# POLITIQUE DE CERTIFICATION

# AUTORITÉ DE CERTIFICATION
# SFR CERTIFICAT CLIENT
## *(certificat de signature en ligne)*

# Récapitulatif des éditions

| Version | Date | Nom du rédacteur | Nature de la modification |
|---|---|---|---|
| 0.1 | 08/08/13 | Christian BOUVIER | Rédaction initiale |
| | | | |
| | | | |
| | | | |

# Table des matières

# 1 Introduction

## 1.1 Présentation générale de la politique de certification

La *Politique de Certification* (P.C.) a une grande importance pour établir la confiance à l'égard d'un certificat.

L'attention du lecteur est attirée sur le fait que la compréhension de la présente P.C. suppose que le lecteur soit familiarisé avec les notions liées à la technologie des Infrastructures à Clés Publiques (I.G.C.).

Le présent document constitue la politique de certification de SFR agissant en tant qu'Autorité de Certification ***SFR AC Certificat Client*** ci-après dénommée « A.C. **»**, délivrant des certificats de signature électronique « **simple** » dans le cadre de la signature électronique en ligne des mandats de prélèvement **SEPA**. Il expose les pratiques appliquées par SFR et par les différentes entités de l'I.G.C. pour l'émission, la gestion du cycle de vie et de la publication des certificats.

## 1.2 Identification de la P.C.

Le présent document est identifié par l'O.I.D n° 1.2.250.1.35.25.2.1.2.10.1.

La déclaration des pratiques de certification (D.P.C) est identifiée par l'O.I.D n°1.2.250.1.35.25.2.1.2.11.1.

Ces documents sont désignés sous les noms de P.C. « P.C. *SFR AC Certificat Client – Certificat de signature en ligne* » et de D.P.C. de « D.P.C. *SFR AC Certificat Client – Certificat de signature en ligne* ».

## 1.3 Les entités intervenant dans l'I.G.C.

Dans le processus de création, de gestion et de publication d'un certificat de signature électronique, plusieurs entités interviennent :

**Autorité de Certification Racine (A.C.R. ou A.C. Root)**
Une relation de confiance hiérarchique peut lier des A.C. successives. Une Autorité est alors à la base de toutes les A.C., on l'appelle « Autorité de Certification Racine ». Elle est prise comme référence par la communauté de porteurs des certificats émis par ces A.C.

**Autorité de certification (A.C.)**
L'Autorité de Certification crée les certificats pour chaque demandeur en respectant le processus de certification (après vérification par l'Autorité d'Enregistrement de la demande de certificat et des données propres à chaque demandeur). L'Autorité de Certification réalise les révocations, elle met à jour et publie une liste de certificats révoqués. L'Autorité de Certification est responsable de la publication des certificats qu'elle génère. Elle est aussi responsable de tous les processus de gestion de vie des certificats qu'elle émet dans le cadre du respect des conditions dans le présent document.

SFR intervenant en qualité d'A.C. peut déléguer tout ou partie de ses services, en fonction de sa P.C., à différents acteurs tels qu'une autorité d'enregistrement.

**Autorité d'enregistrement (A.E.)**
L'Autorité d'Enregistrement est l'interface entre le demandeur de certificat et l'Autorité de Certification. Elle vérifie les données propres au demandeur de certificat ainsi que le respect des contraintes liées à l'usage d'un certificat, conformément à la Politique de Certification. Elle transmet ensuite ces données à l'Autorité de Certification qui génère le certificat.

L'A.E. agit conformément à la politique de certification et aux pratiques de certification définies par l'A.C.

Cette mission sera assurée par les distributeurs agréés pour la mise en place de la dématérialisation des actes en point de vente.

**Opérateur de Certification (O.C.)**
L'Opérateur de Certification (O.C.) assure la fourniture et la gestion du cycle de vie des certificats. Il met en œuvre une plate-forme opérationnelle, fonctionnelle, sécurisée, dans le respect des exigences énoncées dans la présente Politique de Certification (P.C.) et dont les modalités de mises en œuvre sont détaillées dans la Déclaration des Pratiques de Certification (D.P.C.).

**Utilisateur de certificat**
L'utilisateur est celui qui valide l'utilisation d'un certificat électronique dans le cadre d'opérations d'authentification, de signature électronique ou de chiffrement.. Il agit pour son propre compte. Le certificat ne lui est pas remis.

**Porteur de certificat**
Il s'agit de la personne pour laquelle le certificat a été émis. Son identité est reportée dans les champs d'identification du certificat électronique émis par l'A.C.

# 1.4 Usages des certificats

## 1.4.1 Domaines d'utilisation applicables

L'Autorité de Certification *SFR AC Certificat Client - Signature en ligne* distribue des certificats électroniques aux clients de SFR afin de leur permettre de signer électroniquement tout type de document et, en particulier les mandats de prélèvements SEPA depuis les services web en ligne de SFR.

## 1.4.2 Domaines d'utilisation interdits

Les domaines d'utilisation qui ne sont pas spécifiés sont interdits.

# 1.5 Gestion de la P.C

## 1.5.1 Entité gérant la P.C

LA SOCIÉTÉ FRANÇAISE DU RADIOTÉLÉPHONE (SFR) est responsable de cette P.C.

**LA SOCIÉTÉ FRANÇAISE DU RADIOTÉLÉPHONE (SFR)**

**42, avenue de Friedland**

**75008 Paris**

Ci-après dénommée « **SFR** ».

## 1.5.2 Point de contact

Toute demande relative à la Politique de Certification doit être adressée au Responsable de l'A.C à la Direction de la Fraude et de la Sécurité de l'Information de SFR.

Ses coordonnées sont :

**SFR**

**Direction Fraude et Sécurité de l'Information**

**1, place Carpeaux**

**92915 Paris La Défense cedex**

### 1.5.3 Entité déterminant la conformité d'une D.P.C. à la P.C.

L'Autorité de Certification a la responsabilité du bon fonctionnement des composants de l'I.G.C. conformément aux dispositions énoncées dans le présent document. Le responsable de l'A.C. détermine l'adéquation et l'applicabilité de cette P.C.

### 1.5.4 Procédures d'approbation de la conformité de la D.P.C.

Seules les personnes habilitées de SFR sont en mesure de demander la conformité de la D.P.C. à la P.C. par l'intermédiaire d'experts sécurité indépendants spécialisés dans le domaine des Infrastructures de Gestion de Clés.

## 1.6 Abréviations et définitions

### 1.6.1 Liste des abréviations

| Abréviations | Signification |
|---|---|
| A.C. | Autorité de Certification |
| A.E. | Autorité d'Enregistrement |
| CGU | Conditions Générales d'Utilisation |
| CRL | Certificate Revocation List |
| D.P.C. | Déclaration des Pratiques de Certification |
| HSM | Hardware Security Module |
| HTTP | Hyper Text Transfer Protocol |
| I.G.C. | Infrastructure à Gestion de Clés |
| L.C.R. | Liste de Certificats Révoqués |
| P.C. | Politique de Certification |
| R.G.S. | Référentiel Général de Sécurité |

### 1.6.2 Définitions

Le symbole (*) signifie que le terme est défini dans ce paragraphe. Il est utilisé dans le reste du document lorsqu'il est important de renvoyer à la définition du terme employé.

**Application utilisatrice :** désigne un service applicatif exploitant les certificats émis par l'Autorité de Certification pour des besoins de signature du porteur de certificat.

**Autorité d'horodatage :** Autorité responsable de la gestion d'un service d'horodatage.

**Infrastructure de gestion de clés (I.G.C.) :** Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une I.G.C. 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.

**Autorité de certification (A.C.) :** désigne l'autorité responsable des certificats* émis et signés en son nom conformément aux règles définies dans la politique de certification et la déclaration des pratiques de certification associée.

**Autorité d'enregistrement (A.E.) :** désigne l'autorité qui vérifie, conformément à la politique de certification, les données propres au demandeur de certificat ou à le porteur de certificat.

**Bi-clé :** désigne un couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptologie basée sur des algorithmes asymétriques.

