Sunnystamp PKI

Sunnystamp Natural Persons CA

Politique de Certification / Déclaration des Pratiques de Certification

Version 1.2

Technopole de l'Aube en Champagne – CS 90601 – 10901 Troyes Cedex 9
Tél. : +33 (0)3 25 43 90 78 – Fax : +33 (0)9 81 40 30 08 – www.lex-persona.com
SARL au capital de 30 000 Euros – R.C.S. Troyes 480 622 257 – Code NAF 6202A – TVA FR01480622257

Sunnystamp PKI

Sunnystamp Natural Persons CA

Politique de Certification /

Déclaration des Pratiques de Certification

Version 1.2

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) 10
1.3.3 Autorité d'Enregistrement (AE) 10
1.3.4 Sujet 10
1.3.5 Souscripteur 10
1.3.6 Utilisateur de Certificat (UC) 10
1.4 Usage des Certificats 11
1.4.1 Domaines d'utilisation applicables 11
1.4.2 Domaines d'utilisation interdits 11
1.5 Gestion de la PC 11
1.5.1 Entité gérant la PC 11
1.5.2 Entité déterminant la conformité de la PC/DPC 11
1.5.3 Procédure d'approbation de la conformité de la PC/DPC 11
1.6 Définitions et Acronymes 11
1.6.1 Définitions 11
1.6.2 Acronymes 13
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 14
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 17
3.1.5 Unicité des noms 17
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 d'un 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 18
3.3 Identification et validation d'une demande de renouvellement des clés 18
3.3.1 Identification et validation d'un renouvellement courant 18
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 20
4.3 Délivrance du Certificat 20
4.3.1 Actions de l'AC concernant la délivrance du Certificat 20
4.3.2 Notification par l'AC de la délivrance du Certificat au Sujet 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
4.6.1 Causes possibles de renouvellement d'un Certificat 22
4.6.2 Origine d'une demande de renouvellement 22
4.6.3 Procédure de traitement d'une demande de renouvellement 22
4.6.4 Notification au Sujet de l'établissement du nouveau Certificat 22
4.6.5 Démarche d'acceptation du nouveau Certificat 22
4.6.6 Publication du nouveau Certificat 22
4.6.7 Notification par l'AC aux autres entités de la délivrance du nouveau Certificat 22
4.7 Délivrance d'un nouveau Certificat suite au changement de la bi-clé 22
4.7.1 Causes possibles de changement d'une bi-clé 23
4.7.2 Origine d'une demande d'un nouveau Certificat 23
4.7.3 Procédure de traitement d'une demande d'un nouveau Certificat 23
4.7.4 Notification au Sujet de l'établissement du nouveau Certificat 23
4.7.5 Démarche d'acceptation du nouveau Certificat 23

4.7.6 Publication du nouveau Certificat 23
4.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau Certificat 23
4.8 Modification du Certificat 23
4.8.1 Causes possibles de modification d'un Certificat 23
4.8.2 Origine d'une demande de modification d'un Certificat 23
4.8.3 Procédure de traitement d'une demande de modification d'un Certificat 23
4.8.4 Notification au Sujet de l'établissement du Certificat modifié 23
4.8.5 Démarche d'acceptation du Certificat modifié 23
4.8.6 Publication du Certificat modifié 23
4.8.7 Notification par l'AC aux autres entités de la délivrance du Certificat modifié 24
4.9 Révocation et suspension des Certificats 24
4.9.1 Causes possibles d'une révocation 24
4.9.2 Origine d'une demande de révocation 24
4.9.3 Procédure de traitement d'une demande de révocation 25
4.9.4 Délai accordé au demandeur pour formuler la demande de révocation 25
4.9.5 Délai de traitement par l'AC d'une demande de révocation 26
4.9.6 Exigences de vérification de la révocation par les UC 26
4.9.7 Fréquence d'établissement des LCR 26
4.9.8 Délai maximum de publication d'une LCR 26
4.9.9 Disponibilité d'un système de vérification en ligne de l'état des Certificats 26
4.9.10 Exigences de vérification en ligne du statut de révocation des Certificats par les UC 26
4.9.11 Autres moyens disponibles d'information sur les révocations 26
4.9.12 Exigences spécifiques en cas de compromission de la Clé Privée 26
4.9.13 Causes possibles d'une suspension 27
4.9.14 Origine d'une demande de suspension 27
4.9.15 Procédure de traitement d'une demande de suspension 27
4.9.16 Limites de la période de suspension d'un Certificat 27
4.10 Fonction d'information sur l'état des Certificats 27
4.10.1 Caractéristiques opérationnelles 27
4.10.2 Disponibilité de la fonction 27
4.10.3 Dispositifs optionnels 27
4.11 Fin de la relation entre le Souscripteur et l'AC 27
4.12 Séquestre de clé et recouvrement 27
4.12.1 Politique et pratiques de recouvrement par séquestre des clés 27
4.12.2 Politique et pratiques de recouvrement par encapsulation des clés de session 27
5 Mesures de sécurité non techniques 28
5.1 Mesures de sécurité physique 28
5.1.1 Situation géographique et construction des sites 28
5.1.2 Accès physique 28
5.1.3 Alimentation électrique et climatisation 28
5.1.4 Vulnérabilité aux dégâts des eaux 28
5.1.5 Prévention et protection incendie 28
5.1.6 Conservation des supports 28
5.1.7 Mise hors service des supports 29
5.1.8 Sauvegardes hors site 29
5.2 Mesures de sécurité procédurales 29

