



Sunnystamp PKI

Sunnystamp Legal Persons CA

Politique de Certification / Déclaration des Pratiques de Certification

Version 1.4

Date d'entrée en vigueur : 15/05/2020

Tous droits réservés

Table des matières

1	Introduction	8
1.1	Présentation générale.....	8
1.2	Identification du document	9
1.3	Entités intervenant dans l'IGC.....	9
1.3.1	LEX PERSONA Certification Service Provider Board (LPCSP Board)	9
1.3.2	Autorité de Certification (AC).....	9
1.3.3	Autorité d'Enregistrement (AE).....	10
1.3.4	Sujet.....	10
1.3.5	Souscripteur.....	10
1.3.6	Responsable de la Clé Privé du Sujet (RCPS)	10
1.3.7	Utilisateur de Certificat (UC).....	11
1.4	Usage des Certificats.....	11
1.4.1	Domaines d'utilisation applicables	11
1.4.2	Domaines d'utilisation interdits	12
1.5	Gestion de la PC	12
1.5.1	Entité gérant la PC.....	12
1.5.2	Entité déterminant la conformité de la PC/DPC	12
1.5.3	Procédure d'approbation de la conformité de la PC/DPC	12
1.6	Définitions et Acronymes	12
1.6.1	Définitions	12
1.6.2	Acronymes	14
2	Responsabilité concernant la mise à disposition des informations devant être publiées	14
2.1	Entités chargées de la mise à disposition des informations	14
2.2	Informations devant être publiées	15
2.3	Délais et fréquences de publication	15
2.4	Contrôle d'accès aux informations publiées	15
3	Identification et authentification	15
3.1	Nommage.....	15
3.1.1	Types des noms.....	15
3.1.2	Nécessité d'utilisation de noms explicites	16
3.1.3	Anonymisation et pseudonymisation des Sujets.....	16
3.1.4	Règles d'interprétation des différentes formes de nom	16
3.1.5	Unicité des noms.....	16
3.1.6	Identification, authentification et rôle des marques déposées	17
3.2	Validation initiale de l'identité.....	17
3.2.1	Méthodes pour prouver la possession de la Clé Privée.....	17
3.2.2	Validation de l'identité d'une Entité Légale	17
3.2.3	Validation de l'identité du Sujet	17
3.2.4	Informations non vérifiées du Sujet.....	18
3.2.5	Validation de l'autorité du Souscripteur.....	18
3.2.6	Critères d'interopérabilité	19
3.3	Identification et validation d'une demande de renouvellement des clés	19
3.3.1	Identification et validation d'un renouvellement courant.....	19
3.3.2	Identification et validation pour un renouvellement après révocation	19

3.4	Identification et validation d'une demande de révocation	19
4	Exigences opérationnelles sur le cycle de vie des Certificats	19
4.1	Demande de Certificat	19
4.1.1	Origine d'une demande de Certificat	19
4.1.2	Processus et responsabilités pour l'établissement d'une demande de Certificat.....	19
4.2	Traitement d'une demande de Certificat	20
4.2.1	Exécution des processus d'identification et de validation de la demande	20
4.2.2	Acceptation ou rejet de la demande	20
4.2.3	Durée d'établissement du Certificat	21
4.3	Délivrance du Certificat	21
4.3.1	Actions de l'AC concernant la délivrance du Certificat.....	21
4.3.2	Notification par l'AC de la délivrance du Certificat au RCPS.....	21
4.4	Acceptation du Certificat.....	21
4.4.1	Démarche d'acceptation du Certificat.....	21
4.4.2	Publication du Certificat	21
4.4.3	Notification par l'AC aux autres entités de la délivrance du Certificat.....	21
4.5	Usages de la bi-clé et du Certificat	22
4.5.1	Utilisation de la Clé Privée et du Certificat par le Sujet	22
4.5.2	Utilisation de la Clé Publique et du Certificat par l'UC	22
4.6	Renouvellement d'un Certificat.....	22
4.7	Délivrance d'un nouveau Certificat suite au changement de la bi-clé	22
4.8	Modification du Certificat.....	22
4.9	Révocation et suspension des Certificats	22
4.9.1	Causes possibles d'une révocation.....	22
4.9.2	Origine d'une demande de révocation.....	23
4.9.3	Procédure de traitement d'une demande de révocation	24
4.9.4	Délai accordé au demandeur pour formuler la demande de révocation.....	24
4.9.5	Délai de traitement par l'AC d'une demande de révocation	24
4.9.6	Exigences de vérification de la révocation par les UC	24
4.9.7	Fréquence d'établissement des LCR	25
4.9.8	Délai maximum de publication d'une LCR	25
4.9.9	Disponibilité d'un système de vérification en ligne de la révocation et de l'état des Certificats.....	25
4.9.10	Exigences de vérification en ligne du statut de révocation des Certificats par les UC	25
4.9.11	Autres moyens disponibles d'information sur les révocations.....	25
4.9.12	Exigences spécifiques en cas de compromission de la Clé Privée	25
4.9.13	Causes possibles d'une suspension.....	25
4.9.14	Origine d'une demande de suspension	25
4.9.15	Procédure de traitement d'une demande de suspension	25
4.9.16	Limites de la période de suspension d'un Certificat	25
4.10	Fonction d'information sur l'état des Certificats.....	25
4.10.1	Caractéristiques opérationnelles	25
4.10.2	Disponibilité de la fonction	26
4.10.3	Dispositifs optionnels.....	26
4.11	Fin de la relation entre le Souscripteur et l'AC	26
4.12	Séquestre de clé et recouvrement	26

4.12.1	Politique et pratiques de recouvrement par séquestre des clés	26
4.12.2	Politique et pratiques de recouvrement par encapsulation des clés de session ...	26
5	Mesures de sécurité non techniques	26
5.1	Mesures de sécurité physique	26
5.1.1	Situation géographique et construction des sites	26
5.1.2	Accès physique.....	26
5.1.3	Alimentation électrique et climatisation	26
5.1.4	Vulnérabilité aux dégâts des eaux.....	27
5.1.5	Prévention et protection incendie.....	27
5.1.6	Conservation des supports	27
5.1.7	Mise hors service des supports	27
5.1.8	Sauvegardes hors site	27
5.2	Mesures de sécurité procédurales	28
5.2.1	Rôles de confiance	28
5.2.2	Nombre de personnes requises par tâche	28
5.2.3	Identification et authentification pour chaque rôle.....	28
5.2.4	Rôles exigeant une séparation des attributions.....	29
5.3	Mesures de sécurité vis-à-vis du personnel	29
5.3.1	Qualifications, compétences et habilitations requises.....	29
5.3.2	Procédures de vérification des antécédents	29
5.3.3	Exigences en matière de formation initiale.....	29
5.3.4	Exigences et fréquence en matière de formation continue.....	30
5.3.5	Fréquence et séquence de rotation entre différentes attributions	30
5.3.6	Sanctions en cas d'actions non autorisées.....	30
5.3.7	Exigences vis-à-vis du personnel des prestataires externes	30
5.3.8	Documentation fournie au personnel	30
5.4	Procédure de constitution des données d'audit	30
5.4.1	Type d'évènements à enregistrer.....	30
5.4.2	Fréquence de traitement des journaux d'évènements.....	31
5.4.3	Période de conservation des journaux d'évènements	31
5.4.4	Protection des journaux d'évènements.....	31
5.4.5	Procédure de sauvegarde des journaux d'évènements.....	31
5.4.6	Système de collecte des journaux d'évènements	31
5.4.7	Notification de l'enregistrement d'un évènement au responsable de l'évènement ...	31
5.4.8	Évaluation des vulnérabilités	31
5.5	Archivage des données.....	32
5.5.1	Types de données à archiver.....	32
5.5.2	Période de conservation des archives	32
5.5.3	Protection des archives	32
5.5.4	Procédure de sauvegarde des archives	32
5.5.5	Exigences d'horodatage des données.....	32
5.5.6	Système de collecte des archives.....	32
5.5.7	Procédures de récupération et de vérification des archives	33
5.6	Changement de clé d'AC.....	33
5.7	Reprise suite à la compromission et sinistre	33
5.7.1	Procédures de remontée et de traitement des incidents et des compromissions	33

5.7.2	Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données).....	34
5.7.3	Procédures de reprise en cas de compromission de la clé privée d'une composante	34
5.7.4	Capacités de continuité d'activité suite à un sinistre	34
5.8	Fin de vie de l'AC.....	34
6	Mesures de sécurité techniques.....	35
6.1	Génération et installation de bi-clés	35
6.1.1	Génération des bi-clés	35
6.1.2	Transmission de la clé privée à son propriétaire	35
6.1.3	Transmission de la clé publique à l'AC	35
6.1.4	Transmission de la clé publique de l'AC aux UC	35
6.1.5	Tailles des clés	35
6.1.6	Vérification de la génération des paramètres des bi-clés et de leur qualité.....	36
6.1.7	Objectifs d'usage de la clé.....	36
6.2	Mesures de sécurité pour la protection des clés privées et pour les dispositifs cryptographiques	36
6.2.1	Standards et mesures de sécurité pour les dispositifs cryptographiques	36
6.2.2	Contrôle de la Clé Privée	36
6.2.3	Séquestre de la Clé Privée	36
6.2.4	Copie de secours de la Clé Privée	36
6.2.5	Archivage de la Clé Privée	37
6.2.6	Transfert de la clé privée vers / depuis le dispositif cryptographique.....	37
6.2.7	Stockage de la clé privée dans un dispositif cryptographique	37
6.2.8	Méthode d'activation de la clé privée	37
6.2.9	Méthode de désactivation de la Clé Privée	37
6.2.10	Méthode de destruction d'une Clé Privée.....	38
6.2.11	Niveau de qualification des dispositifs cryptographiques	38
6.3	Autres aspects de la gestion des bi-clés.....	38
6.3.1	Archivage des clés publiques.....	38
6.3.2	Durées de vie des bi-clés et des Certificats.....	38
6.4	Données d'activation	38
6.4.1	Génération et installation des données d'activation	38
6.4.2	Protection des données d'activation.....	38
6.4.3	Autres aspects liés aux données d'activation	39
6.5	Mesures de sécurité des systèmes informatiques	39
6.5.1	Exigences de sécurité technique spécifiques aux systèmes informatiques	39
6.5.2	Niveau de qualification des systèmes informatiques.....	39
6.6	Mesures de sécurité liées au développement des systèmes	39
6.6.1	Mesures de sécurité liées au développement des systèmes	39
6.6.2	Mesures liées à la gestion de la sécurité	39
6.6.3	Niveau d'évaluation sécurité du cycle de vie des systèmes	39
6.7	Mesures de sécurité réseau	40
6.8	Horodatage / Système de datation	40
7	Profils des Certificats, OCSP et des LCR	40
7.1	Certificat de l'AC.....	40
7.2	Certificat d'un Sujet.....	41

7.3	Profil des LCR	43
7.4	Profil OCSP	44
8	Audit de conformité et autres évaluations	45
8.1	Fréquences et / ou circonstances des évaluations	45
8.2	Identités / qualifications des évaluateurs	45
8.3	Relations entre évaluateurs et entités évaluées	45
8.4	Sujets couverts par les évaluations	45
8.5	Actions prises suite aux conclusions des évaluations	45
8.6	Communication des résultats	46
9	Autres problématiques métiers et légales	46
9.1	Tarifs	46
9.1.1	Tarifs pour la fourniture ou le renouvellement de Certificats	46
9.1.2	Tarifs pour accéder aux Certificats	46
9.1.3	Tarifs pour accéder aux informations d'état et de révocation des Certificats	46
9.1.4	Tarifs pour d'autres services	46
9.1.5	Politique de remboursement	46
9.2	Responsabilité financière	47
9.2.1	Couverture par les assurances	47
9.2.2	Autres ressources	47
9.2.3	Couvertures et garantie concernant les entités utilisatrices	47
9.3	Confidentialité des données professionnelles	47
9.3.1	Périmètre des informations confidentielles	47
9.3.2	Informations hors du périmètre des informations confidentielles	47
9.3.3	Responsabilités en termes de protection des informations confidentielles	47
9.4	Protection des données personnelles	48
9.4.1	Politique de protection des données personnelles	48
9.4.2	Informations à caractère personnel	48
9.4.3	Informations à caractère non personnel	48
9.4.4	Responsabilité en termes de protection des données personnelles	48
9.4.5	Notification et consentement d'utilisation des données personnelles	48
9.4.6	Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives	48
9.4.7	Autres circonstances de divulgation d'informations personnelles	48
9.5	Droits sur la propriété intellectuelle et industrielle	48
9.6	Interprétations contractuelles et garanties	49
9.6.1	LPCSP Board	49
9.6.2	AC	49
9.6.3	Autorité d'Enregistrement	50
9.6.4	RCPS et Souscripteur	50
9.6.5	UC	51
9.7	Limite de garantie	52
9.8	Limite de responsabilité	52
9.9	Indemnités	52
9.10	Durée et fin anticipée de validité de la PC/DPC	53
9.10.1	Durée de validité	53
9.10.2	Fin anticipée de validité	53
9.10.3	Effets de la fin de validité et clauses restant applicables	53