**Certificat électronique :** Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement dans le certificat. Il est délivré par une **Autorité de Certification**. En signant le certificat, l'A.C. valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Dans le cadre de la présente P.C., le terme "certificat électronique" désigne uniquement un certificat délivré à une personne physique et portant sur une bi-clé de signature, sauf mention explicite contraire (certificat d'A.C., certificat d'une composante, …).

**Composante :** Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'I.G.C.

**Déclaration des pratiques de certification (D.P.C.) :** Une D.P.C. identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'A.C. applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

**Dispositif de création de signature :** Il s'agit du dispositif matériel ou logiciel utilisé par le porteur de certificat pour stocker et mettre en œuvre sa clé privée de signature (ex : Service de signature électronique Universign).

**Entité :** Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

**Politique de certification (P.C.) :** Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une A.C. 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 P.C. peut également, si nécessaire, identifier les obligations et exigences portant sur les différents intervenants, notamment les porteurs de certificats.

**Politique de signature :** Ensemble de règles pour la création et la validation d'une signature électronique vis-à-vis desquelles la signature peut être déterminée comme valide.

**Utilisateur de certificat :** Toute personne physique majeure qui utilise un certificat et un dispositif de création de signature pour la mise en œuvre de sa clé privée. Il agit pour son propre compte. Le certificat ne lui est pas remis.

# 2 Responsabilités concernant la mise à disposition des informations devant être publiées

## 2.1 Entités chargées de la mise à disposition des informations

SFR, en tant qu'A.C, met à disposition publiquement la présente PC. La présente P.C est disponible via le réseau Internet sur le site web : http://www.sfr.fr/signature-electronique/

Les informations relatives aux pratiques de certification destinées à être publiquement diffusées se trouvent dans la présente PC.

### 2.1.1 Les informations devant être publiées

L'A.C. s'engage à publier les informations suivantes :

- la présente politique de certification et celle de l'A.C. « SFR Public AC Racine »
- la liste des certificats révoqués
- le certificat de l'A.C. et le certificat de l'AC Racine.
- Les CGU applicables

Tous ces documents sont accessibles gratuitement sur le site web suivant :
http://www.sfr.fr/signature-electronique/

Toutes les anciennes versions de la PC et des CGU sont archivées sur le site web.

### 2.1.2 Publication de la L.C.R.

La liste des certificats révoqués (L.C.R.) est publiée sur le lien suivant :

http://crl.sfr.fr/sfr_client.crl

### 2.1.3 Délais et fréquences de publication

Les informations liées à l'I.G.C. sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'A.C.

Les certificats d'A.C. sont diffusés préalablement à toute diffusion de certificats de porteurs ou de L.C.R. correspondants.

La Politique de Certification est publiée avant toute émission d'un certificat électronique encadré par la Politique.

#### 2.1.3.1 Fréquence de publication du certificat d'A.C.

Le certificat d'A.C. est diffusé dans un délai maximum de 24 heures à l'issue de sa génération et avant toute signature d'un certificat final rattaché à ce certificat d'AC.

#### 2.1.3.2 Fréquence de publication de la L.C.R.

L'A.C. publie sa L.C.R. à la fréquence d'une fois par jour.

### 2.1.4 Contrôles d'accès aux informations publiées

L'accès en modification aux systèmes de publication des informations d'états des certificats (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'I.G.C. à travers un contrôle d'accès fort. Les contrôles d'accès aux autres fonctions de publication sont publiés dans la D.P.C.

# 3 Identification et authentification

## 3.1 Nommage

### 3.1.1 Type de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500.

Dans chaque certificat X509v3 l'A.C. émettrice (*issuer*) et le porteur de certificat (*subject*) sont identifiés par un « *Distinguished Name* » (DN) de type X.501 dont le format exact est précisé dans le chapitre 7.2 décrivant le profil des certificats.

### 3.1.2 Nécessité d'utilisation de noms explicites

Le DN du porteur de certificat est construit à partir du nom, prénom de son état civil tel qu'ils sont renseignés lors de la souscription en ligne.

### 3.1.3 Anonymisation ou pseudonymique des porteurs de certificats

L'utilisation d'un pseudonyme n'est pas autorisée. Le certificat délivré par l'A.C. « *SFR AC Certificat Client – Certificat signature en ligne* » ne peut en aucun cas être anonyme.

### 3.1.4 Règles d'interprétation des différentes formes de nom

Aucune interprétation particulière n'est à faire des informations portées dans le champ "subject" de chaque certificat de porteur. Ces informations sont établies par l'A.C *« SFR AC Certificat Client.- Certificat signature en ligne* » selon les règles suivantes :

- Tous les caractères sont au format PrintableString, en majuscules, sans accent ni caractères spécifiques à la langue française et de manière conforme au standard X.501.
- Les prénoms et noms composés sont séparés par des espaces " ".
- Aucun nom d'usage n'est utilisé : seuls les noms patronymiques sont utilisés.

Pour des informations complémentaires, consulter le chapitre 7.

### 3.1.5 Unicité des noms

L'unicité d'un certificat est établie par le numéro de série, au sein de l'Autorité de Certification. L'unicité du DN est elle-même garantie par l'unicité des informations permettant de construire le DN :

- nom et du prénom du porteur de certificat
- le numéro de RUM (Référence Unique du Mandat SEPA).

## 3.2 Validation initiale de l'identité

La validité de l'enregistrement du demandeur est réalisée auprès de l'A.E.

### 3.2.1 Méthode pour prouver la possession de la clé privée

Le porteur de certificat ne génère pas sa bi-clé. Celle-ci est générée par la plate-forme de signature lors du processus de signature en ligne.

### 3.2.2 Validation de l'identité de l'organisme

Sans objet. Le certificat est délivré uniquement à des personnes physiques.

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

Le demandeur remplit ses informations sur un formulaire web en ligne. L'A.E se laisse la possibilité de demander à posteriori des pièces justificatives par courrier ou en ligne.

### 3.2.4 Informations non vérifiées du porteur de certificat

Les informations non vérifiées sont le nom d'usage, l'adresse postale et l'adresse e-mail.
Il est donc de la responsabilité du porteur de fournir des informations valides lors de la souscription en ligne.

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

Du fait de la durée de vie très courte des certificats, ce paragraphe est sans objet.

# 4 Exigences Opérationnelles sur le cycle de vie des certificats

## 4.1 Demande de certificat

Le certificat est demandé auprès de l'A.C automatiquement après la reconnaissance de la vérification des informations saisies et l'acceptation des conditions d'utilisation de la signature électronique par le porteur.

### 4.1.1 Processus et responsabilités pour l'établissement d'une demande

Les informations suivantes font partie de la demande de certificat :

- les données saisies lors de la souscription en ligne
  - nom ;
  - prénom ;
- le numéro de RUM .
- l'e-mail en option ;
- date de la demande

Le dossier de demande de certificat est établi électroniquement depuis l'A.E. Il est transmis automatiquement à l'A.C. Le dossier d'enregistrement est conservé numériquement par l'A.C.

## 4.2 Traitement d'une demande de certificat

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

L'A.E. transmet à l'A.C une demande de certificat avec les données du porteur.

### 4.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, l'A.E. informe le porteur du certificat.

En cas d'acceptation, la demande de certificat est adressée automatiquement et traitée immédiatement.

### 4.2.3 Durée d'établissement du certificat

Les certificats émis dans le cadre de la présente politique ont une durée de validité de **30 minutes.**

## 4.3 Délivrance du certificat

### 4.3.1 Actions de l'A.C. concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'A.E. à travers un réseau sécurisé, l'A.C. déclenche les processus de génération et de préparation du certificat destiné à la plate-forme de signature électronique pour le porteur de certificat.

L'A.C. génère et déclenche le processus de génération du certificat de manière sécurisée : l'ordonnancement des opérations est assuré par l'architecture de l'I.G.C. qui assure l'intégrité et l'authentification entre les composants.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres 5 et 6 ci-dessous, notamment la séparation des rôles de confiance (cf. chapitre 5.2).

