SunPKI

Sunnystamp Legal Persons CA 1

Politique de Certification / Déclaration des Pratiques de Certification

Version 1.7

Date d'entrée en vigueur : 25/09/2026

Tous droits réservés

9 Av Maréchal Leclerc - 10120 ST ANDRE LES VERGERS - FRANCE
Tél. : +33 (0)3 25 43 90 78 – www.goodflag.com
SAS au capital de 26 739 euros – R.C.S. Troyes 480 622 257 – Code APE 5829C – TVA FR01480622257

Table des matières

1 Introduction 6

1.1 Présentation générale 6

1.2 Identification du document 7

1.3 Entités intervenant dans l'IGC 7

1.3.1 Lex Persona Trust Service Provider Board (LPTSP Board) 7

1.3.2 Autorité de Certification « Sunnystamp Legal Persons CA 1 » (AC) 8

1.3.3 Autorité d'Enregistrement (AE) 8

1.3.4 Sujet 8

1.3.5 Souscripteur 8

1.3.6 Responsable de la Clé Privé du Sujet (RCPS) 8

1.3.7 Utilisateur de Certificat (UC) 9

1.4 Usage des Certificats 9

1.4.1 Domaines d'utilisation applicables 9

1.4.2 Domaines d'utilisation interdits 9

1.5 Gestion de la PC 9

1.5.1 Entité gérant la PC 9

1.5.2 Entité déterminant la conformité de la PC/DPC 10

1.5.3 Procédure d'approbation de la conformité de la PC/DPC 10

1.6 Définitions et Acronymes 10

1.6.1 Définitions 10

1.6.2 Acronymes 13

1.7 Documents associés 13

1.7.1 Documents normatifs 13

1.7.2 Politique Générale des Services de Confiance 14

1.7.3 Politique de Certification de l'AC « Sunnystamp Root CA G2 » 15

1.7.4 Formulaire de demande de Certificat 15

1.7.5 Formulaire de demande de révocation de Certificat 15

1.7.6 Formulaire de demande de changement de RCPS de Certificat 15

1.7.7 Liste des dispositifs qualifiés de création de signature et de création de Cachet 15

2 Responsabilité concernant la mise à disposition des informations devant être publiées 15

2.1 Entités chargées de la mise à disposition des informations 15

2.2 Informations devant être publiées 15

2.3 Délais et fréquences de publication 16

2.4 Contrôle d'accès aux informations publiées 16

3 Identification et authentification 16

3.1 Nommage 16

3.1.1 Types des noms 16

3.1.2 Nécessité d'utilisation de noms explicites 17

3.1.3 Anonymisation et pseudonymisation des Sujets 17

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 de l'Entité Légale 18
3.2.3 Validation de l'identité du Sujet 18
3.2.4 Archivage des informations de validation 19
3.2.5 Informations non vérifiées du Sujet 19
3.2.6 Validation de l'autorité du Souscripteur 19
3.2.7 Critères d'interopérabilité 19
3.3 Identification et validation d'une demande de renouvellement des clés 19
3.4 Identification et validation d'une demande de révocation 20
4 Exigences opérationnelles sur le cycle de vie des Certificats 20
4.1 Demande de Certificat 20
4.1.1 Origine d'une demande de Certificat 20
4.1.2 Processus et responsabilités pour l'établissement d'une demande de Certificat 20
4.1.3 Contrôle annuel des QSCD 20
4.2 Traitement d'une demande de Certificat 21
4.2.1 Exécution des processus d'identification et de validation de la demande 21
4.2.2 Acceptation ou rejet de la demande 21
4.2.3 Durée d'établissement du Certificat 21
4.3 Délivrance du Certificat 21
4.3.1 Actions de l'AC concernant la délivrance du Certificat 21
4.3.2 Notification par l'AC de la délivrance du Certificat au Sujet 22
4.4 Acceptation du Certificat 22
4.4.1 Démarche d'acceptation du Certificat 22
4.4.2 Publication du Certificat 22
4.4.3 Notification par l'AC aux autres entités de la délivrance du Certificat 22
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 23
4.6 Renouvellement d'un Certificat 23
4.7 Délivrance d'un nouveau Certificat suite au changement de la Bi-clé 23
4.8 Modification du Certificat 23
4.9 Révocation et suspension des Certificats 23
4.9.1 Causes possibles d'une révocation 23
4.9.2 Origine d'une demande de révocation 24
4.9.3 Procédure de traitement d'une demande de révocation 24
4.9.4 Délai accordé pour formuler la demande de révocation 25
4.9.5 Délai de traitement par l'AC d'une demande de révocation 25
4.9.6 Exigences de vérification de la révocation par les UC 25
4.9.7 Fréquence d'établissement des LCR 25
4.9.8 Délai maximum de publication d'une LCR 25
4.9.9 Disponibilité d'un système de vérification en ligne de l'état des Certificats 25
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 26
4.9.14 Origine d'une demande de suspension 26
4.9.15 Procédure de traitement d'une demande de suspension 26
4.9.16 Limites de la période de suspension d'un Certificat 26
4.10 Fonction d'information sur l'état des Certificats 26
4.10.1 Caractéristiques opérationnelles 26

4.10.2 Disponibilité de la fonction 26
4.10.3 Dispositifs optionnels 26
4.11 Fin de la relation entre le Souscripteur et l'AC 26
4.12 Séquestre de clé et recouvrement 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 27
5.1 Mesures de sécurité physique 27
5.2 Mesures de sécurité procédurales 27
5.3 Mesures de sécurité vis-à-vis du personnel 27
5.4 Procédure de constitution des données d'audit 27
5.5 Archivage des données 27
5.6 Changement de clé d'AC 28
5.7 Reprise suite à la compromission et sinistre 28
5.8 Fin de vie de l'AC 28
6 Mesures de sécurité techniques 29
6.1 Génération et installation de Bi-clés 29
6.1.1 Génération des Bi-clés 29
6.1.2 Transmission de la Clé Privée à son propriétaire 29
6.1.3 Transmission de la Clé Publique à l'AC 29
6.1.4 Transmission de la Clé Publique de l'AC aux UC 29
6.1.5 Tailles des clés 30
6.1.6 Vérification de la génération des paramètres des Bi-clés et de leur qualité 30
6.1.7 Objectifs d'usage de la clé 30
6.2 Mesures de sécurité pour la protection des clés privées et pour les dispositifs cryptographiques 30
6.2.1 Standards et mesures de sécurité pour les dispositifs cryptographiques 30
6.2.2 Contrôle de la Clé Privée 30
6.2.3 Séquestre de la Clé Privée 31
6.2.4 Copie de secours de la Clé Privée 31
6.2.5 Archivage de la Clé Privée 31
6.2.6 Transfert de la Clé Privée vers / depuis le dispositif cryptographique 31
6.2.7 Stockage de la Clé Privée dans un dispositif cryptographique 32
6.2.8 Méthode d'activation de la Clé Privée 32
6.2.9 Méthode de désactivation de la Clé Privée 32
6.2.10 Méthode de destruction d'une Clé Privée 32
6.2.11 Niveau de qualification des dispositifs cryptographiques 32
6.3 Autres aspects de la gestion des Bi-clés 33
6.3.1 Archivage des clés publiques 33
6.3.2 Durées de vie des Bi-clés et des Certificats 33
6.4 Données d'activation 33
6.4.1 Génération et installation des données d'activation 33
6.4.2 Protection des données d'activation 33
6.4.3 Autres aspects liés aux données d'activation 34
6.5 Mesures de sécurité des systèmes informatiques 34

