# PC
# INFOGREFFE

**POLITIQUE DE CERTIFICATION D'INFOGREFFE**
*En support aux Services de Certification*
*de classe 3+*

---

**Version : V1.~~1~~2**

**Date de ~~1~~ère ~~-~~mise à jourédition ~~:~~ ~~23/05/01~~01/06/2002**
**~~Date d'application : 06/11/2001~~01/06/2002**

## POLITIQUE DE CERTIFICATION INFOGREFFE

## TABLE DES MATIERES

# 1 Introduction

Une Politique de Certification (PC) est un ensemble de règles identifié par un nom, qui indique les conditions d'applicabilité d'un certificat pour une communauté donnée, ou pour des applications ayant des besoins de sécurité communs.
La PC est définie indépendamment des détails concernant l'environnement de mise en oeuvre de l'infrastructure à clé publique (ICP) à laquelle elle s'applique. La PC établit ce à quoi il faut se conformer lors de la gestion des certificats concernés.
La gestion d'un certificat comprend toutes les phases du cycle de vie d'un certificat, de la demande d'attribution d'un certificat à la fin de vie de ce certificat (péremption, révocation).
Cette PC vise la conformité au document «Procédures et Politiques de Certification de Clés ($PC^2$)» émis par la Commission Interministérielle pour la Sécurité des Systèmes d'information (CISSI) et la Politique de Certification-type du MINEFI. Compte tenu de la nature des informations échangées entre les déclarants et les services du MINEFI le niveau de conformité recherché est le niveau moyen pour ce qui concerne la mise en oeuvre de la signature numérique.

## *1.1 Présentation générale*

### 1.1.1 Résumé de la Politique de Certification

#### 1.1.1.1 Aperçu général

La Politique de Certification définie dans le présent document est destinée à être utilisée pour les services de certification notamment pour les greffiers des tribunaux de commerce et les entreprises. A cette fin elle s'appuie sur les résultats des groupes de travail organisés par le Conseil National des Greffiers des Tribunaux de Commerce (CNG). La Politique de Certification couvre la gestion et l'utilisation des clés et des certificats servant aux fonctions de non-répudiation, d'authentification et d'intégrité. Par exemple, les certificats délivrés en vertu de la présente politique pourraient servir à vérifier l'identité du signataire d'un bilan envoyé aux Greffes des Tribunaux de Commerce, ou d'une télédéclaration de TVA au MINEFI.
La délivrance d'un certificat en vertu de la présente politique ne signifie pas que le client ou l'Abonné soit autorisé de quelque façon que ce soit à faire des transactions commerciales, ou autres, au nom de l'organisation qui exploite l'AC.
L'AC sera assujettie aux lois et règlements en vigueur sur le territoire de la République française tels que décrits au §12, ainsi qu'aux normes européennes en vigueur et aux conventions internationales ratifiées par la France, et qui touchent à l'application, l'élaboration, l'interprétation et la validité des politiques de certification mentionnées dans le présent document.

#### 1.1.1.2 Aperçu de la politique

La Politique de Certification s'applique aux certificats de type entreprise.

Cette politique a été conçue pour être utilisée dans certaines situations, et indique par conséquence les rôles et responsabilités spécifiques de l'AC qui délivre ce type de certificat, et ceux des autorités d'enregistrement qui doivent effectuer les tâches qui leurs sont assignés par l'AC. Les Abonnés et les Utilisateurs de certificat (ces termes sont définis au §1.1.2.2) ont également des obligations spécifiques qui sont définies dans cette politique.

INFOGREFFE décline toute responsabilité concernant l'utilisation de ces certificats pour tout usage autre que ceux permis par la présente PC.

Tout litige concernant la gestion des clés ou des certificats, en vertu de cette politique , doit être réglé par les parties concernées au moyen d'une procédure appropriée comme la négociation, la médiation ou l'arbitrage.

Les Utilisateurs de ce document doivent consulter l'AC émettrice afin d'obtenir plus de détails sur la mise en œuvre de cette politique si cela est nécessaire. L'applicabilité de ces certificats dépendra de leurs utilisations envisagées.

Les certificats pourront être émis en vertu de cette politique après authentification de l'identité de l'Abonné. L'identification se fera de la manière décrite dans cette politique.

Aucun renseignement personnel recueilli par une AC ne peut être divulgué sans le consentement de l'Abonné, à moins que la loi ne le prescrive.

Cette PC met en œuvre des certificats de classe 3+ tels que définis ci-après. Selon cette politique sont émis des clés privées et des certificats de clés publiques de classe 3+ utilisés pour l'identification des individus désirant accéder à des données ou des systèmes d'informations, et pour s'assurer de l'identité du signataire d'un document.

~~? Classe 3+ : certificats de classe 3 Télé-déclaration :~~

~~Dans ce cas, le~~Le certificat ne sera délivré que sur enregistrement de l'Abonné en personne dans une procédure en face à face avec une AE.
Pour permettre le service de non-répudiation à l'émission dans de bonnes conditions, INFOGREFFE impose l'utilisation de modules cryptographiques de type carte à puce (la clé secrète reste dans la carte).

