POLITIQUE DE CERTIFICATION

AUTORITÉ DE CERTIFICATION
SFR CERTIFICAT CLIENT

Récapitulatif des éditions

Version	Date	Nom du rédacteur	Nature de la modification
1.0	05/2011	Christian Bouvier	Création du document

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.

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 et d'authentification avec un dispositif de création de signature électronique « **simple** » dans le cadre des actes de souscription et de gestion des actes dématérialisés en point de vente SFR et des usages sur mobile. 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.

La politique de certification a été rédigée selon le document *Politique de certification type « Signature »*, version 2.3, tirée du *Référentiel général de sécurité* (R.G.S.), version 1.0, et conformément à la norme *ETSI TS 101 456* v1.4.3 du 15-05-2007 (AFNOR Z 74-400).

1.2 Identification de la P.C.

Le présent document est identifié par l'O.I.D n° 1.2.250.1.35.25.2.1.2.7.1.

La déclaration des pratiques de certification (D.P.C) est identifiée par l'O.I.D n°1.2.250.1.35.25.2.1.2.2.1.

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

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 d'utilisateurs 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 la validité des certificats qu'elle émet dans le cadre du respect des conditions de révocation.

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 d'autorité d'enregistrement (O.E)
L'opérateur d'autorité d'enregistrement est un salarié du distributeur agréé en charge de l'accueil des clients, de la commercialisation des produits et des opérations de contractualisation.

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 sont détaillées dans la Déclaration des Pratiques de Certification (D.P.C.).

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.

1.4 Usages des certificats

1.4.1 Domaines d'utilisation applicables

L'Autorité de Certification *SFR AC Certificat Client* distribue des certificats électroniques aux clients de SFR afin de leur permettre de signer électroniquement tout type de document et, en particulier, tout acte de souscription et de gestion dématérialisés en point de vente ou sur mobile.

L'utilisation de ces certificats est réservée aux clients 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. effectuera donc en ce sens des contrôles réguliers de conformité et de bon fonctionnement des composantes de cette I.G.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

Abréviations	Signification
HSM	*Hardware Security Module*
HTTP	*Hyper Text Transfer Protocol*
I.G.C.	Infrastructure à Gestion de Clés
L.C.R.	Liste de Certificats Révoqués
LDAP	*Light-weight Directory Access Protocol*
NAT	*Network Address Translation*
O.S.C.	Opérateur de Services de Certification
OTA	*Over The Air*
PIN	*Personal Identification Number*
PKI	*Public Key Infrastructure*
P.C.	Politique de Certification
PUK	*Personal Unlocking Key*
R.G.S.	Référentiel Général de Sécurité
SIM	*Subscriber Identity Module*
SMS	*Short Message Service*
SSCD	*Secure Signature-Creation Device*
URL	*Uniform Resource Locator*

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 de l'utilisateur 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 l'utilisateur 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 l'utilisateur de certificat pour stocker et mettre en œuvre sa clé privée de signature (ex : Carte SIM).

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 utilisateurs 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.

La notion de personne majeure pourra éventuellement évoluée, à la cible on pourra accepter aussi les mineurs émancipés.

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

2.1 Entités chargées de la mise à disposition des informations

L'A.C. a mis en œuvre au sein de son I.G.C. une fonction de publication et une fonction d'information sur l'état des certificats.

Entité chargée de la publication des certificats :

Direction Commerciale de SFR

Entité chargée de l'information sur l'état des certificats :

(sans objet : fonction non mise en œuvre)

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
- la liste des certificats de l'A.C. et les certificats de la hiérarchie des A.C.
- les parties publiques de la Déclaration des pratiques de certification de l'A.C. « SFR AC Certificat Client »
- les *Conditions générales d'utilisation* et les informations nécessaires pour permettre aux utilisateurs d'accéder au portail de gestion de leur certificat

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

2.1.2 Publication de la L.C.R.

La liste des certificats révoqués (L.C.R.) est publiée sur à l'adresse suivante :

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

La liste des autorités révoquées (L.A.R.) est publiée sur les annuaires *LDAP* suivants :

(sans objet)

2.1.3 Délais et fréquences de publication

Les informations liées à l'I.G.C. (nouvelle version de la P.C., formulaires, etc.) doivent être 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 systèmes publiant les informations liées à l'I.G.C. ont une disponibilité de 99,99 % (contractuellement) (minimum requis : les Jours ouvrés).