## 4.4 Acceptation du certificat

Le certificat est considéré accepté implicitement après l'action du porteur sur le bouton « signer » disponible lors du processus de signature électronique en ligne sur les services de SFR.

## 4.5 Usages de la bi-clé et du certificat

L'utilisation de la clé privée et du certificat associé du porteur de certificat est strictement limitée à la signature électronique personnelle du porteur et, en particulier, de signature électronique en ligne de mandat SEPA sur les services Web de SFR.

L'usage autorisé de la bi-clé et du certificat associé du porteur de certificat est indiqué dans le certificat lui-même, via les extensions concernant les usages des clés.

## 4.6 Renouvellement d'un certificat

Du fait de la durée de vie très courte des certificats, ce paragraphe est sans objet.

## 4.7 Délivrance d'un nouveau certificat suite à changement de la bi-clé

Du fait de la durée de vie très courte des certificats, ce paragraphe est sans objet.

## 4.8 Modification du certificat

La modification du certificat n'est pas autorisée.

## 4.9 Révocation et suspension des certificats

### 4.9.1 Causes possibles de révocation

#### 4.9.1.1 Porteurs de Certificats

Les circonstances suivantes peuvent être à l'origine de la révocation automatique d'un certificat de porteur de certificat :

- le certificat n'a pas été transmis correctement à la plate-forme de signature électronique Universign (erreur technique).
- Tous les autres cas de révocation sont exclus en raison de l'usage unique du certificat et de sa durée de validité très limitée.

Lorsqu'une des circonstances ci-dessus se réalise et que l'A.C. en a eu connaissance, le certificat concerné est révoqué et le numéro de série placé dans la *liste de certificats révoqués* (L.C.R.). La clé privée est détruite.

#### 4.9.1.2 Certificats d'une composante de l'I.G.C.

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'I.G.C. (y compris un certificat d'A.C. pour la génération de certificats, de L.C.R

- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- décision de changement de composante de l'I.G.C. suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la D.P.C. (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- cessation d'activité de l'entité opérant la composante.

### 4.9.2 Origines d'une demande de révocation

#### 4.9.2.1 Porteurs de Certificats

Seule l'AC émettrice du certificat génère automatiquement la révocation conformément au 4.9.1.

#### 4.9.2.2 Certificats d'une composante de l'I.G.C.

La révocation d'un certificat d'A.C. ne peut être décidée que par l'entité responsable de l'A.C., ou par les autorités judiciaires via une décision de justice.

La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'A.C. sans délai.

### 4.9.3 Procédure de traitement d'une demande de révocation

#### 4.9.3.1 Porteurs de Certificats

Sans objet.

#### 4.9.3.2 Certificats d'une composante de l'I.G.C.

L'A.C précise dans sa D.P.C les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.

En cas de révocation d'un des certificats de la chaîne de certification, l'A.C. informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs concernés que leurs certificats ne sont plus valides.

Afin de faciliter la révocation du certificat de l'AC, une nouvelle LAR sera publiée afin que tous les porteurs de certificats puissent prendre en compte la révocation.

L'A.C informera directement ses clients sur le site web http://www.sfr.fr/signature-electronique/

### 4.9.4 Délai accordé au porteur de certificat pour formaliser la demande de révocation

Sans objet.

### 4.9.5 Délai de traitement par l'A.C. d'une demande de révocation

#### 4.9.5.1 Porteurs de Certificats

Sans objet.

#### 4.9.5.2 Certificats d'une composante de l'I.G.C.

La révocation d'un certificat d'une composante de l'I.G.C. est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'A.C. qui a émis le certificat, et que cette liste est accessible au téléchargement. La révocation d'un certificat de signature de l'A.C.

(signature de certificats, de L.C.R., de L.A.R.) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

### 4.9.6 Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur est tenu de vérifier l'état des certificats et de la chaîne correspondante.

### 4.9.7 Fréquence d'établissement de la L.C.R.

Une nouvelle L.C.R. est produite au moins une fois par jour (en pratique, toutes les 12 heures) et remplace la précédente L.C.R.

### 4.9.8 Délai maximum de publication de la L.C.R.

La L.C.R. est publiée au minimum une fois toute les 72 heures.

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

Les L.C.R. sont l'unique moyen de vérifier l'état des certificats.

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

Sans objet.

### 4.9.11 Autres moyens disponibles d'information sur les révocations

D'autres moyens d'information sur les révocations peuvent être mis en place à condition qu'ils respectent les exigences d'intégrité, de disponibilité et de délai de publication décrite dans la présente P.C.

### 4.9.12 Exigences spécifiques en cas de compromission de la clé privée de l'A.C.

Pour les certificats d'A.C., la révocation suite à une compromission de la clé privée fera l'objet d'une information clairement diffusée au moins sur le site Internet de l'A.C. et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

### 4.9.13 Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente P.C.

## 4.10 Fonction d'information sur l'état des certificats

### 4.10.1 Caractéristiques opérationnelles

L'A.C. fournit à l'application utilisatrice de certificats (le dispositif de signature électronique en ligne Universign) les informations lui permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante.

### 4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24 heures sur 24 et 7 jours sur 7.

## 4.11 Fin de la relation entre le porteur de certificat et l'A.C.

Du fait de la durée de vie très courte des certificats, ce paragraphe est sans objet.

## 4.12 Séquestre de clé et recouvrement

Il n'y a pas de séquestre des clés privées des porteurs de certificats. Ce paragraphe est sans objet.

# 5 Mesures de sécurité non techniques

## 5.1 Mesures de sécurité physique

### 5.1.1 Situation géographique et construction des sites

La construction du site d'exploitation des services de l'A.C. respecte les règlements et normes en vigueur ainsi que, suivant l'analyse de risque réalisée, des exigences spécifiques face à des risques de type tremblement de terre ou explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques,…).

### 5.1.2 Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'I.G.C. et l'interruption des services de l'A.C., les accès aux locaux des différentes composantes de l'I.G.C. sont contrôlés.

L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

Les mesures de contrôle sont détaillées dans la D.P.C.

### 5.1.3 Alimentation électrique et climatisation

Les installations de fourniture d'électricité et de climatisation sont suffisantes pour le fonctionnement de l'A.C.

### 5.1.4 Vulnérabilité aux dégâts des eaux

Les composantes de l'A.C ne sont pas exposées aux inondations et protégées de toute exposition aux liquides.

### 5.1.5 Prévention et protection incendie

L'A.C. met en œuvre des mesures de prévention contre les incendies et ses composantes sont protégées par un système d'extinction d'incendies.

### 5.1.6 Conservation des supports

Les supports de stockage utilisés par l'A.C sont protégés des menaces environnementales telles que l'humidité, la température et les champs magnétiques.

### 5.1.7 Mise hors service des supports

L'A.C. s'assure de l'effacement et réinitialisation ou de la destruction des supports lorsqu'ils arrivent en fin de vie.

### 5.1.8 Sauvegardes hors site

L'A.C. réalise des sauvegardes hors-site afin de permettre la reprise des services de l'A.C. après un sinistre. Les modalités de sauvegarde sont détaillées dans la D.P.C.

## 5.2 Mesures de sécurité procédurales

### 5.2.1 Rôles de confiance

Pour le bon fonctionnement de l'I.G.C., il a été défini les cinq rôles fonctionnels de confiance suivants :

**Responsable de sécurité** - Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

**Responsable d'application** - Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'I.G.C. au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.

**Administrateur système** - Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.

**Opérateur de certification** - Un opérateur au sein d'une composante de l'I.G.C. réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.

**Auditeurs systèmes** - Personne désignée par l'AC et dont le rôle est de procéder de manière régulière à des contrôles sur les journaux de l'I.G.C. et à l'analyse des incidents techniques.

### 5.2.2 Nombre de personnes requises par tâches

Pour des raisons de sécurité, les fonctions sensibles seront réparties sur plusieurs personnes. Le cumul de certains rôles n'est pas autorisé. Les règles de cumul des rôles sont définies dans la D.P.C.