5.2.1 Rôles de confiance 29
5.2.2 Nombre de personnes requises par tâche 30
5.2.3 Identification et authentification pour chaque rôle....30
5.2.4 Rôles exigeant une séparation des attributions....30
5.3 Mesures de sécurité vis-à-vis du personnel 30
5.3.1 Qualifications, compétences et habilitations requises....30
5.3.2 Procédures de vérification des antécédents....31
5.3.3 Exigences en matière de formation initiale 31
5.3.4 Exigences et fréquence en matière de formation continue 31
5.3.5 Fréquence et séquence de rotation entre différentes attributions....31
5.3.6 Sanctions en cas d'actions non autorisées....31
5.3.7 Exigences vis-à-vis du personnel des prestataires externes 31
5.3.8 Documentation fournie au personnel....32
5.4 Procédure de constitution des données d'audit 32
5.4.1 Type d'évènements à enregistrer 32
5.4.2 Fréquence de traitement des journaux d'évènements....32
5.4.3 Période de conservation des journaux d'évènements 32
5.4.4 Protection des journaux d'évènements....32
5.4.5 Procédure de sauvegarde des journaux d'évènements....32
5.4.6 Système de collecte des journaux d'évènements 32
5.4.7 Notification de l'enregistrement d'un évènement au responsable de l'évènement....33
5.4.8 Évaluation des vulnérabilités 33
5.5 Archivage des données....33
5.5.1 Types de données à archiver 33
5.5.2 Période de conservation des archives 33
5.5.3 Protection des archives....34
5.5.4 Procédure de sauvegarde des archives....34
5.5.5 Exigences d'horodatage des données 34
5.5.6 Système de collecte des archives 34
5.5.7 Procédures de récupération et de vérification des archives....34
5.6 Changement de clé d'AC....34
5.7 Reprise suite à la compromission et sinistre 35
5.7.1 Procédures de remontée et de traitement des incidents et des compromissions....35
5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) 35
5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante35
5.7.4 Capacités de continuité d'activité suite à un sinistre 36
5.8 Fin de vie de l'AC....36
6 Mesures de sécurité techniques 36
6.1 Génération et installation de bi-clés....36
6.1.1 Génération des bi-clés....36
6.1.2 Transmission de la clé privée à son propriétaire 37
6.1.3 Transmission de la clé publique à l'AC 37
6.1.4 Transmission de la clé publique de l'AC aux UC....37
6.1.5 Tailles des clés....37
6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité....37
6.1.7 Objectifs d'usage de la clé 37

6.2 Mesures de sécurité pour la protection des clés privées et pour les dispositifs cryptographiques 37
6.2.1 Standards et mesures de sécurité pour les dispositifs cryptographiques 37
6.2.2 Contrôle de la Clé Privée 38
6.2.3 Séquestre de la Clé Privée 38
6.2.4 Copie de secours de la Clé Privée 38
6.2.5 Archivage de la Clé Privée 38
6.2.6 Transfert de la Clé Privée vers / depuis le dispositif cryptographique 38
6.2.7 Stockage de la Clé Privée dans un dispositif cryptographique 39
6.2.8 Méthode d'activation de la clé privée 39
6.2.9 Méthode de désactivation de la Clé Privée 39
6.2.10 Méthode de destruction d'une Clé Privée 39
6.2.11 Niveau de qualification des dispositifs cryptographiques 39
6.3 Autres aspects de la gestion des bi-clés 40
6.3.1 Archivage des clés publiques 40
6.3.2 Durées de vie des bi-clés et des Certificats 40
6.4 Données d'activation 40
6.4.1 Génération et installation des données d'activation 40
6.4.2 Protection des données d'activation 40
6.4.3 Autres aspects liés aux données d'activation 40
6.5 Mesures de sécurité des systèmes informatiques 40
6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques 40
6.5.2 Niveau de qualification des systèmes informatiques 41
6.6 Mesures de sécurité liées au développement des systèmes 41
6.6.1 Mesures de sécurité liées au développement des systèmes 41
6.6.2 Mesures liées à la gestion de la sécurité 41
6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes 41
6.7 Mesures de sécurité réseau 41
6.8 Horodatage / Système de datation 42
7 Profils des Certificats, OCSP et des LCR 42
7.1 Certificat de l'AC 42
7.2 Certificat d'un Sujet 43
7.2.1 Certificat multi-transactions 43
7.2.2 Certificat mono-transaction 44
7.3 Profil des LCR 45
7.4 Profil OCSP 46
8 Audit de conformité et autres évaluations 47
8.1 Fréquences et / ou circonstances des évaluations 47
8.2 Identités / qualifications des évaluateurs 47
8.3 Relations entre évaluateurs et entités évaluées 47
8.4 Sujets couverts par les évaluations 47
8.5 Actions prises suite aux conclusions des évaluations 47
8.6 Communication des résultats 48
9 Autres problématiques métiers et légales 48
9.1 Tarifs 48
9.1.1 Tarifs pour la fourniture ou le renouvellement de Certificats 48
9.1.2 Tarifs pour accéder aux Certificats 48

