# SunPKI

# Sunnystamp Natural Persons CA

# Politique de Certification / Déclaration des Pratiques de Certification

Version 1.12

Date d'entrée en vigueur : 11/10/2024



9 Av Maréchal Leclerc - 10120 ST ANDRE LES VERGERS - FRANCE
Tél. : +33 (0)3 25 43 90 78 – www.lex-persona.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

## 1.1 Présentation générale

Dans le cadre de son offre de services de confiance, Lex Persona fournit un service de génération de Certificats de signature électronique 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 Client pour une personne physique, appelée Signataire, qui sera le porteur du Certificat délivré. Ce Certificat permettra au Signataire de signer électroniquement, via le Service de signature, les documents que lui aura soumis le Client à travers une Transaction de signature.

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 des Certificats à des personnes physiques pouvant être rattachées ou non à une Entité Légale. Ces Certificats ont une durée de validité maximale de 1 heure et ne peuvent être utilisés que pour signer les documents de la Transaction de signature pour laquelle ils ont été spécialement créés.

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.

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

L'AC délivre six types de Certificats :

1. Les Certificats utilisés par ses répondeurs OCSP pour signer les réponses OCSP.
2. Les Certificats « ETSI LCP avec possibilité de révocation », conformes à la norme [ETSI_319_411-1] pour le niveau LCP avec possibilité de révocation.
3. Les Certificats « OPEN REG », pour lesquels la présente PC/DPC laisse l'Autorité d'Enregistrement libre de définir le processus d'enregistrement appliqué pour authentifier et vérifier l'identité des Signataires.
4. Les Certificats « FranceConnect », délivrés à la suite d'une authentification du Signataire par un Fournisseur d'identité proposé par FranceConnect (*https://franceconnect.gouv.fr*).

5. Les Certificats « MIE eIDAS » », conformes à la norme [ETSI_319_411-2] pour le niveau QCP-n-qscd, délivrés à la suite d'une authentification du Signataire en ayant recours à l'une ou l'autre des modalités suivantes :
    - Un moyen d'identification électronique notifié conforme aux exigences énoncées à l'article 8 du règlement eIDAS version 2 en ce qui concerne le niveau de garantie « élevé »[1] ;
    - Un moyen d'identification qui permet d'identifier une personne physique avec un degré de confiance élevé et dont la conformité est confirmée par un organisme d'évaluation de la conformité[2].
6. Les Certificats « ETSI LCP sans possibilité de révocation », conformes à la norme [ETSI_319_411-1] pour le niveau LCP sans possibilité de révocation.

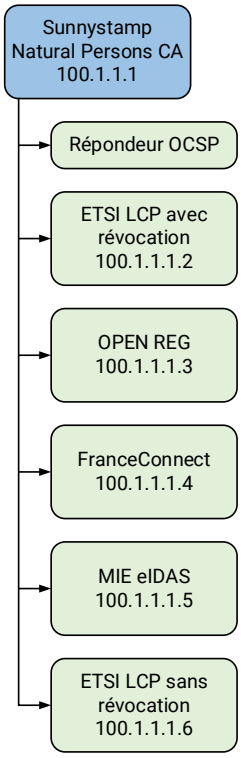


Figure 1 : hiérarchie des Certificats de l'AC

## 1.2 Identification du document

Le présent document est identifié sous l'OID suivant :

- **1.3.6.1.4.1.22542.100.1.1.1**.

Les politiques contenues dans ce document concernent les Certificats suivants :

- Les Certificats de répondeur OCSP ;

[1] Autrement dit, ces Certificats qualifiés sont émis conformément à l'article 24, paragraphe 1a, alinéa a, du règlement eIDAS v2.
[2] Autrement dit, ces Certificats qualifiés sont émis conformément à l'article 24, paragraphe 1a, alinéa c, du règlement eIDAS v2.

- Les Certificats **ETSI LCP avec possibilité de** révocation ayant pour OID **1.3.6.1.4.1.22542.100.1.1.1.2** ;
- Les Certificats **OPEN REG** ayant pour OID **1.3.6.1.4.1.22542.100.1.1.1.3** ;
- Les Certificats **FranceConnect** ayant pour OID **1.3.6.1.4.1.22542.100.1.1.1.4** ;
- Les Certificats **MIE eIDAS** ayant pour OID **1.3.6.1.4.1.22542.100.1.1.1.5** ;
- Les Certificats **ETSI LCP sans possibilité de révocation** ayant pour OID **1.3.6.1.4.1.22542.100.1.1.1.6**.