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

Les systèmes publiant les certificats d'A.C. et les L.C.R. ont une disponibilité de 99,99 % (contractuellement) (minimum requis de 24 heures sur 24 et 7 jours sur 7).

Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites en 4.10.

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.

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

L'A.C. publie sa L.C.R. à la fréquence suivante : une fois par jour (en pratique, toutes les 12 heures)

2.1.3.3 Fréquence de publication de la L.A.R.

La liste des autorités révoquées est publiée (sans objet).

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.

3 Identification et authentification

3.1 Nommage

3.1.1 Type de noms

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

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

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les utilisateurs de certificats doivent être explicites.

Le DN de l'utilisateur de certificat est construit à partir du nom, prénom de son état civil tel qu'ils sont portés sur les pièces justificatives présentées à l'A.E. et lues par le Terminal.

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

3.1.3 Anonymisation ou pseudonymique des utilisateurs de certificats

L'utilisation d'un pseudonyme n'est pas autorisée dans le certificat.

3.1.4 Règles d'interprétation des différentes formes de nom

Seul le nom patronymique lu par le Terminal à partir de la piste *MRZ* est reconnu, dans la limite de 25 caractères.

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 de l'utilisateur de certificat
- le numéro de titulaire du client.

3.1.6 Identification, authentification et rôle des marques déposées

Sans objet. Aucun nom de marque n'est présent dans le nom d'utilisateur inscrit dans le certificat.

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

L'utilisateur de certificat ne génère pas sa bi-clé. Celle-ci est générée par la carte SIM qui lui sera remise à la fin du processus de contractualisation.

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

Ce chapitre ne concerne que l'enregistrement d'un demandeur à titre particulier.

Le demandeur doit se présenter en personne auprès de l'A.E. afin de procéder à la procédure de demande de certificat. L'A.E., par l'intermédiaire des opérateurs A.E., assure les procédures d'identification et de vérification des identités sur la base des pièces justificatives remises en face à face.

L'authentification de l'identité d'un demandeur est basée sur les éléments suivants :

- nom patronymique ;
- prénom ;
- date de naissance ;
- pièce d'identité officielle valide (avec photo) comportant une piste *MRZ* (*Machine Readable Zone)* telle que :
    - Carte d'identité Nationale avec piste *MRZ*
    - Carte de séjour avec piste *MRZ*
    - Passeport avec piste *MRZ*

Les données lues sur les pièces présentées, l'horodatage, l'adresse IP de le Terminal ainsi que les éléments biométriques (vitesse et pression) de la signature digitale manuscrite, le fichier PDF de la demande de certificat constituent le dossier d'enregistrement ; ce dossier est conservé en numérique par l'A.C.

3.2.4 Informations non vérifiées de l'utilisateur de certificat

Les informations non vérifiées sont l'adresse postale, l'adresse e-mail et le nom d'usage.

3.2.5 Validation de l'autorité du demandeur

Sans objet pour le particulier.

3.2.6 Critères d'interopérabilité

Sans objet.

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

3.3.1 Identification et validation pour un renouvellement courant

Lors du premier renouvellement, la vérification de l'identité de l'utilisateur est optionnelle.

Lors du renouvellement suivant, l'A.E., saisie de la demande, identifiera l'utilisateur selon la même procédure que pour l'enregistrement initial ou une procédure offrant un niveau de garantie équivalent.

3.3.2 Identification et validation pour un renouvellement après révocation

La procédure d'identification et de renouvellement suite à révocation est identique à celle de l'enregistrement initial.