9.1.3 Tarifs pour accéder aux informations d'état et de révocation des Certificats 48
9.1.4 Tarifs pour d'autres services 48
9.1.5 Politique de remboursement 48
9.2 Responsabilité financière.....48
9.2.1 Couverture par les assurances 48
9.2.2 Autres ressources.....48
9.2.3 Couvertures et garantie concernant les entités utilisatrices 49
9.3 Confidentialité des données professionnelles.....49
9.3.1 Périmètre des informations confidentielles 49
9.3.2 Informations hors du périmètre des informations confidentielles.....49
9.3.3 Responsabilités en termes de protection des informations confidentielles 49
9.4 Protection des données personnelles 49
9.4.1 Politique de protection des données personnelles.....49
9.4.2 Informations à caractère personnel.....49
9.4.3 Informations à caractère non personnel 50
9.4.4 Responsabilité en termes de protection des données personnelles 50
9.4.5 Notification et consentement d'utilisation des données personnelles.....50
9.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives.....50
9.4.7 Autres circonstances de divulgation d'informations personnelles 50
9.5 Droits sur la propriété intellectuelle et industrielle 50
9.6 Interprétations contractuelles et garanties 50
9.6.1 LPCSP Board.....51
9.6.2 AC.....51
9.6.3 Autorité d'Enregistrement 52
9.6.4 Sujet et Souscripteur 52
9.6.5 UC.....53
9.7 Limite de garantie.....53
9.8 Limite de responsabilité.....53
9.9 Indemnités.....54
9.10 Durée et fin anticipée de validité de la PC/DPC 54
9.10.1 Durée de validité.....54
9.10.2 Fin anticipée de validité 54
9.10.3 Effets de la fin de validité et clauses restant applicables.....54
9.11 Notification individuelles et communications entre les participants.....54
9.12 Amendements.....54
9.12.1 Procédures d'amendements 54
9.12.2 Mécanisme et période d'information sur les amendements.....55
9.12.3 Circonstances selon lesquelles l'OID doit être changé.....55
9.13 Dispositions concernant la résolution de conflits 55
9.14 Juridictions compétentes 55
9.15 Conformité aux législations et réglementations.....55
9.16 Dispositions diverses 55
9.16.1 Accord global.....55
9.16.2 Transfert d'activités 55
9.16.3 Conséquences d'une clause non valide 55
9.16.4 Application et renonciation 55

9.16.5 Force majeure 55
9.17 Autres dispositions 56
10 Références 56

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 « personne physique », délivrés par une Autorité de Certification appartenant à l'Infrastructure de Gestion de Clés (IGC) Sunnystamp.

Une demande de génération de Certificat est effectuée par un Souscripteur pour une personne physique qui sera le Sujet du Certificat délivré.

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

Dans le cadre de cette PC/DPC, l'AC délivre ces 2 types de Certificats :

- Les certificats de type « mono-transaction » qui ont une durée de validité maximale de 12 heures et qui peuvent être utilisés pour signer exclusivement les documents de la transaction de signature pour laquelle ils ont été spécialement créés ;
- Les certificats de type « multi-transactions » qui ont une durée de validité maximale de 3 ans et qui peuvent être utilisé pour signer les documents de différentes transactions de signature.

Le présent document constitue la Politique de Certification et la Déclaration des Pratiques de Certification (PC/DPC) de l'AC. Il 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 LCP pour l'émission de certificats de type « mono-transaction » délivrés à des personnes physiques pouvant être rattachées ou non à une Entité Légale.