6.6 Mesures de sécurité liées au développement des systèmes 34
6.7 Mesures de sécurité réseau 34
6.8 Horodatage / Système de datation 34
7 Profils des Certificats, OCSP et des LCR 34
7.1 Certificat de l'AC 34
7.2 Certificat d'un Sujet 35
7.3 Profil des LCR 36
7.4 Profil OCSP 37
8 Audit de conformité et autres évaluations 38
9 Autres problématiques métiers et légales 38
9.1 Tarifs 38
9.1.1 Tarifs pour la fourniture ou le renouvellement de Certificats 38
9.1.2 Tarifs pour accéder aux Certificats 38
9.1.3 Tarifs pour accéder aux informations d'état de révocation des Certificats 38
9.1.4 Tarifs pour d'autres services 38
9.1.5 Politique de remboursement 38
9.2 Responsabilité financière 38
9.2.1 Couverture par les assurances 38
9.2.2 Autres ressources 38
9.2.3 Couvertures et garantie concernant les entités utilisatrices 39
9.2.4 Confidentialité des données professionnelles 39
9.3 Protection des données personnelles 39
9.4 Droits sur la propriété intellectuelle et industrielle 39
9.5 Interprétations contractuelles et garanties 39
9.5.1 AC 39
9.5.2 AE 40
9.5.3 RCPS et Souscripteur 40
9.5.4 UC 41
9.6 Limite de garantie 41
9.7 Limite de responsabilité 41
9.8 Indemnités 42
9.9 Durée et fin anticipée de validité de la PC/DPC 42
9.10 Notification individuelles et communications entre les participants 42
9.11 Amendements 42
9.12 Dispositions concernant la résolution de conflits 42
9.13 Juridictions compétentes 42
9.14 Conformité aux législations et réglementations 42
9.15 Dispositions diverses 42
9.16 Autres dispositions 42

1 Introduction

1.1 Présentation générale

Au début de l'année 2025, la société Lex Persona a adopté le nom commercial Goodflag. En revanche, toutes les références techniques et organisationnelles, telles que les gabarits des Certificats, les Certificats d'AC, l'organe de gouvernance de l'AC, etc., conservent le nom Lex Persona et sont toujours en vigueur.

Dans le cadre de son offre de services de confiance, Goodflag fournit un service de génération de Certificats d'Entité Légale, nommés « Certificats d'Entité » dans la suite du document, délivrés par une Autorité de Certification appartenant à l'Infrastructure de Gestion de Clés (IGC) Sunnystamp.

Une demande de génération de Certificat d'Entité est effectuée par un Souscripteur, agissant dans le cadre d'une personne morale, et qui mandate pour cela une personne physique appelée Responsable de la Clé Privée du Sujet (RCPS), en charge d'assurer le suivi du cycle de vie de ce Certificat. Ce Certificat permettra au Souscripteur d'apposer un Cachet électronique qualifié à distance, via le Service de Cachet Electronique A Distance (SCEQAD), sur les documents qui auront été soumis à travers une Transaction de Cachet.

Cette Autorité de Certification est dénommée « Sunnystamp Legal Persons CA 1 » et sera nommée « AC » dans le reste du document.

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 Goodflag et toutes les parties concernées.

Dans le cadre de cette PC/DPC, l'AC délivre des Certificats à des RCPS nommés et identifiés par un Représentant Légal de l'Entité Légale du Souscripteur. Ces Certificats ont une durée de validité maximale de 3 ans et ne peuvent être utilisés que par le SCEQAD opéré par Goodflag.

Les procédures internes propres à la Déclaration des Pratiques de Certification (DPC) sont confidentielles et ne sont pas exposées dans ce document.

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

L'AC délivre deux types de Certificats :

1. Les Certificats utilisés par ses répondeurs OCSP pour signer les réponses OCSP ;
2. Les Certificats d'Entité à destination de personnes morales, conformes à la norme [ETSI_319_411-2] pour le niveau QCP-l-qscd.

L'AC est certifiée conforme aux normes ETSI indiquées ci-dessus et est qualifiée suivant le processus de qualification de l'ANSSI défini par [ANSSI-QCP].

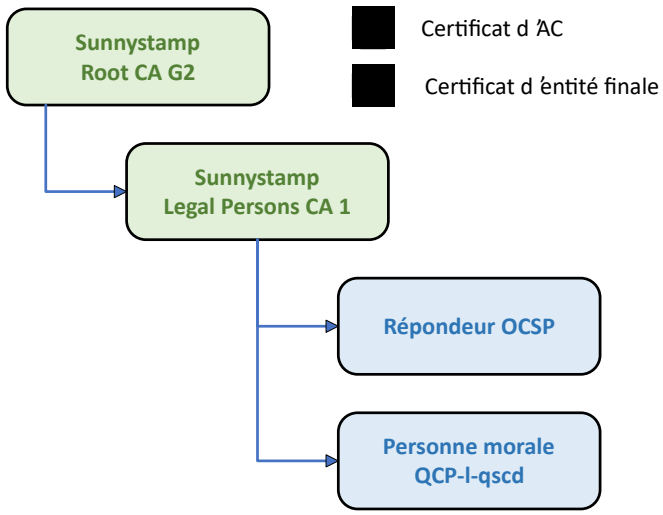

Figure 1 : hiérarchie des Certificats de l'AC

1.2 Identification du document

La politique contenue dans ce document et couvrant les Certificats de Cachets est identifiée suivant l'OID :

- **1.3.6.1.4.1.22542.100.1.1.3.2** pour les Certificats de Cachets **ETSI QCP-l-qscd**.

Lorsque rien n'est précisé, les exigences de cette PC/DPC s'appliquent pour tous les profils de Certificats de Cachets, dans le cas contraire les exigences feront référence à l'OID ou au profil concerné de manière explicite.