3.3.3 Identification et validation d'une demande de révocation

Pour révoquer son certificat, l'utilisateur s'authentifie sur le portail client de SFR en utilisant les questions personnelles configurées lors de son enrôlement (authentification à plusieurs facteurs).

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 ne peut être effectuée que sur place en face à face entre le demandeur et l'opérateur de l'Autorité d'Enregistrement.

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

Les informations suivantes doivent faire partie de la demande de certificat :

- les données lues sur le Terminal sur les pièces présentées
  - nom patronymique ;
  - prénom ;
  - date de naissance ;
- Les images scannées des pièces d'identité
- l'adresse ;
- l'e-mail ;
- les données techniques de la demande ;
- l'horodatage de la demande ;
- l'adresse IP du Terminal ;
- les éléments biométriques (vitesse et pression) de la signature digitale manuscrite ;
- le fichier PDF de la demande de certificat.

Le dossier de demande de certificat est établi électroniquement depuis le Terminal de l'A.E. Il est transmis automatiquement à l'A.C. et 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

Les informations d'identification du demandeur sont vérifiées conformément au chapitre 3.2.3.

L'A.E. doit effectuer les opérations suivantes :

- valider l'identité du futur utilisateur de certificat ;
- vérifier la cohérence des pièces justificatives ;
- enregistrer les pièces justificatives à travers le Terminal par lecture des bandes *MRZ* ou magnétiques ;
- s'assurer que le demandeur a apposé une signature manuscrite digitalisée sur la demande de certificat ;
- vérifier que le dossier de demande électronique a été envoyé pour archivage.

4.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, l'A.E. en informe l'utilisateur de certificat en justifiant les causes.

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 3 ans.

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 l'utilisateur 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).

4.3.2 Notification par l'A.C. de la délivrance du certificat à l'utilisateur

Le certificat complet et exact doit être mis à la disposition de son utilisateur.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Le certificat est considéré accepté à partir du moment où l'utilisateur a validé l'écran d'acceptation et a utilisé le certificat lors de la signature de son contrat.

4.4.2 Publication du certificat

Les certificats des utilisateurs ne sont pas publiés.

4.5 Usages de la bi-clé et du certificat

L'utilisation de la clé privée et du certificat associé de l'utilisateur de certificat est strictement limitée à la signature électronique et l'authentification personnelle de l'utilisateur et, en particulier, de tout acte de souscription et de gestion dématérialisée en point de vente SFR ou sur le mobile.

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

4.6 Renouvellement d'un certificat

Sans objet. Dans la cadre de la présente politique, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante.

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

4.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi, les bi-clés des utilisateurs, et les certificats correspondants, seront renouvelés au minimum tous les 3 ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat de l'utilisateur.

4.7.2 Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat de l'utilisateur peut-être automatique ou bien à l'initiative de l'utilisateur.

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

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre 4.3.1.

Pour les actions de l'A.C., voir chapitre 4.3.1.

4.7.4 Notification à l'utilisateur de l'établissement du nouveau certificat

Voir chapitre 4.3.2.

4.7.5 Démarche d'acceptation du nouveau certificat

Voir chapitre 4.4.1.

4.7.6 Publication du nouveau certificat

Voir chapitre 0.

4.7.7 Notification par l'A.C. aux autres entités de la délivrance du nouveau certificat

Voir chapitre 4.3.

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 Certificats d'utilisateurs

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

- le certificat n'a pas été transmis correctement au Terminal (erreur technique)
- L'utilisateur refuse son certificat lors du processus de remise
- les informations de l'utilisateur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat
- l'utilisateur n'a pas respecté les modalités applicables d'utilisation du certificat

- l'utilisateur ou, le cas échéant, le M.C. ou l'entité n'ont pas respecté leurs obligations découlant de la P.C. de l'A.C.
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement de l'utilisateur
- la clé privée de l'utilisateur est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées)
- l'utilisateur ou une entité autorisée (représentant légal de l'entité ou M.C. par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée de l'utilisateur ou de son support)
- le décès de l'utilisateur

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.).