## 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 (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 Signataires ;
- Authentifier et transmettre à l'AC les demandes de création et de révocation de Certificats ;
- Archiver les données relatives à l'identification des Signataires.

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 Clients et des Signataires.

### 1.3.4 Client

Le Client est une entité légale qui a contracté avec Lex Persona et qui demande un Certificat pour un Signataire.

### 1.3.5 Signataire

Un Signataire 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 et utilisant cette Clé Privé pour signer des documents électroniques.

### 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 Signataires ;
- Les LCR ;
- Les Certificats de répondeurs OCSP.

#### 1.4.1.2 Certificat d'un Signataire

La Clé Privée associée à la Clé Publique du Certificat d'un Signataire est utilisée pour signer des documents électroniques au sein d'une Transaction de signature électronique.

#### 1.4.1.3 Certificat de répondeur OCSP

La Clé Privée associée à la Clé Publique d'un Certificat de répondeur OCSP est utilisée pour signer les Réponses OCSP récupérées au sein d'une Transaction de signature électronique.

### 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
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 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**

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 Signataire 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 propriétaire de la Clé Publique ;
- La Clé Publique ;
- Le(s) usage(s) autorisé(s) de la Clé Publique ;

- La durée de vie du Certificat ;
- L'identité de l'AC ;
- La signature du Certificat par 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 Signataire.

**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**

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 Signataire est rattaché, le cas échéant, et au nom de laquelle ce dernier utilise son Certificat.

**Fournisseur d'Identité**
Entité tierce chargée par l'AE d'identifier et d'authentifier les Signataires. Le Fournisseur d'identité, après avoir vérifié l'identité de l'Utilisateur, produit un Jeton d'identité attestant de cette identité. Ce Jeton est validé et exploité par l'AE de sorte que l'AC délivre le Certificat du Signataire sur la base des informations d'identité qu'il contient.

**FranceConnect**

FranceConnect est une solution d'identification créée par l'État français pour faciliter la connexion à différents services en ligne. Dans le cadre de la présente PC, pour les Certificats émis sous l'OID 1.3.6.1.4.1.22542.100.1.1.1.4**,** FranceConnect est utilisé par l'AE pour identifier le Signataire via le Fournisseur d'Identité qu'il aura choisi parmi ceux que lui aura proposé FranceConnect.

**Infrastructure de Gestion de Clés**

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 produites par un Fournisseur d'Identité à la suite de l'authentification d'une personne physique et contenant notamment les informations d'identité de cette personne (nom, prénom, etc.).

**Liste des Certificats Révoqués**

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

**Moyen d'authentification**

Moyen connu ou utilisable uniquement par le Signataire 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 courriel, OTP envoyé par SMS, etc.

**Politique de Certification**

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 Signataires et les Utilisateurs de Certificats.

**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.

**Service de signature**

Service de confiance de création de signatures et de délivrance de Certificats de signature générés « à la volée », mis à disposition par Lex Persona à ses clients pour leur permettre de faire signer des documents à des personnes physiques. Dans le cadre de la présente PC, le Service de signature est une composante de l'AE. Il identifie et authentifie les Signataires afin de leur délivrer un Certificat « à la volée » dédié à une Transaction de signature particulière. La Clé Privée du Signataire, associée au Certificat, est générée et utilisée de manière sécurisée par le Service de signature pour signer les documents de la Transaction de signature et est immédiatement détruite une fois les documents signés.

**Transaction de signature**

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

### 1.6.2 Acronymes

Les acronymes utilisés dans la présente PC/DPC sont les suivants (les définitions en langue anglaise sont formatées en italique) :

| | |
|---|---|
| **AC** | Autorité de Certification « Sunnystamp Natural Persons CA » |
| **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 |
| **OPEN REG** | Open Registration |
| **OTP** | One Time Password |
| **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 |
| **SMS** | Short Message Service |
| **UC** | Utilisateurs de Certificat |
| **UUID** | Universally Unique IDentifier |