Les Certificats OCSP traités dans le cadre de la présente PC ne font pas l'objet d'une identification par OID.

Toute modification majeure de cette PC/DPC fait l'objet d'une mise à jour du présent document, du dernier indice de son OID et d'une publication dans le dépôt d'informations officielles de Goodflag.

1.3 Entités intervenant dans l'IGC

1.3.1 Lex Persona Trust Service Provider Board (LPTSP Board)

L'AC est sous la responsabilité du LPTSP Board. Le LPTSP Board est représenté par Lex Persona. Il est composé des membres suivants :

- Le responsable du LPTSP 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 LPTSP Board.

Les missions principales du LPTSP 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 « Sunnystamp Legal Persons CA 1 » (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 ;
- Vérifier l'identité des RCPS et la légitimité de ces derniers à représenter le Souscripteur ;
- Authentifier et transmettre à l'AC les demandes de création et de révocation de Certificats ;
- Archiver les données relatives à l'identification des RCPS, des Sujets et des Souscripteurs.

L'AE est gérée et opérée par Lex Persona, laquelle peut déléguer contractuellement toute ou partie de cette activité à une entité tierce. Lex Persona, en tant qu'AC, reste toujours responsable des obligations qui lui incombent vis-à-vis des Souscripteurs, des RCPS et des Sujets.

1.3.4 Sujet

Un Sujet est une application, un service, un serveur qui utilise le Certificat d'Entité pour cacheter électroniquement des informations afin de garantir leur intégrité et leur authenticité.

Le Sujet est identifié dans le Certificat comme étant en capacité de mettre en œuvre la Clé Privée associée à la Clé Publique contenue dans le Certificat.

1.3.5 Souscripteur

Le Souscripteur est une Entité Légale qui demande un Certificat pour un Sujet par l'intermédiaire d'un RCPS.

Goodflag peut endosser le rôle de Souscripteur dans le cas où elle est amenée à demander un Certificat pour un composant interne.

1.3.6 Responsable de la Clé Privé du Sujet (RCPS)

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

- La responsabilité de porteur de la Clé Privée associée à la Clé Publique contenue dans le Certificat ;
- La responsabilité des étapes du cycle de vie du Certificat, et en particulier celles qui consistent à :
  - S'assurer que la bi-clé est générée dans un dispositif cryptographique satisfaisant aux exigences de la section 6.2.11 de [PC/DPC] ;
  - Demander un Certificat à l'AE ;
  - Se faire remettre un Certificat par l'AE ;
  - Procéder le cas échéant à la demande de révocation d'un Certificat.

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

La nomination d'un RCPS est obligatoire.

Dès lors qu'un RCPS ne peut plus assumer les responsabilités décrites ci-dessus, du fait :

- D'un changement d'affectation ;
- Du départ de l'entreprise ;
- De la rupture du contrat de service avec le RCPS ou l'entité de laquelle il dépend ;
- De la perte ou de la suspicion de compromission de l'un ou des deux moyens nécessaires à l'appel du SCEQAD ;

le Souscripteur doit, au choix :

- Renouveler la nomination du présent RCPS ou nommer un nouveau RCPS à l'aide du Formulaire de Changement de RCPS de Certificat d'Entité ;
- Effectuer une demande de révocation du Certificat d'Entité auprès de l'AE à l'aide du Formulaire de Révocation de Certificat d'Entité.

1.3.7 Utilisateur de Certificat (UC)

Un UC désigne une personne physique ou morale qui utilise des Certificats générés par l'AC pour vérifier des Cachets 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 finaux de Cachets ;
- Les LCR ;
- Les Certificats de répondeurs OCSP.

1.4.1.2 Certificat de Cachet

La Clé Privée associée à la Clé Publique du Certificat de Cachet d'un Sujet est utilisée pour cacheter des documents numériques au sein d'une Transaction de Cachet mise en œuvre par le SCEQAD.

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 (Goodflag)
9 AVENUE MARECHAL LECLERC
10120 ST-ANDRE-LES-VERGERS

FRANCE
Courriel : *pki@sunnystamp.com*
Téléphone : +33 (0)3 25 43 90 78

1.5.2 Entité déterminant la conformité de la PC/DPC

Le LPTSP 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 LPTSP 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 Électronique (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.

Cachet

Chiffrement de l'empreinte de données à cacheter avec la Clé Privée associée à un Certificat de personne morale.

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'Entité d'un Sujet.

Clé Privée

Clé d'une Bi-clé d'une Entité Légale devant être utilisée exclusivement par cette Entité Légale.

Clé Publique

Clé d'une Bi-clé d'une Entité Légale 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.

Demandeur

Terme utilisé pour désigner la personne qui remplit un Formulaire. Le Demandeur peut être toute personne physique qui dispose des informations et justificatifs nécessaires et qui est habilitée par les parties prenantes à se substituer à elles pour compléter le Formulaire en question. Le Demandeur n'est pas nécessairement partie prenante du Formulaire, à l'exception d'une demande de révocation, qui, elle, doit impérativement être signée électroniquement par le Demandeur.

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 d'Entité.

Formulaire

Terme qui désigne l'un des documents suivants fournis par l'AE : demande de Certificat, demande de révocation de Certificat et demande de changement de Responsable de la Clé Privée du Sujet (RCPS) de Certificat. Ces documents peuvent être au format PDF ou au format Web interactif. A un Formulaire peu(ven)t être associée(s) une ou plusieurs pièce(s) jointe(s) au format PDF.

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.

Liste des Certificats Révoqués (LCR)

Fichier daté et signé, comportant, pour une période donnée, les informations relatives aux Certificats délivrés par une AC et qui ont été révoqués.

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).

Règlement eIDAS

Règlement de l'Union européenne no 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance. Lorsqu'il est fait spécifiquement référence à des modifications apportées par le règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le Règlement eIDAS, on citera alors le Règlement eIDAS (« version 2 »).

Réponse OCSP

Information retournée par l'AC, en temps réel et sur demande, par le biais d'un répondeur OCSP, indiquant le statut de révocation d'un Certificat délivré par l'AC.

Représentant Légal (RL)

Au sens de la présente PC/DPC, le RL est une personne physique disposant des pouvoirs de représenter le Sujet, de par la loi ou de par une délégation de pouvoir, et habilitée à procéder à des demandes d'émission et de révocation de Certificats au bénéfice des Sujets qu'elle aura expressément définis.

Responsable de la Clé Privée du Sujet (RCPS)

Cf. section 1.3.6

Service de Cachet Electronique Qualifiés A Distance (SCEQAD)

Service de confiance de création de Cachets électroniques qualifiés à distance, opéré par Goodflag, pouvant être mis à disposition d'un Souscripteur pour lui permettre de cacheter électroniquement, à l'aide d'un Certificat d'Entité délivré par l'AC au Souscripteur, des documents dans le cadre d'une Transaction de Cachet. La Clé Privée du Sujet, associée au Certificat d'Entité, est utilisée de manière sécurisée par le SCEQAD et par l'AC pour signer les documents de la Transaction de Cachet.

