf mention contraire dans le contrat liant une AC Primaire et une AC Intermédiaire, il n'y a pas de délai minimal de traitement de la demande de certificat par une AC Primaire. 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 Primaire crée un certificat à l'issue du processus de validation de la demande de certificat défini dans la section 4.2. Le certificat émis est conforme aux informations contenues dans la demande de certificat et au profil défini dans

6. Le Comité d'Approbation peut refuser un dossier pour motif non technique.

la section 7.1. Le certificat est généré dans des locaux sécurisés sous le contrôle d'au moins deux personnels en rôle de confiance.

Les personnes en rôles de confiance ayant la possibilité d'émettre des certificats sont authentifiés au moyen de plusieurs facteurs.

La clé publique d'une AC Intermédiaire doit être remise à une AC Primaire en main propre et de façon sécurisée.

4.3.2 Notification par l'AC de la délivrance du certificat

Universign notifie dans un délai raisonnable le Contact Principal 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

L'acceptation d'un certificat d'une AC Primaire par une AC Intermédiaire doit être fait de façon formelle par un document d'acceptation envoyé à l'AC Primaire. En cas d'absence d'acceptation formelle après un temps raisonnable et plusieurs relances, le certificat sera révoqué par l'AC Primaire.

4.4.2 Publication du certificat

Une AC Primaire ne publie pas les certificats émis sans l'accord préalable de l'AC Intermédiaire.

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

Lorsqu'un nouveau certificat est délivré, l'ensemble des Acteurs Essentiels de Confiance (voir Annexe B) est notifié dès que l'AC Intermédiaire l'a accepté.

4.5 Usage de la bi-clé et du certificat

AC Intermédiaire :

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 Primaire et l'AC Intermédiaire, le cas échéant ;

- l'extension KeyUsage ou tout autre extension contraignant l'utilisation de la clé, définie dans le certificat émis.

Conformément aux exigences de l'Annexe A, une AC Intermédiaire s'engage :

- à protéger sa ou ses clé privées ;
- en cas de compromission de sa clé privée, l'AC Intermédiaire s'engage à ne plus l'utiliser et notifier sans délai l'AC Primaire de la compromission ;
- en cas de compromission de la clé privée de l'AC Primaire qui a émis le certificat, l'AC Intermédiaire 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 Primaire. 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 Primaire 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 Primaire 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 selon la même procédure que la 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 Primaire sont les suivantes :

- demande motivée d'une AC Intermédiaire ;

- une AC Intermédiaire n'a pas respecté ou ne respecte plus ses engagement vis-à-vis d'une AC Primaire, en particulier les exigences définies dans l'annexe A ;
- 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 ;
- le contrat prend fin entre une AC Primaire et une AC Intermédiaire ;
- une AC Intermédiaire n'a pas versé le paiement relatif à l'émission du certificat, le cas échéant ;
- arrêt définitif d'activité d'une AC Primaire 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 ;
- Universign estime que l'utilisation dudit certificat lui est préjudiciable.

4.9.2 Origine d'une demande de révocation

Les personnes pouvant demander une révocation de certificat d'AC Intermédiaire sont les suivantes :

- le Comité d'Approbation d'Universign ;
- le Contact Principal de l'AC Intermédiaire ;
- un représentant légal de l'entité opérant l'AC Intermédiaire.

4.9.3 Procédure de traitement d'une demande de révocation

Le Contact Principal (ou le Comité d'Approbation) transmet une demande de révocation qui doit *a minima* contenir les informations suffisantes à la révocation :

- l'identifiant de l'AC Intermédiaire (voir la Sect. 3.1.1) ;
- le numéro de série du certificat à révoquer ;
- son nom complet ;
- éventuellement la cause de révocation. Cette donnée est à titre informatif et n'apparaît pas dans la LCR.

L'AC Primaire Universign authentifie la demande de révocation et révoque le certificat à l'aide de sa paire de clés. Toutes les opérations 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 Primaire Universign informe le Contact Principal de la révocation effective de son certificat et du changement de statut. Toute révocation est définitive.

4.9.4 Délai accordé à une AC Intermédiaire 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, 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. Pour cela, l'Utilisateur peut consulter la dernière LCR publiée par l'AC Primaire qui a émis le certificat. Cette LCR est publiquement accessible, comme décrit à la Section [4.10.1](#).

4.9.7 Fréquence d'établissement des LCR

Les LCRs sont émises a minima toutes les 60 minutes.