## 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.<br>ANSSI, version 1.2 du 25 mars 2021.<br>*https://cyber.gouv.fr/sites/default/files/2022-09/eidas_delivrance-certificats-qualifies_v1.2_anssi.pdf* |
| [ETSI_319_411-1] | ETSI EN 319 411-1 V1.3.1 (2021-05)<br>Policy and security requirements for Trust Service Providers issuing certificates.<br>Part 1: General requirements.<br>*https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.03.01_60/en_31941101v010301p.pdf* |
| [ETSI_319_411-2] | ETSI EN 319 411-2 V2.4.1 (2021-11)<br>Policy and security requirements for Trust Service Providers issuing certificates.<br>Part 2: Requirements for trust service providers issuing EU qualified certificates.<br>*https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.03.01_60/en_31941102v020301p.pdf* |
| [ETSI_319_412-1] | ETSI EN 319 412-1 V1.4.4 (2021-05)<br>Certificate Profiles.<br>Part 1: Overview and common data structures.<br>*https://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.04.04_60/en_31941201v010404p.pdf* |
| [ETSI_319_412-2] | ETSI EN 319 412-2 V2.2.1 (2020-07)<br>Certificate Profiles.<br>Part 2: Certificate profile for certificates issued to natural persons.<br>*https://www.etsi.org/deliver/etsi_en/319400_319499/31941202/02.02.01_60/en_31941202v020201p.pdf* |
| [PKCS#10] | PKCS #10: Certification Request Syntax Specification Version 1.7.<br>*https://tools.ietf.org/html/rfc2986* |
| [RFC_5280] | Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.<br>*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.
*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 Liste des dispositifs qualifiés de création de signature et de création de cachet

[EU_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 à l'adresse *https://pki2.sunnystamp.com/repository* les informations suivantes :

- La PC/DPC ;
- La Déclaration d'IGC ;
- Les Certificats X.509 de l'AC « Sunnystamp Natural Persons CA » et de l'AC racine « Sunnystamp Root CA G2 » ainsi que leur empreinte de hachage ;

L'AC publie également en ligne 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* ;

L'AC publie également 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*.

Les CGU du Service de signature sont publiées et consultables par les Signataires depuis l'environnement propre au Client du Service de signature.

## 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, les CGU et la Déclaration d'IGC sont publiées 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 Signataire est identifié dans le champ `subject`.

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`.

L'attribut `OU` doit contenir l'identifiant de la Transaction de signature.

Les attributs contenus dans le champ `subject` des Certificats émis par l'AC dépendent du type de Certificat.

#### 3.1.1.1 Certificats ETSI LCP avec ou sans possibilité de révocation

| Attribut | Description | Obligatoire ? |
|---|---|---|
| serialNumber | Identifiant interne unique du Certificat du Signataire | Oui |
| CN | Prénom usuel suivi d'un espace et du nom de l'état civil ou, le cas échéant, du nom d'usage du Signataire | Oui |
| GN | Prénom usuel ou prénoms de l'état civil du Signataire | Oui |
| SN | Nom de l'état civil ou nom d'usage du Signataire | Oui |
| OU | Identifiant de la Transaction de signature | Oui |
| C | Code ISO 3166 du pays qui a délivré la pièce d'identité du Signataire | Oui |

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

#### 3.1.1.2 Certificats OPEN REG

| Attribut | Description | Obligatoire ? |
|---|---|---|
| serialNumber | Identifiant interne unique du Certificat du Signataire | Oui |
| CN | Prénom(s) suivi d'un espace et du nom de l'état civil ou, le cas échéant, du nom d'usage du Signataire | Oui |
| GN | Prénom usuel ou prénoms de l'état civil du Signataire | Oui |
| SN | Nom de l'état civil ou nom d'usage du Signataire | Oui |
| T | Fonction du Signataire dans l'Entité Légale à laquelle il est rattaché | Non |
| OU | Identifiant de la Transaction de signature | Oui |
| OI | Identifiant unique de l'Entité Légale à laquelle le Signataire est rattaché (structuré conformément à la section 5.1.4 de la norme [ETSI_319_412-1]). | Non |
| O | Nom de l'Entité Légale à laquelle le Signataire est rattaché | Non |
| C | Code pays associé au Signataire. | Non |

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

#### 3.1.1.3 Certificats FranceConnect

| Attribut | Description | Obligatoire ? |
|---|---|---|
| serialNumber | Identifiant interne unique du Certificat du Signataire | Oui |
| CN | Prénom(s) suivi d'un espace et du nom de naissance ou, le cas échéant, du nom d'usage du Signataire | Oui |
| GN | Prénom usuel ou prénoms de l'état civil du Signataire | Oui |
| SN | Nom de naissance (état civil) ou nom d'usage du Signataire | Oui |
| OU | Identifiant de la Transaction de signature | Oui |
| C | Pays de naissance (état civil) | Oui |