### 5.2.3 Identification et authentification pour chaque rôle

Des mesures d'identification et d'authentification sont mises en place afin de supporter la mise en œuvre de la politique de contrôle d'accès et la traçabilité des opérations ; la politique de contrôle d'accès limite l'accès aux seules personnes autorisées conformément à leur besoin d'en connaître. Les rôles attribués sont notifiés par écrit aux personnes concernées.

### 5.2.4 Rôles exigeant une séparation des attributions

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

L'AC garantit que les opérations de sécurité sont séparées des opérations d'exploitation classiques et qu'elles sont réalisées systématiquement sous couvert d'une personne ayant un Rôle de Confiance.

## 5.3 Mesures de sécurité vis-à-vis du personnel

### 5.3.1 Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'I.G.C. sont soumis à une clause de confidentialité vis-à-vis de leur employeur. Chaque entité opérant une composante de l'I.G.C. s'assure que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement possède l'expertise appropriée à son rôle et est familier des procédures de sécurité en vigueur au sein de l'I.G.C.

Toute personne intervenant dans des rôles de confiance de l'I.G.C est informée :

- de ses responsabilités relatives aux services de l'I.G.C. ;
- des procédures liées à la sécurité du système et au contrôle du personnel.

### 5.3.2 Procédures de vérification des antécédents

L'opérateur de certification met en œuvre tous les moyens légaux dont il dispose pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein des composantes de l'I.G.C.

### 5.3.3 Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.

Le personnel a connaissance et comprend les implications des opérations dont il a la responsabilité.

### 5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, en fonction de la nature de ces évolutions.

### 5.3.5 Fréquence et séquence de rotation entre différentes attributions

Ce point est précisé dans la D.P.C.

### 5.3.6 Sanctions en cas d'actions non autorisées

Ce point est précisé dans la D.P.C.

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

Ce point est précisé dans la D.P.C.

### 5.3.8 Documentation fournie au personnel

Les règles de sécurité sont communiquées au personnel lors de la prise de poste, en fonction du rôle affecté à l'intervenant. Les personnes appelées à occuper un rôle opérationnel dans l'I.G.C disposent des procédures correspondantes.

## 5.4 Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique. Les fichiers résultants, sous forme papier ou électronique, rendent possible la traçabilité et l'imputabilité des opérations effectuées.

### 5.4.1 Type d'évènements à enregistrer

L'A.C prend les mesures nécessaires pour enregistrer les événements suivants :

- événements systèmes des différentes composantes de l'IGC (démarrage des serveurs, accès réseau, ...) ;
- événements techniques des applications composant l'IGC ;
- événements fonctionnels des applications composant l'IGC (demande de certificats, validation, révocation, ...) ;
- opérations effectuées, intégrant entre autre les actions d'authentification des personnes ayant un rôle de confiance.

Des enregistrements d'événements non informatiques sont réalisés pour :

- l'accès au site de production ;
- les actions de maintenance et de changement de configuration ;
- les changements de personnels ;
- les actions sur les supports contenant des informations confidentielles.

### 5.4.2 Fréquence de traitement des journaux d'évènements

Les journaux d'événements sont exploités systématiquement en cas de remontée d'événement anormal.

### 5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont externalisés tous les mois puis sauvegardés sur un serveur de sauvegarde dans les locaux de l'Opérateur de Certification.

Ces archives sont conservées jusqu'à l'expiration du dernier certificat émis par l'AC.

### 5.4.4 Protection des journaux d'évènements

Les journaux d'événements sont rendus accessibles uniquement au personnel habilité de l'A.C. Ils ne sont pas modifiables de manière non autorisée.

### 5.4.5 Procédure de sauvegarde des journaux d'évènements

Les journaux sont sauvegardés régulièrement sur un support externe.

### 5.4.6 Système de collecte des journaux d'évènements

Ce point est précisé dans la D.P.C.

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

Ce point est précisé dans la D.P.C.

### 5.4.8 Évaluation des vulnérabilités

La DPC détaille la procédure d'analyse du contenu des journaux d'évènements mise en place pour détecter les vulnérabilités du système et détecter les attaques dont il ferait l'objet.

## 5.5 Archivage des données

### 5.5.1 Types de données à archiver

Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les P.C. ;
- les D.P.C. ;
- les certificats et LCR tels qu'émis ou publiés ;
- les journaux d'évènements des demandes de certificats ;
- les journaux d'évènements des différentes entités de l'I.G.C.

### 5.5.2 Dossiers de demande de certificat

Tout dossier d'enregistrement est archivé jusqu'à la fin de vie de l'A.C + 5 ans.

Le dossier d'enregistrement doit pouvoir être présenté par l'A.C. lors de toute sollicitation par les personnes habilitées.

**Certificats et LCR émis par l'A.C.**
Les certificats de d'AC, ainsi que les LCR produites, sont archivés pendant au moins cinq ans après l'expiration de ces certificats.

**Journaux d'évènements**
Les journaux d'événements sont archivés et conservés pendant 10 ans après leur génération.

### 5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, sont :

- protégées en intégrité ;
- accessibles aux personnes autorisées ;
- en capacité d'être relues et exploitées.

Ce point est précisé dans la D.P.C.

### 5.5.4 Procédure de sauvegarde des archives

Les procédures de sauvegarde des archives sont précisées dans la D.P.C. Le niveau de protection des sauvegardes est au moins équivalent au niveau de protection des archives.

### 5.5.5 Exigences d'horodatage des données

Le chapitre 6.8 précise les exigences en matière de datation / horodatage.

### 5.5.6 Système de collecte des archives

Ce point est précisé dans la D.P.C.

### 5.5.7 Procédures de récupération et de vérification des archives

Les archives électroniques peuvent être récupérées dans un délai ne dépassant pas 72 heures, sachant que seule l'A.C. peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'I.G.C. qui ne peut récupérer et consulter que les archives de la composante considérée).

## 5.6 Changement de clé d'A.C.

L'A.C. ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'A.C. Pour cela L'A.C s'engage à renouveler son certificat 6 mois avant l'expiration .

Dès qu'une nouvelle bi-clé d'A.C. est générée, seule la nouvelle clé privée est utilisée pour signer des certificats.

## 5.7 Reprise suite à compromission et sinistre

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

Chaque entité opérant une composante de l'I.G.C. met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'A.C., l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'A.C. Le cas de l'incident majeur est traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, est faite dans la plus grande urgence sur le site Internet.

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

Un plan de continuité est mis en place permettant de répondre aux exigences de disponibilité des différentes composantes de l'IGC. Ce plan est testé au moins une fois tous les trois ans.

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

Le cas de compromission d'une composante est traité dans le plan de continuité de la composante.

Dans le cas de compromission d'une clé d'A.C., le certificat correspondant est immédiatement révoqué et un processus de révocation de tous les certificats émis par cette AC encore en cours de validité est lancé.

### 5.7.4 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'I.G.C. disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente P.C. L'opérateur de certification est engagé contractuellement à mettre en œuvre ces moyens.

## 5.8 Fin de vie de l'I.G.C.

Une ou plusieurs composantes de l'I.G.C. peuvent être amenées à cesser leur activité ou à la transférer à une autre entité.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'I.G.C. ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'A.C. en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'I.G.C. comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

### 5.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'I.G.C.

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'A.C. a les obligations suivantes:

- mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs de certificats et des informations relatives aux certificats) ;
- assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente P.C. et jusqu'à la fin de vie du dernier certificat émis ;

Les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue sont détaillés dans la D.P.C.

### 5.8.2 Cessation d'activité affectant l'A.C.

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées ci-dessous soient à exécuter par l'A.C., ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'A.C. ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements

pris dans sa P.C. Une fois le dernier certificat émis expiré ou révoqué, l'A.C. est détachée de ses obligations.

Lors de l'arrêt du service, l'A.C. doit :

- détruire sa clé privée lui ayant permis d'émettre des certificats ;
- **r**évoquer son certificat auprès de l'A.C Racine ;
- informer via le site Web Internet.