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. ou de réponses O.C.S.P.) :

- 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 Certificats d'utilisateur

Les personnes et entités qui peuvent demander la révocation d'un certificat utilisateur sont les suivantes :

- L'utilisateur au nom duquel le certificat a été émis
- l'A.C. émettrice du certificat ou l'une de ses composantes (A.E.)

Nota : L'utilisateur doit être informé des personnes et entités susceptibles d'effectuer une demande de révocation pour son certificat.

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 Certificats d'utilisateurs

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre 3.3.3.

La procédure est déclenchée par l'un des événements suivants :

- L'utilisateur dépose une demande de révocation sur son portail *SelfCare* (portail client de SFR)

Le demandeur de la révocation doit être informé du bon déroulement de l'opération et de la révocation effective du certificat. De plus, si l'utilisateur du certificat n'est pas le demandeur, il doit également être informé de la révocation effective de son certificat.

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

Voir la D.P.C.

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

Le point de contact identifié sur le site http://www.references.modernisation.gouv.fr doit être immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification. La D.G.M.E. et l'A.N.S.S.I. se réservent le droit de diffuser par tout moyen l'information auprès des promoteurs d'applications au sein des autorités administratives et auprès des usagers.

4.9.4 Délai accordé à l'utilisateur de certificat pour formaliser la demande de révocation

Dès que l'utilisateur (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

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

4.9.5.1 Certificats d'utilisateurs

Par nature, une demande de révocation doit être traitée en urgence.

La fonction de gestion des révocations doit être disponible 24h/24h.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) inférieure à 2 heures (jours ouvrés) et une durée maximale totale d'indisponibilité par mois inférieure à 16 heures (jours ouvrés).

Toute demande de révocation d'un certificat utilisateur doit être traitée dans un délai inférieur à 72 heures, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

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. doit être 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. ou de réponses O.C.S.P.) doit être effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

4.9.6 Exigences de vérification de la révocation par les destinataires de certificats

Toute personne recevant un certificat d'utilisateur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante.

La méthode utilisée (L.C.R., L.C.R., O.C.S.P., …) est à l'appréciation de celle-ci, selon sa disponibilité et les contraintes liées à son application.

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.

Les L.C.R. doivent être publiées 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. Voir ci-dessous pour la disponibilité des L.C.R.

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

Voir 4.9.6.

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.

4.9.14 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

L'A.C. fournit à l'application utilisatrice de certificats (le dispositif de signature du Terminal et le dispositif de signature pour le mobile) 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.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) inférieure à 4 heures (jours ouvrés) et une durée maximale totale d'indisponibilité par mois inférieure à 32 heures (jours ouvrés).

4.10.3 Dispositifs optionnels

Sans objet.

4.11 Fin de la relation entre l'utilisateur de certificat et l'A.C.

En cas de fin de relation contractuelle entre l'A.C. et l'utilisateur avant la fin de validité du certificat, la désactivation de la carte SIM entraîne *de facto* l'impossibilité d'utiliser le certificat (plus précisément, la clé privée associée).

4.12 Séquestre de clé et recouvrement

Sans objet. Pas de séquestre des clés privées des utilisateurs de certificats.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

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

Sans objet.

5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

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.

Les sites d'A.E. sont sous la surveillance du personnel travaillant sur place, d'autres personnels ou par des équipes de sécurité. Les sites sont ouverts au public de manière limitée à certains horaires et pour des raisons précises. Les stations de travail des A.E. doivent être situées dans des emplacements restreints au personnel autorisé et où les visiteurs sont accompagnés.

5.1.3 Alimentation électrique et climatisation

L'A.C. s'assure que les installations de fourniture d'électricité et de climatisation sont suffisantes pour son fonctionnement.