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

#### 3.1.1.4 Certificats MIE eIDAS

| Attribut | Description | Obligatoire ? |
|---|---|---|
| serialNumber | Identifiant interne unique du Certificat du Signataire | Oui |
| CN | Prénom(s) suivi d'un espace et du nom de naissance ou, le cas échéant, du nom d'usage du Signataire | Oui |
| GN | Prénom usuel ou prénoms de l'état civil du Signataire | Oui |
| SN | Nom de naissance (état civil) ou nom d'usage du Signataire | Oui |
| T | Fonction du Signataire dans l'Entité Légale à laquelle il est rattaché | Non |
| OU | Identifiant de la Transaction de signature | Oui |
| OU | Nom de la sous-organisation, département ou service de l'Entité Légale auquel le Signataire est rattaché | Non |
| OI | Identifiant unique de l'Entité Légale à laquelle le Signataire est rattaché (structuré conformément à la section 5.1.4 de la norme [ETSI_319_412-1]). | Non |
| O | Nom de l'Entité Légale à laquelle le Signataire est rattaché | Non |
| C | Pays de naissance (état civil) | Oui |

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

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

### 3.1.2 Nécessité d'utilisation de noms explicites

Le contenu des attributs `CN`, `GN`, `SN` et `C` du champ `subject` du Certificat permet de garantir l'utilisation d'un nom explicite permettant d'identifier le Signataire.

### 3.1.3 Anonymisation et pseudonymisation des Signataires

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 les attributs SN et GN 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 Clients 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 Signataire ou 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 Signataire est générée et stockée de manière sécurisée par le Service de signature à la suite de l'identification et de l'authentification du Signataire 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.

En aucun cas Lex Persona ne pourra utiliser cette Clé Privée pour son propre usage ou pour le compte d'une autre personne que le Signataire.

### 3.2.2 Validation de l'identité d'une Entité Légale

Si le Signataire 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 Signataire est effectivement rattaché à cette entité. Ces vérifications sont réalisées lors de l'enregistrement de la personne physique se réclamant du rattachement (cf. section 3.2.3.2).

### 3.2.3 Validation de l'identité d'un Signataire

#### 3.2.3.1 Signataire non rattaché à une Entité Légale

<u>Pour les Certificats ETSI LCP avec ou sans possibilité révocation ayant respectivement comme OID 1.3.6.1.4.1.22542.100.1.1.1.2 ou 1.3.6.1.4.1.22542.100.1.1.1.6 :</u>

- L'AE est en charge de la vérification de l'identité du Signataire qui doit obligatoirement fournir un document officiel d'identité (carte nationale d'identité, passeport ou titre de séjour) en cours de validité avec photographie comportant ses nom, prénom(s), date et lieu de naissance.
- L'AE doit également vérifier que le Signataire est bien le propriétaire du numéro de téléphone portable communiqué par le Client.

Pour les Certificats OPEN REG ayant comme OID 1.3.6.1.4.1.22542.100.1.1.1.3 :

- L'AE délègue au Client la vérification de l'identité du Signataire, et le Client doit documenter d'une manière appropriée la procédure de vérification effectuée et conserver la traçabilité du respect de cette procédure.

Pour les Certificats FranceConnect ayant comme OID 1.3.6.1.4.1.22542.100.1.1.1.4 :

- L'AE délègue la validation de l'identité du Signataire à FranceConnect et récupère les informations d'identités suivantes du Signataire :
  - Nom de naissance ;
  - Prénom(s) ;
  - Date de naissance ;
  - Pays de naissance.

Pour les Certificats MIE eIDAS ayant comme OID 1.3.6.1.4.1.22542.100.1.1.1.5 :

- L'AE délègue la validation de l'identité du Signataire au moyen d'identification électronique, et récupère les informations d'identités suivantes du Signataire :
  - Nom de naissance ;
  - Prénom(s) ;
  - Date de naissance ;
  - Pays de naissance.
- L'AE s'assure que les MIE auxquels elle délègue la validation d'identité répondent bien aux exigences de l'article 24, paragraphe 1, alinéa a ou c, du Règlement eIDAS.

#### 3.2.3.2 Signataire rattaché à une Entité Légale

Pour les Certificats ETSI LCP avec ou sans possibilité de révocation ayant respectivement comme OID 1.3.6.1.4.1.22542.100.1.1.1.2 ou 1.3.6.1.4.1.22542.100.1.1.1.6 :

- Le Signataire ne peut pas être rattaché à une Entité Légale.

Pour les Certificats OPEN REG ayant comme OID 1.3.6.1.4.1.22542.100.1.1.1.3 :

- L'AE délègue au Client la vérification de l'identité du Signataire, et le Client doit documenter d'une manière appropriée la procédure de vérification effectuée et conserver la traçabilité du respect de cette procédure.
- L'AE délègue également au Client la vérification de l'existence de l'Entité Légale et le rattachement du Signataire à ladite Entité Légale, et le Client doit documenter d'une manière appropriée la procédure de vérification effectuée et conserver la traçabilité du respect de cette procédure.