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

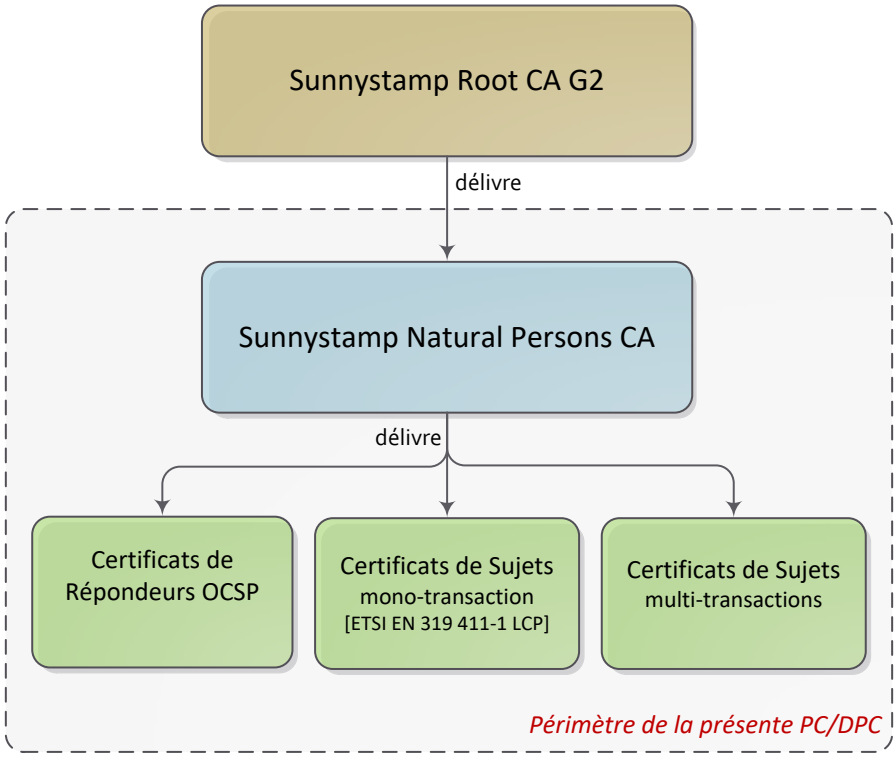

Figure 1 : hiérarchie des certificats de l'AC

1.2 Identification du document

Ce document est identifié par les OID correspondants aux deux types de Certificats suivants :

- Certificat de type « multi-transactions » : 1.3.6.1.4.1.22542.100.1.1.1.1 ;
- Certificat de type « mono-transaction » : 1.3.6.1.4.1.22542.100.1.1.1.2.

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

- « Certificat multi-transactions », pour désigner un Certificat de type « multi-transactions » ;
- « Certificat mono-transaction », pour désigner un Certificat de type « mono-transaction ».

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 personne physique, rattachée ou non à une Entité Légale, identifiée 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 est une personne physique ou une Entité Légale qui demande un Certificat pour un Sujet. Deux cas sont possibles :

- Le Souscripteur et le Sujet sont une seule et même personne physique ;
- Le Souscripteur est une Entité Légale et le Sujet est un Représentant légal de ladite Entité Légale.

1.3.6 Utilisateur de Certificat (UC)

Un UC désigne une personne physique ou morale qui utilise des Certificats générés par l'AC pour vérifier des signatures électroniques.

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 signer des documents électroniques.

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
Téléphone : 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, le cas échéant, et au nom de laquelle ce dernier utilise son Certificat. Dans la présente PC/DPC, seule les Entités Légales inscrites au Registre français du Commerce et des Sociétés sont prises en charge.

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.

Jeton d'identité
Ensemble de données signé par l'AE, constitué des informations d'identités du Sujet qui ont été vérifiées par l'AE. Un Jeton d'identité est généré par l'AE suite à l'identification et l'authentification du Sujet et possède une durée de validité de quelques minutes. Il permet d'une part à l'AC d'authentifier les demandes de délivrance et de révocation de Certificats provenant de l'AE, et d'autre part, au Serveur de signature d'authentifier le Sujet pour activer sa Clé Privée afin de lui permettre de signer des documents.

Moyen d'authentification
Moyen connu ou utilisable uniquement par le Sujet pour s'authentifier auprès de l'AE afin d'utiliser le Service de signature pour signer des documents.
Exemples : mot de passe, OTP envoyé par e-mail, OTP envoyé par SMS.

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
Toute personne physique disposant des pouvoirs de représenter l'Entité Légale du Sujet de par la loi. Elle aura la faculté de procéder à des demandes d'émission et de révocation de Certificat au bénéfice des Sujets qu'elle aura expressément et personnellement désignés.

Service de signature
Service mis à disposition par la plateforme Sunnystamp de LEX PERSONA et permettant à des Sujets de créer des signatures électroniques en mode « serveur » avec un Certificat délivré par une Autorité de Certification Sunnystamp. La Clé Privée associée au Certificat est générée et conservée de manière sécurisée par le Service de signature, qui impose au Sujet à qui elle appartient, de s'authentifier tout d'abord auprès de l'AE pour obtenir un jeton d'identité qui lui permettra ensuite de s'authentifier sur le Serveur de signature pour signer des documents.

Transaction de signature
Opération de courte durée, gérée par le Service de signature, durant laquelle un Sujet doit s'authentifier auprès de l'AE pour signer les documents de cette transaction avec sa Clé Privée « distante » associée à son Certificat.

1.6.2 Acronymes

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

AC	Autorité de Certification « Sunnystamp Natural 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
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
UC	Utilisateurs de Certificat
UUID	Universally Unique IDentifier

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 PC/DPC ;
- L'accord de souscription ;
- La déclaration d'IGC ;
- L'accord d'utilisation des Certificats ;

- Le certificat X.509 de l'AC et de l'AC racine « Sunnystamp Root CA G2 » ainsi que leur empreinte de hachage ;
- La LCR consultable aux adresses suivantes :
  - http://pki2.sunnystamp.com/crls/sunnystamp-natural-persons-ca.crl ;
  - http://pki3.sunnystamp.com/crls/sunnystamp-natural-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-natural-persons-ca.