Dans le contexte d'utilisation de ce SCEQAD, le Souscripteur, via son RCPS, met en œuvre des mécanismes d'authentification forte, fournis par l'AE, permettant d'assurer que seuls les Certificats d'Entité des Sujets du Souscripteur seront mis en œuvre dans le cadre de ses Transactions de Cachet.

Les Cachets produits par le SCEQAD sont des Cachets électroniques qualifiés au sens du Règlement eIDAS.

Souscripteur

Cf. section 1.3.5

Sujet

Cf. section 1.3.4

Transaction de Cachet

Opération de courte durée, effectuée par le SCEQAD, durant laquelle le Certificat d'un Sujet est mis en œuvre de manière sécurisée pour apposer un Cachet électronique sur les documents de cette transaction avec sa Clé Privée « distante » associée à son Certificat d'Entité.

1.6.2 Acronymes

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

AC	Autorité de Certification « Sunnystamp Legal Persons CA 1 »
AE	Autorité d'Enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CGU	Conditions Générales d'Utilisation
DN	Distinguished Name
DPC	Déclarations des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés
LCP	Lightweight Certificate Policy
LCR	Liste de Certificats Révoqués
LPTSP Board	Lex Persona Trust 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 Électronique
QCP	Qualified Certificate Profile
QSCD	Qualified Seal or Signature Creation Device
RCPS	Responsable de la Clé Privée du Sujet
SCEQAD	Service de Cachet Electronique Qualifié A Distance
UC	Utilisateurs de Certificat

1.7 Documents associés

1.7.1 Documents normatifs

[ANSSI-QCP]
Services de délivrance de Certificats qualifiés de signature électronique, de Cachet électronique et d'authentification de site Internet, Critères d'évaluation de la conformité au règlement eIDAS. ANSSI, version 1.2 du 25 mars 2021

https://cyber.gouv.fr/documents/358/eidas_delivrance-certificats-qualifies_v1.2_anssi.pdf

[ETSI_319_411-1]
ETSI EN 319 411-1 V1.5.1 (2025-04). Policy and security requirements for Trust Service Providers issuing certificates. Part 1: General requirements.
https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.05.01_60/en_31941101v010501p.pdf

[ETSI_319_411-2]
ETSI EN 319 411-2 V2.6.1 (2025-06). Policy and security requirements for Trust Service Providers issuing certificates. Part 2: Requirements for trust service providers issuing EU qualified certificates
https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.06.01_60/en_31941102v020601p.pdf

[ETSI_319_412-1]
ETSI EN 319 412-1 V1.6.1 (2025-06). Certificate Profiles. Part 1: Overview and common data structures.
https://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.06.01_60/en_31941201v010601p.pdf

[ETSI_319_412-3]
ETSI EN 319 412-3 V1.3.1 (2023-09). Certificate Profiles. Part 3: Certificate profile for certificates issued to legal persons.
https://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.03.01_60/en_31941203v010301p.pdf

[ETSI_319_412-5]
ETSI EN 319 412-5 V2.5.1 (2025-06). Certificate Profiles. Part 2: QC Statements.
https://www.etsi.org/deliver/etsi_en/319400_319499/31941205/02.05.01_60/en_31941205v020501p.pdf

[PKCS#10]
PKCS #10: Certification Request Syntax Specification Version 1.7.
https://tools.ietf.org/html/rfc2986

[RFC_5280]
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
https://tools.ietf.org/html/rfc5280

[RFC_6960]
Online Certificate Status Protocol – OCSP. June 2013. https://tools.ietf.org/html/rfc6960

1.7.2 Politique Générale des Services de Confiance

[PGSC]
Politique Générale des Services de Confiance de Lex Persona (Goodflag).
https://pki2.sunnystamp.com/repository

1.7.3 Politique de Certification de l'AC « Sunnystamp Root CA G2 »

[PC_RG2]
Politique de Certification de l'Autorité de Certification « Sunnystamp Root CA G2 ».
https://pki2.sunnystamp.com/repository

1.7.4 Formulaire de demande de Certificat

[FR_DEMANDE]
Formulaire de demande de Certificat.
https://zfrmz.eu/xjwbjMCSwZw3Ts1QmXUX

1.7.5 Formulaire de demande de révocation de Certificat

[FR_REVOCATION]
Formulaire de demande de révocation de Certificat.
https://zfrmz.eu/u06x8guDVeHJwcgzwLs1

1.7.6 Formulaire de demande de changement de RCPS de Certificat

[FR_MOD_RCPS]
Formulaire de demande de changement de RCPS de Certificat.
https://zfrmz.eu/285E64keSJqJ1s59Fd1j

1.7.7 Liste des dispositifs qualifiés de création de signature et de création de Cachet

[UE_QSCD]
Liste des dispositifs qualifiés de création de signature et de création de Cachet et des dispositifs sécurisés de création de signature.
https://eidas.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD

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

2.1 Entités chargées de la mise à disposition des informations

Voir chapitre 2 de la [PGSC].

2.2 Informations devant être publiées

L'AC publie en ligne les informations suivantes :

- La PC/DPC ;
- La [PGSC] ;
- Les CGU de l'AC ;
- L'accord d'utilisation des Certificats ;
- Le Formulaire [FR_DEMANDE] ;
- Le Formulaire [FR_REVOCATION] ;

- Le Formulaire [FR_MOD_RCPS] ;
- 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 :
  - *https://pki2.sunnystamp.com/crls/sunnystamp-legal-persons-ca-1.crl ;*
  - *https://pki3.sunnystamp.com/crls/sunnystamp-legal-persons-ca-1.crl ;*
- Le statut de révocation des Certificats qu'elle émet à travers un répondeur OCSP accessible à l'adresse suivante : *https://ocsp2.sunnystamp.com/sunnystamp-legal-persons-ca-1*

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.

La PC/DPC, l'accord de souscription, les CGU 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/DPC.

2.4 Contrôle d'accès aux informations publiées

Voir chapitre 2 de la [PGSC].

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 peut délivrer des Certificats de test, lesquels sont identifiés comme décrit en 3.1.4.

L'AC est identifiée dans le champ `issuer` du Certificat et le Sujet est identifié dans le champ `subject`.