5.1.4 Vulnérabilité aux dégâts des eaux

L'A.C. s'assure que ses composantes 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 s'assure que ses composantes sont protégées par un système d'extinction d'incendies.

5.1.6 Conservation des supports

L'A.C. s'assure que les supports de stockage utilisés 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.

Ingénieur 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 - 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.

Contrôleur - Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'I.G.C. et aux politiques de sécurité de la composante.

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 (Cf. la D.P.C.).

5.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'I.G.C. vérifie l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

- que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'I.G.C.

Ces contrôles doivent être décrits dans la D.P.C. de l'A.C. et doivent être conformes à la politique de sécurité de la composante. Chaque attribution d'un rôle à un membre du personnel de l'I.G.C. doit être notifiée par écrit.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul doivent être respectées.

Les attributions associées à chaque rôle doivent être décrites dans la D.P.C. de l'A.C. et être conformes à la politique de sécurité de la composante concernée.

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur ;
- contrôleur et tout autre rôle ;
- ingénieur système et opérateur.

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 doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'I.G.C.

L'A.C. doit informer toute personne intervenant dans des rôles de confiance de l'I.G.C. :

- 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

Chaque entité opérant une composante de l'I.G.C. doit mettre en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante.

Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions. Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

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.

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont 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, etc. 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

Chaque personnel dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. 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, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

5.3.9 Type d'évènements à enregistrer

Chaque entité opérant une composante de l'I.G.C. journalise au minimum les évènements suivants, automatiquement dès le démarrage d'un système et sous forme électronique, concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre de l'I.G.C. :

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;

- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres évènements sont aussi recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les accès physiques ;
- les actions de maintenance et de changements de la configuration des systèmes ;
- les changements apportés au personnel ;
- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les utilisateurs de certificats,.).

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'I.G.C., des évènements spécifiques aux différentes fonctions de l'I.G.C. sont journalisés notamment :

- réception initiale d'une demande de certificat ;
- validation / rejet d'une demande de certificat ;
- évènements liés aux clés de signature et aux certificats d'A.C. (génération (cérémonie des clés) ;
- sauvegarde / récupération, révocation, destruction,.) ;
- génération des certificats des utilisateurs de certificats ;
- transmission des certificats aux utilisateurs de certificats ;
- publication et mise à jour des informations liées à l'A.C. (PC, certificats d'A.C., etc.) ;
- génération puis publication des LCR ;
- le cas échéant, requêtes / réponses OCSP.

Chaque enregistrement d'un évènement dans un journal contient au minimum les champs suivants :

- type de l'évènement ;
- nom de l'exécutant ou référence du système déclenchant l'évènement ;
- date et heure de l'évènement en heure locale ;
- résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'évènements.

De plus, en fonction du type de l'évènement, chaque enregistrement contient les champs suivants :

- destinataire de l'opération ;
- nom du demandeur de l'opération ou référence du système effectuant la demande ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- cause de l'évènement ;
- toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

Les opérations de journalisation doivent être effectuées au cours du processus.

En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'évènement.

5.3.10 Fréquence de traitement des journaux d'évènements

Les journaux d'évènements sont contrôlés par le personnel de l'A.C. comme décrit au paragraphe 5.3.16.

5.3.11 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pendant au moins un délai de trois mois.

Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous le délai de deux mois.

5.3.12 Protection des journaux d'évènements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Le système de datation des évènements respecte les exigences du chapitre 6.8.

5.3.13 Procédure de sauvegarde des journaux d'évènements

Chaque entité opérant une composante de l'I.G.C. met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente P.C.

5.3.14 Système de collecte des journaux d'évènements

Ce point est précisé dans la D.P.C.

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

Ce point est précisé dans la D.P.C.

5.3.16 Évaluation des vulnérabilités

Chaque entité opérant une composante de l'I.G.C. est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements sont contrôlés régulièrement afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux doivent être analysés dans leur totalité au moins une fois par mois. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fera apparaître les anomalies et les falsifications constatées.