2.3 Délais et fréquences de publication

La 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 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 :

Attribut	Description	Obligatoire ?
CN	Prénom usuel suivi d'un espace et du nom de l'état civil ou, le cas échéant, du nom d'usage du Sujet	Oui
GN	Prénom usuel ou prénoms de l'état civil du Sujet	Oui
SN	Nom de l'état civil ou nom d'usage du Sujet	Oui
C	Code pays de la nationalité du Sujet	Oui
serialNumber	Identifiant interne unique du Certificat du Sujet	Oui
OU	Identifiant de la transaction dans le cas d'un certificat mono-transaction.	Non
O	Nom de l'Entité Légale à laquelle le Sujet est rattaché	Non
OI	Identifiant unique de l'Entité Légale à laquelle le Sujet est rattaché (structuré conformément à la section 5.1.4 de la norme [EN 319 412-1]).	Non
T	Fonction du Sujet dans l'Entité Légale à laquelle il est rattaché	Non

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

L'attribut `CN` est la concaténation du contenu de l'attribut `GN`, d'un espace et du contenu de l'attribut `SN`.

Dans le cas d'un certificat mono-transaction, l'attribut `OU` est obligatoire et doit contenir l'identifiant de la transaction de signature préfixé par la chaîne « Transaction- ».

Dans le cas d'un Sujet rattaché à une Entité Légale, les attributs `O` et `OI` doivent obligatoirement être renseignés, l'attribut `T` étant optionnel.

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

3.1.2 Nécessité d'utilisation de noms explicites

Le contenu des attributs `CN`, `GN` et `SN` du champ `subject` du Certificat permet 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 est un UUID qui 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

La Clé Privée du Sujet est générée et stockée de manière sécurisée par le Service de signature suite à l'identification et l'authentification du Sujet par l'AE. La Clé Privée est ensuite utilisée par le Service de signature pour générer une requête de certificat [PKCS#10] et l'envoyer à l'AC après s'être authentifié auprès d'elle.

3.2.2 Validation de l'identité d'une Entité Légale

Si le Sujet est rattaché à une Entité Légale, alors l'AE doit procéder à la vérification de l'existence de l'Entité Légale et vérifier que le Sujet est effectivement rattaché à cette entité. Ces vérifications sont réalisées lors de l'enregistrement de la personne physique se réclamant du rattachement.

Dans la présente PC/DPC, le Sujet rattaché à une Entité Légale ne peut être qu'un Représentant légal de ladite Entité Légale.

3.2.3 Validation de l'identité d'un Sujet

3.2.3.1 Sujet non rattaché à une Entité Légale

Dans le cas où le Sujet n'est pas rattaché à une Entité Légale, l'AE est en charge de la vérification de l'identité du Sujet qui doit obligatoirement fournir :

- Pour les Certificats mono-transaction : un document officiel d'identité (carte nationale d'identité, passeport ou carte de séjour) en cours de validité avec photographie comportant ses nom, prénom(s), date et lieu de naissance ;
- Pour tous les Certificats : son adresse e-mail et son numéro de téléphone portable.

Parmi ces informations, seuls les nom et prénom(s) seront mentionnés dans le Certificat.

3.2.3.2 Sujet rattaché à une Entité Légale

Dans le cas où le Sujet est rattaché à une Entité Légale, l'AE est en charge de la vérification de l'identité du Sujet qui doit obligatoirement fournir :

- Pour les Certificats mono-transaction :
  - Un document officiel d'identité (carte nationale d'identité, passeport ou carte de séjour) en cours de validité avec photographie comportant ses nom, prénom(s), date et lieu de naissance ;
  - Les pages d'un extrait Kbis de moins de 3 mois de l'Entité Légale comportant son numéro d'identifiant unique et faisant apparaître la liste de ses Représentants légaux.
- Pour tous les Certificats : son adresse e-mail et son numéro de téléphone portable et sa fonction.

Dans ce cas, seuls les nom et prénom(s) du Sujet, le nom de l'Entité Légale, son numéro d'identification unique, et de manière optionnelle la fonction occupée par le Sujet dans l'Entité Légale, seront mentionnés dans le Certificat.

3.2.3.3 Archivage des informations de validation

L'AE doit archiver toutes les informations utilisées pour vérifier l'identité, et, le cas échéant, tout attribut spécifique du Sujet, y compris toute référence à la documentation utilisée pour la vérification, et toute réserve concernant leurs limitations d'usage.

3.2.4 Informations non vérifiées du Sujet

Toutes les informations contenues dans les attributs du champ `subject` du Certificat sont vérifiées par l'AE à l'exception de l'attribut `serialNumber`.

3.2.5 Validation de l'autorité du Souscripteur

La validation de l'autorité du Souscripteur dans le cas où le Sujet est rattaché à une Entité Légale correspond pour l'AE à vérifier que la souscription a bien été effectuée par un Représentant légal de ladite l'Entité Légale.

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

3.3.1 Identification et validation d'un renouvellement courant

Si le Sujet a déjà demandé un Certificat à l'AE, alors le Sujet a la possibilité de demander un nouveau Certificat en s'authentifiant auprès de l'AE à condition que les informations utilisées initialement par l'AE pour vérifier l'identité et les attributs du Sujet soient toujours valides.

Pour un Certificat mono-transaction :
Le Sujet doit s'authentifier avec au moins 2 moyens d'authentification.

Pour un Certificat multi-transaction :
Le Sujet doit s'authentifier avec au moins 1 moyen d'authentification.