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

Attribut	Description	Obligatoire ?
CN	Nom de l'application, du service ou du serveur du Sujet	Oui
C	Code du pays dans lequel le Sujet est établi	Oui
O	Nom légal du Sujet	Oui
OI	Identifiant unique du Sujet (structuré conformément à la section 5.1.4 de la norme [ETSI_319_412-1]).	Oui
serialNumber	Identifiant interne unique du Certificat du Sujet généré par l'AC	Oui
OU	Attribut utilisé pour préciser le Sujet.	Non
L	Attribut utilisé pour désigner la ville dans laquelle le Sujet est enregistré	Non

3.1.2 Nécessité d'utilisation de noms explicites

Le contenu des attributs `CN`, `SN` et `C` 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.

Les Certificats de test sont identifiés par la présence du préfixe « `TEST-` » dans l'attribut `CN` du sujet.

3.1.5 Unicité des noms

L'attribut `serialNumber` contenu dans le champ `subject` du Certificat est un UUID généré par l'AE, 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

Sans objet, la clé privée étant générée par l'AC.

3.2.2 Validation de l'identité de l'Entité Légale

L'AE procède à la validation de l'identité de l'Entité Légale du Sujet en vérifiant que l'Entité Légale existe bien à l'aide d'une pièce justificative à valeur légale de l'existence du Souscripteur comportant son numéro d'identifiant unique (exemples : un avis de situation SIRENE, la première page d'un extrait Kbis de moins de 3 mois pour une entreprise française, etc.). Cette pièce justificative est appelée [PJ1_DEMANDE] est communiquée à l'AE avec le Formulaire [FR_DEMANDE].

3.2.3 Validation de l'identité du Sujet

La validation de l'identité du Sujet est effectuée lors du traitement par l'AE de la demande de Certificat matérialisée par le Formulaire [FR_DEMANDE]. Elle résulte de 4 étapes de validation :

1. Validation de l'identité du RCPS ;
2. Validation du RL en relation avec l'Entité Légale ;
3. Validation des attributs du Sujet en relation avec l'Entité Légale ;
4. Validation de la nomination du RCPS par le RL.

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

Le RCPS fournit les informations suivantes à l'AE dans le Formulaire de demande signé par le RCPS :

- Ses nom et prénom(s) ;
- Son pays de naissance ;
- Son adresse courriel.

La validation de l'identité du RCPS est effectuée par l'AE à l'aide des opérations suivantes :

- Vérification de la signature qualifiée du Formulaire [FR_DEMANDE] par le RCPS, conformément aux exigences du document [ANSSI_QCP] ;
- Vérification que la signature qualifiée date de moins de 3 mois par rapport à la date de la validation.

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

Le RL fournit les informations suivantes à l'AE :

- Ses nom et prénom(s) ;
- Son pays de naissance ;
- Son adresse courriel.

Avec le Formulaire [FR_DEMANDE] est également fournie une troisième pièce justificative à valeur légale indiquant la qualité de RL de l'Entité Légale (exemples : Kbis de l'Entité Légale du Souscripteur mentionnant le RL, procès-verbal d'assemblée générale désignant le RL, etc.). Cette pièce justificative est appelée [PJ3_DEMANDE] et peut ne pas être fournie si, le cas échéant, celle-ci est identique à [PJ2_DEMANDE].

La validation de l'identité du RL pour un Certificat à émettre est effectuée est effectuée par l'AE à l'aide des opérations suivantes :

- Vérification de la signature qualifiée du Formulaire [FR_DEMANDE] par le RL, conformément aux exigences du document [ANSSI_QCP] ;

- Vérification que la signature qualifiée date de moins de 3 mois par rapport à la date de la validation.

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

L'AE vérifie tous les attributs du champ `subject` à renseigner dans le Certificat, à l'exception de l'attribut `serialNumber`, en utilisant les justificatifs fournis avec le Formulaire [FR_DEMANDE] et tout document permettant de justifier le lien entre l'attribut `O` et l'Entité Légale du Souscripteur si ces informations diffèrent.

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

Le Formulaire [FR_DEMANDE] contient les Conditions Générales d'Utilisation qui correspondent à cette PC/DPC et qui seront donc signées électroniquement par le RCPS et le RL.

Ce Formulaire [FR_DEMANDE] précise également la nomination par le RL du RCPS et l'acceptation par ce dernier de cette nomination.

L'acceptation des Conditions Générales d'Utilisation par le RL et le RCPS ainsi que la validation de la nomination du RCPS par le RL est effectuée lors de la signature qualifiée du Formulaire [FR_DEMANDE].

Le RCPS pouvant éventuellement démissionner de ses fonctions, il existe un Formulaire de changement de RCPS désigné [FR_MOD_RCPS] qui doit être signé par le RL et le nouveau RCPS. Ce formulaire doit également être utilisé en cas de licenciement du RCPS, ou dès lors qu'il y a une suspicion de compromission du Certificat d'authentification du RCPS ou des données d'activation de la Clé Privée du Certificat du Sujet.

3.2.4 Archivage des informations de validation

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

3.2.5 Informations non vérifiées du Sujet

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

3.2.6 Validation de l'autorité du Souscripteur

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

3.2.7 Critères d'interopérabilité

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

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

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

3.4 Identification et validation d'une demande de révocation

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

- Le RCPS ;
- Le RL ;
- L'AE ;
- Un membre du LPTSP Board.

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

L'authentification de la demande de révocation se fait à travers la signature qualifiée du Formulaire [FR_REVOCATION].

4 Exigences opérationnelles sur le cycle de vie des Certificats

4.1 Demande de Certificat

4.1.1 Origine d'une demande de Certificat

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

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

La demande de Certificat est matérialisée par le Formulaire [FR_DEMANDE] disponible en ligne et transmis à l'AE, comportant :

- Les informations décrites dans la section 3.2.3 ;
- Les informations du Sujet ;
- Les CGU ;
- Les pièces justificatives [PJ1_DEMANDE] et de manière optionnelle [PJ2_DEMANDE] ;
- La signature qualifiée du RCPS ;
- La signature qualifiée du RL.

Dans le cas où le RCPS et/ou le RL ne dispose(nt) pas d'une signature qualifiée, celle-ci pourra être réalisée à l'aide d'une solution de signature qualifiée mise à disposition par l'AE.

4.1.3 Contrôle annuel des QSCD

L'AC surveille le statut de certification de ses QSCD en cours d'utilisation et vérifie chaque année que chacun de ses QSCD est reconnu en vérifiant la validité du Certificat Critères Communs émis pour le QSCD ou qu'il est toujours valide dans la liste de la Commission Européenne des QSCD notifiés par les États membres. Si la validité d'un QSCD concerné est expirée en raison d'une modification, l'AC conduira une enquête sur la cause de la modification auprès de l'État membre responsable et/ou de l'organisme de certification désigné. Si la certification du QSCD est expirée ou invalidée, l'AC prendra les mesures suivantes :

- Elle notifiera immédiatement l'ANSSI et l'organisme d'évaluation de la conformité ;

- Elle révoquera les Certificats d'authentification délivrés aux RCPS en fonction des résultats de l'enquête ;
- Elle informera tous les souscripteurs et UC concernés.