9.11	Notification individuelles et communications entre les participants	53
9.12	Amendements.....	53
9.12.1	Procédures d'amendements.....	53
9.12.2	Mécanisme et période d'information sur les amendements	53
9.12.3	Circonstances selon lesquelles l'OID doit être changé.....	53
9.13	Dispositions concernant la résolution de conflits	53
9.14	Juridictions compétentes.....	54
9.15	Conformité aux législations et réglementations	54
9.16	Dispositions diverses.....	54
9.16.1	Accord global.....	54
9.16.2	Transfert d'activités.....	54
9.16.3	Conséquences d'une clause non valide	54
9.16.4	Application et renonciation	54
9.16.5	Force majeure.....	54
9.17	Autres dispositions	54
10	Références	54

1 Introduction

1.1 Présentation générale

Dans le cadre de son offre de services de confiance Sunnystamp, LEX PERSONA fournit un service de génération de Certificats de type « cachetage » ou de type « horodatage », délivrés par une Autorité de Certification appartenant à l'Infrastructure de Gestion de Clés (IGC) Sunnystamp.

Cette Autorité de Certification est dénommée « Sunnystamp Legal Persons CA » et sera nommée « AC » dans le reste du document.

Cette AC délivre des Certificats d'une durée de validité de 3 années au maximum.

Le présent document constitue la Politique de Certification et la Déclaration des Pratiques de Certification (PC/DPC) de l'AC, décrit les exigences de toutes les phases du cycle de vie des Certificats délivrés par l'AC et fixe les règles et engagements que doivent respecter LEX PERSONA et toutes les parties concernées. Les procédures internes propres à la Déclaration des Pratiques de Certification (DPC) sont confidentielles et ne sont pas exposées dans ce document.

Cette PC/DPC est conforme à la norme [EN 319 411-1] niveau NCP+.

L'AC est délivrée par l'Autorité de Certification racine « Sunnystamp Root CA G2 ».

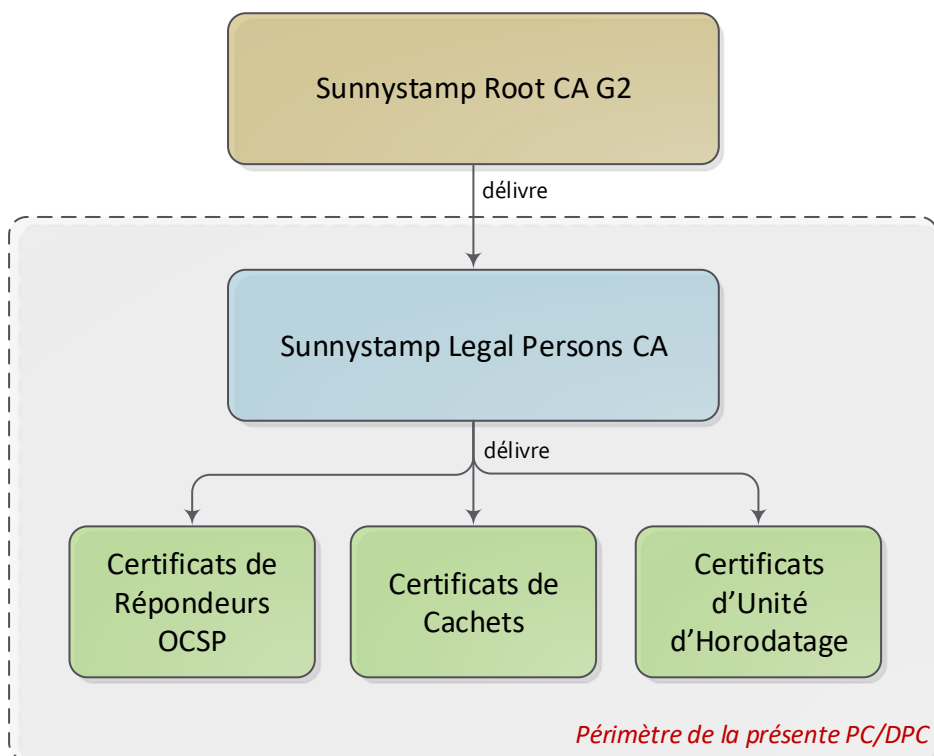


Figure 1 : hiérarchie des certificats de l'AC

1.2 Identification du document

Les politiques contenues dans ce document sont les suivantes :

- 1.3.6.1.4.1.22542.100.1.1.2.1 pour les Certificats de type « cachetage » de niveau NCP+ de la norme [EN 319 411-1] ;
- 1.3.6.1.4.1.22542.100.1.1.2.2 pour les Certificats de type « horodatage » de niveau NCP+ de la norme [EN 319 411-1] ;
- 1.3.6.1.4.1.22542.100.1.1.2.3 pour les Certificats de type « horodatage logiciel ».

Dans la suite du document, pour en faciliter la lecture, les expressions suivantes seront utilisées :

- « Certificat de cachetage », pour désigner un Certificat délivré par l'AC selon l'OID 1.3.6.1.4.1.22542.100.1.1.2.1 ;
- « Certificat d'horodatage ETSI », pour désigner un Certificat délivré par l'AC selon l'OID 1.3.6.1.4.1.22542.100.1.1.2.2 ;
- « Certificat d'horodatage logiciel », pour désigner un Certificat délivré par l'AC selon l'OID 1.3.6.1.4.1.22542.100.1.1.2.3.

1.3 Entités intervenant dans l'IGC

1.3.1 LEX PERSONA Certification Service Provider Board (LPCSP Board)

L'AC est sous la responsabilité du LPCSP Board. Le LPCSP Board est représenté par LEX PERSONA. Il est composé des membres suivants :

- Le responsable du LPCSP Board qui est un représentant légal de LEX PERSONA ;
- Des intervenants spécialisés dans le management de la sécurité des systèmes d'information et nommés par le responsable du LPCSP Board.

Les missions principales du LPCSP Board dans le cadre de l'AC sont les suivantes :

- Rédiger et approuver la PC/DPC ;
- Approuver le corpus documentaire de l'AC ;
- Définir le processus d'examen et de mise à jour de la PC/DPC ;
- Définir et attribuer les rôles de confiance au sein de l'AC ;
- Approuver le rapport annuel d'audit interne des composantes de l'IGC.

1.3.2 Autorité de Certification (AC)

L'AC est responsable de la fourniture des prestations de gestion des Certificats durant leur cycle de vie (génération, délivrance, révocation, diffusion, etc.) en mettant en œuvre différents services dans une Infrastructure de Gestion de Clés (IGC) opérée par LEX PERSONA.

1.3.3 Autorité d'Enregistrement (AE)

Les missions principales de l'AE consistent à :

- Vérifier l'identité des Sujets ;
- Authentifier et transmettre à l'AC les demandes de création et de révocation de Certificats ;
- Archiver les données relatives à l'identification des Sujets.

L'AE est gérée et opérée par LEX PERSONA.

L'AE peut déléguer une partie de ses missions à une entité tierce sous contrat avec LEX PERSONA mais reste toujours responsable des obligations qui lui incombent vis-à-vis des Souscripteurs et des Sujets.

1.3.4 Sujet

Un Sujet est une Entité Légale (qui peut être une Organisation, une unité, un département ou un service identifié comme étant associé à cette Organisation) qui souhaite :

- Pour les Certificats de cachetage : effectuer des opérations de cachetage sur des données afin de garantir leur intégrité et leur authenticité ;
- Pour les Certificats d'horodatage ETSI : effectuer des opérations d'horodatage sur des données afin de garantir leur intégrité et leur antériorité par rapport à une date et une heure de référence ;
- Pour les Certificats d'horodatage logiciel : effectuer des opérations d'horodatage sur des données afin de garantir leur intégrité et leur antériorité par rapport à une date et une heure de référence.

Dans tous les cas le Sujet est identifié dans le Certificat comme étant le porteur de la Clé Privée associée à la Clé Publique contenue dans le Certificat.

1.3.5 Souscripteur

Le Souscripteur qui demande un Certificat pour un Sujet est soit :

- Une personne physique ou morale habilitée à représenter le Sujet (un représentant légal (RL) du Sujet ou une personne physique ou morale qui détient le Sujet) ;
- Un RL qui demande un Certificat pour une filiale, une unité, un département ou un service du Sujet.

L'AC peut endosser le rôle de Souscripteur dans le cas où elle est amenée à demander un Certificat pour elle-même.

1.3.6 Responsable de la Clé Privée du Sujet (RCPS)

Un RCPS est une personne physique agissant pour le compte du Souscripteur et qui est dûment mandatée par le Souscripteur et qui lui délègue les responsabilités suivantes :

- La responsabilité de porteur de la Clé Privée associée à la Clé Publique contenue dans le Certificat ;

- La responsabilité des étapes du cycle de vie du Certificat, et en particulier celles qui consistent à :
 - Générer la bi-clé dans un dispositif cryptographique satisfaisant aux exigences de la section 6.2.11, pour les Certificats de cachetage et pour les Certificats d'horodatage ETSI ;
 - Demander un Certificat à l'AE ;
 - Se faire remettre un Certificat par l'AE ;
 - Procéder le cas échéant à la demande de révocation d'un Certificat.

Le RCPS est enregistré par l'AE et est en relation directe avec elle.

La présence d'un RCPS est obligatoire. A défaut, un RL du Souscripteur peut s'enregistrer auprès de l'AE en tant que RCPS.

Dès lors qu'un RCPS ne peut plus assumer les responsabilités décrites ci-dessus (du fait d'un changement d'affectation, du départ de l'entreprise, de la rupture du contrat de service avec le RCPS ou l'entité de laquelle il dépend, etc.), le Souscripteur doit effectuer une demande de révocation auprès de l'AE.

1.3.7 Utilisateur de Certificat (UC)

Un UC désigne une personne physique ou morale qui utilise des Certificats délivrés par l'AC pour vérifier des signatures, des cachetages et des horodatages.

1.4 Usage des Certificats

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Certificat de l'AC

La Clé Privée associée à la Clé Publique du Certificat de l'AC est utilisée pour signer :

- Les Certificats des Sujets ;
- Les LCR ;
- Les Certificats de répondeurs OCSP.

1.4.1.2 Certificat de Sujet

La Clé Privée associée à la Clé Publique du Certificat d'un Sujet est utilisée :

- Pour les Certificats de cachetage : effectuer des opérations de cachetage sur des données afin de garantir leur intégrité et leur authenticité ;
- Pour les Certificats d'horodatage ETSI et logiciel : effectuer des opérations d'horodatage sur des données afin de garantir leur intégrité et leur antériorité par rapport à une date et une heure de référence.

1.4.2 Domaines d'utilisation interdits

Les usages autres que ceux listés dans la section 1.4.1 sont interdits.
De plus, les Certificats doivent être utilisés dans la limite des lois et réglementations en vigueur.

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

LEX PERSONA
2 RUE GUSTAVE EIFFEL
CS 90601
10901 TROYES CEDEX 9
FRANCE
E-mail : pki@sunnystamp.com
Phone : 0033 325 439 078

1.5.2 Entité déterminant la conformité de la PC/DPC

Le LPCSP Board détermine la conformité de la PC/DPC en réalisant des audits et des contrôles de conformité.

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

Le LPCSP Board approuve la PC/DPC après avoir notamment déterminé la conformité de la PC/DPC.