Pour les Certificats FranceConnect ayant comme OID 1.3.6.1.4.1.22542.100.1.1.1.4 :

- Le Signataire ne peut pas être rattaché à une Entité Légale.

Pour les Certificats MIE eIDAS ayant comme OID 1.3.6.1.4.1.22542.100.1.1.1.5 :

- Le Signataire peut être rattaché à une Entité Légale si le moyen d'identification électronique le permet et que l'identité qu'il porte contient les informations relatives à ce rattachement.

#### 3.2.3.3 Archivage des informations de validation

L'AE doit archiver toutes les informations utilisées pour vérifier l'identité du Signataire, et, le cas échéant, tout attribut spécifique du Signataire, 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 Signataire

Toutes les informations présentes[3] 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 demandeur

Pour les Certificats ETSI LCP avec ou sans possibilité de révocation :

- Le Signataire ne peut pas être rattaché à une Entité Légale.

Pour les Certificats OPEN REG :

- Cf. section 3.2.3.2.

Pour les Certificats FranceConnect :

- Le Signataire ne peut pas être rattaché à une Entité Légale.

Pour les Certificats MIE eIDAS :

- Si rattachement à une Entité légale il y a, celle-ci est automatiquement validée par le moyen d'identification électronique.

### 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] Autrement dit, l'AE n'est pas tenue de vérifier les informations relatives aux attributs optionnels si ceux-ci n'apparaissent pas dans le Certificat émis.

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

### 3.3.1 Identification et validation d'un renouvellement courant

Si le Signataire a déjà demandé un Certificat à l'AE, alors le Signataire 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 Signataire soient toujours valides.

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

Pour les Certificats ETSI LCP avec ou sans possibilité de révocation :

- Le Signataire doit s'authentifier avec au moins un moyen d'authentification, devant être associé au numéro de téléphone portable enregistré par l'AE lors de la vérification initiale de son identité.

Pour les Certificats OPEN REG :

- L'AE doit décrire la manière dont elle procède pour authentifier le Signataire.

Pour les Certificats FranceConnect :

- Le Signataire doit s'authentifier via FranceConnect, à chaque Transaction de signature, pour obtenir un nouveau Certificat.

Pour les Certificats MIE eIDAS :

- Le Signataire doit s'authentifier via son moyen d'identification électronique, à chaque Transaction de signature, pour obtenir un nouveau Certificat.

### 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 est automatiquement demandée à l'Autorité de Certification par le Service de signature dès lors que le Signataire annule la Transaction de signature pour laquelle le Certificat a été déjà spécialement créé. Cette annulation se produit lorsque les 2 conditions suivantes sont réunies :

- L'application de signature demande pour le signataire concerné la génération d'un Certificat OPEN REG (OID 1.3.6.1.4.1.22542.100.1.1.1.3) ou ETSI LCP avec possibilité de révocation (OID 1.3.6.1.4.1.22542.100.1.1.1.2) ;

- Une fois le Certificat généré : le Signataire refuse de signer les documents de la Transaction de signature ou le Signataire ne valide pas les informations contenues dans son Certificat qui lui sont présentées dans la page de signature.

Pour les autres OID, aucune révocation n'est possible :

- FranceConnect (OID 1.3.6.1.4.1.22542.100.1.1.1.4) ;
- MIE eIDAS (OID 1.3.6.1.4.1.22542.100.1.1.1.5) ;
- ETSI LCP sans possibilité de révocation (OID 1.3.6.1.4.1.22542.100.1.1.1.6).

# 4 Exigences opérationnelles sur le cycle de vie des Certificats

## 4.1 Demande de Certificat

### 4.1.1 Origine d'une demande de Certificat

La demande de Certificat provient du besoin par le Signataire de signer, au sein d'une Transaction de signature, les documents que lui a soumis le Client.

### 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 Client, et le cas échéant le Signataire, doivent fournir à l'AE les différentes informations requises dans la section 3.2.3 en garantissant leur exactitude ;
- Le Signataire doit enregistrer auprès de l'AE :
  - Pour un Certificat OPEN REG : au moins 1 moyen d'authentification ;
  - Pour un Certificat ETSI LCP avec ou sans possibilité de révocation : son numéro de téléphone portable qui sera utilisé comme un moyen d'authentification.

  Ces moyens d'authentification permettront à l'AE de l'authentifier ultérieurement pour lui permettre de demander un nouveau Certificat (cf. section 3.3.1) sans avoir besoin que son identité soit de nouveau vérifiée par l'AE.
- Le Signataire doit approuver explicitement les CGU ;
- 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.