4.9.8 Délai maximum de publication d'une LCR

Les LCR sont publiées dans un délai raisonnable après leur émission. En général, la publication est réalisée automatiquement dans un délai maximum de 30 minutes suivant l'émission de la LCR.

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

Sans objet.

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

Sans objet.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Universign préviendra directement et sans délai l'ensemble des Acteurs Essentiels de Confiance (voir Section **B**) dès détection d'une compromission de la clé privée.

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 sont publiées 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. Les LCR 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 une AC Intermédiaire et une AC Primaire

La fin de la relation entre une AC Primaire et une AC Intermédiaire est régie par le contrat entre une AC Primaire et l'AC Intermédiaire, qui peut définir des obligations se poursuivant après l'expiration ou la révocation du certificat. En l'absence d'une telle clause, la relation expire au terme de la durée de validité du certificat ou à sa révocation.

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

Universign a défini sa Politique de Sécurité de l'Information (PSI). Elle décrit l'approche et les solutions à mettre en place en terme de gestion de la sécurité.

La PSI est maintenue à jour et approuvée par la direction générale d'Universign.

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

Universign héberge ses services de certification dans des locaux sécurisés. Ces sites et locaux disposent de mécanismes de sécurité physique décrits dans ce

chapitre (tels que des zones verrouillées, un service de gardiennage, des mécanismes de détection d'intrusion) permettant d'assurer une forte protection contre les accès non autorisés.

Les locaux sont composés de plusieurs zones de sécurité physique successives. Le passage d'une zone à la suivante se fait via un accès sécurisé, tel qu'une porte verrouillée par badge d'accès ou des sas à identification biométrique, qui assure un strict contrôle d'accès aux seules personnes autorisées. Chaque zone successive offre un accès plus restreint et de plus grande sécurité physique contre l'accès non autorisé, du fait que chaque zone sécurisée est encapsulée dans la précédente.

En particulier, les composants de l'AC Primaire racines de l'IGC sont physiquement isolés des autres composants.

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.

Les AC Primaires sont opérées exclusivement dans la zone la plus sécurisée, dont l'accès à une AC Primaire ne peut se faire que sous le contrôle simultané de deux membres autorisés.

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 conformité 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 Primaire 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 Primaire et des personnels habilités.

Les AC Primaires 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 destructions 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 fabricant.
- 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 ainsi que 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 Primaire.

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

Opérateur d'enregistrement : il assure l'ensemble des opérations d'enregistrement des futurs porteurs de certificats.

A l'instar de l'ensemble des employés de l'AC Primaire, 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 Primaire. Universign s'assure régulièrement que l'ensemble des rôles de confiance sont pourvus afin d'assurer une continuité de l'activité.

5.2.2 Nombre de personnes requises par tâches

Chaque AC Primaire 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 telles que redémarrage de l'IGC, restauration des clés ou la génération de certificats.

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

Chaque AC Primaire 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 Primaires. Cette analyse de risque est revue périodiquement et lors de changements structurels significatifs d'une AC Primaire. De plus, la méthodologie util-

isée pour effectuer l'analyse de risque permet de s'assurer que l'inventaire Universign est maintenu à jour.

5.3 Mesures de sécurité vis-à-vis du personnel

L'AC Primaire Universign, par le biais de sa politique de ressources humaines, emploie un personnel qualifié et ayant l'expertise et l'expérience nécessaire vis-à-vis des services offerts par Universign. Ce personnel doit être suffisant pour assurer le service.

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.

5.3.2 Procédures de vérification des antécédents

Universign procède avant la nomination d'une personne à un Rôle de Confiance à la vérification des antécédents judiciaires et professionnelles, 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 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 évolu-

tion 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 portées à la connaissance de 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 Primaire . Un prestataire externe ne peut avoir accès à une zone sécurisée d'Universign que sous la responsabilité et la supervision de personnes occupant un Rôle de Confiance.

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

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

5.3.8 Documentation fournie au personnel

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'ensemble des évènements liés à l'enregistrement (demande de certificat) ;
- l'ensemble des évènements liés au cycle de vie des clés des AC Primaires ;

- l'ensemble des événements liés au cycle de vie des certificats émis par les AC Primaires, y compris les événements liés à la révocation ;
- l'ensemble des événements des différentes composantes de l'IGC (démarrage des serveurs, accès réseau, ...).

Ces journaux permettent d'assurer la traçabilité et l'imputabilité des actions effectuées (horodatage, affectation à l'intervenant), en particulier en cas de demande émanant d'une autorité judiciaire ou administrative.