# 6 MESURES DE SECURITE TECHNIQUES

### 6.1.1 Génération et installation de bi clés

### 6.1.2 Génération des bi-clés

#### 6.1.2.1 Clés d'A.C.

La génération des clés de signature de l'A.C. est effectuée dans un environnement sécurisé. Les clés de signature d'A.C. sont générées et mises en œuvre dans un module cryptographique certifié FIPS 140-2 niveau 3 ou EAL4+. Les modalités de génération de clés sont exprimées dans la D.P.C.

La génération des clés de signature d'A.C. est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance, dans le cadre de la « cérémonie de clés ». La cérémonie des clés est contrôlée par deux personnes ayant des rôles de confiance et en présence d'un huissier de justice. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini. Un procès-verbal est établi pour attester du bon déroulement de la cérémonie. Ce procès-verbal est archivé par l'A.C.

#### 6.1.2.2 Clés des porteurs de certificats

La génération des clés des porteurs de certificats est effectuée dans un environnement logiciel sur la plate-forme de signature électronique Universign.

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

Sans objet. La clé privée reste dans l'environnement logiciel de la plateforme de signature électronique Universign et elle est détruite après les opérations de signature électronique.

### 6.1.4 Transmission de la clé publique à l'A.C.

La clé publique du porteur de certificat vers une composante de l'A.C. est protégée à travers un lien sécurisé.

### 6.1.5 Transmission de la clé publique de l'A.C. aux utilisateurs de certificats

Les clés publiques de vérification de signature de l'A.C. sont diffusées auprès des utilisateurs de certificats dans les mandats SEPA signés sous format PDF qui assure l'intégrité de bout en bout.

Une clé publique d'A.C. est diffusée dans un certificat rattaché à une hiérarchie d'A.C. jusqu'à une A.C. racine. La clé publique de l'A.C. ainsi que les informations correspondantes (certificats, empreintes numériques, déclaration d'appartenance) sont disponibles et peuvent être récupérables dans le fichier PDF.

#### 6.1.6 Tailles des clés

Les certificats des porteurs de certificats ont une taille de clés de 2048 bits et respectent les caractéristiques techniques qui sont définies dans la D.P.C.

La taille des clés de l'A.C. est fixée à 2048 bits.

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

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

#### 6.1.8 Objectifs d'usage de la clé

L'utilisation de la clé privée du porteur de certificat est strictement limitée à la signature électronique personnelle et, en particulier, la signature électronique de mandat SEPA en ligne sur les services de SFR.

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

#### 6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

##### 6.2.1.1 Modules cryptographiques de l'A.C.

Les modules cryptographiques, utilisés par l'A.C., pour la génération et la mise en œuvre de ses clés de signature, utilisent des modules cryptographiques (HSM) conforme à une certification FIPS 140-2 niveau 3 ou EAL4+.

##### 6.2.1.2 Dispositifs de création de signature des porteurs de certificats

Le dispositif de création de signature des porteurs de certificats, pour la mise en œuvre de leurs clés privées de signature répond aux exigences d'un niveau sécurité attendu pour une signature dite « simple ». Le dispositif mis en œuvre est un dispositif logiciel centralisé sur la plateforme de signature Universign.

### 6.2.2 Contrôle de la clé privée de l'A.C. par plusieurs personnes

Le contrôle des clés privées de signature de l'A.C. est assuré par du personnel de confiance (porteur de secrets d'I.G.C.) et via un outil mettant en œuvre le partage des secrets.

### 6.2.3 Séquestre de la clé privée

Pas de séquestre de clé privée.

### 6.2.4 Copie de secours de la clé privée

Les clés privées des porteurs de certificats ne font l'objet d'aucune copie de secours par l'A.C.

Les clés privées d'A.C. font l'objet de copies de secours, hors d'un module cryptographique sous format chiffré avec un mécanisme de contrôle d'intégrité. Les opérations de chiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'A.C. ne sont à aucun moment en clair en dehors du module cryptographique. Les copies de secours sont stockées dans une armoire forte.

### 6.2.5 Archivage de la clé privée

Les clés privées de l'A.C. ne sont pas archivées. Les clés privées des porteurs de certificats ne sont pas archivées ni par l'A.C. ni par aucune des composantes de l'I.G.C.

### 6.2.6 Stockage de la clé privée dans un module cryptographique

Les clés privées d'A.C. sont stockées dans un module cryptographique conforme à une certification FIPS 140-2 niveau 3 ou EAL4+.

### 6.2.7 Méthode d'activation de la clé privée

#### 6.2.7.1 Clés privées d'A.C.

L'activation des clés privées d'A.C. dans un module cryptographique est contrôlée via une authentification forte et fait intervenir au moins deux personnes dans des rôles de confiance.

#### 6.2.7.2 Clés privées des porteurs de certificats

Les clés sont activées, uniquement par le dispositif de signature électronique Universign lors des opérations de signature électronique en ligne de mandat SEPA.

#### 6.2.8 Méthode de destruction des clés privées

##### 6.2.8.1 Clés privées d'A.C.

En fin de vie d'une clé privée d'A.C., normale ou anticipée (révocation), cette clé est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

##### 6.2.8.2 Clés privées des porteurs de certificats

En fin de session de l'opération de signature, la clé privée stockée dans la mémoire vive du dispositif de signature électronique Universign est détruite. Il n'est alors plus possible de l'obtenir sous quelques moyens que ce soient.

#### 6.2.9 Niveau d'évaluation sécurité du module cryptographique

Les modules cryptographiques de l'A.C. sont évalués au niveau correspondant à l'usage visé.

## 6.3 Autres aspects de la gestion des bi-clés

#### 6.3.1 Archivage des clés publiques

Les clés publiques de l'A.C. et des porteurs de certificats sont archivées dans le cadre de l'archivage correspondant.

#### 6.3.2 Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des porteurs de certificats ont une durée de vie de 30 minutes.

La durée de vie des clés de signature d'A.C. et des certificats correspondants est de 10 ans.

## 6.4 Données d'activation

#### 6.4.1 Données d'activation correspondant à la clé privée de l'A.C.

Les données d'activation de la clé privée de l'A.C. sont des secrets détenus par des personnes ayant des rôles de confiance.

#### 6.4.2 Données d'activation correspondant à la clé privée du porteur de certificat

Il n'y a pas de donnée d'activation pour la clé du porteur de certificat.

## 6.5 Mesures de sécurité des systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'I.G.C. est défini dans la D.P.C. de l'A.C. Il répond aux objectifs de sécurité suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique) ;
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- protection du réseau contre toute intrusion d'une personne non autorisée ;
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- fonctions d'audits (non-répudiation et nature des actions effectuées) ;

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle fait l'objet de mesures particulières.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) sont mis en place.

Les mesures de sécurité sont précisées dans la D.P.C.

## 6.6 Mesures de sécurité liées au développement des systèmes

Les infrastructures de développement et d'essai sont séparées des infrastructures opérationnelles de l'IGC.

Les configurations du système des composantes de l'I.G.C. ainsi que toute modification et mise à niveau sont documentées et contrôlées.

Toute mise à jour d'une des composantes de l'IGC bénéficie d'une procédure de recette.

## 6.7 Mesures de sécurité réseau

Les échanges entre composantes au sein de l'I.G.C. mettent en œuvre des mesures particulières (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

Les mesures de sécurité sont précisées dans la D.P.C.

## 6.8 Horodatage / Système de datation

Plusieurs exigences de la présente P.C. nécessitent la datation par les différentes composantes de l'I.G.C. d'évènements liés aux activités de l'I.G.C.

Pour dater ces évènements, les différentes composantes de l'I.G.C. recourent à un système de datation d'un tiers horodateur de confiance qualifié RGS.