### 4.1.3 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 désactivera immédiatement les Pages de Consentement qui mettent en œuvre le QSCD en fonction des résultats de l'enquête ;
- Elle informera les Utilisateurs 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 s'assure que le Signataire a bien lu et accepté les CGU ;
- L'AE valide les différentes informations requises dans la section 3.2.3 ;
- L'AE vérifie et enregistre, le cas échéant, les moyens d'authentification du Signataire qui lui permettront de s'authentifier ultérieurement auprès de l'AE sans avoir besoin de retransmettre à l'AE les informations décrites dans la section 3.2.3.

### 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 Signataire 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 :

- Le Service de signature génère la bi-clé du Signataire ;
- Le Service de signature crée la requête de Certificat après la validation par l'AE ;
- 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 Signataire contenues dans la demande.

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

L'AC ne notifie pas le Signataire de la délivrance de son Certificat.

## 4.4 Acceptation du Certificat

### 4.4.1 Démarche d'acceptation du Certificat

Une fois le Certificat généré, ou juste avant sa création, les informations du Signataire, qui sont ou seront contenues dans le champ `subject` du Certificat, sont portées à la connaissance du Signataire afin qu'il puisse les accepter explicitement avant de déclencher la création ou l'utilisation de la Clé Privée associé à son Certificat pour signer les documents de la Transaction de signature.

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

### 4.4.2 Publication du Certificat

L'AC ne publie pas directement le Certificat qui est publié via les documents signés au cours de la Transaction de signature.

### 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 Signataire

L'utilisation par le Signataire, 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 ;
- Les CGU ;
- Toute obligation supplémentaire éventuellement imposée au Signataire par le Client, ne remettant pas en cause les clauses précédentes.

La Clé Privée du Signataire est gérée exclusivement par le Service de signature qui la crée, l'utilise et la détruit dans le cadre d'une Transaction de signature spécifique.

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

Voir section 9.6.4.

## 4.6 Renouvellement d'un Certificat

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

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

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

## 4.8 Modification du Certificat

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

## 4.9 Révocation et suspension des Certificats

Cette section ne s'applique qu'aux Certificats OPEN REG et ETSI LCP avec possibilité de révocation.

### 4.9.1 Causes possibles d'une révocation

#### 4.9.1.1 Certificat d'un Signataire

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

- Le Signataire refuse de signer les documents de la Transaction de signature ;
- Le Signataire ne valide pas les informations contenues dans son Certificat qui lui sont présentées dans la page de signature ;
- La révocation du Certificat de l'AC ayant généré le Certificat d'un Signataire.

#### 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) ;
- Rupture cryptographique des algorithmes utilisés pour générer la Clé Privée de l'AC ;
- Cessation d'activité de l'entité opérant la composante.

### 4.9.2 Origine d'une demande de révocation

#### 4.9.2.1 Certificat d'un Signataire

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

- Le Signataire, en refusant de signer les documents de la Transaction de signature ou en ne validant pas les informations contenues dans son Certificat qui lui sont présentées dans la page de signature.

#### 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 Signataire

Une demande de révocation peut être transmise à l'AE par le Signataire ou le Client 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 demande à l'AC de procéder à la révocation du Certificat ;
- L'AC révoque le Certificat de manière définitive.

#### 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://cyber.gouv.fr/contacter-lanssi* ;
- L'ensemble des Clients et des Signataires 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 d'un Signataire

Une demande de révocation du Certificat d'un Signataire 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 le Certificat d'un Signataire, 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 le Certificat d'une 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 Client et l'AC

La relation entre le Client 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 Client et l'AC.

## 4.12 Séquestre de clé et recouvrement

Les Clés Privées de l'AC, des répondeurs OCSP et des Signataires 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].

## 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 Clients ;
- Les dossiers d'enregistrement, incluant notamment la preuve d'acceptation des CGU par les Signataires, et :
  - Une copie du rapport de vérification de la pièce d'identité des Signataires dans le cas des Certificats ETSI LCP,
  - Le jeton OpenID Connect d'authentification des Signataires au service FranceConnect dans le cas des Certificats FranceConnect,
  - Le jeton OpenID Connect d'authentification des Signataires au MIE eIDAS dans le cas des Certificats MIE eIDAS ;
- 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.

## 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 très courte, la bi-clé de l'AC sera par conséquent renouvelé au plus tard 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 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 Signataires 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 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 Signataire

Pour les Certificats ETSI LCP avec ou sans possibilité de révocation, FranceConnect et MIE eIDAS :

La génération de la bi-clé d'un Signataire 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 deux (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 Signataires. 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.