Une AC Primaire décrit dans ses procédures internes le détail des événements et des données enregistrées.

Les procédures de traçabilité mises en place par l'AC Primaire 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 traités quotidiennement et exploités systématiquement en cas de remontée d'un événement 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 pendant la durée nécessaire aux besoins de fourniture de preuve dans le cadre de procédures judiciaires conformément à la loi applicable.

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 Primaire Universign n'est pas accessible en termes de réseau et met en place les contrôles suivants :

- contrôle des accès physiques au sein de la salle "off-line" quotidien ;
- contrôle des publications de LCR quotidien ;
- récupération des événements et sauvegarde de l'AC mensuelle. L'ensemble des événements est ensuite analysé par 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 événements 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 AC Intermédiaires et des Contacts Principaux ;
 - la preuve de l'acceptation de l'Accord de souscription par les AC Intermédiaires (voir Section 4.1.2) ;
 - les demandes d'enregistrement des AC Intermédiaires (voir Section 4.1.2) ;
 - une copie des éléments ayant permis de vérifier l'identité du Contact Principal (voir Section 3.2.3) ;
 - une copie des éléments ayant permis de vérifier le lien entre le Contact Principal et l'AC Intermédiaire (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 Primaire et la date/heure précise d'occurrence de l'évènement.
 - les évènements relatifs aux opérations sur les clés et les certificats émis par l'AC Primaire et la date/heure précise d'occurrence de l'évènement.

Universign décrit dans ses procédures internes 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 Primaire.

Journaux d'évènements :

Les journaux d'évènements sont archivés et conservés jusqu'à 7 ans après l'expiration du dernier certificat émis par l'AC.

L'ensemble des archives est conservé en conformité avec la législation en vigueur (voir Sect. 9.4.1) et les obligations inhérentes à Universign en sa qualité de PSC (voir Sect. 5.8).

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 Primaire 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 Primaire doit appliquer toutes les actions nécessaires pour éviter tout arrêt des opérations des utilisateurs du certificat de l'AC Primaire. 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 Primaire 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 Primaire a mis en place un plan de réponse en cas d'incident majeur, tel qu'une compromission de ses mécanismes de publication ou de son mécanisme d'émission de certificat.

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

Universign maintient une liste de contact à prévenir (voir Annexe B). Universign s'engage à prévenir directement et sans délai chaque contact de la liste.

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 Primaire 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 Primaire. Des mesures similaires sont prises si l'algorithme utilisé ou les paramètres utilisés par l'AC Primaire ou les AC Intermédiaires deviennent d'une robustesse insuffisante pour les usages de l'AC Primaire.

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 Primaire met en place ce plan afin de restaurer les services touchés. En particulier, chaque AC Primaire 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 Primaire 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 Primaire, Universign met en place un plan de fin de vie de cette AC Primaire. Ce plan de fin de vie pourra entre autre adresser les points suivants :

1. information directe à l'ensemble des AC Intermédiaires , aux Acteurs Essentiels de Confiance (voir Annexe B) et à l'ensemble des entités avec lesquelles l'AC Primaire est sous contrat (en particulier pour leur interdire de traiter toute nouvelle demande d'enregistrement) ;
2. potentielle révocation de tous les certificats émis encore en cours de validité ;
3. sort de la clé privée de l'AC Primaire, qui devra être détruite ou rendue inutilisable ;
4. 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 AC Intermédiaires.
5. mise à disposition des informations pour les Utilisateurs ;

Ce plan est vérifié et maintenu à jour régulièrement.

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération et installation de bi-clés

Clés d'AC Primaire :

Les clés de l'AC Primaire 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.

La génération des clés suit une procédure précise (appelé cérémonie des clés) et donne lieu à la création d'un procès-verbal en fin de cérémonie.

Clés d'AC Intermédiaire :

Les exigences relatives aux AC Intermédiaires sont définies en Annexe A.

6.1.2 Transmission de la clé privée à une AC Intermédiaire

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

6.1.3 Transmission de la clé publique à une AC primaire

La clé publique d'une AC Intermédiaire est transmise sur site à l'AC par le Contact Principal lors d'un face-à-face physique.

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

Les certificats racines des AC Primaires d'Universign et leurs empreintes sont publiés sur le site : <http://docs.universign.eu>.

Les certificats doivent contenir les informations présentées dans le chapitre 7 de la présente politique de certification.