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 vérifie la cohérence des informations contenues dans le Formulaire [FR_DEMANDE] que lui a transmis le RCPS ;
- L'AE vérifie l'identité et la qualité du RCPS et du RL et l'identité de l'entité (cf. §3.2).
- L'AE doit valider les informations du Formulaire [FR_DEMANDE] en conformité avec la présente PC/DPC ;
- L'AE effectue une signature qualifiée du Formulaire [FR_DEMANDE] et des pièces jointes associées pour formaliser sa validation de la demande de Certificat ;
- L'AE transmet de manière sécurisée la demande de Certificat à l'AC.

4.2.2 Acceptation ou rejet de la demande

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

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

4.2.3 Durée d'établissement du Certificat

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

4.3 Délivrance du Certificat

4.3.1 Actions de l'AC concernant la délivrance du Certificat

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

- L'AC s'assure que la demande de Certificat provient de l'AE en vérifiant la signature qualifiée par l'AE de [FR_DEMANDE] et des pièces justificatives associées ;
- L'AC génère la Bi-clé du Sujet ;
- L'AC crée la requête de Certificat ;
- L'AC vérifie la signature de la requête de Certificat ;
- 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 Signataire contenues dans la demande ;
- L'AC génère ensuite le Certificat d'authentification utilisé pour transmettre de manière sécurisée au RCPS les données d'activation du Certificat d'Entité permettant au RCPS de

contrôler la Clé Privée du Certificat d'Entité, conformément aux informations fournies par le RCPS dans le Formulaire [FR_DEMANDE] ;

- L'AC associe la Clé Publique du Certificat d'authentification au Certificat d'Entité correspondant, afin d'assurer l'authentification du serveur métier qui accède au SCEQAD ;
- L'AC communique à l'AE dans un fichier texte :
  - Le Certificat d'Entité au format PEM ;
  - Le Certificat d'authentification associé au RCPS au format PEM ;
  - Les données d'activation du Certificat d'Entité chiffrées à l'aide de la clé publique du Certificat d'authentification associé au RCPS au format texte encodé en Base64 ;
  - L'URL du SCEQAD.
- L'AE transmet ensuite ce fichier texte au RCPS et au Demandeur du Certificat, le cas échéant.

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

Une fois généré, le RL est notifié de manière appropriée de la remise du Certificat au RCPS.

4.4 Acceptation du Certificat

4.4.1 Démarche d'acceptation du Certificat

Une fois le Certificat généré, un courriel de livraison contenant le fichier texte décrit à la section 4.3.1, est transmis au RCPS par l'AE. Cette étape est un prérequis obligatoire, avant toute utilisation dudit Certificat. L'absence de réclamation auprès de l'AE dans un délai de 24h après l'envoi du courriel de livraison vaut acceptation du Certificat.

4.4.2 Publication du Certificat

L'AC ne publie pas directement le Certificat. Le Certificat sera néanmoins présent dans les documents cachetés au cours d'une Transaction de Cachet.

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

L'AC informe l'AE de la délivrance du Certificat.

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 SCEQAD et doit respecter :

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

La Clé Privée du Sujet est gérée exclusivement par l'AC qui l'a créé, et qui l'utilise dans le cadre d'une Transaction de Cachet spécifique du SCEQAD. L'accès au SCEQAD nécessite d'une part la connaissance par le RCPS des données d'activation de la Clé Privée du Certificat du Sujet et d'autre part l'authentification forte du RCPS au travers du Certificat d'authentification transmis lors du processus de demande de Certificat d'Entité.

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

Voir section 9.5.

4.6 Renouvellement d'un Certificat

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

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

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

A l'expiration du Certificat, le RCPS doit demander un nouveau Certificat par la procédure de demande initiale.

4.8 Modification du Certificat

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

4.9 Révocation et suspension des Certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificat de Sujet

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

- Le RCPS n'a pas respecté, ou ne respecte plus, les obligations découlant de la présente PC/DPC et de l'accord de souscription ;
- Le Souscripteur n'a pas respecté, ou ne respecte plus, les obligations découlant de la présente PC/DPC et de l'accord de souscription ;
- Une erreur a été détectée dans la procédure d'enregistrement du Sujet ;
- L'inexactitude ou la caducité des informations du Certificat ou encore si ces informations portent atteintes aux droits d'un tiers ;
- Les informations contenues dans le Certificat ne sont plus exactes ;
- Le Souscripteur ou le RCPS demande la révocation ;
- Fin du contrat ;
- Le Souscripteur ne s'est pas acquitté, le cas échéant, du paiement relatif à l'émission du Certificat ;
- La Clé Privée du Sujet est compromise ou suspectée de l'être ;
- Les données d'activation permettant au RCPS d'activer la Clé Privée du Sujet sont suspectées de compromission, compromises, perdues ou volées ;

- L'AC est révoquée ;
- Le RCPS ne valide pas les informations contenues dans le Certificat qui lui sont présentées avant sa génération.

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 du Certificat d'un Sujet sont les suivantes :

- Le RCPS ;
- Le RL
- Un membre de l'AE ;
- Le LPTSP Board.

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 LPTSP 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 d'un Sujet

La demande de révocation d'un Certificat consiste, pour le Demandeur, à remplir le Formulaire [FR_REVOCATION].

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

- L'AE réceptionne et traite le Formulaire [FR_REVOCATION] ;
- 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 et s'assure de la destruction de la Clé Privée correspondante ;
- L'AE notifie le Demandeur, le RCPS et le RL de la révocation du Certificat.

4.9.3.2 Certificat d'une composante de l'IGC

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

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

4.9.4 Délai accordé 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 d'un 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 d'établissement des LCR est de 24 heures *a minima* et après chaque révocation.

4.9.8 Délai maximum de publication d'une LCR

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

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 sur plusieurs serveurs de publication, assurant ainsi une disponibilité en fonctionnement normal de 24h/24 et 7j/7.

4.10.3 Dispositifs optionnels

Sans objet.

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

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

En cas de fin de contrat, le Certificat est révoqué s'il n'est pas encore expiré, la Clé Privée est détruite et les habilitations du RCPS sont supprimées. Le Certificat d'authentification associé au Certificat de Cachet est révoqué. Le paramétrage du SCEQAD est également modifié pour supprimer le Certificat d'authentification du RCPS et, le cas échéant, l'adresse IP du serveur métier qui y accède.

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

Voir chapitre 4.1 de la [PGSC].