Pour les Certificats OPEN REG :

La génération de la bi-clé d'un Signataire est réalisée par le Service de signature dans un conteneur sécurisé de manière à garantir l'intégrité, la confidentialité et le contrôle exclusif de sa Clé Privée.

### 6.1.2 Transmission de la clé privée à son propriétaire

La Clé Privée d'un Signataire n'est pas transmise à son propriétaire. Elle est générée et conservée de manière sécurisée par le Service de signature.

### 6.1.3 Transmission de la clé publique à l'AC

La Clé Publique d'un Signataire est transmise par le Service de signature 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 Signataires (hors OID 1.3.6.1.4.1.22542.100.1.1.1.5) : RSA 2048 bits ou supérieur.

Clés des Signataires pour l'OID 1.3.6.1.4.1.22542.100.1.1.1.5 : RSA 3072 bits ou supérieur.

### 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 Signataires 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 sécurisés 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 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 Signataire

La Clé Privée d'un Signataire 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 Signataires 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 Signataires 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 Signataire, associée à un Certificat ETSI LCP, 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 Signataire, 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 d'AC et des Clés Privées associées aux Certificats ETSI LCP 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 Signataire

L'activation de la Clé Privée d'un Signataire est réalisée par le Service de signature, après l'authentification du Signataire 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.

### 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 Signataire est réalisée lorsque le Certificat correspondant est révoqué ou 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 Signataire

Pour les Certificats ETSI LCP avec ou sans possibilité de révocation, FranceConnect et MIE eIDAS, le dispositif cryptographique des Signataires est un HSM certifié FIPS 140-2 level 3, 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 Signataires ont une durée de vie maximale de 1 heure. 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 Signataire ainsi que de la taille et du nombre de fichiers à signer dans la Transaction de signature.

## 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

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 [ETSI_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<br>OI = NTRFR-480622257<br>OU=0002 480622257<br>O = Lex Persona<br>C = FR |
| Sujet | CN = Sunnystamp Natural Persons CA<br>OI = NTRFR-480622257<br>OU = 0002 480622257<br>O = Lex Persona<br>C = FR |
| Validité | 10 ans maximum |
| Signature | RSAwithSHA512 |
| Clé publique | RSA 4096 bits |

Extensions :

| Champ | Critique | Valeur |
|---|---|---|
| AuthorityInfoAccess | Non | id-ad-caIssuers=<br>*https://pki2.sunnystamp.com/certs/sunnystamp-root-ca-g2.cer* |
| AuthorityKeyIdentifier | Non | |
| BasicConstraints | Oui | CA=true<br>pathLenConstraint=0 |
| CertificatePolicies | Non | OID=2.5.29.32.0 |
| CRLDistributionPoints | Non | *http://pki2.sunnystamp.com/crls/sunnystamp-root-ca-g2.crl*<br>*http://pki3.sunnystamp.com/crls/sunnystamp-root-ca-g2.crl* |
| SubjectKeyIdentifier | Non | |
| Key Usage | Oui | keyCertSign(5), cRLSign(6) |

## 7.2 Certificat d'un Signataire

Les Certificats des Signataires sont des Certificats au format X.509 v3 conforme aux exigences de la [RFC 5280] et qui respectent le profil [ETSI_319_412-2] à l'exception de l'attribut `C` (Country) qui ne sera pas nécessairement présent dans le champ `subject` des Certificats OPEN REG.

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 Natural Persons CA<br>OI = NTRFR-480622257<br>OU=0002 480622257<br>O = Lex Persona<br>C = FR |
| Sujet | Voir 3.1.1 |
| Validité | 1 heure maximum |
| Signature | RSAwithSHA256 |
| Clé publique | Tous OID sauf 1.3.6.1.4.1.22542.100.1.1.1.5 : 2048 bits<br><br>OID 1.3.6.1.4.1.22542.100.1.1.1.5 : 3072 bits |