5.4 Archivage des données

5.4.1 Types de données à archiver

Des dispositions en matière d'archivage sont également prises par l'A.C. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'I.G.C.

Il doit également permettre la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

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 accords contractuels avec d'autres A.C. ;
- les certificats et LCR tels qu'émis ou publiés ;
- les demandes de certificats ;
- les dossiers d'enregistrement des utilisateurs de certificats ;
- les journaux d'évènements des différentes entités de l'I.G.C.

5.4.2 Période de conservation des archives

Les journaux d'événements doivent être conservés sur site pendant au moins 1 mois.

Ils doivent être archivés le plus rapidement possible après leur génération et au plus tard sous le délai de 1 mois (recouvrement possible entre la période de conservation sur site et la période d'archivage).

5.4.3 Dossiers de demande de certificat

Tout dossier d'enregistrement est archivé pendant au moins 10 ans après la résiliation mettant fin à la relation contractuelle.

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

Ce dossier, complété par les mentions consignées par l'A.E., doit permettre de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'A.C.

Certificats et LCR émis par l'A.C.
Les certificats des utilisateurs de certificat et de l'A.C., ainsi que les LCR / LAR produites, sont archivés pendant 10 ans après l'expiration de ces certificats.

Journaux d'évènements
Les journaux d'évènements traités au chapitre 5.3 seront archivés pendant 10 ans après leur génération. Les moyens mis en œuvre par l'A.C. pour leur archivage devront offrir le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements sera assurée tout au long de leur cycle de vie.

5.4.4 Protection des archives

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

- être protégées en intégrité ;
- être accessibles aux personnes autorisées ;

- pouvoir être relues et exploitées.

Ce point est précisé dans la D.P.C.

5.4.5 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.

5.4.6 Exigences d'horodatage des données

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

5.4.7 Système de collecte des archives

Ce point est précisé dans la D.P.C.

5.4.8 Procédures de récupération et de vérification des archives

Les archives électroniques doivent pouvoir être récupérées dans un délai inférieur à 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).

5.5 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 la période de validité de ce certificat de l'A.C. doit être supérieure à celle des certificats qu'elle signe.

Au regard de la date de fin de validité de ce certificat, son renouvellement doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'A.C. 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.

5.6 Reprise suite à compromission et sinistre

5.6.1 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, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé …).

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

Chaque composante de l'I.G.C. dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'I.G.C. découlant de la présente P.C. et des résultats de l'analyse de risque de l'I.G.C., notamment en ce qui concerne les fonctions liées à la publication ou liées à la révocation des certificats.

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle 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.

5.6.4 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.

5.7 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.

5.7.1 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. doit respecter d'autres obligations :

- 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 utilisateurs 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.

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.

5.7.2 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 aux 1), 2), et 3) 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.

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

- s'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- révoquer son certificat ;
- révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- informer (par exemple par récépissé) tous les utilisateurs de certificat des certificats révoqués ou à révoquer.

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.

6.1.2.2 Clés des utilisateurs de certificats

La génération des clés des utilisateurs de certificats est effectuée sur une carte SIM insérée dans le Terminal ou sur le mobile en présence des utilisateurs de certificats. Transmission de la clé privée à son propriétaire

La clé privée est transmise au porteur lorsqu'on lui remet sa carte SIM à la fin du processus de contractualisation.

6.1.3 Transmission de la clé publique à l'A.C.

La clé publique de l'utilisateur de certificat vers une composante de l'A.C. est protégée à travers un tunnel chiffré et son origine est authentifiée par un certificat et une adresse IP.

6.1.4 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 par un moyen qui assure l'intégrité de bout en bout et qui en authentifie l'origine à travers un tunnel sécurisé.

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 disponible et peuvent être récupérables.

6.1.5 Tailles des clés

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

6.1.6 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.

6.1.7 Objectifs d'usage de la clé

L'utilisation de la clé privée de l'utilisateur de certificat et du certificat associé est strictement limitée au service de signature électronique des actes dématérialisés en point de vente et d'authentification ou de signature électronique d'actes dématérialisés sur mobile.