5.2 Mesures de sécurité procédurales

Voir chapitre 4.2 de la [PGSC].

En plus des rôles de confiance définis dans le chapitre 4.2.1 de la [PGSC], les rôles de confiance suivants sont définis :

- **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.

5.3 Mesures de sécurité vis-à-vis du personnel

Voir chapitre 4.3 de la [PGSC].

5.4 Procédure de constitution des données d'audit

Voir chapitre 4.4 de la [PGSC].

5.5 Archivage des données

Voir chapitre 4.5 de la [PGSC].

Les données archivées sont les suivantes :

- Toutes les versions de la présente PC/DPC ;
- Les accords contractuels entre l'AC et les Souscripteurs ;

- Les Formulaires de demande de Certificat contenant notamment la preuve d'acceptation des Conditions Générales d'Utilisation par les Souscripteurs et les éléments ayant permis de vérifier l'identité physique des RCPS ;
- Les Formulaires de demande de révocation ;
- 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.

Ces archives sont conservées pendant toute la durée de vie de l'AC à l'exception des journaux d'événements et des dossiers d'enregistrement qui sont conservés pendant 7 ans après l'expiration du Certificat.

5.6 Changement de clé d'AC

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

Une nouvelle clé d'AC requiert un nouveau Certificat d'AC.

Dès qu'une nouvelle Bi-clé d'AC est générée, seule la nouvelle Clé Privée doit être utilisée pour signer des Certificats. Le Certificat d'AC 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 LPTSP 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

Voir chapitre 4.6 de la [PGSC].

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 dernière LCR ayant une date de validité positionnée au 31 décembre 9999, 23h59m59s ;
- Prend toutes les mesures pour détruire sa Bi-clé et les éventuelles copies de secours ;
- Informe (par exemple par récépissé) tous les Sujets et les RCPS 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 deux (2) personnes ayant des rôles de confiance et en présence de témoins ne faisant pas parties des rôles de confiance, attestant de l'exactitude du procès-verbal. 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 l'AC 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 deux (2) personnes ayant des rôles de confiance dans l'AC, 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 conservée de manière sécurisée par le SCEQAD.

6.1.3 Transmission de la Clé Publique à l'AC

L'AC génère elle-même la 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).

Clés des Sujets : RSA (3072 bits)

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

Le LPTSP 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 6.2.11.1.

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

Les dispositifs cryptographiques utilisés pour la génération et la mise en œuvre des Bi-clés des Sujets sont des HSM certifiés satisfaisant aux exigences définies dans la section 6.2.11.2.

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 a été remise dans une carte à puce personnelle et protégée par un code PIN qu'ils ont eux-mêmes défini.

6.2.2.2 Clé Privée du Sujet

La Clé Privée d'un Sujet est protégée par des données d'activation générées par l'AC et demeurant sous le contrôle du RCPS afin que lui seul soit en mesure d'activer ou de faire activer la Clé Privée pour l'utiliser.

Le RCPS doit sous son contrôle faire générer un Certificat d'authentification qu'il transmettra dans le processus de demande à l'AC. Ce Certificat d'authentification doit contenir les informations suivantes au minimum :

`SubjectDN` du Certificat d'authentification

Attribut	Description	Obligatoire
`CN`	Nom et prénom du RCPS	Oui
`C`	Code pays du `SubjectDN` du Certificat d'Entité	Oui
`O`	Organisation du `SubjectDN` du Certificat d'Entité	Oui
`serialNumber`	Identifiant interne unique du Certificat d'authentification généré par l'AC	Oui
`OU`	Valeur du champ `OI` du `SubjectDN` du Certificat d'Entité	Oui

`SubjectAltName` du Certificat d'authentification
`rfc822Name`=[Adresse courriel du RCPS]

Les informations ci-dessus sont reprises des Formulaires [FR_DEMANDE] ou [FR_MOD_RCPS] le cas échéant.

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.

Les Clés Privées des Sujets ne sont pas sauvegardées.

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 peut être 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 l'AC.

6.2.7 Stockage de la Clé Privée dans un dispositif cryptographique

Le stockage des Clés Privées d'AC et des Clés Privées des Sujets est réalisé dans un HSM satisfaisant aux exigences définies dans la section 6.2.11.

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 avec les données d'activation sous le contrôle du RCPS.

6.2.9 Méthode de désactivation de la Clé Privée

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

L'AC peut également modifier les données d'activation de la Clé Privée du Sujet ou désactiver cette dernière via l'interface d'administration du SCEQAD.

L'AC peut également révoquer le Certificat d'authentification du RCPS.

6.2.10 Méthode de destruction d'une Clé Privée

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

La destruction de la Clé Privée d'un Sujet est de toute façon réalisée lorsque le Certificat correspondant est révoqué ou expiré.

6.2.11 Niveau de qualification des dispositifs cryptographiques

6.2.11.1 AC

Le dispositif cryptographique de l'AC est un HSM certifié Critères Communs EAL4.

6.2.11.2 Sujet

Le dispositif cryptographique des Sujets est un HSM certifié QSCD et présent sur la liste [EU_QSCD].

6.3 Autres aspects de la gestion des Bi-clés

6.3.1 Archivage des clés publiques

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

6.3.2 Durées de vie des Bi-clés et des Certificats

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

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

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

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

6.4.1.1 Clés d'AC

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 de témoins ne portant pas de rôles de confiance. 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.

6.4.1.2 Clés des Sujets

La génération des données d'activation d'accès de la Clé Privée associée au Certificat d'Entité d'un Souscripteur est réalisée par l'AC qui transmet ces informations de manière sécurisée au RCPS et qui restent sous son contrôle.

L'installation de ces données d'activation est faite à deux niveaux :

- Par le RCPS, dans son environnement pour permettre l'accès à la Clé Privée du Certificat d'Entité ;
- Par l'AC, en associant les données d'activation au Certificat d'Entité lors du paramétrage du SCEQAD.

6.4.2 Protection des données d'activation

6.4.2.1 Clés d'AC

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.

6.4.2.2 Clés des Sujets

Les moyens de protection des données d'Activation de la Clé Privée des Sujets sont laissés à l'appréciation du RCPS tant que ces données sont protégées en confidentialité et en intégrité.

6.4.3 Autres aspects liés aux données d'activation

Pour les données d'activation des Clés d'AC, 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

Voir chapitre 5.2 de la [PGSC].

6.6 Mesures de sécurité liées au développement des systèmes

Voir chapitre 5.3 de la [PGSC].

6.7 Mesures de sécurité réseau

Voir chapitre 5.4 de la [PGSC].

6.8 Horodatage / Système de datation

Voir chapitre 5.5 de la [PGSC].