Si tout ou partie des informations du Sujet à mettre dans le Certificat (voir la section 3.1.1 ci-dessus) ont changé alors l'enregistrement doit être réalisé avec la procédure définie dans la section 3.2 ci-dessus.

3.3.2 Identification et validation pour un renouvellement après révocation

Le renouvellement de la bi-clé associé à un Certificat révoqué n'est pas autorisé par cette PC/DPC.

3.4 Identification et validation d'une demande de révocation

La révocation d'un Certificat mono-transaction est déclenchée automatiquement dès lors que le Sujet annule la Transaction de signature pour laquelle le Certificat a été spécialement créé. Cette annulation se produit dans les cas suivants :

- Si le Sujet refuse explicitement de signer les documents de la Transaction de signature ;
- Si le Sujet ne valide pas les informations contenues dans son Certificat qui lui sont présentées dans la page de signature suite à la génération de son Certificat.

La révocation d'un Certificat multi-transactions, est déclenchée à l'initiative du Sujet qui doit s'authentifier auprès de l'AE avec au moins un moyen d'authentification.

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 le cas échéant :

- Du Souscripteur personne physique, si le Sujet et le Souscripteur sont une seule et même personne physique ;
- Du Représentant légal du Souscripteur si le Souscripteur est une Entité Légale à laquelle est rattachée le Sujet ;

Dans les sections suivantes, ces deux personnes physiques sont conjointement nommées le demandeur de Certificat.

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 demandeur de Certificat doit fournir à l'AE les différentes informations requises dans la section 3.2.3 en garantissant leur exactitude ;
- Le demandeur doit enregistrer auprès de l'AE au moins 2 moyens d'authentification qui permettront à l'AE de l'authentifier ultérieurement pour lui permettre :
  - De signer des documents en utilisant le Service de signature qui opère sa Clé Privée ;

  - De demander un nouveau Certificat (cf. section 3.3.1).
- Le demandeur de Certificat doit signer l'accord de souscription ; cet accord contient en particulier l'engagement du demandeur de Certificat à ce que la bi-clé du Sujet soit générée dans un dispositif cryptographique satisfaisant aux exigences de la section 6.2.11 ; le Sujet doit signer la partie de l'accord qui le concerne si celui-ci est différent du demandeur de Certificat ;
- Le demandeur doit enregistrer auprès de l'AE au moins 2 moyens d'authentification qui permettront à l'AE de l'authentifier ;
- 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 ainsi que le Sujet si le Sujet est différent du demandeur de Certificat ;
- L'AE valide les différentes informations requises dans la section 3.2.3 ;
- L'AE enregistre les moyens d'authentification du Sujet qui lui permettront de s'authentifier ultérieurement auprès de l'AE sans avoir nécessairement besoin de transmettre à l'AE les informations décrites dans la section 3.2.3 ;
- L'AE génère un Jeton d'identité ;

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 :

- Après avoir vérifié l'identité du Sujet, l'AE génère un Jeton d'identité et le transmet au Service de Signature ;

- Le Service de signature vérifie la validité du Jeton d'identité et génère la bi-clé du Sujet ;
- Le Service de signature crée la requête de certificat ;
- Le Service de signature s'authentifie auprès de l'AC et lui transmet la requête de certificat ;
- L'AC vérifie la signature de la requête de certificat transmise par le Service de signature ;
- 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 Sujet

Une fois généré, le Sujet est notifié de la délivrance du Certificat qui lui est transmis de manière appropriée.

4.4 Acceptation du Certificat

4.4.1 Démarche d'acceptation du Certificat

Une fois le Certificat généré, le contenu du champ `subject` et de la période de validité du Certificat sont portés à la connaissance du Sujet qui a également la possibilité de télécharger le fichier contenant le Certificat.

Pour les Certificats mono-transaction :

L'acceptation est tacite dès la notification par l'AC de la délivrance du Certificat au Sujet, dès lors que le Sujet a utilisé la Clé Privée associée à la Clé Publique contenue dans le Certificat pour signer.

Pour les Certificats multi-transactions :

L'acceptation est tacite dès la notification par l'AC de la délivrance du Certificat au Sujet, dès lors que l'une des conditions suivantes est satisfaite :

- Le Sujet n'a pas émis d'objection sur le contenu du Certificat en le révoquant lors de sa présentation au Sujet une fois la génération réalisée ;
- Le Sujet a utilisé la Clé Privée associée à la Clé Publique contenue dans le Certificat pour signer.

L'acceptation d'un Certificat par le Sujet emporte le consentement par le Sujet 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 Sujet.

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 Sujet, de sa Clé Privée et de son Certificat associé, est strictement limitée au Service de Signature et 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 Sujet par le Souscripteur, ne remettant pas en cause les clauses précédentes.

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.

4.6.1 Causes possibles de renouvellement d'un Certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification au Sujet de l'établissement du nouveau Certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau Certificat

Sans objet.

4.6.6 Publication du nouveau Certificat

Sans objet.

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

Sans objet.

4.7 Délivrance d'un nouveau Certificat suite 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.

4.7.1 Causes possibles de changement d'une bi-clé

Sans objet.

4.7.2 Origine d'une demande d'un nouveau Certificat

Sans objet.

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

Sans objet.