1.6 Définitions et Acronymes

1.6.1 Définitions

Autorité de Certification

Au sein d'un Prestataire de Service de Certification Electronique (PSCE), une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une PC/DPC et est identifiée comme telle, en tant qu'émetteur (champ « issuer » du Certificat), dans les Certificats émis au titre de cette PC/DPC.

Autorité d'Enregistrement (AE)

Cf. section 1.3.3.

Bi-clé

Combinaison d'une Clé Privée et d'une Clé Publique utilisée pour effectuer des opérations cryptographiques.

Certificat

Ensemble d'informations garantissant l'association entre l'identité d'un Sujet et une Clé Publique, grâce à une signature électronique de ces données effectuée à l'aide de la Clé Privée de l'AC qui délivre le Certificat. Un Certificat contient des informations telles que :

- L'identité du Sujet du Certificat ;

- La Clé Publique du Sujet du Certificat ;
- Le(s) usage(s) autorisé(s) de la Clé Publique ;
- La durée de vie du Certificat ;
- L'identité de l'AC ;
- La signature de l'AC.

Le format standard de certificat est défini dans la recommandation X.509 v3 et dans la [RFC 5280].

Dans le cadre de la présente PC/DPC, le terme Certificat sans épithète sera utilisé pour désigner le Certificat d'un Sujet.

Clé Privée

Clé d'une bi-clé d'une entité devant être utilisée exclusivement par cette entité.

Clé Publique

Clé d'une bi-clé d'une entité pouvant être rendue publique.

Déclaration des Pratiques de Certification (DPC)

Ensemble de pratiques qu'une Autorité de Certification met en œuvre pour émettre, gérer, révoquer et renouveler les Certificats qu'elle émet dans le cadre d'une Politique de Certification.

Entité Légale

Terme utilisé dans ce document pour désigner exclusivement la personne morale à laquelle le Sujet est rattaché et au nom de laquelle ce dernier utilise son Certificat.

Infrastructure de Gestion de Clés (IGC)

Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs Certificats utilisés par des services de confiance. Une IGC peut être composée d'une Autorité de Certification, d'un Opérateur de Certification, d'une Autorité d'Enregistrement centralisée et/ou locale, de Mandataires de Certification, d'une entité d'archivage, d'une entité de publication, etc.

Politique de Certification (PC)

Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une Autorité de Certification se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un Certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC/DPC peut également, si nécessaire, identifier les obligations et les exigences portant sur les autres intervenants, notamment les Sujets et les Utilisateurs de Certificats (UC).

Représentant Légal (RL)

Au sens de la présente PC/DPC, le RL est une personne physique disposant des pouvoirs de représenter le Sujet de par la loi. Elle dispose de la faculté de procéder à des demandes d'émission et de révocation de Certificat au bénéfice des Sujets qu'elle aura expressément défini.

1.6.2 Acronymes

Les acronymes utilisés dans la présente PC/DPC sont les suivants :

AC	Autorité de Certification « Sunnystamp Legal Persons CA »
AE	Autorité d'Enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
DN	Distinguished Name
DPC	Déclarations des Pratiques de Certification
eIDAS	electronic identification and trust services for electronic transactions
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés
LCR	Liste de Certificats Révoqués
LPCSP Board	LEX PERSONA Certification Service Provider Board
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PC	Politique de Certification
PCA	Plan de Continuité d'Activité
PSCE	Prestataire de Service de Certification Electronique
RCPS	Responsable de la Clé Privée du Sujet
UC	Utilisateurs de Certificat

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

2.1 Entités chargées de la mise à disposition des informations

LEX PERSONA est chargée de la mise en place et de la mise à disposition, aux Souscripteurs, aux Sujets et aux UC, des informations devant être publiées.

Ces informations, énumérées dans la section suivante, sont publiées sur le site de publication suivant : <https://pki2.sunnystamp.com/repository>.

2.2 Informations devant être publiées

L'AC publie en ligne les informations suivantes :

- La présente PC/DPC ;
- La déclaration d'IGC ;
- L'accord d'utilisation des Certificats ;
- Le formulaire de demande de Certificat ;
- Le formulaire de demande de révocation d'un Certificat ;
- Le certificat X.509 de l'AC et de l'AC Racine ainsi que leur empreinte de hachage ;
- La LCR consultable aux adresses suivantes :
<http://pki2.sunnystamp.com/crls/sunnystamp-legal-persons-ca.crl> ;
<http://pki3.sunnystamp.com/crls/sunnystamp-legal-persons-ca.crl> ;
- Le statut de révocation des Certificats qu'elle émet à travers un répondeur OCSP accessible à l'adresse suivante : <http://ocsp2.sunnystamp.com/sunnystamp-legal-persons-ca>.

2.3 Délais et fréquences de publication

La présente PC/DPC et le certificat de l'AC sont disponibles en permanence sur le site de publication de l'AC.

Ils sont publiés avant la délivrance par l'AC de son premier Certificat.

L'accord de souscription, la déclaration d'IGC et l'accord d'utilisation des Certificats sont publiés après chaque mise à jour.

Les LCR sont publiées comme spécifié à la section 4.9 de la présente PC.

2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées sont librement accessible en lecture. En revanche, l'accès en modification aux données publiées est strictement limité aux personnes habilitées de l'IGC.

3 Identification et authentification

3.1 Nommage

3.1.1 Types des noms

Les Certificats et les noms qu'ils contiennent sont conformes à la norme [RFC 5280]. L'AC émettrice est identifiée dans le champ `issuer` du Certificat et le Sujet est identifié dans le champ `subject`.

Le champ `subject` du Certificat émis par l'AC comporte les attributs suivants :

Sunnystamp Legal Persons CA – PC/DPC	Version 1.4 Page 15 / 55	Copyright LEX PERSONA 2020
--------------------------------------	-----------------------------	----------------------------

Attribut	Description	Obligatoire ?
CN	Nom courant utilisé par le Sujet pour se représenter : Une unité, un département, un service ou une filiale du Sujet	Oui
C	Code du pays dans lequel le Sujet est établi	Oui
O	Nom légal du Sujet	Oui
OI	Identifiant unique du Sujet (structuré conformément à la section 5.1.4 de la norme [EN 319 412-1]).	Oui
serialNumber	Identifiant interne unique du Certificat du Sujet généré par l'AC	Oui
OU	Attribut utilisé pour préciser le Sujet : une unité, un département, un service ou une filiale du Sujet	Non
L	Attribut utilisé pour désigner la ville dans laquelle le Sujet est enregistré	Non

Chaque `subject` émis par l'AC doit être unique. Cette unicité est garantie grâce à l'attribut `serialNumber`.

Toutes les informations contenues dans les attributs énumérés ci-dessus sont vérifiées par l'AE à l'exception du `serialNumber`.

L'AC se réserve le droit d'émettre des certificats de test. Dans ce cas, les champs CN et OU doivent contenir le terme « TEST ».

3.1.2 Nécessité d'utilisation de noms explicites

Le contenu des attributs du champ `subject` du Certificat doit permettre de garantir l'utilisation d'un nom explicite permettant d'identifier le Sujet.

3.1.3 Anonymisation et pseudonymisation des Sujets

Ces pratiques sont interdites par cette PC/DPC.

3.1.4 Règles d'interprétation des différentes formes de nom

Les éléments contenus dans les sections 3.1.1, 3.1.2 et 3.1.3 fournissent les explications permettant d'interpréter correctement les différentes formes de nom.

3.1.5 Unicité des noms

L'attribut `serialNumber` contenu dans le champ `subject` du Certificat permet de garantir l'unicité des noms.

3.1.6 Identification, authentification et rôle des marques déposées

L'AC ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par des Souscripteurs de marques déposées, de marques notoires et de signes distinctifs, ainsi que de noms de domaine.

Si un tel cas se produit, l'AE pourra refuser de délivrer le Certificat au Sujet et l'AC pourra prendre la décision de révoquer le Certificat.

3.2 Validation initiale de l'identité

3.2.1 Méthodes pour prouver la possession de la Clé Privée

Le RCPS prouve à l'AC qu'il possède bien la Clé Privée correspondant à la Clé Publique à certifier en transmettant lui-même à l'AE la requête de certificat au format [PKCS#10] signée avec la Clé Privée.

3.2.2 Validation de l'identité d'une Entité Légale

L'AE procède à la validation de l'identité de l'Entité Légale du Sujet en vérifiant que le RCPS est effectivement désigné par un RL de cette Entité Légale. Ces vérifications sont réalisées lors de la validation de l'identité du Sujet.

3.2.3 Validation de l'identité du Sujet

La validation de l'identité du Sujet est effectuée lors du traitement par l'AE de la demande de Certificat. Elle résulte de 4 étapes de validation :

- Validation de l'identité du RCPS ;
- Validation de l'identité de l'Entité Légale et de son RL ;
- Validation des attributs du Sujet en relation avec l'Entité Légale ;
- Validation de la nomination du RCPS par le RL.

3.2.3.1 Validation de l'identité du RCPS pour un Certificat à émettre

Le RCPS fournit les informations suivantes à l'AE qui les vérifie :

- Un document officiel d'identité en cours de validité avec photographie comportant ses nom, prénom(s), date et lieu de naissance ;
- Son adresse e-mail, son numéro de téléphone portable et sa fonction.

Au cours du traitement de la demande de Certificat, l'AE procède à la vérification de l'identité du RCPS lors d'un face-à-face physique en contrôlant la pièce d'identité fournie par le RCPS (état général, points de vérification habituels, vérification de la correspondance entre la photo figurant sur la pièce d'identité avec le RCPS). Ce face-à-face physique n'est pas nécessaire dès lors que le RCPS a signé le formulaire de demande de Certificat à l'aide d'un certificat de niveau supérieur ou équivalent au niveau RGS 2* ou ETSI EN 319 411-1 NCP+.

3.2.3.2 Validation de l'identité de l'Entité Légale et de son RL pour un Certificat à émettre

Le RCPS fournit à l'AE qui la vérifie une preuve valide à valeur légale de l'existence du Souscripteur comportant son numéro d'identifiant unique (exemples : un avis de situation SIRENE, la première

page d'un extrait Kbis de moins de 3 mois pour une entreprise française, etc.) ainsi qu'une preuve valide à valeur légale de la qualité de RL de l'Entité Légale (exemples : page d'un extrait Kbis de l'Entité Légale du Souscripteur mentionnant le RL, procès-verbal d'assemblée générale désignant le RL, etc.).

3.2.3.3 Validation des attributs du Sujet en relation avec l'Entité Légale pour un Certificat à émettre

Le RCPS fournit à l'AE qui les vérifie, tous les attributs du champ `subject` à renseigner dans le Certificat, à l'exception de l'attribut `serialNumber`, et tout document permettant de justifier le lien entre l'attribut `o` et l'Entité Légale du Souscripteur si ces informations diffèrent.

3.2.3.4 Validation de la nomination du RCPS par le RL pour un Certificat à émettre

Le RCPS fournit à l'AE qui le vérifie le mandat contenant les conditions générales d'utilisation du Certificat, daté de moins de 3 mois, désignant le RCPS comme étant habilité à être responsable du Certificat du Sujet considéré.

Ce mandat est d'abord signé par le RCPS, puis co-signé pour acceptation par le RL de l'Entité Légale représentée par le Sujet.

L'AE vérifie la signature électronique du RL en s'appuyant sur le référentiel d'autorités de confiance de la plate-forme www.sunnystamp.com pour s'assurer de l'intégrité et de l'authenticité de la signature et de la validité de la chaîne de certification du certificat du signataire.

Concernant la vérification de la signature électronique du mandat par le RCPS, elle est traitée au paragraphe 4.1.2 et ne concerne que l'accord de souscription.

Le RCPS pouvant éventuellement démissionner de ses fonctions, il existe une procédure de révocation permettant au RL ou à l'AE de révoquer le Certificat.

Enfin, le RCPS est informé que les informations personnelles d'identité le concernant pourront être utilisées comme éléments d'authentification lors de la demande de révocation, en particulier si le RCPS a oublié ou perdu le code de révocation fourni par l'AE lors de la remise du Certificat.