Les certificats dédiés aux greffiers seront validés par une AE supplémentaire réservée à ce seul usage.

Les certificats de classe 3+ comportent un niveau d'assurance garantie, précisé par contrat et accessible à la partie utilisatrice. Lors de l'enregistrement initial, l'identité des détenteurs potentiels de certificats doit être vérifiée en personne (face à face) par l'AE. L'AE garantit le lien qui existe entre le détenteur du certificat ou un mandataire de sécurité lié contractuellement avec l'AC au titre de la PC, et une paire de clés. Les clés privées et les certificats sont délivrés sous forme physique (carte à puce)
Les demandes de certificats feront l'objet d'une vérification d'identité en face à face de l'Abonné ou du mandataire de sécurité.

Ce service d'INFOGREFFE est mis en oeuvre sous la forme d'une Autorité de Certification nommée AC CERTIGREFFE.

### 1.1.2 Définitions générales

#### 1.1.2.1 Liste des acronymes

| | |
|---|---|
| AA | Agence Autorité ( environnement MINEFI) |
| AC | Autorité de Certification |
| AE | Autorité d'Enregistrement |
| C | Country (Pays) |
| CISSI | Commission Interministérielle pour la Sécurité des Systèmes d'information |
| CN | Common Name |
| DN | Distinguished Name |

| | |
|---|---|
| DPC | Déclaration relative aux Pratiques de Certification |
| EAR | Entité d'Audit et de Référencement |
| ICP | Infrastructure à Clé Publique |
| LCR | Liste des Certificats Révoqués |
| MINEFI | MINistère de l'Economie des Finances et de l'Industrie |
| O | Organisation |
| OID | Object IDentifier |
| OSC | Opérateur de Service de Certification |
| PC | Politique de Certification |
| $PC^2$ | Procédures et Politiques de Certification de Clés |
| PIN | Personal Identification Number |
| PKCS | Public Key Cryptographic Standard |
| PKIX | Public Key Infrastructure X.509 |
| RSA | Rivest Shamir Adelman |
| S/MIME | Secure / Multipurpose Internet Mail Extensions |
| SHA-1 | Secure Hash Algorithm One |
| SSL | Secure Sockets Layer |
| URL | Unique Resource Locator |

#### 1.1.2.2 Définitions

**Abonné** : entité, personne morale, personne physique ou entreprise, qui obtient des services de l'AC pour émettre des télédéclarations signées.
L'Abonné peut également être désigné sous le nom de *porteur de certifica*t.
Dans la phase amont de certification il est un *demandeur* de certificat et dans le contexte du certificat X.509 il est un *suje*t.
**Autorité de Certification (AC)** : terme employé ici pour nommer l'autorité chargée de créer et d'attribuer les certificats. Cette entité est responsable des certificats signés en son nom.
**Autorité d'Enregistrement (AE)** : entité qui vérifie que les demandeurs ou les porteurs de certificat sont identifiés, que leur identité est authentique et que les contraintes liées à l'usage d'un certificat sont remplies. Elle est également en charge de vérifier l'authenticité d'une demande de révocation.
**Autorité de Politique (AP)** : entité qui :

- pour les usages qui la concerne, établit les besoins et les exigences en termes de sécurité dans l'ensemble du processus de certification et d'utilisation des certificats. Elle établit des lignes directrices, qui peuvent prendre la forme d'un canevas de Politique de Certification.
- définit et fait appliquer les politiques de certification et les déclarations des pratiques de certification par l'ICP, ainsi que la politique de sécurité générale de l'ICP.

Son rôle est celui d'une autorité morale qui indique par l'accréditation la confiance que l'on peut accorder à une Autorité de Certification.
**Bi-clé** : un bi-clé est un couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en oeuvre d'une prestation de cryptographie basée sur des algorithmes asymétriques.
**Chaîne de confiance** : Ensemble des certificats nécessaires pour valider la généalogie d'un certificat porteur. Dans le cadre de la présente PC, la chaîne se compose du certificat du porteur, du certificat de l'~~AC INFOGREFFE~~AC CERTIGREFFE et du certificat de l'AC à laquelle l'~~AC INFOGREFFE~~AC CERTIGREFFE est subordonnée.
**Client** : personne, physique ou morale, qui contracte avec l'Autorité de Certification pour bénéficier de ses services.
**Common Name (CN)** : identité réelle ou pseudonyme de l'Abonné titulaire du certificat (exemple CN = Jean Dupont).