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

6.1.5 Tailles des clés

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

Certificat	Taille des clés	Format
AC Primaire	2048	RSA

Les clés des AC Intermédiaires et les clés associées aux certificats délivrés par les AC Intermédiaires doivent être conformes aux dispositions de l'Annexe A.

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

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

En particulier, l'AC Primaire met en place les procédures nécessaires pour :

- s'assurer de l'intégrité des HSM durant leur transport depuis le fournisseur ;
- s'assurer de leur intégrité durant leur stockage précédant la cérémonie des clés ;
- s'assurer que les opérations d'activation, de sauvegarde et de restauration des clés de signature sont réalisées sous le contrôle de deux personnels ayant des Rôles de Confiance ;

- s’assurer que le HSM fonctionne correctement ;
- s’assurer que les clés contenues dans le HSM sont bien détruites lorsque celui-ci est dé-commissionné.

6.2.2 Contrôle de la clé privée

Les clés privées des AC Primaires Universign sont contrôlées par plusieurs personnes à l’aide de 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 Primaire 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 Primaire 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 Primaire 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 Primaire ne sont pas archivées.

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

Les clés privées de l’AC Primaire 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 Primaires et des AC Intermédiaires sont protégées par leurs modules cryptographiques.

À des fins de copie de secours, le stockage des clés privées des AC Primaires 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 Primaire 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 Primaire :

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 Primaire :

La destruction de la clé privée de l'AC Primaire est effectuée à partir de son module cryptographique. En cas de destruction, l'AC Primaire 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 Primaire : Le HSM utilisé par l'AC Primaire 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.

Module cryptographique des AC Intermédiaires : L'AC Primaire ne fournit pas les HSM des AC Intermédiaires. Les HSM des AC Intermédiaires doivent satisfaire au minimum aux certifications définies dans l'Annexe [A](#).

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques des AC Primaires et des AC Intermédiaires sont archivées au minimum 5 ans après l'expiration du certificat d'AC correspondant. Les conditions d'archivages sont similaires à celles décrites dans la section [5.5](#).

6.3.2 Durées de vie des bi-clés et des certificats

Une AC Primaire ne délivre pas à une AC Intermédiaires de certificats dont la date de validité dépasserait la durée de vie de la clé privée de l'AC Primaire.

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 Primaire 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 responsabilité d'un porteur de secret. Le secret est protégé par un code secret (code PIN ou mot de passe) ou un dispositif équivalent qui est personnel au porteur de secret. Les cartes à puce sont ensuite stockées dans des coffres forts sécurisés individuels. Chaque porteur de secret est responsable de sa part de secret d'activation. Il accepte cette responsabilité en signant un accord d'engagement.

6.4.3 Autres aspects liés aux données d'activation

Transmission des données d'activation

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

Destruction des données d'activation

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

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Mesures de sécurité techniques spécifiques aux systèmes informatiques

Chaque AC Primaire met en place, en fonction du système à protéger, des mécanismes de contrôle appropriés à la plate-forme à sécuriser (tels que des antivirus, des antimalware, *etc*) afin de se protéger contre l'exécution de code non autorisé ou potentiellement dangereux sur son système.

Chaque AC Primaire met en place des mécanismes de contrôle d'accès et d'authentification pour toutes les rôles permettant la génération de nouveaux certificats. Universign maintient ces systèmes de sécurité en permanence.

Ces mécanismes sont décrits dans ce chapitre.

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.

Tout utilisateur non 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.

Les procédures de contrôle d'accès en place assurent que les administrateurs du réseau de Universign n'ont pas d'accès au système d'émission de certificat.

Administration et exploitation :

L'utilisation de programmes utilitaires est restreinte et contrôlée sur les infrastructures 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 Primaires ont les capacités de stockage et de production suffisantes.

Intégrité des composants :

Les composants du réseau local sont maintenues dans un environnement physiquement sécurisé. Des vérifications périodiques de conformité de leur configuration sont effectuées. Les correctifs de vulnérabilités sont appliqués, après qualification, dans un délai raisonnable suivant leur parution.

Sécurité des flux :

Des mesures de sécurité sont mises en œuvre de manière à garantir l'authen-

tification 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. Cela permet notamment d'informer les personnes concernées lorsqu'un incident de sécurité est détecté.

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 et assure une traçabilité de l'ensemble des modifications apportées sur son SI.

Les infrastructures de développement et d'essai sont séparées des infrastructures opérationnelles de l'IGC. En particulier, les certificats de tests sont émis par une AC dédiée dont le CN est "Test Universign CA".

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.