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 utilisateurs de certificats

Le dispositif de création de signature des utilisateurs 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 ».

6.2.2 Contrôle de la clé privée 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 utilisateurs 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 utilisateurs 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 utilisateurs de certificats

Les clés sont activées par le dispositif de signature dans le Terminal lors des opérations de signature électronique des actes dématérialisés en point de vente ou sur le mobile.

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 utilisateurs de certificats

La carte SIM permet une désactivation sécurisée des clés privées des utilisateurs.

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.

Le dispositif de création de signature des utilisateurs de certificats est évalué 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 utilisateurs de certificats sont archivées dans le cadre de l'archivage des certificats correspondants.

6.3.2 Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des utilisateurs de certificats ont une durée de vie de 3 ans.

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 de l'utilisateur de certificat

Les données d'activation de la clé privée de l'utilisateur sont configurées par celui-ci durant le processus d'enrôlement (code PIN de signature sur la carte SIM).

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) ;
- éventuellement, gestion des reprises sur erreur.

Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires.

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

L'implémentation du système permettant de mettre en œuvre les composantes de l'I.G.C. est documentée et respecte dans la mesure du possible des normes de modélisation et d'implémentation.

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

Toute évolution significative d'un système d'une composante de l'I.G.C. est signalée à l'A.C. pour validation. Elle est documentée et apparait dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

6.7 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'I.G.C.

De plus, les échanges entre composantes au sein de l'I.G.C. mettent en œuvre des mesures particulières en fonction du niveau de sensibilité des informations (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 interne.

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 bit)

Champ	Valeur
Modulus	00:d4:94:56:eb:d2:a9:ac:00:67:5c:c6:35:1f:d5: 15:b3:be:30:ec:24:8c:28:08:5b:ea:1d:7b:a9:f4: 41:67:01:dd:5c:0e:c5:cc:84:d6:bb:8f:21:07:55: 81:09:51:08:19:d3:93:e1:f1:32:9c:47:5f:f0:4f: 02:3e:a7:8e:b1:00:af:e5:68:04:04:0a:ac:cf:32: 24:50:91:a4:72:9e:dd:04:00:b5:40:74:06:58:8e: 5b:e8:17:73:c7:fe:52:46:64:60:07:b8:a0:a2:b7: 28:bf:4c:d8:bb:56:92:2f:36:a9:86:97:4c:89:c7: d2:65:3f:c2:88:13:a4:d6:19:a3:c5:d6:df:37:23: 23:12:96:7a:72:54:58:69:2b:78:34:e6:e8:ae:cd: 9d:bf:3f:1a:55:56:af:b3:74:8a:de:ac:d9:73:6c: 7d:40:ce:c8:03:83:d5:6a:da:59:5a:2a:09:29:a7: ec:d0:61:51:8c:0a:59:8e:a3:c3:f7:cd:f2:0d:69: 0c:bf:a7:aa:d4:4c:cb:a5:27:2c:d5:79:14:3e:93: 84:f2:20:63:4b:ad:95:6f:60:9e:1b:a4:dd:08:9c: fd:44:bc:b1:ff:a3:a6:1c:28:3f:fe:09:42:78:08: f4:db:75:f8:67:23:b3:3a:be:57:50:41:9c:46:2d: 91:2f
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

Champ	Valeur
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 utilisateurs

Les certificats des utilisateurs de certificats émis dans le cadre de l'A.C. **SFR AC Certificat Client** respectent la norme X.509 V.3.