3.2.3.5 Archivage des informations de validation

L'AE archive toutes les informations utilisées pour vérifier l'identité du RCPS, du RL du Souscripteur, et, le cas échéant, tous les attributs du Sujet, y compris toute référence à la documentation utilisée pour leur vérification, et toute réserve concernant leurs limitations d'usage.

3.2.4 Informations non vérifiées du Sujet

Toutes les informations contenues dans le champ `subject` du Certificat, à l'exception du numéro de série, sont vérifiées par l'AE.

3.2.5 Validation de l'autorité du Souscripteur

La validation de l'autorité du Souscripteur correspond pour l'AE à vérifier que la souscription a bien été effectuée par un RL du Souscripteur.

3.2.6 Critères d'interopérabilité

L'AC gère et documente les demandes d'accords et les accords de reconnaissance avec des AC extérieures au domaine de sécurité auquel l'AC appartient.

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

Le renouvellement de la bi-clé et du Certificat d'un Sujet n'est pas autorisé par cette PC/DPC.

3.3.1 Identification et validation d'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

Les personnes qui peuvent demander la révocation d'un Certificat sont les suivantes :

- Le RCPS ;
- Le RL ;
- Un membre de l'AC.

Dès que l'une des causes de révocation décrite dans la présente PC/DPC est détectée par l'une de ces personnes, elle doit, sans délai, demander à l'AE de révoquer le Certificat.

La demande de révocation d'un Certificat consiste pour le demandeur à effectuer les tâches suivantes :

- Remplir le formulaire de demande de révocation d'un Certificat disponible à l'adresse [FR_Revocation] ;
- Envoyer le formulaire en pièce jointe d'un e-mail à l'adresse ae-slp@sunnystamp.com.

4 Exigences opérationnelles sur le cycle de vie des Certificats

4.1 Demande de Certificat

4.1.1 Origine d'une demande de Certificat

L'origine d'une demande de Certificat provient d'un RCPS dûment mandaté par un RL du Souscripteur.

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

Le processus d'enregistrement pour une demande de Certificat se déroule de la façon suivante :

- Le RCPS doit fournir à l'AE les différentes informations requises dans la section 3.2.3 en garantissant leur exactitude ;

- Le RCPS doit signer l'accord de souscription intégré au formulaire de demande de Certificat transmis par Lex Persona, en respectant le processus documenté dans le Guide du RCPS remis avec le formulaire et qui s'appuie sur la plate-forme de signature électronique en ligne www.sunnystamp.com ; cet accord contient en particulier, lorsqu'il s'agit d'un Certificat de cachetage ou d'un certificat d'horodatage ETSI, l'engagement du RCPS à ce que la bi-clé du Sujet soit générée dans un dispositif cryptographique satisfaisant aux exigences de la section 6.2.11 ; le RCPS doit signer la partie de l'accord qui le concerne ;
- Lors du processus de signature électronique, le RCPS peut, s'il le souhaite, signer l'accord de souscription à l'aide d'un certificat nominatif en sa possession, sous réserve qu'il soit de niveau RGS 2* ou supérieur, ou respectant la norme ETSI EN 319 411-1 NCP+ ou supérieure ; dans ce cas, l'authentification en face-à-face de l'identité du RCPS par l'AE n'est pas nécessaire ;
- Le RCPS doit fournir à l'AE, une preuve de la possession de la Clé Privée du Sujet conformément à la section 3.2.1 ;
- Le RCPS doit faire co-signer l'accord de souscription par le RL du Souscripteur qui s'engage sur l'habilitation du RCPS à demander un Certificat pour le compte de l'Entité Légale du RL ;
- L'AE doit valider les informations du dossier d'enregistrement en conformité avec la présente PC/DPC ;
- L'AE doit transmettre de manière sécurisée à l'AC la demande de Certificat.

4.2 Traitement d'une demande de Certificat

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

Le processus d'identification et de validation d'une demande de Certificat se déroule de la façon suivante :

- L'AE s'assure que le demandeur de Certificat a bien lu et accepté l'accord de souscription ;
- L'AE doit authentifier, le cas échéant, le service de gestion de la bi-clé du Sujet (cf. section 3.2.1) ;
- L'AE valide les différentes informations requises dans la section 3.2.3 ;
- L'AE s'assure que le RCPS lui a remis, à destination de l'AC, une preuve de possession de la Clé Privée du Sujet ;
- L'AE doit faire vérifier la signature de l'accord de souscription par le RL du Souscripteur qui s'engage sur l'habilitation du RCPS à demander un Certificat pour le compte de l'Entité Légale du RL ;
- L'AE doit enfin vérifier l'identité du RCPS en présence physique de ce dernier ou par tout autre moyen garantissant un niveau de vérification équivalent (voir 3.2.3.1).

4.2.2 Acceptation ou rejet de la demande

Pour que la demande de Certificat soit acceptée, toutes les étapes du processus décrit dans la section précédente doivent être effectuées avec succès.

Dans le cas contraire, l'AE rejette la demande de Certificat et en informe le Souscripteur dans les meilleurs délais.

4.2.3 Durée d'établissement du Certificat

La demande de certificat reste active tant qu'elle n'est pas validée ou rejetée. Une fois la demande de Certificat validée, l'AC émet le Certificat dans les meilleurs délais.

4.3 Délivrance du Certificat

4.3.1 Actions de l'AC concernant la délivrance du Certificat

Les actions de l'AC concernant la délivrance du Certificat sont les suivantes :

- L'AC s'assure que la demande de Certificat provient de l'AE ;
- L'AC vérifie la signature de la requête de certificat [PKCS#10] en utilisant la Clé Publique qu'elle contient ;
- L'AC crée le Certificat, en conformité avec le profil du Certificat défini dans la section 7.2 en certifiant, avec la Clé Privée de l'AC, l'association de la Clé Publique récupérée avec les informations d'identification du Sujet contenues dans la demande.

4.3.2 Notification par l'AC de la délivrance du Certificat au RCPS

Une fois généré, le RCPS et le RL sont notifiés de la remise du Certificat qui est transmis au RCPS de manière appropriée.

4.4 Acceptation du Certificat

4.4.1 Démarche d'acceptation du Certificat

L'acceptation d'un Certificat par le RCPS est tacite dès la notification par l'AC de la remise du Certificat au RCPS, et dès lors que l'une des conditions suivantes est satisfaite :

- Le RCPS a utilisé la Clé Privée associée à la Clé Publique contenue dans le Certificat pour cacheter ou horodater ;
- Le RCPS a validé explicitement la remise du Certificat ;

L'acceptation d'un Certificat emporte le consentement par le RCPS à la publication par l'AC du Certificat.

4.4.2 Publication du Certificat

L'AC ne peut publier un Certificat qu'après avoir obtenu le consentement du RCPS.

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

Sans objet.

4.5 Usages de la bi-clé et du Certificat

4.5.1 Utilisation de la Clé Privée et du Certificat par le Sujet

L'utilisation par le RCPS, de la Clé Privée du Sujet et du Certificat associé, doit respecter :

- Les exigences définies dans cette PC/DPC, en particulier les usages définis dans la section 1.4 ;
- L'accord de Souscription ;
- Toute obligation supplémentaire éventuellement imposée au RCPS par le Souscripteur, ne remettant pas en cause les clauses précédentes.

Le RCPS s'engage par ailleurs :

- A protéger sa Clé Privée dans un dispositif satisfaisant aux exigences de la section 6.2.11 ;
- A ne plus utiliser sa Clé Privée en cas de compromission de celle-ci et à demander la révocation du Certificat à l'AC sans délai ;
- A ne plus utiliser sa Clé Privée en cas de révocation du certificat de l'AC.

4.5.2 Utilisation de la Clé Publique et du Certificat par l'UC

Voir section 9.6.6.

4.6 Renouvellement d'un Certificat

Aucun renouvellement de Certificat n'est autorisé par l'AC.

4.7 Délivrance d'un nouveau Certificat suite au changement de la bi-clé

Aucune délivrance d'un nouveau Certificat suite au changement de la bi-clé n'est autorisée par l'AC.

4.8 Modification du Certificat

La présence PC n'autorise pas la modification du Certificat.

4.9 Révocation et suspension des Certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificat de Sujet

Les circonstances suivantes peuvent être à l'origine de la révocation du Certificat d'un Sujet :

- Le RCPS n'a pas respecté, ou ne respecte plus, les obligations découlant de la présente PC/DPC et de l'accord de souscription ;
- Le Souscripteur n'a pas respecté, ou ne respecte plus, les obligations découlant de la présente PC/DPC et de l'accord de souscription ;
- Une erreur a été détectée dans la procédure d'enregistrement du Sujet ;

- L'inexactitude ou la caducité des informations du Certificat ou encore si ces informations portent atteintes aux droits d'un tiers ;
- Les informations contenues dans le Certificat ne sont plus exactes ;
- Le Souscripteur ou le RCPS demande la révocation ;
- Le Souscripteur ne s'est pas acquitté, le cas échéant, du paiement relatif à l'émission du Certificat ;
- La Clé Privée du Sujet est compromise ou suspectée de l'être ;
- Les données d'activation permettant au RCPS d'activer la Clé Privée du Sujet sont perdues ou volées ;
- L'AC est révoquée.

4.9.1.2 Certificat d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC :

- Suspicion de compromission, compromission, perte ou vol de Clé Privée de la composante ;
- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la présente PC/DPC ou dans les procédures internes (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificat de Sujet

Les personnes autorisées à demander la révocation d'un Certificat sont les suivantes :

- Le Souscripteur ;
- Le RCPS ;
- Un membre de l'AE ;
- Le responsable de l'AC ;
- Le LPCSP Board, en cas d'urgence et d'absence du responsable de l'AC.

4.9.2.2 Certificats d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC peut être demandée par un membre de l'AC.

Les entités autorisées à demander la révocation du certificat de l'AC sont les suivantes :

- Le LPCSP Board ;
- Une autorité judiciaire suite à une décision de justice.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Certificat de Sujet

Une demande de révocation peut être transmise à l'AE selon l'une des manières décrites dans la section 3.4.

Le traitement d'une demande de révocation se déroule de la façon suivante :

- L'AE authentifie le demandeur comme indiqué dans la section 3.4 ;
- L'AE vérifie que la demande est complète ;
- L'AE demande à l'AC de procéder à la révocation du Certificat ;
- L'AC révoque le Certificat de manière définitive ;
- L'AE notifie le RCPS et le RL de la révocation du Certificat.

4.9.3.2 Certificat d'une composante de l'IGC

En cas de révocation du certificat de l'AC, cette dernière doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) :

- L'ANSSI à travers le point de contact identifié sur le site <https://www.ssi.gouv.fr/agence/contacts> ;
- L'ensemble des Souscripteurs et des Sujets concernés, en leur précisant que leur Certificat est révoqué et qu'ils ne doivent plus utiliser la Clé Privée correspondante ;
- L'ensemble des entités avec laquelle l'AC est sous contrat.

4.9.4 Délai accordé au demandeur pour formuler la demande de révocation

La demande de révocation doit être transmise au plus tôt à l'AE.

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

4.9.5.1 Certificat de Sujet

Une demande de révocation du Certificat d'un Sujet est traitée dans un délai inférieur à 24 heures après l'authentification effective du demandeur de la révocation.

4.9.5.2 Certificat d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC doit être effectuée dès la détection de l'évènement décrit dans les causes de révocation. En particulier, la révocation d'un certificat d'AC ou d'un certificat de répondeur OCSP doit être effectuée immédiatement, notamment en cas de compromission de la Clé Privée associée.

4.9.6 Exigences de vérification de la révocation par les UC

L'UC est tenu de vérifier, avant son utilisation, l'état des Certificats de la chaîne de certification. La méthode utilisée (LCR ou OCSP) pour vérifier le statut de révocation des Certificats est laissé à l'appréciation de l'UC.

4.9.7 Fréquence d'établissement des LCR

La fréquence de publication des LCR est de 24 heures.

4.9.8 Délai maximum de publication d'une LCR

Les LCR sont publiées au maximum 30 minutes après leur génération.

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

Un répondeur OCSP est mis à disposition par l'AC pour fournir publiquement le statut de révocation des Certificats qu'elle émet. Il est disponible en fonctionnement normal 24h/24 et 7j/7.