Universign s'assure également que les supports sont stockés et gérés de façon à en assurer leur sécurité en disponibilité et en intégrité.

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

Sans objet.

6.7 Mesures de sécurité réseau

L'AC Primaire Universign est une AC hors-ligne non connectée au réseau. La propagation d'information comme la mise à disposition des LCR se fait à travers un canal de communication mono-directionnel. De ce fait, le mécanisme d'émission de certificat de l'AC Primaire est strictement isolé des autres serveurs et systèmes. De plus, les composants critiques sont placés dans les zones les plus sécurisées.

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

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

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

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

L'AC Primaire 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 de confiance autorisées.

6.8 Horodatage / Système de datation

Les serveurs de l'AC Primaire d'Universign se synchronisent plusieurs fois par jour avec avec la même source de temps (UTC). Cependant, l'AC Primaire d'Universign est une AC hors-ligne ; ainsi, lors d'une opération de l'AC, une vérification

de l'horloge est opérée pour garantir que les serveurs de l'IGC sont correctement synchronisés entre eux selon UTC.

7 Profil des certificats, des OCSP et des LCR

7.1 Profil des certificats

Tous les certificats émis par Universign sont conformes aux standards X.509, [ETSI 319 412-2] et [ETSI 319 412-3].

A noter : les certificats d'AC racines et intermédiaires sont compatibles avec le standard [ETSI TS 102 042] jusqu'à leur renouvellement.

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 [type] ⁷
Validité	30 ans
Subject DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Primary CA [type] ⁸
Clé publique	RSA 2048 bits

7. [type] doit être remplacé par hardware pour une AC primaire matérielle et par software pour une AC primaire logicielle

8. [type] doit être remplacé par hardware pour une AC primaire matérielle et par software pour une AC primaire logicielle

Extensions du certificat

Champ	OID	Critique	Valeur
Subject Key Identifier	2.5.29.14	Non	
KeyIdentifier			RFC 5280 - Méthode 1
Key Usage	2.5.29.15	Oui	
digitalSignature			Faux
nonRepudiation			Faux
keyEncipherment			Faux
dataEncipherment			Faux
keyAgreement			Faux
keyCertSign			Vrai
cRLSign			Vrai
encipherOnly			Faux
decipherOnly			Faux
Basic Constraint	2.5.29.19	Oui	
CA			Vrai
Maximum Path Length			Absent

7.1.2 Certificat de l'AC Intermédiaire**Champs de base**

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 Primary CA [type] ⁹
validité	Voir Sect. 6.3.2
Subject DN	Voir Sect. 3.1
Clé publique	Voir Sect. 6.1.5

9. [type] doit être remplacé par hardware pour une AC primaire matérielle et par software pour une AC primaire logicielle

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 ¹⁰
CRL Distribution Points	2.5.29.31	Faux	
fullName			http://crl.universign.eu/universign_primary_ca_[type].crl ¹¹
reasons			Absent
cRLIssuer			Absent

En accord avec Universign, une AC Intermédiaire peut ajouter d'autres extensions conformes à la norme [RFC 3647], telles que Certificate Policy.

10. Cette version de la PC/DPC limite le paramètre Maximum Path Length à 0.

11. [type] doit être remplacé par hardware ou software en accord avec les conditions définies dans l'annexe A

7.2 Profil des LCRs

Champs de base

Champ	Valeur
Version	v2
Signature	RSA/SHA-256 ¹² .
Issuer DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Primary CA [type] ¹³
Next Update	This Update + 7 jours

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 en accordance avec [RFC 5280]

En accord avec Universign, une AC Intermédiaire peut ajouter d'autres extensions conformes à la norme [[RFC 5280](#)].

7.3 Profil des OCSPs

Sans objet.

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 Primaire, et lors de toute modification significative.

Universign bénéficie de plusieurs types d'audit :

- un audit interne ;

¹². ou tout autre algorithme approprié et

¹³. [type] doit être remplacé par hardware pour une AC primaire matérielle et par software pour une AC primaire logicielle

- un audit de certification à la norme [ETSI 319 411-1], réalisé tous les 2 ans 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 Primaire 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 Primaire 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 Primaire auditée, sur toute ou partie de la mise en œuvre :

- de la PC/DPC ;
- des composantes de l'AC Primaire, ce qui inclue également les éventuels sous traitants.

Avant chaque audit, les évaluateurs proposeront au Comité d'Approbation de l'AC Primaire une liste de composantes, et procédures qu'ils souhaitent 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 Primaire auditée un avis parmi les suivants : "réussite", "échec", "à confirmer".