# 7 PROFILS DES CERTIFICATS

## 7.1 Profil des certificats de l'A.C.

### 7.1.1 Certificat de signature des certificats

| Champ | Valeur |
|---|---|
| **Version** | 3 (0x2) |
| **Serial Number** | fe:ff:40:98:ab:bd:11:a8:dc:69:d3:01:af:24:e3:47 |
| **Signature Algorithm** | sha512WithRSAEncryption |
| **Issuer** | C=FR, O=SFR, CN=SFR Public AC Racine |
| **Not Before** | Mar 17 12:58:00 2008 GMT |
| **Not After** | Mar 17 12:58:00 2018 GMT |
| **Subject** | C=FR, O=SFR, CN=SFR AC Certificat Client |
| **Public Key Algorithm** | rsaEncryption |
| **Public-Key** | (2048 bits) |
| **Modulus** | 00:d4:94:56:eb:d2:a9:ac:00:67:5c:c6:35:1f:d5:<br>15:b3:be:30:ec:24:8c:28:08:5b:ea:1d:7b:a9:f4:<br>41:67:01:dd:5c:0e:c5:cc:84:d6:bb:8f:21:07:55:<br>81:09:51:08:19:d3:93:e1:f1:32:9c:47:5f:f0:4f:<br>02:3e:a7:8e:b1:00:af:e5:68:04:04:0a:ac:cf:32:<br>24:50:91:a4:72:9e:dd:04:00:b5:40:74:06:58:8e:<br>5b:e8:17:73:c7:fe:52:46:64:60:07:b8:a0:a2:b7:<br>28:bf:4c:d8:bb:56:92:2f:36:a9:86:97:4c:89:c7:<br>d2:65:3f:c2:88:13:a4:d6:19:a3:c5:d6:df:37:23:<br>23:12:96:7a:72:54:58:69:2b:78:34:e6:e8:ae:cd:<br>9d:bf:3f:1a:55:56:af:b3:74:8a:de:ac:d9:73:6c:<br>7d:40:ce:c8:03:83:d5:6a:da:59:5a:2a:09:29:a7:<br>ec:d0:61:51:8c:0a:59:8e:a3:c3:f7:cd:f2:0d:69:<br>0c:bf:a7:aa:d4:4c:cb:a5:27:2c:d5:79:14:3e:93:<br>84:f2:20:63:4b:ad:95:6f:60:9e:1b:a4:dd:08:9c:<br>fd:44:bc:b1:ff:a3:a6:1c:28:3f:fe:09:42:78:08:<br>f4:db:75:f8:67:23:b3:3a:be:57:50:41:9c:46:2d:<br>91:2f |

| Champ | Valeur |
|---|---|
| **Exponent** | 65537 (0x10001) |
| **X509v3 extensions** | |
| **Basic Constraints (critical)** | CA:TRUE, pathlen:0 |
| **Key Usage (critical)** | Certificate Sign, CRL Sign |
| **Subject Key Identifier** | 0C:7A:2D:C6:C4:ED:F4:2F:A0:A6:69:1E:FC:66:42:75:D5:0B:F8:0C |
| **Authority Key Identifier** | keyid:D9:3C:76:06:0F:7C:5D:15:3B:CE:D1:E6:FD:16:22:B0:B9:59:3F:F9 |
| **Signature Algorithm** | sha512WithRSAEncryption |
| **Signature Value** | e9:71:7a:b6:d5:19:4a:52:32:0b:af:92:39:71:87:b3:39:6f:8c:35:3a:9f:81:7f:9d:a2:74:8d:14:16:e4:94:fb:f4:6f:db:93:35:b6:96:bb:15:e5:36:6b:8b:92:e2:60:b8:d1:46:66:e6:62:76:ce:61:14:2d:e6:2f:7d:a6:63:b7:ce:24:d4:9a:bd:a2:0e:40:b8:cd:ef:3c:c7:3f:a4:76:55:a1:78:8f:58:56:50:73:52:a9:35:42:e0:d5:e1:6a:14:5c:d2:40:b0:61:7d:bf:b4:28:03:30:f1:94:e6:a9:3e:5c:88:ee:89:60:5a:30:db:be:b6:99:13:94:c3:32:6c:e6:2f:a7:5d:4d:2e:26:c5:54:cc:8e:08:f7:57:99:ac:37:7c:63:e8:34:93:8d:be:1a:98:06:aa:0e:da:5e:fd:56:6b:c8:44:6d:9d:3c:00:30:c7:60:c3:9b:33:7c:a8:31:88:e0:9c:92:7a:49:39:b0:4e:b3:dc:ec:14:b3:56:13:39:2a:87:6d:82:0a:27:f5:f7:19:7f:32:ae:e9:ac:47:9f:09:49:bf:29:ec:33:46:c3:c0:60:25:5f:b5:3b:c1:54:46:54:0f:1b:9b:1e:a4:20:95:00:f6:59:2c:23:84:d8:b2:d2:ac:f2:53:dc:0d:1b:dc:36:6f:f9:79:a7:3b:b8:5c:66:e6:83:3e:4d:b7:1b:38:b0:46:40:8f:aa:8e:bf:12:f2:7a:ba:67:ec:95:4d:4e:b7:9b:22:ed:f6:ba:29:19:9e:a8:e2:8f:22:9e:b3:ef:c9:1c:d7:14:33:91:b9:f0:79:90:6a:4f:9e:02:92:05:32:54:eb:89:4a:a6:e8:a4:72:d0:90:2f:03:10:ab:bd:58:71:ee:bc:b5:8a:0d:d1:11:23:0d:6e:19:26:82:34:45:98:3a:cd:d7:f5:02:79:4f:42:c6:ab:3c:82:b0:1c:f8:ba:b0:ec:9f:31:05:bd:64:37:27:bd:e9:9f:fe:e9:ad:90:4d:48:af:42:bb:88:6b:30:0b:89:a1:09:f6:61:bf:ea:06:12:3c:50:18:86:45:4e:84:7e:0f:5a:f3:27:e2:8d:45:16:66:c6:37:e0:06:6c:62:cf:fc:5c:b9:20:54:2a:9c:7d:fd:f3:28:db:d7:fa:51:55:b8:46:0b:e9:09:ce:e3:b1:90:ab:0e:26:af:18:c2:1f:d6:0c:e3:68:9a:ab:13:2e:4c:c4:63:ae:bd:80:a6:ce:19:42:1e:62:d5:18:1c:9f:29:7b:ee:c6:4a:c5:e8:d1:0f:f9:8a:cc:1a:ab:c1:75:85:07:97:31:c8:63:66:9e:2c:ab:b7:fc:82:c0 |

```
-----BEGIN CERTIFICATE-----
MIIEnDCCAoSgAwIBAgIRAP7/QJirvRGo3GnTAa8k40cwDQYJKoZIhvcNAQENBQAw
OjELMAkGA1UEBhMCRlIxDDAKBgNVBAoTA1NGUjEdMBsGA1UEAxMUU0ZSIFB1Ymxp
YyBBQyBSYWNpbmUwHhcNMDgwMzE3MTI1ODAwWhcNMTgwMzE3MTI1ODAwWjA+MQsw
CQYDVQQGEwJGUjEMMAoGA1UEChMDU0ZSMSEwHwYDVQQDExhTRlIgQUMgQ2VydGlm
aWNhdCBDbGllbnQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDUlFbr
0qmsAGdcxjUf1RWzvjDsJIwoCFvqHXup9EFnAd1cDsXMhNa7jyEHVYEJUQgZ05Ph
8TKcR1/wTwI+p46xAK/laAQECqzPMiRQkaRynt0EALVAdAZYjlvoF3PH/lJGZGAH
uKCityi/TNi7VpIvNqmGl0yJx9JlP8KIE6TWGaPF1t83IyMSlnpyVFhpK3g05uiu
zZ2/PxpVVq+zdIrerNlzbH1AzsgDg9Vq2llaKgkpp+zQYVGMClmOo8P3zfINaQy/
p6rUTMulJyzVeRQ+k4TyIGNLrZVvYJ4bpN0InP1EvLH/o6YcKD/+CUJ4CPTbdfhn
I7M6vldQQZxGLZEvAgMBAAGjgZgwgZUwLwYDVR0fBCgwJjAkoCKgIIYeaHR0cDov
L2NybC5zZnIuZnIvc2ZyX3Jvb3QuY3JsMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYD
VR0PAQH/BAQDAgEGMB0GA1UdDgQWBBQMei3GxO30L6CmaR78ZkJ11Qv4DDAfBgNV
HSMEGDAWgBTZPHYGD3xdFTvO0eb9FiKwuVk/+TANBgkqhkiG9w0BAQ0FAAOCAgEA
6XF6ttUZSlIyC6+SOXGHszlvjDU6n4F/naJ0jRQW5JT79G/bkzW2lrsV5TZri5Li
YLjRRmbmYnbOYRQt5i99pmO3ziTUmr2iDkC4ze88xz+kdlWheI9YVlBzUqk1QuDV
4WoUXNJAsGF9v7QoAzDxlOapPlyI7olgWjDbvraZE5TDMmzmL6ddTS4mxVTMjgj3
V5msN3xj6DSTjb4amAaqDtpe/VZryERtnTwAMMdgw5szfKgxiOCcknpJObBOs9zs
FLNWEzkqh22CCif19xl/Mq7prEefCUm/KewzRsPAYCVftTvBVEZUDxubHqQglQD2
WSwjhNiy0qzyU9wNG9w2b/l5pzu4XGbmgz5Ntxs4sEZAj6qOvxLyerpn7JVNTreb
Iu32uikZnqjijyKes+/JHNcUM5G58HmQak+eApIFMlTriUqm6KRy0JAvAxCrvVhx
7ry1ig3RESMNbhkmgjRFmDrN1/UCeU9Cxqs8grAc+Lqw7J8xBb1kNye96Z/+6a2Q
TUivQruIazALiaEJ9mG/6gYSPFAYhkVOhH4PWvMn4o1FFmbGN+AGbGLP/Fy5IFQq
nH398yjb1/pRVbhGC+kJzuOxkKsOJq8Ywh/WDONomqsTLkzEY669gKbOGUIeYtUY
HJ8pe+7GSsXo0Q/5iswaq8F1hQeXMchjZp4sq7f8gsA=
-----END CERTIFICATE-----
```