4.7.4 Notification au Sujet de l'établissement du nouveau Certificat

Sans objet.

4.7.5 Démarche d'acceptation du nouveau Certificat

Sans objet.

4.7.6 Publication du nouveau Certificat

Sans objet.

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

Sans objet.

4.8 Modification du Certificat

Pour modifier un Certificat en cours de validité, il est nécessaire de le révoquer puis de demander la délivrance d'un nouveau Certificat.

4.8.1 Causes possibles de modification d'un Certificat

Sans objet.

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

Sans objet.

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

Sans objet.

4.8.4 Notification au Sujet de l'établissement du Certificat modifié

Sans objet.

4.8.5 Démarche d'acceptation du Certificat modifié

Sans objet.

4.8.6 Publication du Certificat modifié

Sans objet.

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

Sans objet.

4.9 Révocation et suspension des Certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificat de Sujet

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

- Le Sujet 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 ;
- Les informations contenus dans le Certificat ne sont plus exactes ;
- Le Souscripteur ou le Sujet 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 moyens d'authentification permettant au Sujet d'activer sa Clé Privée 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 de Sujet sont les suivantes :

- Le Souscripteur ;
- Le Sujet ;

- 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 par le Sujet ou le Souscripteur 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 demandeur de la révocation effective du Certificat et le cas échéant le Sujet, si ce n'est pas lui qui a fait la demande.

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 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 en fonctionnement normal 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 établit 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 data centers hautement sécurisés qui respectent les règlements et normes en vigueur et qui fournissent une protection robuste contre les accès non autorisés.

Ces deux data centers sont localisés sur le territoire français et sont séparés l'un de l'autre par une distance en ligne droite supérieure à 200 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 stockées 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. 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 Operator** : cette personne est responsable de l'exploitation des applications pour les fonctions mises en œuvre par les composantes de l'IGC.
- **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 Administrator et System Operator.

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 confiances 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'évènements 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 ;
- La preuve d'acceptation des Conditions Générales d'Utilisation par les Souscripteurs et les Sujets (s'ils diffèrent des Souscripteurs) ;
- Les dossiers d'enregistrement ;
- Dans le cas des certificats mono-transaction : une copie des éléments ayant permis de vérifier l'identité physique des Sujets, auxquels il faudra ajouter, en cas de rattachement d'un Sujet à une Entité Légale, une copie des éléments ayant permis de vérifier l'existence de l'Entité Légale ainsi que le lien du Sujet avec ladite Entité Légale ;
- Les Certificats d'AC, les Certificats des répondeurs 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 au minimum 7 ans après l'expiration du dernier Certificat émis par l'AC :

- Les journaux d'événements ;
- La preuve d'acceptation des Conditions Générales d'Utilisation par les Souscripteurs et les Sujets (s'ils diffèrent des Souscripteurs).

Les dossiers d'enregistrement sont conservés durant toute la durée de vie de l'AC.

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.

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 par le Service de signature dans un HSM satisfaisant aux exigences définies dans la section 6.2.11. Le HSM est initialisé lors d'une

cérémonie des clés, par au moins 2 personnes ayant des rôles de confiance dans le Service de signature, au cours de laquelle une clé de wrap est générée dans le but de sécuriser l'exportation des Clés Privées des Sujets. Lors de cette cérémonie une copie de secours de cette clé de wrap est réalisée conformément aux exigences définies à la section 6.2.4.

6.1.2 Transmission de la clé privée à son propriétaire

La Clé Privée d'un Sujet n'est pas transmise à son propriétaire. Elle est générée et stockée sur le HSM du Service de signature.

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 et des Sujets 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 le Service de signature qui met en œuvre des moyens techniques et organisationnels pour garantir que seul le propriétaire d'une Clé Privée puisse l'utiliser pour signer.

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.

Après sa génération, la Clé Privée d'un Sujet est exportée hors du HSM sous forme chiffrée et avec un mécanisme de contrôle d'intégrité afin d'offrir un niveau de sécurité équivalent ou supérieur au

stockage au sein du HSM. Cet export de la Clé Privée du Sujet, chiffré par la clé de wrap du HSM, est conservé de manière sécurisée par le Service de signature.

6.2.7 Stockage de la Clé Privée dans un dispositif cryptographique

Le stockage des Clés Privées est réalisé dans un HSM satisfaisant aux exigences définies dans la section 6.2.11 ou en dehors d'un tel HSM moyennant le respect des exigences définies à la section 6.2.4.

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 HSM 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 Service de signature, après l'authentification du Sujet par l'AE.

6.2.9 Méthode de désactivation de la Clé Privée

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

La Clé Privée d'un Sujet est immédiatement désactiver par le Service de signature après sa génération.

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.

La destruction de la Clé Privée d'un Sujet est réalisée lorsque le Certificat correspondant est révoqué ou, dans le cas d'un Certificat mono-transaction, lorsque la Transaction de signature est terminée.

6.2.11 Niveau de qualification des dispositifs cryptographiques

6.2.11.1 AC

Le dispositif cryptographique de l'AC est un HSM certifié FIPS 140-2 level 3 ou équivalent.