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

En cas de résultat "à confirmer", l'équipe d'audit identifie les non-conformités, et les hiérarchisent. Il appartient à l'AC Primaire 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 Primaire 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 Primaire sont tenus à la disposition des organismes de certification en charge de chacune de AC Primaire et des Acteurs Essentiels de Confiance.

9 Autres problématiques métiers et légales

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Une AC Primaire est autorisée à tarifier ses services de génération de certificats.

9.1.2 Tarif pour accéder aux certificats

Une AC Primaire offre un accès gratuit à son site de publication et aux certificats émis.

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

Une AC Primaire offre un accès gratuit au service de publication des LCR et au service de révocation. Cependant, dans le cas où une AC Primaire 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 Primaire 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 dérivés 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, permettant en particulier de couvrir les engagements auxquels Universign est soumis en sa qualité de PSC.

Universign encourage ses clients, en particulier les AC Intermédiaires, 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 Primaires,
- les données d'activation associées aux clés privées des AC Primaires 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'autres 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 et applique des procédures de sécurité pour garantir la confidentialité des informations identifiées dans la section [9.3.1](#).

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

Universign collecte et traite les données à caractère personnel conformément aux réglementations française et européenne relative à la protection des données à caractère personnel en vigueur.

En particulier

- L'AC Primaire garantit la confidentialité et la protection des données fournies par les Contacts Principaux ;
- L'AC Primaire garantit aux personnes concernées par les traitements des données à caractère personnel l'exercice de leur droit d'accès, de rectification et de suppression dans les limites prévues par la réglementation applicable, sur simple demande au point de contact identifié en section [1.5.2](#) ;
- L'AC Primaire tient à disposition ses archives à des fins de preuves pour des besoins de certification et pour des besoins légaux (voir Sect [9.4.6](#)).

9.4.2 Informations à caractère personnel

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

9.4.3 Informations à caractère non personnel

Pas d'engagement spécifique.

9.4.4 Responsabilité en termes de protection des données personnelles

Universign est responsable du traitement des données à caractères personnels au sens de l'article 3 de la loi 78-17 du 6 janvier 1978 modifiée en 2004.

9.4.5 Notification et consentement d'utilisation des données personnelles

Sauf cas défini dans la présente PC/DPC ou dans l'accord formel entre une AC Primaire et une AC Intermédiaire, une AC Primaire 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 développés dans l'IGC par Universign sont la propriété d'Universign.

Les AC Intermédiaires 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 révocations 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 son 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 Une AC Intermédiaire garde la propriété intellectuelle, le cas échéant, des marques et noms déposés contenu dans le dossier d'enregistrement ou dans le champ DN du certificat émis.

Propriété intellectuelle sur les clés

Les bi-clés des AC Primaires sont la propriété intellectuelle de Universign. Les bi-clés des AC Intermédiaires sont la propriété de l'entité propriétaire de chaque AC Intermédiaire. Les données d'activation des bi-clés des AC Primaires 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 Primaire et les documents qui en découlent ;
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC Primaire ;
- 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 Primaire 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 Primaire n'a pas fait procéder à l'enregistrement de la révocation d'un certificat, et n'a pas publié cette information conformément à ses engagements.

9.6.2 Service d'enregistrement

Cf. ci-dessus.

9.6.3 Abonné

Le Contact Principal d'une AC Intermédiaire :

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

Le Contact Principal est enregistré auprès de l'AC Primaire 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 Primaire 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

Sans objet.

9.7 Limite de garantie

Les limites des garanties offertes par les AC Primaires sont décrites dans l'Accord de souscription et l'Accord d'utilisation, et sont applicables dans la limite des lois et règlements en vigueur.

9.8 Limite de responsabilité

Universign ne pourra pas être tenu pour responsable d'une utilisation non autorisée ou non conforme par la présente PC/DPC 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'AC Intermédiaire.

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 sur les 6 derniers mois 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

Une AC Primaire s'autorise à demander des indemnités à une AC Intermédiaire si celle-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 d'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 Abonnés 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

Universign a mis en place une procédure de gestion des plaintes.

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 COMPÉTENCE EXCLUSIVE EST ATTRIBUÉE AU TRIBUNAL 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 à la réglementation [[CNIL](#)].

9.16 Dispositions diverses

9.16.1 Accord global

Sans objet.

9.16.2 Transfert d'activités

Sans objet.

9.16.3 Divisibilité

Sans objet.