Extensions :

| Champ | Critique | Valeur |
|---|---|---|
| AuthorityInfoAccess | Non | id-ad-caIssuers=<br>*https://pki2.sunnystamp.com/certs/sunnystamp-natural-persons-ca.cer*<br>id-ad-ocsp=<br>*http://ocsp2.sunnystamp.com/sunnystamp-natural-persons-ca* |
| AuthorityKeyIdentifier | Non | |
| BasicConstraints | Oui | cA=false |
| CertificatePolicies | Non | Pour les Certificats ETSI LCP avec possibilité de révocation :<br>OID=0.4.0.2042.1.3<br>OID=1.3.6.1.4.1.22542.100.1.1.1.2<br>URL=*https://pki2.sunnystamp.com/repository*<br><br>Pour les Certificats OPEN REG :<br>OID=1.3.6.1.4.1.22542.100.1.1.1.3<br>URL=*https://pki2.sunnystamp.com/repository*<br><br>Pour les Certificats FranceConnect :<br>OID=1.3.6.1.4.1.22542.100.1.1.1.4<br>URL=*https://pki2.sunnystamp.com/repository*<br><br>Pour les Certificats MIE eIDAS :<br>OID=0.4.0.194112.1.2<br>OID= 1.3.6.1.4.1.22542.100.1.1.1.5<br>URL=*https://pki2.sunnystamp.com/repository*<br><br>Pour les Certificats ETSI LCP sans possibilité de révocation :<br>OID=0.4.0.2042.1.3<br>OID=1.3.6.1.4.1.22542.100.1.1.1.6<br>URL=*https://pki2.sunnystamp.com/repository* |
| CRLDistributionPoints | Non | *http://pki2.sunnystamp.com/crls/sunnystamp-natural-persons-ca.crl*<br>*http://pki3.sunnystamp.com/crls/sunnystamp-natural-persons-ca.crl* |
| Key Usage | Oui | nonRepudiation |
| SubjectKeyIdentifier | Non | |

Pour les Certificats MIE eIDAS, les `qcStatements` suivants sont présents.

| | |
|---|---|
| esi4-qcStatement-1 | id-etsi-qcs-QcCompliance |
| esi4-qcStatement-6 | id-etsi-qct-esign |

| | |
|---|---|
| esi4-qcStatement-4 | id-etsi-qcs-QcSSCD |

## 7.3 Profil des LCR

Champs de base :

| Champ | Valeur |
|---|---|
| Version | 1 |
| Émetteur | CN = Sunnystamp Natural Persons CA<br>OI = NTRFR-480622257<br>OU=0002 480622257<br>O = Lex Persona<br>C = FR |
| Validité | 7 jours |
| Signature | RSAwithSHA512 |

Extensions :

| Champ | Critique | Valeur |
|---|---|---|
| AuthorityKeyIdentifier | Non | |
| CRLNumber | Non | Défini par l'AC |
| ExpiredCertsOnCRL | Non | GeneralizedTime (X509) : 20/03/2023 |

## 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 Natural Persons CA<br>OI = NTRFR-480622257<br>OU=0002 480622257<br>O = Lex Persona |

| Champ | Valeur |
|---|---|
| | C = FR |
| Sujet | CN = OCSP Responder $X (où X est un nombre entier)<br>serialNumber = Identifiant unique généré par l'AC<br>OI = NTRFR-480622257<br>OU = 0002 480622257<br>O = Lex Persona<br>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 | |
| ArchiveCutoff | Non | Date de création du 1er Certificat qualifié produit |

# 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 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

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 causes de révocation des Certificats des Signataires ;
- Les données d'enregistrement des Signataires 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.

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 Clients et des UC si :

- Les informations d'un Signataire présentes dans un Certificat ne correspondent pas à celles transmises par le Client 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 Signataires ;
- 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 Signataire ;

- 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 Signataire

Les obligations du Signataire sont les suivantes :

- Respecter les exigences indiquées dans la présente PC/DPC qui concernent le Signataire ;
- Respecter les modalités d'usages précisées dans le chapitre 4.5 de la PC ;
- Fournir des informations correctes à l'AE lors de la phase d'enregistrement ;
- Confirmer l'exactitude des informations contenues, ou qui seront contenues, dans son Certificat ;
- Informer l'AE de toute modification des informations contenues dans son Certificat.
- Accepter les CGU ;
- Protéger ses moyens d'authentification ;
- Accepter l'accord relatif à l'utilisation d'un dispositif cryptographique satisfaisant aux exigences de la section 6.2.11.

### 9.5.4 Client

Les obligations du Client sont les suivantes :

- Respecter les obligations qui lui incombent et qui sont décrites dans l'accord de souscription ;
- Respecter les modalités d'usages précisées dans le chapitre 1.4 de la PC ;
- Fournir des informations correctes à l'AE lors de la phase d'enregistrement ;
- Informer l'AE de toute modification des informations contenues dans le Certificat.

### 9.5.5 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 Signataire 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 Client.

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 Client sur les 3 derniers mois et ce dans le respect et les limites de la loi applicable. Sauf prescription légale contraire, toute action du Client 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].