### 7.1.2 Certificat de signature des L.C.R.

Le certificat de signature des L.C.R. est le même que celui utilisé pour signer les certificats.

### 7.1.3 Certificat de signature des L.A.R.

Sans objet.

### 7.1.4 Certificat de signature des réponses O.C.S.P.

Sans objet.

## 7.2 Profils des certificats porteurs

Les certificats des porteurs de certificats émis dans le cadre de l'A.C. **SFR AC Certificat Client - Signature en ligne** respectent la norme X.509 V3.

| Champ | Valeur/profil | Description |
|---|---|---|
| **Version** | 3 (0x2) | |
| **Serial Number** | Numéro de série du certificat | Nombre aléatoire de 32 octets |
| **Signature Algorithm** | Sha256WithRSAEncryption | |
| **Issuer** | C=FR, O=SFR, CN=SFR AC Certificat Client | |
| **Not Before** | $T_0$ | Date de début de validité du certificat |
| **Not After** | $T_0$+30 minutes | Date de fin de validité du certificat |
| **Subject** | CN=*{Prénom et nom du porteur, séparés par un espace}*<br>EMAILADDRESS={adresse e-mail si présente}<br>SERIALNUMBER={numéro de RUM}<br>O=SFR<br>C=FR | |
| **Public Key Algorithm** | rsaEncryption | |
| **Public-Key** | 2048 bit | Clé publique du porteur |
| **Modulus** | … | Module de la clé |
| **Exponent** | … | Exposant de la clé |
| **X509v3 extensions** | | |
| **Basic Constraints (critical)** | CA:FALSE | |
| **Key Usage (critical)** | Non Repudiation | |

| Champ | Valeur/profil | Description |
|---|---|---|
| **Subject Key Identifier** | … | Identifiant de la clé publique du porteur |
| **CRL Distribution Points** | Full Name:<br>URI:http://crl.sfr.fr/sfr_client.crl | |
| **Certificate Policies** | Policy:1.2.250.1.35.25.2.1.2.10.1 | |
| **Authority Key Identifier** | keyid:0C:7A:2D:C6:C4:ED:F4:2F:A0:A6:69:1E:FC:66:42:75:D5:0B:F8:0C | Identifiant de la clé publique de l'A.C. *SFR AC Certificat Client* (voir 7.1.1 ci-dessus) |
| **Signature Algorithm** | Sha256WithRSAEncryption | |
| **Signature Value** | … | Valeur de la signature du certificat |

## 7.3 Profil des L.C.R.

| Champ | Valeur/profil | Description |
|---|---|---|
| **Version** | 2 (0x1) | |
| **Signature Algorithm** | Sha256WithRSAEncryption | |
| **Issuer** | C=FR, O=SFR, CN=SFR AC Certificat Client | |
| **Last Update** | $T_0$ | Date d'émission de la L.C.R. |
| **Next Update** | $T_0$+26heures | Date d'émission de la prochaine L.C.R. |
| **CRL extensions** | | |
| **CRL Number** | … | Numéro de la L.C.R. |
| **Issuing Distribution Point (critical)** | Full Name:<br>URI:http://crl.sfr.fr/sfr_client.crl | |
| **Authority Key Identifier** | keyid:0C:7A:2D:C6:C4:ED:F4:2F:A0:A6:69:1E:FC:66:42:75:D5:0B:F8:0C | Identifiant de la clé publique de l'A.C. *SFR AC Certificat Client* (voir 7.1.1 ci-dessus) |

| Champ | Valeur/profil | Description |
|---|---|---|
| **Revoked Certificates** | | *(une entrée par certificat de la liste)* |
| **Serial Number** | … | Numéro de série du certificat révoqué |
| **Revocation Date** | … | Date et heure de révocation |
| **CRL entry extensions** | `Invalidity Date:…` | Date et heure d'invalidité (identique à celle de révocation) |
| **CRL's signature** | | |
| **Signature Algorithm** | `Sha256WithRSAEncryption` | |
| **Signature Value** | … | Valeur de la signature de la L.C.R. |

# 8 Audit de conformité et autres évaluations

L'A.C. contrôle les exigences de la présente P.C. via des audits réalisés par des prestataires de services de confiance.

## 8.1 Fréquences ou circonstances des évaluations

Avant la mise en service de l'I.G.C. ou suite à toute modification significative d'un des composants de l'I.G.C., l'A.C. procède à un contrôle de conformité par rapport aux exigences présentées dans la P.C. et aux déclarations des pratiques énoncées dans la D.P.C.

L'A.C. procède régulièrement à un contrôle de conformité (au minimum tous les ans).

## 8.2 Identité et qualification des évaluateurs

Le contrôle d'une composante est assigné par l'A.C. à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

## 8.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit n'appartient pas à l'entité opérant la composante de l'I.G.C. contrôlée, quelle que soit cette composante, et est dûment autorisée à pratiquer les contrôles visés.

## 8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'I.G.C. (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'I.G.C. (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définis dans la P.C. de l'A.C. et dans la D.P.C. qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

## 8.5 Actions prises suite aux conclusions des évaluations

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

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

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'A.C. qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'A.C. et doit respecter ses politiques de sécurité internes.

- En cas de résultat "A confirmer", l'A.C. remet à la composante un avis précisant sous quel délai les non-conformités doivent être réparées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.

- En cas de réussite, l'A.C. confirme à la composante contrôlée la conformité aux exigences de la P.C. et de la D.P.C.

## 8.6 Communication des résultats

Les résultats des audits de conformité sont confidentiels et conservés par l'A.C. Ils sont communiqués par l'A.C. uniquement aux composantes concernées par l'audit.

# 9 Autres problématiques métiers et légales

## 9.1 Tarifs

La fourniture de certificats ne fait l'objet d'aucune facturation lors de la signature en ligne pour les clients SFR.

## 9.2 Responsabilité financière

### 9.2.1 Couverture par les assurances

Sans objet. Usage interne à SFR.