4.9.10 Exigences de vérification en ligne du statut de révocation des Certificats par les UC

Un UC doit obligatoirement vérifier le statut de révocation d'un Certificat avant de l'utiliser (cf. section 4.9.6).

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

Pour un Certificat de Sujet, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la Clé Privée.

Pour un certificat d'AC, la révocation suite à une compromission de la Clé Privée fait l'objet d'une information clairement diffusée par l'AC. En cas de révocation de l'AC, tous les certificats délivrés par cette AC et qui sont encore en cours de validité sont révoqués.

4.9.13 Causes possibles d'une suspension

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

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un Certificat

Sans objet.

4.10 Fonction d'information sur l'état des Certificats

4.10.1 Caractéristiques opérationnelles

Les LCR et le répondeur OCSP sont accessibles via les URL de publications décrites dans la section 2.2.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des Certificats est disponible sur plusieurs serveurs de publication, assurant ainsi 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 le Souscripteur et l'AC

Cette relation cesse naturellement au terme de la durée de validité du Certificat ou suite à sa révocation sauf cas contraire précisé dans un contrat établi entre le Souscripteur et l'AC.

4.12 Séquestre de clé et recouvrement

Les Clés Privées de l'AC, des répondeurs OCSP et des Sujets ne sont pas séquestrées.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

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

Sans objet.

5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

L'ensemble des ressources matérielles de l'IGC sont hébergées dans deux Datacenters hautement sécurisés qui respectent les règlements et normes en vigueur et qui fournissent une protection robuste contre les accès non autorisés.

Ces deux Datacenters sont localisés sur le territoire français et sont séparés l'un de l'autre par une distance en ligne droite supérieure à 100 km.

5.1.2 Accès physique

L'accès au site d'hébergement de l'IGC est contrôlé et est strictement limité aux seules personnes autorisées à pénétrer dans les locaux. Les personnes non autorisées doivent toujours être accompagnées par des personnes autorisées.

5.1.3 Alimentation électrique et climatisation

LEX PERSONA assure que les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les exigences de la présente PC/DPC en matière de disponibilité de ses fonctions.

La baie dédiée à l'infrastructure de LEX PERSONA dispose d'une alimentation électrique redondante.

5.1.4 Vulnérabilité aux dégâts des eaux

LEX PERSONA respecte les exigences de protection contre les dégâts des eaux, elles permettent de respecter les exigences de la présente PC/DPC en matière de disponibilité de ses fonctions.

5.1.5 Prévention et protection incendie

Les risques d'incendie ont été pris en compte pour l'installation de l'IGC. Les règles de sécurité incendie permettent de respecter les exigences de la présente PC/DPC en matière de disponibilité de ses fonctions, notamment, les fonctions de gestion des révocations et d'information sur l'état des Certificats.

5.1.6 Conservation des supports

Les différents supports utilisés par l'IGC sont stockés de manière sécurisée.

L'AC assure que les différentes informations nécessaires intervenant dans l'activité de l'IGC sont listées, et les besoins en sécurité sont définis. Les supports correspondant à ces informations sont gérés en fonction de leur besoin en sécurité.

L'AC met en œuvre les moyens nécessaires pour que les supports soient protégés contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC est engagée à conserver ces informations.

Les documents papiers sont conservés par l'AC dans des locaux fermés à clés et sont stockés dans un coffre-fort fermé à clé, que seul le responsable de l'AC ou les personnes autorisées pourront ouvrir.

5.1.7 Mise hors service des supports

En fin de vie, les supports sont détruits de manière sécurisée ou réinitialisés en vue d'une réutilisation.

5.1.8 Sauvegardes hors site

Des sauvegardes hors site sont mises en œuvre par l'IGC vers un site de secours afin d'assurer une reprise des fonctions de l'IGC le plus rapidement possible après incident, conformément aux exigences de la présente PC/DPC et aux engagements de l'AC en matière de disponibilité et plus particulièrement en ce qui concerne la fonction d'information de l'état de révocation des Certificats.

Le site de secours offre un niveau de sécurité au moins équivalent au site principal et garantit notamment que les informations sauvegardées hors site respecteront les mêmes exigences de la présente PC/DPC en matière de confidentialité et d'intégrité.

La procédure de sauvegarde hors site est détaillée dans la procédure de sauvegarde.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les rôles de confiance sont définis de telle sorte qu'il n'y ait aucun conflit d'intérêt possible entre ces rôles.

Les rôles de confiance suivants sont définis :

- **Security Officer** : cette personne est chargée de la mise en œuvre et du contrôle de la politique de sécurité des composantes de l'IGC. Elle gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Elle est habilitée à prendre connaissance des archives et des journaux d'évènements.
- **System Operator** : cette personne est responsable de l'exploitation des applications pour les fonctions mises en œuvre par les composantes de l'IGC. Elle est responsable des opérations de génération et de révocation des certificats.
- **System Administrator** : cette personne est chargée de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Elle assure l'administration technique des systèmes et des réseaux des composantes de l'IGC.
- **HSM Administrator** : cette personne est chargée de l'administration des HSM de l'AC.
- **System Auditor** : cette personne est autorisée à accéder à l'IGC et est en charge de l'analyse régulière des archives et de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.
- **Registration Officer** : cette personne est chargée de vérifier les informations requises pour la délivrance d'un Certificat et d'approuver les demandes de Certificats envoyés par les Souscripteurs à l'AE.
- **Revocation Officer** : cette personne est chargée d'approuver les demandes de révocation de Certificats envoyées à l'AE.
- **Key Holder** : cette personne assure la confidentialité, l'intégrité et la disponibilité des parts de secrets qui lui sont confiées et qui sont liées aux clés d'AC.

5.2.2 Nombre de personnes requises par tâche

En fonction des opérations réalisées, une ou plusieurs personnes avec des rôles différents sont requises.

5.2.3 Identification et authentification pour chaque rôle

Toute personne intervenant dans le fonctionnement de l'AC doit avoir préalablement reçu le rôle correspondant.

L'accès physique est autorisé aux seules personnes qualifiées. L'accès logiciel est protégé par des politiques de sécurité fortes.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

Les cumuls des rôles suivants par une même personne physique sont interdits :

- Security Officer et System Administrator ;
- System Operator et System Administrator.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Tout le personnel de l'AC est soumis à une clause de confidentialité et a notamment signé la charte de sécurité de l'AC.

Les fonctions demandées à chaque membre du personnel de l'AC sont compatibles avec ses compétences. Le personnel d'encadrement dispose de l'expertise nécessaire et est familier des procédures de sécurité.

Le LPCSP Board informe toute personne intervenant dans les rôles de confiance de l'AC :

- Des responsabilités relatives aux services de l'IGC qui lui incombent ;
- Des procédures liées à la sécurité du système et au contrôle du personnel qu'elle doit respecter.

5.3.2 Procédures de vérification des antécédents

Le personnel travaillant pour l'une des composantes de l'AC est soumis à une procédure de vérification des antécédents lors de leur prise de fonction.

Les vérifications portent sur les points suivants :

- Les éventuelles condamnations en justice de la personne ne devront pas être contraires à ses fonctions ;
- Les rôles de confiance de la personne ne devront pas se trouver dans un conflit d'intérêt préjudiciable à l'impartialité de ses tâches.

5.3.3 Exigences en matière de formation initiale

Le recrutement du personnel de l'AC permet de vérifier que chacun dispose de la formation initiale adéquate à la réalisation de ses fonctions.

Le personnel sera formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met œuvre et doit respecter.

Les exigences en matière de formation initiale s'appliquent également à l'AE.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel recevra une formation adaptée préalablement aux évolutions dans l'IGC (procédures, organisation, application, etc.) concernant la ou les composantes sur lesquelles il intervient.

D'autre part, le personnel de l'AC participe régulièrement à des séances de formation sur la sécurité des systèmes d'information.

Les exigences en matière de formation continue s'appliquent également à l'AE.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

Si une personne a réellement fait ou est soupçonnée d'avoir fait une action non autorisée dans l'accomplissement de ses tâches en rapport avec l'exploitation d'une AC ou d'une AE, le LPCSP Board peut lui interdire l'accès aux composantes de l'IGC sur lesquelles elle intervenait.

En outre, si les faits sont avérés, le LPCSP Board pourra prendre à son encontre toutes sanctions disciplinaires adéquates.

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

Les exigences de la section 5.3 sont applicables aux prestataires externes.

5.3.8 Documentation fournie au personnel

Tout le personnel de l'AC a accès à des procédures et manuels complémentaires concernant leurs fonctions et leurs responsabilités.

Ces exigences s'appliquent également à l'AE et à son personnel.

5.4 Procédure de constitution des données d'audit

5.4.1 Type d'évènements à enregistrer

Les événements ci-dessous sont enregistrés de manière manuelle ou automatique :

- Création / modification / suppression de comptes Utilisateur et des données d'authentification correspondantes ;
- Démarrage et arrêt des systèmes informatiques et des applications ;
- Evènement liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes ;
- Les accès physiques ;

- Les actions de maintenance et de changement de la configuration des systèmes ;
- Les changements apportés au personnel ;
- Les actions de destruction des supports.

Les types d'événements à enregistrer sont détaillés dans la procédure de sauvegarde.

5.4.2 Fréquence de traitement des journaux d'évènements

Les journaux d'événements sont systématiquement analysés en cas de remontée d'un événement anormal (cf. section 5.4.8).

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'événements sont conservés pendant au moins un mois sur site avant d'être archivés pendant une période de conservation indiquée dans la procédure de sauvegarde.

5.4.4 Protection des journaux d'évènements

Le mode de conservation des journaux d'événements protège leur intégrité et leur disponibilité. Ils ne sont accessibles qu'au personnel autorisé à les exploiter.

5.4.5 Procédure de sauvegarde des journaux d'évènements

Les journaux d'évènement sont régulièrement sauvegardés et exportés sur le site de secours.

5.4.6 Système de collecte des journaux d'évènements

Sans objet.

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

Sans objet.

5.4.8 Évaluation des vulnérabilités

Pour détecter les vulnérabilités et plus généralement les anomalies, l'AC met en place les contrôles suivants :

- Analyse quotidienne des journaux d'événements de l'AC ;
- Contrôle de l'accès aux LCR toutes les heures ;
- Vérification quotidienne de la publication et de l'archivage des LCR ;
- Vérification de la disponibilité du répondeur OCSP toutes les heures ;
- Vérification de la disponibilité du site de publication toutes les heures ;
- Réalisation régulière de tests d'intrusion et de scans de vulnérabilités sur les équipements et serveurs de l'IGC.

5.5 Archivage des données

5.5.1 Types de données à archiver

Les données archivées sont les suivantes :

- Toutes les versions de la présente PC/DPC ;
- Les accords contractuels entre l'AC et les Souscripteurs ;
- Les formulaires de demande de Certificat ;
- Les éléments ayant permis de vérifier l'identité physique des RCPS ;
- Les Certificats d'AC, les Certificats des répondants OCSP et les LCR ;
- Les journaux d'évènements des différentes composantes de l'IGC ;
- Les rapports d'audit.

Les différents types de données à archiver sont détaillés dans la procédure d'archivage.

5.5.2 Période de conservation des archives

Les informations suivantes sont conservées pendant 10 ans :

- Les journaux d'évènements ;
- Les formulaires de demande de Certificat contenant notamment la preuve d'acceptation des Conditions Générales d'Utilisation par les Souscripteurs.

La période de conservation des archives est détaillée dans la procédure d'archivage.

5.5.3 Protection des archives

Les archives, qu'elles soient au format papier ou électronique, sont conservées de façon à garantir leur intégrité et leur confidentialité afin que seules les personnes autorisées puissent y accéder.

Les modalités de protection des archives sont décrites dans la procédure d'archivage.

5.5.4 Procédure de sauvegarde des archives

Les archives sont périodiquement sauvegardées sous forme électronique et sont exportées sur le site de secours de l'IGC en conservant le même niveau de sécurité en matière d'intégrité et de confidentialité.

Les détails sur la procédure de sauvegarde des archives sont décrits dans la procédure de sauvegarde.

5.5.5 Exigences d'horodatage des données

Voir 6.8.

5.5.6 Système de collecte des archives

Le système de collecte des archives est uniquement interne et est détaillé dans la procédure d'archivage.