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

9.17.1 Obligation de loyauté

Universign s'assure que les activités réalisées ne sont pas discriminatoires.

De plus, les personnes en rôles de confiance sont libres de toute pression commerciale, financière ou autre qui pourrait influencer sur la confiance des services Universign. En particulier, les personnes intervenant sur la génération et la révocation des certificats sont organisées de manière à garantir l'impartialité des opérations.

9.17.2 Accessibilité

Universign s'assure que les services proposés sont accessibles à tout le monde, y compris les personnes handicapées.

A Exigence de l'AC intermédiaire

Cette annexe présente les exigences relatives aux AC Intermédiaires. L'organisation opérant une AC Intermédiaire s'engage à ce que son AC Intermédiaire respecte les exigences suivantes :

1. l'AC Intermédiaire doit émettre des certificats respectant la norme X.509 v3.
2. l'AC Intermédiaire doit rédiger sa propre PC et sa propre DPC pour ses opérations d'IGC en conformité avec les exigences de cette annexe ;
3. l'AC Intermédiaire doit être conforme à l'un des standards suivant ou un standard équivalent accepté par UNIVERSIGN :
 - ETSI EN 319 411-1 [ETSI 319 411-1] ;
 - ETSI EN 319 411-2 [ETSI 319 411-2].
4. l'AC Intermédiaire doit réaliser un audit annuel permettant de démontrer la conformité à un des standards ci-dessus. Les résultats des audits doivent être transmis à Universign.
5. l'AC Intermédiaire doit avoir en permanence un Contact Principal ; le Contact Principal doit être nommé expressément et avoir autorité pour effectuer les opérations relatives au cycle de vie des certificats (demande, révocation, etc). En cas de changement de Contact Principal, l'AC Intermédiaire doit prévenir Universign immédiatement et en nommer un autre dans les plus brefs délais.
6. une AC Intermédiaire doit générer et utiliser ses clés privées dans des matériels sécurisés répondant aux exigences suivantes ou a des exigences supérieures ou équivalentes :
 - FIPS 140-2 Level 3 ; ou
 - Common Criteria ISO/CEI 15408 EAL4+ (conforme au Profil de protection CWA 14167-2 ou CWA 14167-3) ;
7. une AC Intermédiaire s'engage à utiliser des clés privées de type RSA 2048-bit ou d'une robustesse cryptographique supérieure ou équivalente et un algorithme de hachage au moins équivalent à la famille SHA-2 (256/384/512).
8. les AC Intermédiaires doivent utiliser leur équipement de génération de bi-clés avec des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé. Elles doivent également documenter dans leur PC les paramètres et algorithmes de signature utilisés.
9. une AC Intermédiaire s'engage à émettre des certificats uniquement pour des clés privées de type RSA 1024-bit (ou au moins cryptographiquement équivalente)

10. si le certificat de l'AC Intermédiaire est de type *Certificat Matériel* (OID : 1.3.6.1.4.1.15819.5.1.2.1), les clés privées associées aux certificats émis par l'AC Intermédiaire doivent être générées et utilisées dans des matériels sécurisés répondant aux exigences suivantes :
 - FIPS 140-2 Level 2 ou supérieur ; ou
 - Common Criteria ISO/CEI 15408 EAL4+ ou supérieur (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 équivalent).
11. une AC Intermédiaire ne délivre pas de certificats dont la date de validité dépasserait la durée de vie de leur clé privée.
12. dans le cas où l'AC Intermédiaire n'est pas opérée dans les locaux sécurisés d'Universign par le personnel d'Universign, l'AC Intermédiaire doit être opérée dans des conditions de sécurité équivalentes ou supérieures. Universign se réserve le droit de réaliser des audits ou d'exiger un audit indépendant des locaux et des pratiques de l'AC Intermédiaire afin de s'assurer que le niveau de sécurité requis est atteint ;
13. l'AC Intermédiaire doit prévenir Universign dans les plus brefs délais en cas :
 - de perte, de compromission ou soupçon de compromission d'une de ses clés privées ;
 - de perte de contrôle sur sa clé privée (par la perte ou la compromission des données d'activation par exemple) ;
 - d'incorrection des informations contenues dans le certificat ;
 - d'intrusion majeure ou soupçon d'intrusion majeure au sein de son système d'information.
 - de changement majeur de sa PC.
14. en cas de compromission de sa clé privée, une AC Intermédiaire s'engage à immédiatement faire une demande de révocation et à ne plus utiliser sa clé privée pour émettre de nouveaux certificats.