7 Profils des Certificats, OCSP et des LCR

7.1 Certificat de l'AC

Le Certificat de l'AC est un Certificat au format X.509 v3 conforme aux exigences de la [RFC_5280] et qui respecte le profil [EN 319 412-1].

Champs de base :

Champ	Valeur
Version	2 (correspond à la v3 de X.509)
Numéro de série	Défini lors de la création
Emetteur	CN = Sunnystamp Root CA G2 OI = NTRFR-480622257 OU=0002 480622257 O = Lex Persona C = FR
Sujet	CN = Sunnystamp Legal Persons CA 1 OI = NTRFR-480622257 OU = 0002 480622257 O = Lex Persona C = FR
Validité	10 ans maximum

Champ	Valeur
Signature	RSAwithSHA512
Clé publique	RSA 4096 bits

Extensions :

Champ	Critique	Valeur
AuthorityInfoAccess	Non	id-ad-calssuers= *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 conformes aux exigences de la [RFC_5280] et qui respectent le profil [ETSI_319_412-3].

Champs de base :

Champ	Valeur
Version	2 (correspond à la v3 de X.509)
Numéro de série	Défini lors de la création
Émetteur	CN = Sunnystamp Legal Persons CA 1 OI = NTRFR-480622257 OU=0002 480622257 O = Lex Persona C = FR
Sujet	CN = Nom du Sujet C = Code du pays dans lequel le Sujet est établi O = Nom légal du Sujet OI = Identifiant unique du Sujet (structuré conformément à la section 5.1.4 de la norme [ETSI_319_412-1]). serialNumber = Identifiant unique généré par l'AC OU = Attribut utilisé pour préciser des informations sur le Sujet L = Attribut utilisé pour désigner la Ville dans laquelle le Sujet est enregistré

Champ	Valeur
Validité	3 ans maximum
Signature	RSAwithSHA256
Clé publique	3072 bits

Extensions :

Champ	Critique	Valeur
AuthorityInfoAccess	Non	id-ad-calssuers= *https://pki2.sunnystamp.com/certs/sunnystamp-legal-persons-ca1.cer* id-ad-ocsp= *http://ocsp2.sunnystamp.com/sunnystamp-legal-persons-ca-1*
AuthorityKeyIdentifier	Non	Empreinte SHA1 de la Clé Publique de l'émetteur
BasicConstraints	Oui	cA=false
CertificatePolicies	Non	OID=0.4.0.194112.1.3 OID=1.3.6.1.4.1.22542.100.1.1.3.2 URL=*https://pki2.sunnystamp.com/repository*
CRLDistributionPoints	Non	*http://pki2.sunnystamp.com/crls/sunnystamp-legal-persons-ca-1.crl* *http://pki3.sunnystamp.com/crls/sunnystamp-legal-persons-ca-1.crl*
Key Usage	Oui	digitalSignature, nonRepudiation
SubjectKeyIdentifier	Non	Empreinte SHA1 de la Clé Publique du sujet

Les `qcStatements` suivants sont présents.

esi4-qcStatement-1	id-etsi-qcs-QcCompliance
esi4-qcStatement-4	id-etsi-qcs-QcSSCD
esi4-qcStatement-6	id-etsi-qct-eseal

7.3 Profil des LCR

Champs de base :

Champ	Valeur
Version	1
Émetteur	CN = Sunnystamp Legal Persons CA1 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
ExpiredCertsOnCRL	Non	GeneralizedTime (X509) : <date de génération du Certificat d'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
Émetteur	CN = Sunnystamp Legal Persons CA1 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 3072 bits

Extensions :

Champ	Critique	Valeur
AuthorityKeyIdentifier	Non	

Champ	Critique	Valeur
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

Voir chapitre 6 de la [PGSC].

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 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

Voir chapitre 7.2 de la [PGSC].

9.2.2 Autres ressources

Voir chapitre 7.2 de la [PGSC].

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.

9.2.4 Confidentialité des données professionnelles

Voir chapitre 7.3 de la [PGSC].

Sont considérées comme confidentielles, toutes les informations énumérées dans le chapitre 7.3.1 de la [PGSC] ainsi que les dossiers d'enregistrement de l'AC.

Ne sont pas considérées comme confidentielles, toutes les informations publiées par l'AC.

9.3 Protection des données personnelles

Voir chapitre 7.4 de la [PGSC].

Les informations considérées comme personnelles sont les suivantes :

- Les informations personnelles liées au dossier du RCPS ;
- Les causes de révocation des Certificats des Sujets ;
- Les données d'enregistrement des Sujets qui n'apparaissent pas dans les Certificats.

9.4 Droits sur la propriété intellectuelle et industrielle

Voir chapitre 7.5 de la [PGSC].

9.5 Interprétations contractuelles et garanties

Voir chapitre 7.6 de la [PGSC].

9.5.1 AC

L'AC est Lex Persona (Goodflag).

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 ;
- Mentionner les obligations des sous-traitants dans des documents internes.

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.

9.5.2 AE

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.

9.5.3 RCPS et Souscripteur

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

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

La première partie mentionne :

- Le respect des obligations de l'accord qui concernent le Souscripteur ;
- Le respect des exigences indiquées dans la présente PC/DPC qui concernent le Souscripteur ;
- L'obligation pour le Souscripteur d'associer à tout Certificat un RCPS ;
- 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 RCPS, et de toute révocation ultérieure ainsi que de l'identité et des attributs spécifiques du Certificat ;
  - Du transfert de ces informations à des tiers aux mêmes conditions que celles définies dans la présente PC/DPC, en cas de fin de vie de l'AC ;
- Si et sous quelles conditions le Souscripteur demande et le Sujet consent à la publication du Certificat ;
- La confirmation que l'information contenue dans le Certificat est correcte ;
- Les obligations applicables au RCPS situées dans la deuxième partie.

La deuxième partie mentionne :

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

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

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

9.5.4 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.

9.6 Limite de garantie

Les limites des garanties offertes par l'AC sont décrites dans l'accord d'utilisation des Certificats.

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

9.7 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.

Également, 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.

9.8 Indemnités

Sans objet.

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

Voir chapitre 7.10 de la [PGSC].

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

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.

9.10 Notification individuelles et communications entre les participants

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

9.11 Amendements

Voir chapitre 7.12 de la [PGSC].

9.12 Dispositions concernant la résolution de conflits

Voir chapitre 7.13 de la [PGSC].

9.13 Juridictions compétentes

Voir chapitre 7.14 de la [PGSC].

9.14 Conformité aux législations et réglementations

Voir chapitre 7.15 de la [PGSC].

9.15 Dispositions diverses

Voir chapitre 7.16 de la [PGSC].

9.16 Autres dispositions

Voir chapitre 7.17 de la [PGSC].