5.5.7 Procédures de récupération et de vérification des archives

Les archives, qu'elles soient au format papier ou électronique, peuvent être récupérées dans un délai inférieur à 2 jours ouvrés suite à l'acceptation par l'AC de la demande de récupération de l'archive.

Les détails sur les procédures de récupération et de vérification des archives sont décrits dans la procédure d'archivage.

5.6 Changement de clé d'AC

L'AC ne peut pas générer de Certificat dont la date de fin serait postérieure à la date d'expiration de son certificat. Pour cela la période de validité du certificat de l'AC doit toujours être supérieure à celle des Certificats qu'elle délivre. C'est pourquoi, la bi-clé de l'AC est renouvelée au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats émis. Les Certificats délivrés par l'AC ayant une durée de validité de 3 ans, la bi-clé de l'AC sera par conséquent renouvelé au plus tard 3 ans et 1 mois avant la date d'expiration du certificat d'AC.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle Clé Privée doit être utilisée pour signer des Certificats. Le Certificat précédent reste utilisable pour valider les Certificats émis sous cette clé et ce au moins jusqu'à ce que tous les Certificats signés avec la Clé Privée correspondante aient expiré.

D'autre part, le LPCSP Board se charge de changer la bi-clé de l'AC et le Certificat correspondant dès que les algorithmes cryptographiques utilisés dans la bi-clé ou le Certificat cessent d'être conformes aux recommandations de sécurité cryptographique concernant la taille des clés ou les algorithmes de calculs d'empreintes.

5.7 Reprise suite à la compromission et sinistre

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

L'AC met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements.

L'AC a mis en place un Plan de Continuité d'Activité (PCA) qui décrit la procédure à exécuter en cas d'incident majeur impactant le bon fonctionnement de l'AC et plus particulièrement ses mécanismes de publication de l'état de révocation des Certificats qu'elle délivre.

Un incident majeur tel que la perte, la suspicion de compromission, la compromission ou encore le vol de la clé privée de l'AC, est immédiatement notifié au LPCSP Board qui peut alors décider, si cela est nécessaire, de demander la révocation du certificat de l'AC. Dans ce cas il devra notifier dans les plus brefs délais, et au maximum dans les 24 heures, le point de contact identifié sur le site <https://www.ssi.gouv.fr>.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou les Sujets devient insuffisant pour son utilisation prévue restante, alors l'AC doit publier l'information sur son site Web et révoquer tout Certificat concerné.

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

Le PCA définit notamment les procédures de reprise en cas de corruption des ressources informatiques ainsi que les procédures visant à assurer le maintien des services de révocation et de publication de l'état de révocation des certificats qu'elle délivre.

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

Si la Clé Privée de l'AC est compromise, soupçonnée d'être compromise, perdue ou détruite :

- Le LPCSP Board, après enquête, demande la révocation du certificat de l'AC ;
- La procédure de révocation de l'AC est appliquée ;
- Les Sujets ayant un Certificat en cours de validité et les autres entités avec lesquels l'AC a passé des accords ou d'autres formes de relations établies sont notifiés dans les plus brefs délais de la révocation de l'AC ;
- L'AC indique sur son site de publication que les Certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables ;
- Après avoir corrigé les problèmes qui ont pu causer la révocation du certificat de l'AC, l'AC peut décider de générer une nouvelle bi-clé et un nouveau certificat d'AC.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Le Plan de Continuité d'Activité mis en œuvre par l'AC permet d'assurer la continuité d'activité suite à un sinistre.

5.8 Fin de vie de l'AC

En cas de cessation définitive de l'activité de l'AC, la procédure de fin de vie de l'AC est appliquée.

L'AC procède aux actions suivantes :

- La notification de l'ANSSI et des entités affectées ;
- Le transfert de ses obligations à d'autres parties ;
- La gestion du statut de révocation pour les Certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'AC :

- Révoque tous les Certificats qu'elle a signés et qui seraient encore en cours de validité ;
- Publie une nouvelle CRL ;
- Prend toutes les mesures pour détruire sa Bi-clé et les éventuelles copies de secours ;
- Informe (par exemple par récépissé) tous les Sujets des Certificats révoqués ou à révoquer, ainsi que leur Entité Légale de rattachement le cas échéant ;

- Applique les dispositions qui ont été prises pour transférer les obligations de l'AC afin d'assurer les services suivants :
 - La publication de l'état de révocation des Certificats qu'elle a délivré ;
 - L'archivage des données (cf. section 5.5).

Ce plan est vérifié et maintenu à jour régulièrement.

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'AC

La génération de la bi-clé de l'AC est effectuée dans le cadre d'une cérémonie des clés par au moins 2 personnes ayant des rôles de confiance et en présence d'un huissier de justice. La cérémonie se déroule dans les locaux sécurisés hébergeant l'IGC (cf. section 5.1).

La bi-clé de l'AC est générée dans un HSM satisfaisant aux exigences de la section 6.2.11.

6.1.1.2 Clés d'un Sujet

La génération de la bi-Clé d'un Sujet est réalisée dans un dispositif satisfaisant aux exigences définies dans la section 6.2.11.

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet. La Clé Privée d'un Sujet n'est pas générée par l'AC.

6.1.3 Transmission de la clé publique à l'AC

La Clé Publique d'un Sujet est transmise à l'AC dans une requête de certificat au format PKCS#10 tel que décrit dans la section 3.2.1.

6.1.4 Transmission de la clé publique de l'AC aux UC

La Clé Publique de l'AC est publiée sur le site de publication de l'AC (cf. section 2.1) dans un certificat au format X.509 v3.

L'AC publie également l'empreinte de hachage de son certificat, afin que les UC puissent la comparer avec celle du certificat dont ils disposent.

6.1.5 Tailles des clés

Clé de l'AC : RSA (4096 bits ou supérieur).

Clés des Sujets : RSA (2048 bits ou supérieur) ou ECDSA (P-256 bits ou supérieur).

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

Le LPCSP Board consulte fréquemment les normes et recommandations internationales qui concernent les algorithmes cryptographiques et les longueurs de clés afin de déterminer si les algorithmes utilisés pour les bi-clés et les Certificats sont adaptés.

Les bi-clés de l'AC sont générées dans des dispositifs cryptographiques certifiés avec un paramétrage respectant les normes de sécurité en la matière.

Les bi-clés des Sujets, pour les Certificats de cachetage et d'horodatage ETSI, sont générées dans des dispositifs cryptographiques certifiés avec un paramétrage respectant les normes de sécurité en la matière.

6.1.7 Objectifs d'usage de la clé

Voir l'extension « Key Usage » dans la section 7.

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

6.2.1 Standards et mesures de sécurité pour les dispositifs cryptographiques

Les dispositifs cryptographiques utilisés pour la génération et la mise en œuvre des bi-clés de l'AC et des répondeurs OCSP sont des HSM certifiés satisfaisant aux exigences définies dans la section 6.2.11.

Les HSM de l'AC sont hébergés dans les sites sécurisées de l'IGC et sont gérés exclusivement par les personnes ayant les rôles de confiance requis.

6.2.2 Contrôle de la Clé Privée

6.2.2.1 Clé Privée de l'AC

L'activation de la Clé Privée de l'AC est réalisée par plusieurs porteurs de parts de secret qui ont nécessairement participé à la cérémonie des clés de l'AC et au cours de laquelle leur part de secret leur avait été remise dans une carte à puce personnelle et protégée par un code PIN qu'ils avaient eux-mêmes choisis.

6.2.2.2 Clé Privée du Sujet

La Clé Privée d'un Sujet est protégée par des données d'activation demeurant sous son contrôle exclusif afin que lui seul soit en mesure d'activer sa Clé Privée pour l'utiliser.

6.2.3 Séquestre de la Clé Privée

Les Clés Privées d'AC et des Sujets ne font pas l'objet de séquestre.

6.2.4 Copie de secours de la Clé Privée

La Clé Privée de l'AC est sauvegardée dans le but d'avoir des copies de secours. Elle peut être sauvegardée :

- Soit hors d'un dispositif cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du dispositif cryptographique et, notamment, s'appuyer 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.
- Soit dans un dispositif cryptographique équivalent, opéré dans des conditions de sécurité similaires ou supérieures.

Les sauvegardes sont réalisées sous le contrôle d'au moins deux personnes ayant les rôles de confiance adéquats dans l'AC.

6.2.5 Archivage de la Clé Privée

Les Clés Privées ne sont pas archivées.

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

La Clé Privée de l'AC est transférée uniquement lors de la génération des copies de secours de la Clé Privée tel que décrit dans la section 6.2.4.

La création d'une copie de secours ou son import dans un HSM sont réalisés dans les locaux sécurisés de l'IGC par au moins deux personnes ayant les rôles de confiance adéquats dans l'AC.

6.2.7 Stockage de la clé privée dans un dispositif cryptographique

Le stockage des Clés Privées est réalisé dans un dispositif cryptographique satisfaisant aux exigences définies dans la section 6.2.11 ou en dehors d'un dispositif cryptographique moyennant le respect des exigences définies à la section 6.2.4, sauf en ce qui concerne les Clés Privées des Certificats d'horodatage logiciel, qui peuvent être stockées dans un fichier PKCS#12.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clé privée d'AC

L'activation de la Clé Privée de l'AC est réalisée dans le dispositif cryptographique de l'AC par au moins deux personnes ayant les rôles de confiance adéquats.

6.2.8.2 Clé privée d'un Sujet

L'activation de la Clé Privée d'un Sujet est réalisée par le Sujet avec les données d'activation qui protège sa Clé Privée.

6.2.9 Méthode de désactivation de la Clé Privée

La désactivation de la Clé Privée de l'AC dans le dispositif cryptographique s'opère automatiquement lors de l'arrêt du dispositif cryptographique.

6.2.10 Méthode de destruction d'une Clé Privée

La destruction de la Clé Privée de l'AC ne peut être effectuée qu'à partir du dispositif cryptographique. En cas de destruction, l'AC s'assure que toutes les copies de secours de la Clé Privée de l'AC sont également détruites.

6.2.11 Niveau de qualification des dispositifs cryptographiques

6.2.11.1 AC

Le dispositif cryptographique de l'AC et des bi-clés des répondeurs OCSP est un HSM certifié FIPS 140-2 level 3 ou équivalent.

6.2.11.2 Sujet

Pour les Certificats de cachetage et d'horodatage ETSI, le dispositif cryptographique des Sujets doit être un dispositif cryptographique certifié FIPS 140-2 level 2 ou équivalent.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les Certificats contenant les Clés Publiques de l'AC sont archivés conformément à la section 5.5.

6.3.2 Durées de vie des bi-clés et des Certificats

Les bi-clés et les Certificats de l'AC ont une durée de vie maximale de 10 ans.

Les bi-clés et les Certificats des répondeurs OCSP ont une durée de vie maximale de 1 an.

Les bi-clés et les Certificats des Sujets ont une durée de vie maximale de 3 ans.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

La génération et l'installation des données d'activation de la Clé Privée de l'AC sont réalisées lors de la cérémonie des clés, en présence d'un huissier de justice. Ces données d'activation sont stockées sur des cartes à puce associées au dispositif cryptographique de l'AC et sont remises en main propre, durant la cérémonie, à chacune des personnes ayant le rôle de confiance de Key Holder. Ces personnes doivent prendre les mesures nécessaires pour se prémunir contre la perte, le vol et l'utilisation non autorisée de leurs cartes à puce et des données d'activation qu'elles contiennent.

6.4.2 Protection des données d'activation

Les données d'activation correspondant à la Clé Privée de l'AC sont générées durant la cérémonie des clés par le HSM de l'AC et sont stockées sur des cartes à puce nominatives et personnelles remises en main propre aux personnes ayant le rôle de Key Holder. Chacune de ces personnes est responsable de sa carte à puce protégée par un code PIN qu'elle a spécifiée lors de la cérémonie des clés. Elle a de plus signé une attestation de remise de sa carte à puce.

6.4.3 Autres aspects liés aux données d'activation

La destruction des données d'activation est réalisée par la destruction physique de la carte à puce les contenant ou par leur effacement définitif et irréversible.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

LEX PERSONA définit les objectifs de sécurité suivants :

- Identification et authentification forte des utilisateurs pour l'accès aux systèmes ;
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôle multiple et de séparation des rôles) ;
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- Protection contre toute tentative non autorisée et / ou irrégulière d'accès aux ressources (physique et / ou logique) ;
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent.