B Acteurs Essentiels de Confiance

Universign maintient une liste des Acteurs Essentiels de Confiance pour ses AC Primaires. Les Acteurs Essentiels de Confiance sont des individus ou entités ayant une forte implication dans l'ACU ou du fait de leur statut ont un lien privilégié avec Universign. Ceux-ci sont prévenus lorsque des événements majeurs ont lieu dans la vie de l'AC Primaire.

B.1 Origine des Acteurs Essentiels de Confiance

Il n'y a pas de définition stricte des Acteurs Essentiels de Confiance. Les Acteurs Essentiels de Confiance sont des Utilisateurs de l'ACU reconnus comme tel par Universign. Leurs activités sont fortement impactées par leur confiance dans l'ACU. Typiquement les Acteurs Essentiels de Confiance peuvent être :

- des éditeurs de logiciel contenant un magasin de certificats de confiance ;
- des responsables de Trust-Service Statut List (TSL) ;
- des organismes gouvernementaux ;
- des organismes d'audit.

Cette liste ne saurait être exhaustive.

B.2 Procédure pour devenir Acteur Essentiel de Confiance

L'inscription sur la liste des Acteurs Essentiels de Confiance peut se faire :

- soit sur demande motivée ;
- soit sur invitation d'Universign.

Demande motivée Tout Utilisateur de l'ACU peut demander à devenir Acteur Essentiel de Confiance. La démarche est la suivante :

- Le demandeur enverra une demande au point de contact défini en Section 1.5.2. Cette demande devra contenir *a minima* les informations suivantes :
 - Nom de l'individu et/ou l'entité à inscrire ;
 - Motivation pour être inscrit ;
 - Nom et adresse électronique de la ou des personnes à contacter.
- le Comité d'Approbaton d'Universign traitera la demande d'inscription. Universign prend les mesures qu'elle juge suffisante pour s'assurer de l'origine de la demande. Universign se réserve le droit de refuser une inscription sur la liste des Acteurs Essentiels de Confiance si elle ne juge pas celle-ci pertinente. Universign traitera l'inscription dans des délais raisonnables.

Invitation Le Comité d'Approbaton d'Universign peut décider d'inviter des organismes et ou individus à rejoindre la liste des Acteurs Essentiels de Confiance. Sur une réponse positive de l'invité et sous réserve d'avoir l'ensemble des informations nécessaires, Universign l'ajoute à la liste.

B.3 Désinscription d'un Acteur Essentiel de Confiance

Une personne inscrite sur la liste des Acteurs Essentiels de Confiance peut se désinscrire sur simple demande. Universign vérifiera que la demande émane du

point de contact avant de la désinscrire. Universign peut décider de façon unilatérale de supprimer un point de contact de sa liste. Les causes de suppression peuvent être :

- l'adresse du contact n'est plus valide ;
- la relation qui liait l'Acteur Essentiel de Confiance et Universign s'est arrêtée ou a changée de façon significative.

Cette liste de causes ne saurait être exhaustive. Il est de la responsabilité de l'Acteur Essentiel de Confiance de maintenir en permanence au moins un point de contact. Cependant, si une entité n'a plus de point de contact, Universign mettra en œuvre des moyens raisonnables pour prévenir cette entité, sans avoir d'obligation de résultat.

B.4 Évènements communiqués aux Acteurs Essentiels de Confiance

Les Acteurs Essentiels de Confiance sont prévenus, via le point de contact enregistré par Universign, si l'un des évènements suivants a lieu :

- émission d'un nouveau certificat d'AC Intermédiaire par une AC Primaire ;
- révocation d'un certificat d'AC Intermédiaire par une AC Primaire ;
- compromission d'une clé privée d'une AC Primaire ou d'une AC Intermédiaire ;
- intrusion majeure au sein du système d'information d'une AC Primaire ou d'une AC Intermédiaire ;
- modification majeure de cette PC/DPC ou de celle d'une AC Intermédiaire.

Universign s'autorise également à notifier les Acteurs Essentiels de Confiance pour tout autre évènement qu'elle juge nécessaire.

Références

[RFC 3647]

Network Working Group - Request for Comments : 3647 - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework - (2003-11)

[RFC 5280]

Network Working Group - Request for Comments : 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (2008-05)

[ETSI 319 401]

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

[ETSI 319 411-1]

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

[ETSI 319 411-2]

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

[ETSI 319 412-2]

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

[ETSI 319 412-3]

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

[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.