### 9.2.2 Autres ressources

Sans objet.

### 9.2.3 Couverture et garantie concernant les entités utilisatrices

La présente P.C n'apporte aucune couverture ou garantie financière aux entités utilisatrices.

## 9.3 Confidentialité des données professionnelles

### 9.3.1 Périmètre des informations confidentielles

Les informations suivantes sont considérées comme confidentielles :

- la D.P.C. (Déclaration des Pratiques de Certification) ;
- les clés privées de l'A.C., des composantes et des porteurs de certificats ;
- les données associées aux clés privées d'A.C. et des porteurs de certificats ;
- tous les secrets de l'I.G.C. ;
- les rapports d'audits ;
- le dossier d'enregistrement des demandeurs de certificat ;
- les journaux d'évènements des composantes de l'I.G.C. ;
- les causes de révocations, sauf accord explicite de publication.

### 9.3.2 Responsabilités en terme de protection des informations confidentielles

L'A.C. s'engage à traiter les informations confidentielles recueillies dans le respect des lois et règlements en vigueur.

## 9.4 Protection des données personnelles

### 9.4.1 Politique de protection des données personnelles

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'A.C. et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur, en particulier de la loi dite « Informatique et Libertés » du 6 janvier 1978, modifiée le 6 août 2004.

### 9.4.2 Informations à caractère personnel

Les informations nominatives recueillies dans le cadre du processus de délivrance du certificat sont considérées comme personnelles.

### 9.4.3 Informations à caractère non personnel

Les autres données figurant dans le certificat sont considérées comme non personnelles.

### 9.4.4 Responsabilité en termes de protection des données personnelles

Cf. législation et réglementation en vigueur.

### 9.4.5 Notification et consentement d'utilisation des données personnelles

Cf. législation et réglementation en vigueur.

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

Cf. législation et réglementation en vigueur

### 9.4.7 Autres circonstances de divulgation d'informations personnelles

Sans objet.

## 9.5 Droits sur la propriété intellectuelle et industrielle

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

Le porteur de certificat n'acquiert pas le droit de propriété du certificat en raison de la durée de vie temporaire du certificat et de sa destruction irrémédiable après l'usage.

## 9.6 Obligations

Les obligations communes aux composantes de l'I.G.C. sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ;
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la P.C. de l'A.C. et les documents qui en découlent ;
- respecter et appliquer la partie de la D.P.C. leur incombant (cette partie doit être communiquée à la composante correspondante) ;
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'A.C. (cf. chapitre 8) et l'organisme de qualification ;
- respecter les accords ou contrats qui les lient entre elles ou aux utilisateurs ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

### 9.6.1 Autorités de Certification

L'A.C. a pour obligation de :

- pouvoir démontrer aux porteurs de ses certificats qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, conformément aux exigences du chapitre 4.4 ci-dessus ;
- garantir et maintenir la cohérence de sa D.P.C. avec sa P.C. ;
- prendre toutes les mesures raisonnables pour s'assurer que ses porteurs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'I.G.C.

L'A.C. est responsable de la conformité de sa Politique de Certification, avec les exigences émises dans la présente P.C. pour le niveau de sécurité considéré. L'A.C. assume toute conséquence dommageable résultant du non-respect de sa P.C., conforme aux exigences de la présente P.C., par elle-même ou l'une de ses composantes.

De plus, l'A.C. reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données

personnelles des porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'A.C.

Par ailleurs, l'A.C. reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes.

### 9.6.2 Porteurs de certificats

Le porteur de certificat a le devoir de :

- communiquer des informations exactes et à jour lors de la demande du certificat ;
- respecter les conditions d'utilisation de sa clé privée et du certificat correspondant.

La relation entre le porteur de certificat et l'A.C. ou ses composantes est formalisée par un engagement du porteur visant à certifier l'exactitude des renseignements et des documents fournis.

### 9.6.3 Obligations de l'O.C

En tant que prestataire de services, l'O.C s'engage à respecter la D.P.C et le contrat de service établi avec l'A.C. Il est notamment responsable des niveaux de disponibilité de l'infrastructure et de la mise à disposition des informations de vérification des statuts des certificats.

### 9.6.4 Autres participants

#### 9.6.4.1 Applications utilisatrices

Les applications utilisatrices ont l'obligation de vérifier la validité du certificat qui leur est présenté, en s'assurant que :

- Le certificat est valide au moment de l'opération de signature
- N'est pas inscrit dans la LCR
- Est émis par l'A.C.

## 9.7 Limite de responsabilité

L'A.C. décline toute responsabilité à l'égard de l'usage qui est fait des certificats qu'elle a émis dans des conditions et à des fins autres que celles prévues dans la présente politique de certification que dans tout autre document contractuel applicable associé.

L'A.C. décline toute responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, documents, et

quant aux retards, à l'altération ou autres erreurs pouvant se produire dans la transmission de toute télécommunication.

L'A.C. ne saurait être tenue responsable, et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente politique lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'Article 1148 du Code civil.

De façon expresse, sont considérés comme cas de force majeure ou cas fortuit, ceux habituellement retenus par la jurisprudence des cours et tribunaux français.

## 9.8 Durée et fin anticipée de validité de la P.C.

### 9.8.1 Durée de validité

La P.C. de l'A.C. reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette P.C.

### 9.8.2 Fin anticipée de validité

En fonction de la nature et de l'importance des évolutions apportées dans l'I.G.C., l'A.C. peut faire évoluer la P.C. La publication d'une nouvelle version de la présente politique de certification détaillera le délai et les mesures à apporter pour la mise en conformité.

### 9.8.3 Effets de la fin de validité et clauses restant applicables

Certaines fonctions de l'I.G.C. tel que l'horodatage, l'archivage et la protection des données confidentielles seront maintenues jusqu'à leur terme.

## 9.9 Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'I.G.C., l'A.C. fera valider au plus tard un mois avant le début de l'opération, ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'A.C. et de ses différentes composantes.

La notification auprès des utilisateurs de certificats sera effectuée uniquement en cas d'impact déterminant, à la libre appréciation de l'A.C.

## 9.10 Amendements à la P.C.

### 9.10.1 Procédures d'amendements

L'A.C. contrôlera que tout projet de modification de sa P.C. reste conforme aux exigences de la législation et de la réglementation en vigueur et aux exigences sécurité.

### 9.10.2 Mécanisme et période d'information sur les amendements

Une information sur l'amendement de la P.C. en proposant la nouvelle version à télécharger sera publiée sur le site internet http://www.sfr.fr/signature-electronique/

### 9.10.3 Circonstances selon lesquelles l'OID doit être changé

L'OID de la P.C. de l'A.C. évoluera dès lors qu'un changement majeur (et qui sera signalé comme tel, notamment par une évolution de l'OID de la présente P.C.) intervient dans les exigences de la présente P.C.

## 9.11 Dispositions concernant la résolution de conflits

Tous différends découlant des services de certification doivent, en premier lieu, et dans toute la mesure du possible, être réglés au moyen de négociations amiables entre les parties.

## 9.12 Juridictions compétentes

Tous différends liés à l'interprétation ou à l'exécution de la P.C. seront soumis à la compétence expresse du **Tribunal de Commerce de Paris,** nonobstant pluralité de défendeurs ou appel en garantie, y compris pour les procédures d'urgence ou les procédures conservatoires, en référé ou par requête.

## 9.13 Conformité aux législations et réglementations

Les textes législatifs et réglementaires dont la présente P.C. s'est inspirée pour une signature dite « simple » sont :

- Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
- Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
- Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.
- Loi n° 90-1170 du 29 12 90, modifiée par la loi 91-648 du 11 juillet 1991, modifiée par la loi 96-659 du 26 juillet 1996 sur la réglementation des télécommunications, notamment son article 28.
- Décret n°98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie, modifié par le décret n°2002-688 du 2 mai 2002.
- Arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie.
- Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.

### 9.13.1 Transfert d'activités

Cf. chapitre 5.8 sur la fin de vie de l'I.G.C.

### 9.13.2 Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.