6.5.2 Niveau de qualification des systèmes informatiques

Pas d'exigence.

6.6 Mesures de sécurité liées au développement des systèmes

6.6.1 Mesures de sécurité liées au développement des systèmes

Tous les développements réalisés par LEX PERSONA et impactant l'IGC sont documentés et réalisés via un processus de manière à en assurer la qualité.

La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau est documentée et contrôlée.

LEX PERSONA opère un cloisonnement entre l'environnement de développement et les environnements de pré-production et de production.

6.6.2 Mesures liées à la gestion de la sécurité

Les configurations et les mises à jour des applications sont effectuées de manière sécurisée par le personnel compétent apparaissant dans les rôles de confiance de l'AC.

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

Sans objet.

6.7 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC. De plus les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé.

6.8 Horodatage / Système de datation

Les différents serveurs utilisés par l'AC sont synchronisés au moins une fois par jour avec la même source de temps UTC.

7 Profils des Certificats, OCSP et des LCR

7.1 Certificat de l'AC

Le certificat de l'AC est un certificat au format X.509 v3 conforme aux exigences de la [RFC 5280] et qui respecte le profil [EN 319 412-1].

Champs de base :

Champ	Valeur
Version	2 (correspond à la v3 de X.509)
Numéro de série	Défini lors de la création
Emetteur	CN = Sunnystamp Root CA G2 OI = NTRFR-480622257 OU=0002 480622257 O = LEX PERSONA C = FR
Sujet	CN = Sunnystamp Legal Persons CA OI = NTRFR-480622257 OU = 0002 480622257 O = LEX PERSONA C = FR
Validité	10 ans maximum
Signature	RSAwithSHA512
Clé publique	RSA 4096 bits

Extensions :

Champ	Critique	Valeur
AuthorityInfoAccess	Non	id-ad-caIssuers=

		https://pki2.sunnystamp.com/certs/sunnystamp-root-ca-g2.cer
AuthorityKeyIdentifier	Non	
BasicConstraints	Oui	CA=true pathLenConstraint=0
CertificatePolicies	Non	OID=2.5.29.32.0
CRLDistributionPoints	Non	http://pki2.sunnystamp.com/crls/sunnystamp-root-ca-g2.crl http://pki3.sunnystamp.com/crls/sunnystamp-root-ca-g2.crl
SubjectKeyIdentifier	Non	
Key Usage	Oui	keyCertSign(5), cRLSign(6)

7.2 Certificat d'un Sujet

Les Certificats des Sujets sont des certificats au format X.509 v3 conforme aux exigences de la [RFC 5280] et qui respectent le profil [EN 319 412-3].

Champs de base :

Champ	Valeur
Version	2 (correspond à la v3 de X.509)
Numéro de série	Défini lors de la création
Emetteur	CN = Sunnystamp Legal Persons CA OI = NTRFR-480622257 OU=0002 480622257 O = LEX PERSONA C = FR
Sujet	CN = Nom courant utilisé par le Sujet pour se représenter : une unité, un département, un service ou une filiale du Sujet C = Code du pays dans lequel le Sujet est établi O = Nom légal du Sujet OI = Identifiant unique du Sujet (structuré conformément à la section 5.1.4 de la norme [EN 319 412-1]). serialNumber = Identifiant unique généré par l'AC OU = Attribut utilisé pour préciser des informations sur le Sujet - Peut être une unité, un département, un service ou une filiale du Sujet L = Attribut utilisé pour désigner la Ville dans laquelle le Sujet est enregistré
Validité	3 ans maximum
Signature	RSAwithSHA256

Clé publique	RSA 2048 bits
--------------	---------------

Extensions pour les Certificats de cachetage :

Champ	Critique	Valeur
AuthorityInfoAccess	Non	id-ad-calssuers= https://pki2.sunnystamp.com/certs/sunnystamp-legal-persons-ca.cer id-ad-ocsp= http://ocsp2.sunnystamp.com/sunnystamp-legal-persons-ca
AuthorityKeyIdentifier	Non	
BasicConstraints	Oui	CA=false
CertificatePolicies	Non	OID=0.4.0.2042.1.2 OID=1.3.6.1.4.1.22542.100.1.1.2.1 URL= https://pki2.sunnystamp.com/repository
CRLDistributionPoints	Non	http://pki2.sunnystamp.com/crls/sunnystamp-legal-persons-ca.crl http://pki3.sunnystamp.com/crls/sunnystamp-legal-persons-ca.crl
Key Usage	Oui	digitalSignature
SubjectKeyIdentifier	Non	

Extensions pour les Certificats d'horodatage ETSI :

Champ	Critique	Valeur
AuthorityInfoAccess	Non	id-ad-calssuers= https://pki2.sunnystamp.com/certs/sunnystamp-legal-persons-ca.cer id-ad-ocsp= http://ocsp2.sunnystamp.com/sunnystamp-legal-persons-ca
AuthorityKeyIdentifier	Non	
BasicConstraints	Oui	cA=false
CertificatePolicies	Non	OID=0.4.0.2042.1.2 OID=1.3.6.1.4.1.22542.100.1.1.2.2 URL= https://pki2.sunnystamp.com/repository
CRLDistributionPoints	Non	http://pki2.sunnystamp.com/crls/sunnystamp-legal-persons-ca.crl http://pki3.sunnystamp.com/crls/sunnystamp-legal-persons-ca.crl

ExtendedKeyUsage	Oui	id-kp-timeStamping
Key Usage	Oui	digitalSignature
SubjectKeyIdentifier	Non	

Extensions pour les Certificats d'horodatage logiciel :

Champ	Critique	Valeur
AuthorityInfoAccess	Non	id-ad-caIssuers= https://pki2.sunnystamp.com/certs/sunnystamp-legal-persons-ca.cer id-ad-ocsp= http://ocsp2.sunnystamp.com/sunnystamp-legal-persons-ca
AuthorityKeyIdentifier	Non	
BasicConstraints	Oui	cA=false
CertificatePolicies	Non	OID=1.3.6.1.4.1.22542.100.1.1.2.3 URL= https://pki2.sunnystamp.com/repository
CRLDistributionPoints	Non	http://pki2.sunnystamp.com/crls/sunnystamp-legal-persons-ca.crl http://pki3.sunnystamp.com/crls/sunnystamp-legal-persons-ca.crl
ExtendedKeyUsage	Oui	id-kp-timeStamping
Key Usage	Oui	digitalSignature
SubjectKeyIdentifier	Non	

7.3 Profil des LCR

Champs de base :

Champ	Valeur
Version	1
Emetteur	CN = Sunnystamp Legal Persons CA OI = NTRFR-480622257 OU=0002 480622257 O = LEX PERSONA C = FR
Validité	7 jours
Signature	RSAwithSHA512

Extensions :

Champ	Critique	Valeur
AuthorityKeyIdentifier	Non	
CRLNumber	Non	Défini par l'AC

7.4 Profil OCSP

Le répondeur OCSP de l'AC est conforme à la [RFC 6960].

Les certificats utilisés par le répondeur OCSP pour signer les réponses OCSP sont délivrés par l'AC. Ils sont conformes aux exigences de la [RFC 5280].

Champs de base :

Champ	Valeur
Version	2 (correspond à la v3 de X.509)
Numéro de série	Défini lors de la création
Emetteur	CN = Sunnystamp Legal Persons CA OI = NTRFR-480622257 OU=0002 480622257 O = LEX PERSONA C = FR
Sujet	CN = OCSP Responder \$X (où X est un nombre entier) serialNumber = Identifiant unique généré par l'AC OI = NTRFR-480622257 OU = 0002 480622257 O = LEX PERSONA C = FR
Validité	1 an maximum
Signature	RSAwithSHA256
Clé publique	RSA 2048 bits

Extensions :

Champ	Critique	Valeur
AuthorityKeyIdentifier	Non	
BasicConstraints	Oui	cA=false

ExtendedKeyUsage	Oui	id-kp-OCSPSigning
id-pkix-ocsp-nocheck	Non	NULL
Key Usage	Oui	digitalSignature
SubjectKeyIdentifier	Non	

8 Audit de conformité et autres évaluations

8.1 Fréquences et / ou circonstances des évaluations

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC fait procéder à un audit de conformité de cette composante à la présente PC/DPC.

L'AC réalise des audits internes au moins une fois chaque année et fait réaliser tous les 2 ans, par un organisme accrédité, un audit de certification [EN 319 411-1] pour les Certificats de cachetage et d'horodatage ETSI.

8.2 Identités / qualifications des évaluateurs

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

8.3 Relations entre évaluateurs et entités évaluées

Pour les audits internes, l'auditeur sera nommé par le LPCSP Board et pourra appartenir à LEX PERSONA mais devra nécessairement être indépendant de l'AC.

Pour l'audit de certification, l'auditeur ne devra pas appartenir à LEX PERSONA ou présenter un quelconque conflit d'intérêt.

8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la présente PC/DPC et dans les procédures internes associées.

8.5 Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : « réussite », « échec », « à confirmer ».

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être :

- La cessation (temporaire ou définitive) d'activité,
 - La révocation du Certificat de la composante,
 - La révocation de l'ensemble des Certificats émis depuis le dernier contrôle positif.
- Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.
 - En cas de résultat « à confirmer », l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées.
 - Puis un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
 - En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la présente PC/DPC et des procédures internes.

8.6 Communication des résultats

Les résultats de l'audit de l'AC sont tenus à la disposition de l'organisme de certification en charge de l'AC.

9 Autres problématiques métiers et légales

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de Certificats

L'AC peut appliquer un tarif sur la délivrance de Certificats.

9.1.2 Tarifs pour accéder aux Certificats

Les Certificats de la chaîne de confiance incluant le certificat de l'AC sont mis à disposition des UC gratuitement via le site de publication de l'AC.

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

L'accès aux informations d'état de révocation des Certificats, délivrés par l'AC à travers les LCR qu'elle publie et les réponses OCSP qu'elle produit, est gratuit.

9.1.4 Tarifs pour d'autres services

Sans objet.

9.1.5 Politique de remboursement

Sans objet.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

LEX PERSONA a souscrit une assurance en responsabilité civile professionnelle couvrant ses prestations de PSCE auprès d'une compagnie d'assurance.

9.2.2 Autres ressources

LEX PERSONA dispose des ressources financières suffisantes pour assurer sa mission conformément à cette PC/DPC.

9.2.3 Couvertures et garantie concernant les entités utilisatrices

En cas de dommage subi par une entité intervenant dans l'IGC, et sous contrat avec l'AC, du fait d'un manquement par l'AC à ses obligations, l'AC pourra être amenée à dédommager l'entité dans la limite de la responsabilité de l'AC définie dans le contrat établi entre l'AC et l'entité.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- Les procédures internes de l'AC ;
- Les Clés Privées de l'AC et des composantes de l'IGC ;
- Les données d'activation associées aux Clés Privées d'AC ;
- Les dossiers d'enregistrement des Sujets ;
- Les journaux d'événements des composantes de l'IGC ;
- Les causes de révocation des Certificats ;
- Les rapports d'audit ;
- Tous les secrets de l'IGC.

D'autres informations peuvent être classées comme confidentielles.

9.3.2 Informations hors du périmètre des informations confidentielles

Toutes les informations publiées par l'AC (cf. section 2.2) ne sont pas considérées comme confidentielles.

9.3.3 Responsabilités en termes de protection des informations confidentielles

LEX PERSONA s'engage à traiter les informations confidentielles dans le respect de la législation et de la réglementation en vigueur sur le territoire français.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

LEX PERSONA s'engage à collecter et utiliser les données personnelles en respectant la législation et la réglementation européenne en vigueur relative à la protection des données à caractère personnel.

9.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont les suivantes :

- Les causes de révocation des Certificats des Sujets ;
- Les données d'enregistrement des Sujets qui n'apparaissent pas dans les Certificats.