Champ	Valeur/profil	Description
Version	3 (0x2)	
Serial Number	Numéro de série du certificat	Nombre aléatoire de 32 octets
Signature Algorithm	sha1WithRSAEncryption	
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+3 ans	Date de fin de validité du certificat
Subject	C=FR O=SFR SerialNumber=*{identifiant unique du porteur}* CN=*{Prénom et nom du porteur, séparés par un espace}*	
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, Digital Signature	
Subject Key Identifier	…	Identifiant de la clé publique du porteur
CRL Distribution Points	Full Name: URI:http://crl.sfr.fr/sfr_client.crl	
Certificate Policies	Policy:1.2.250.1.35.25.2.1.2.7.1	

Champ	Valeur/profil	Description
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	sha1WithRSAEncryption	
Signature Value	…	Valeur de la signature du certificat

7.3 Profil des L.C.R.

Champ	Valeur/profil	Description
Version	2 (0x1)	
Signature Algorithm	sha1WithRSAEncryption	
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: 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)
Revoked Certificates		*(une entrée par certificat de la liste)*
Serial Number	…	Numéro de série du certificat révoqué
Revocation Date	…	Date et heure de révocation

Champ	Valeur/profil	Description
CRL entry extensions	`Invalidity Date:…`	Date et heure d'invalidité (identique à celle de révocation)
CRL's signature		
Signature Algorithm	`sha1WithRSAEncryption`	
Signature Value	…	Valeur de la signature de la L.C.R.

8 Audit de conformité

8.1 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.

8.2 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).

8.3 Identité et qualification des évaluateurs

Le contrôle d'une composante doit être 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.

8.4 Relations entre évaluateurs et entités évaluées

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

8.5 Sujets couverts par les évaluations

Les contrôles de conformité porte 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 vise à vérifier le respect des engagements et pratiques définies 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.).

8.6 Actions prises suite aux conclusions des évaluations

À 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.

8.7 Communication des résultats

Les résultats des audits de conformité sont 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

Sans objet.

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

Sans objet.

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 utilisateurs de certificats ;
- les données associées aux clés privées d'A.C. et des utilisateurs 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 Informations hors du périmètre des informations confidentielles

Sans Objet.

9.3.3 Responsabilités en terme de protection des informations confidentielles

L'A.C. respecte la législation et la réglementation 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.

9.4.2 Informations à caractère personnel

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

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.

9.6 Interprétations contractuelles et garanties

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 utilisateurs de ses certificats qu'elle a émis un certificat pour un utilisateur donné et que cet utilisateur a accepté le certificat, conformément aux exigences du chapitre 4.5 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 utilisateurs 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. La relation entre un utilisateur de certificat et l'A.C. est formalisée par un lien contractuel / hiérarchique / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'A.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 utilisateurs 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 Service d'enregistrement

L'A.E. (Autorité d'Enregistrement) s'engage à vérifier l'authenticité des pièces justificatives et l'exactitude des mentions qui établissent l'identité du demandeur selon les procédures décrites.

9.6.3 Utilisateurs de certificats

L'utilisateur 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 l'utilisateur de certificat et l'A.C. ou ses composantes est formalisée par un engagement de l'utilisateur visant à certifier l'exactitude des renseignements et des documents fournis.

9.6.4 Autres participants

Sans objet.

9.7 Limite de garantie

Sans objet.

9.8 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, lettres, 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.

9.9 Indemnités

Sans objet.

9.10 Durée et fin anticipée de validité de la P.C.

9.10.1 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.

9.10.2 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.

9.10.3 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.

9.11 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. devra :

- au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique ou d'audit, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'A.C. et de ses différentes composantes.

9.12 Amendements à la P.C.

9.12.1 Procédures d'amendements

L'A.C. contrôlera que tout projet de modification de sa P.C. reste conforme aux exigences aux documents de référence. En cas de changement important l'A.C. fera appel à une expertise technique pour en contrôler l'impact.

9.12.2 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.

9.12.3 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.

9.13 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.

9.14 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.

9.15 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.

9.15.1 Accord global

Sans objet.

9.15.2 Transfert d'activités

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

9.15.3 Conséquences d'une clause non valide

Sans objet.

9.15.4 Application et renonciation

Sans objet.

9.15.5 Force majeure

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

9.16 Autres dispositions

Sans objet.