6.2.11.2 Sujet

Le dispositif cryptographique des Sujets est un HSM 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.

Pour les Certificats mono-transaction :
Les bi-clés et les Certificats des Sujets ont une durée de vie maximale de 12 heures. Cette durée paramétrable, qui doit être la plus courte possible, permet d'intégrer une durée de transaction plus ou moins longue en fonction du délai de réflexion du Sujet ainsi que de la taille et du nombre de fichiers à signer.

Pour les Certificats multi-transactions :
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 ses cartes à puce, principales et de secours, protégées 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 à partir de serveurs Network Time Protocol (NTP).

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 Natural 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 319 412-2].

7.2.1 Certificat multi-transactions

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 Natural Persons CA OI = NTRFR-480622257 OU=0002 480622257 O = LEX PERSONA C = FR
Sujet	CN = Prénom usuel suivi d'un espace et du nom de l'état civil ou, le cas échéant, du nom d'usage du Sujet GN = Prénom usuel ou prénoms de l'état civil du Sujet SN = Nom de l'état civil ou nom d'usage du Sujet C = Code pays de la nationalité du Sujet serialNumber = Identifiant unique généré par l'AE OI = Identifiant unique de l'Entité Légale (optionnel) O = Nom de l'Entité Légale (optionnel) T = Fonction du Sujet dans l'Entité Légale (optionnel)
Validité	3 ans maximum
Signature	RSAwithSHA256
Clé publique	RSA 2048 bits

Extensions :

Champ	Critique	Valeur
AuthorityInfoAccess	Non	id-ad-calssuers= https://pki2.sunnystamp.com/certs/sunnystamp-natural-persons-ca.cer id-ad-ocsp=

		http://ocsp2.sunnystamp.com/sunnystamp-natural-persons-ca
AuthorityKeyIdentifier	Non	
BasicConstraints	Oui	cA=false
CertificatePolicies	Non	OID=1.3.6.1.4.1.22542.100.1.1.1.1 URL=https://pki2.sunnystamp.com/repository
CRLDistributionPoints	Non	http://pki2.sunnystamp.com/crls/sunnystamp-natural-persons-ca.crl http://pki3.sunnystamp.com/crls/sunnystamp-natural-persons-ca.crl
Key Usage	Oui	nonRepudiation
SubjectKeyIdentifier	Non	

7.2.2 Certificat mono-transaction

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 Natural Persons CA OI = NTRFR-480622257 OU=0002 480622257 O = LEX PERSONA C = FR
Sujet	CN = Prénom usuel suivi d'un espace et du nom de l'état civil ou, le cas échéant, du nom d'usage du Sujet GN = Prénom usuel ou prénoms de l'état civil du Sujet SN = Nom de l'état civil ou nom d'usage du Sujet C = Code pays de la nationalité du Sujet serialNumber = Identifiant unique généré par l'AE OU = Identifiant de la transaction préfixé par « Transaction- » OI = Identifiant unique de l'Entité Légale (optionnel) O = Nom de l'Entité Légale (optionnel) T = Fonction du Sujet dans l'Entité Légale (optionnel)
Validité	12 heures maximum
Signature	RSAwithSHA256
Clé publique	RSA 2048 bits

Extensions :

Champ	Critique	Valeur
AuthorityInfoAccess	Non	id-ad-caIssuers= https://pki2.sunnystamp.com/certs/sunnystamp-natural-persons-ca.cer id-ad-ocsp= http://ocsp2.sunnystamp.com/sunnystamp-natural-persons-ca
AuthorityKeyIdentifier	Non	
BasicConstraints	Oui	cA=false
CertificatePolicies	Non	OID=0.4.0.2042.1.3 OID=1.3.6.1.4.1.22542.100.1.1.1.2 URL=https://pki2.sunnystamp.com/repository
CRLDistributionPoints	Non	http://pki2.sunnystamp.com/crls/sunnystamp-natural-persons-ca.crl http://pki3.sunnystamp.com/crls/sunnystamp-natural-persons-ca.crl
Key Usage	Oui	nonRepudiation
SubjectKeyIdentifier	Non	

7.3 Profil des LCR

Champs de base :

Champ	Valeur
Version	1
Emetteur	CN = Sunnystamp Natural 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 Natural 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].

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

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 Sujet 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 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 ;
- 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 Sujet, 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 Sujet situées dans la deuxième partie.

La deuxième partie mentionne :

- Le respect des obligations de l'accord qui concernent le Sujet ;
- Le respect des exigences indiquées dans la présente PC/DPC qui concernent le Sujet ;

- 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 Sujet, 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 Sujet 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 Sujet s'applique à la deuxième partie.

Dans le cas où le Sujet et le Souscripteur sont la même personne physique, alors la signature du Sujet/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 conforme à l'utilisation du Certificat ;
- Vérifier que l'OID de la présente PC/DPC est contenu dans l'extension « Certificate Policies » du Certificat ;
- 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.

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 règlementation [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

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

[EN 319 411-1]
ETSI EN 319 411-1 V1.1.1 (2016-02)
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 319 412-2]
ETSI EN 319 421-2 V2.1.1 (2016-02)
Certificate Profiles;
Part 2: Certificate profile for certificates issued to natural 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