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données personnelles

LEX PERSONA respecte, pour le traitement et la protection des données à caractère personnel, la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et modifications à venir ainsi que le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

9.4.5 Notification et consentement d'utilisation des données personnelles

Les données personnelles ne sont jamais utilisées, sans le consentement exprès et préalable du Sujet, à d'autres fins que celles définies :

- Dans la présente PC/DPC ;
- Dans l'Accord de Souscription ;
- Dans un accord formel entre l'AC et le Souscripteur s'il existe.

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

Les données personnelles peuvent être mis à la disposition de la justice en cas de besoin pour servir de preuve dans le cadre d'une procédure judiciaire.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par l'AC sont protégés par la loi, règlement et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerces et de services, dessins et modèles, signes distinctifs et droits d'auteur est sanctionnée par le Code de la propriété intellectuelle.

L'AC détient tous les droits de propriété intellectuelle et est propriétaire de la présente PC/DPC et des certificats émis par l'AC. Le Sujet détient tous les droits de propriété intellectuelle sur les informations personnelles contenues dans son Certificat et dont il est propriétaire.

L'Entité Légale du Sujet détient, le cas échéant, tous les droits de propriété intellectuelle sur les informations de l'Entité Légale contenues dans le certificat du Sujet et dont elle est propriétaire.

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 présente PC/DPC et les documents qui en découlent ;
- Respecter et appliquer les procédures internes ;
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. section 8) et l'organisme de qualification ;
- Respecter les accords ou contrats qui les lient entre elles ou aux Sujets ;
- 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 LPCSP Board

Les obligations du LPCSP Board sont les suivantes :

- L'approbation de la présente PC/DPC et de ses évolutions ;
- L'audit de l'AC ;
- La gestion de la relation contractuelle avec les entités intervenant dans l'IGC.

9.6.2 AC

L'AC est LEX PERSONA.

Ses obligations consistent à :

- S'assurer du respect des exigences qui la concernent et qui sont décrites dans la présente PC/DPC ;
- Rédiger les procédures internes et les guides nécessaires aux personnels de confiance de l'AC en vue de l'accomplissement de leur mission ;
- Mettre en œuvre les ressources techniques, humaines et organisationnelles pour effectuer les prestations qui lui incombent et qui sont décrites dans la présente PC/ DPC ;

- Vérifier le respect par les différentes composantes de l'IGC, des principes de sécurité et des contrôles afférents ;
- Assurer la conformité des Certificats qu'elle délivre vis-à-vis de la présente PC/DPC.

L'AC est responsable vis-à-vis des Souscripteurs et des UC si :

- Les informations d'un Sujet présentes dans un Certificat ne correspondent pas à celles transmises par le Souscripteur à l'AE ;
- L'AC n'a pas procédé à la révocation d'un Certificat, consécutivement à une demande de révocation d'un Certificat, ou n'a pas publié cette information conformément aux engagements précisés dans la présente PC/DPC.

9.6.3 Autorité d'Enregistrement

L'AE est LEX PERSONA.

Les obligations de l'AE sont les suivantes :

- Mettre en œuvre les moyens décrits dans la présente PC/DPC relatifs à ses obligations ;
- Définir les procédures d'enregistrement des Sujets ;
- Vérifier avec un soin raisonnable l'apparence de conformité et la cohérence des pièces justificatives ainsi que l'exactitude des mentions qui établissent l'identité du Sujet ;
- Vérifier l'origine et l'exactitude de toute demande de révocation et mettre en œuvre les moyens permettant de les traiter ;
- Avertir l'AC en cas d'incident.

9.6.4 RCPS et Souscripteur

Les obligations du Sujet et du Souscripteur sont mentionnées dans l'accord de Souscription qui comprend deux parties :

- La première partie est relative aux obligations du Souscripteur ;
- La deuxième partie est relative aux obligations du RCPS (qui est la personne physique représentant le Sujet).

La première partie mentionne :

- Le respect des obligations de l'accord qui concernent le Souscripteur ;
- Le respect des exigences indiquées dans la présente PC/DPC qui concernent le Souscripteur ;
- Le respect des conditions relatives à la publication du Certificat ;
- Dans le cas d'un Certificat de cachetage ou d'horodatage ETSI, l'accord relatif à l'utilisation d'un dispositif cryptographique satisfaisant aux exigences de la section 6.2.11 ;
- Le consentement simultané :

- De la conservation par l'AC des informations d'enregistrement, de la fourniture du dispositif au RCPS, et de toute révocation ultérieure ainsi que de l'identité et des attributs spécifiques du Certificat ;
- Du transfert de ces informations à des tiers aux mêmes conditions que celles définies dans la présente PC/DPC, en cas de fin de vie de l'AC ;
- Si et sous quelles conditions le Souscripteur demande et le Sujet consent à la publication du Certificat ;
- La confirmation que l'information contenue dans le Certificat est correcte ;
- Les obligations applicables au RCPS situées dans la deuxième partie.

La deuxième partie mentionne :

- Le respect des obligations de l'accord qui concernent le RCPS ;
- Le respect des exigences indiquées dans la présente PC/DPC qui concernent le RCPS ;
- Dans le cas d'un Certificat de cachetage ou d'horodatage ETSI, l'accord relatif à l'utilisation d'un dispositif cryptographique satisfaisant aux exigences de la section 6.2.11 ;
- Le consentement simultané :
 - De la conservation par l'AC des informations d'enregistrement, de la fourniture du dispositif au RCPS, et de toute révocation ultérieure ainsi que de l'identité et des attributs spécifiques du Certificat ;
 - Du transfert de ces informations à des tiers aux mêmes conditions que celles définies dans la présente PC/DPC, en cas de fin de vie de l'AC ;

Dans le cas où le Souscripteur et le RCPS ne sont pas la même personne, la signature de l'accord de Souscription par le Souscripteur s'applique à la première partie et la signature de l'accord de Souscription par le RCPS s'applique à la deuxième partie.

Dans le cas où le RCPS et le Souscripteur sont la même personne physique, alors la signature du RCPS/Souscripteur s'applique à la fois à la première et à la deuxième partie.

9.6.5 UC

Les obligations des UC sont les suivantes :

- Respecter les obligations décrites dans l'accord d'utilisation des Certificats ;
- Vérifier que l'extension `KeyUsage` contenue dans le Certificat est `digitalSignature` ;
- Pour un Certificat de cachetage :
 - Vérifier que l'OID `1.3.6.1.4.1.22542.100.1.1.2.1` est contenu dans l'extension `CertificatePolicies` du Certificat ;
- Pour un certificat d'horodatage ETSI :
 - Vérifier que l'OID `1.3.6.1.4.1.22542.100.1.1.2.2` est contenu dans l'extension `CertificatePolicies` du Certificat ;

- Vérifier que l'extension `ExtendedKeyUsage` contenue dans le Certificat est `id-kp-timeStamping` ;
- Pour un certificat d'horodatage logiciel :
 - Vérifier que l'OID `1.3.6.1.4.1.22542.100.1.1.2.3` est contenu dans l'extension `CertificatePolicies` du Certificat ;
 - Vérifier que l'extension `ExtendedKeyUsage` contenue dans le Certificat est `id-kp-timeStamping` ;
- Vérifier la validité de la chaîne de certification (dates de validité, signature des Certificats, statut de révocation) en partant du Certificat du Sujet et en remontant au moins jusqu'au certificat de l'AC.

9.7 Limite de garantie

Les limites des garanties offertes par l'AC sont décrites :

- Dans l'accord de souscription pour les Souscripteurs ;
- Dans l'accord d'utilisation des Certificats pour les UC.

Ces limites sont applicables dans la limite des lois et règlements en vigueur.

9.8 Limite de responsabilité

L'AC ne pourra être tenue responsable d'une utilisation non autorisée ou non conforme à la présente PC/DPC des Clés Privées, Certificats associés, informations de révocation, ou de tout équipement ou logiciel mis à disposition dans le cadre de cette utilisation.

Egalement, l'AC ne pourra être tenue responsable pour tout dommage consécutif à des erreurs, inexactitudes ou omissions entachant les informations contenues dans les certificats, dès lors que ces erreurs, inexactitudes ou omissions résultent du caractère erroné des informations communiquées par le Souscripteur.

Enfin, l'AC ne pourra être tenue responsable, dans la limite de la loi française, de perte financière, de perte de données ou de dommage indirect lié à l'utilisation d'un Certificat.

La responsabilité de l'AC sera strictement limitée, quelles que soient les causes, et quels que soient les faits générateurs, et quels que soient les préjudices causés, au montant payé à l'AC par le Souscripteur sur les 3 derniers mois et ce dans le respect et les limites de la loi applicable. Sauf prescription légale contraire, toute action du Souscripteur au titre des présentes devra intervenir au plus tard dans un délai de 3 mois à compter de la survenance du fait générateur fondant l'action.

9.9 Indemnités

Sans objet.

9.10 Durée et fin anticipée de validité de la PC/DPC

9.10.1 Durée de validité

La présente PC/DPC reste en application au moins jusqu'à la fin de vie du dernier Certificat émis par l'AC.

9.10.2 Fin anticipée de validité

La présente PC/DPC reste en application 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 la présente PC/DPC, les intervenants dans l'IGC restent liés par la présente PC/DPC pour tous les Certificats émis lorsqu'elle était encore valide, jusqu'à l'expiration du dernier Certificat non révoqué.

9.11 Notification individuelles et communications entre les participants

Le LPCSP Board publie une nouvelle version de la présente PC/DPC sur le site de publication de l'AC après l'avoir validé.

9.12 Amendements

9.12.1 Procédures d'amendements

Le LPCSP Board est responsable de la création, l'approbation, la maintenance et la modification de la présente PC/DPC.

Seuls les changements mineurs dans la présente PC/DPC tels que la correction de fautes d'orthographe ou d'erreurs ne remettant pas en cause le sens de la présente PC/DPC peuvent être réalisés par le LPCSP Board sans nécessiter de notification.

9.12.2 Mécanisme et période d'information sur les amendements

Lors de tout changement important impactant la présente PC/DPC, le LPCSP Board informera les acteurs au travers d'un communiqué distribué par voie électronique ou sur son site Internet. Si besoin, une communication par courrier postal pourra être réalisée.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

Si le LPCSP Board juge qu'un changement important dans la présente PC/DPC est nécessaire et qu'il a un impact majeur sur les Certificats déjà émis, il devra publier une nouvelle version de la PC/DPC intégrant un nouvel OID.

9.13 Dispositions concernant la résolution de conflits

La présente PC/DPC est soumise au droit français.

L'AC met en place une procédure de gestion des incidents pour le règlement des différends.

Lorsqu'un conflit porte sur l'identité d'un Sujet, l'AE est responsable de la gestion et de la résolution du litige.

9.14 Juridictions compétentes

L'ensemble des documents contractuels est soumis à la législation et à la réglementation en vigueur sur le territoire français.

9.15 Conformité aux législations et réglementations

La présente PC/DPC est conforme à la législation et à la réglementation en vigueur sur le territoire 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 Conséquences d'une clause non valide

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

LEX PERSONA s'assure que les activités qu'elle réalise dans le cadre de cette PC/DPC sont non discriminatoires.

10 Références

[EN 319 411-1]

ETSI EN 319 411-1 V1.2.2 (2018-04)

Policy and security requirements for Trust Service Providers issuing certificates

Part 1 : General requirements

[EN 319 412-1]

ETSI EN 319 412-1 V1.1.1 (2016-02)

Certificate Profiles

Part 1: Overview and common data structures

[EN 319 412-3]

ETSI EN 319 412-3 V1.1.1 (2016-02)

Certificate Profiles

Part 2: Certificate profile for certificates issued to legal persons

[PC_RG2]

Politique de Certification de l'Autorité de Certification "Sunnystamp Root CA G2"

<https://pki2.sunnystamp.com/repository>

[PKCS#10]

PKCS #10 : Certification Request Syntax Specification Version 1.7

November 2000

<https://tools.ietf.org/html/rfc2986>

[RFC 3647]

Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

November 2003

<https://tools.ietf.org/html/rfc3647>

[RFC 5280]

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

May 2008

<https://tools.ietf.org/html/rfc5280>

[RFC 6960]

Online Certificate Status Protocol – OCSP

June 2013

<https://tools.ietf.org/html/rfc6960>

[FR_Revocation]

Formulaire PDF de révocation de Certificat

<https://pki2.sunnystamp.com/repository>