**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 politiques de certification, des déclarations des pratiques de certification et des services effectivement fournis par la composante de l'ICP.
**Déclaration relative aux Procédures de Certification (DPC)** : énoncé des procédures et pratiques de certification effectivement respectées par une AC pour la gestion des certificats.
**Distinguished Name (DN)** : nom distinctif X.500 de l'Abonné pour lequel le certificat est émis.
**Données d'activation** : données privées associées à un Abonné permettant de mettre en oeuvre sa clé privée.
**Emission (d'un certificat)** : fait d'exporter un certificat à l'extérieur d'une AC (pour une délivrance à l'Abonné, une demande de publication).
**Enregistrement (d'un Abonné)** : opération qui consiste pour une Autorité d'Enregistrement à constituer le profil d'un demandeur de certificat à partir de son dossier de demande de certificat, conformément à la Politique de Certification.
**Entité d'Audit et de Référencement** : organisme sous la responsabilité de l'AA chargé du référencement des certificats qualifiés pour la signature de télédéclarations vers le MINEFI.
**Exploitant** : personne travaillant pour le compte de l'ICP et disposant de droits d'accès associés aux rôles qui lui sont attribués.
**Génération (d'un certificat)** : action réalisée par une AC et qui consiste à signer un certificat. Cette génération intervient généralement après authentification de la demande.
**Identificateur d'objet (OID)** : Identificateur alphanumérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques.
**Infrastructure à Clé Publique (ICP)** : ensemble de composants, fonctions et procédures dédiés à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique.
**Liste de Certificats Révoqués (LCR)** : liste de certificats ayant fait l'objet d'une révocation.
**Module cryptographique** : Un module cryptographique est un dispositif matériel, du type carte à mémoire, carte PCMCIA ou autre, permettant de protéger les éléments secrets tels que les clés privées ou les données d'activation, et de procéder à des calculs cryptographiques mettant en oeuvre ces éléments.
**Opérateur de Service de Certification (OSC)** : composante de l'ICP disposant d'une plate-forme lui permettant de générer et émettre des certificats auxquels une communauté d'Utilisateurs fait confiance.
**Politique de Certification (PC)** : ensemble de règles, définissant les exigences auxquelles l'AC se conforme dans la mise en place de prestations adaptées à certains types d'applications. La Politique de Certification doit être identifiée par un OID défini par l'AC.
**Porteurs de (certificats)** : voir Abonnés.
**Publication (d'un certificat)** : opération consistant à mettre un certificat à disposition d'Utilisateurs par exemple pour leur permettre de vérifier une signature (exemple de moyen de publication : annuaire X.500).
**Référencement MINEFI** : opération consistant à contrôler la conformité d'une catégorie de certificats afin que ceux-ci soient acceptés par le MINEFI dans le cadre des télédéclarations. Si le résultat de cette opération est positif, cette catégorie de certificats est inscrite dans la liste tenue par l'EAR du MINEFI.
**Renouvellement (d'un certificat)** : opération effectuée à la demande d'un Abonné ou en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat pour un porteur. La re-génération de certificat après révocation n'est pas un renouvellement.
**Révocation (d'un certificat)** : opération demandée par l'Abonné ou le responsable de l'entreprise mandaté à cet effet, par une AC, une AE, et dont le résultat est la suppression de la caution de l'AC sur un certificat donné, avant la fin de sa période de validité. La demande peut être la conséquence de différents types d'événements tels que la compromission d'une clé, le changement d'informations contenues dans un certificat, etc. L'opération de révocation est

considérée terminée quand le certificat mis en cause est publié dans la liste des certificats révoqués.
**Service de publication** : le service de publication rend disponible les certificats de clés publiques émis par une AC, à l'ensemble des Utilisateurs potentiels de ces certificats. Il publie une liste de certificats reconnus comme valides et une liste de certificats révoqués (LCR). Ce service peut être rendu par un annuaire électronique, un document, un serveur d'information (Web), une application de messagerie, etc.
**Usagers** : terme employé dans le préambule pour désigner les Abonnés potentiels.
**Utilisateurs (de certificats)** : toute entité (Utilisateur humain, organisme ou entité des technologies de l'information) ayant à utiliser des certificats de clé publique à des fins de vérification de signature. Un Utilisateur de certificat ne détient pas forcément de certificat propre. Par exemple, les services du MINEFI gestionnaires des téléprocédures sont des Utilisateurs des certificats INFOGREFFE pour vérifier les signatures des télédéclarants. Dans la suite du document, le terme tiers Utilisateur est également utilisé pour désigner un Utilisateur de certificat.
**Validation (de certificat)** : opération de contrôle du statut d'un certificat ou d'une chaîne de certification.
**Vérification (de signature)** : opération de contrôle d'une signature numérique.

### 1.1.3 Définitions de la Politique INFOGREFFE relatives à la Sécurité

**Procédure sécurité :** Procédure des sites d'hébergement qui fixe les règles générales en matière de protection industrielle, commerciale et de défense et définit la conduite à tenir dans les principaux cas d'espèces. Cette procédure s'applique à l'ensemble de la zone réservée hébergeant les AC et les AE localisées sur le site, ainsi que l'infrastructure associée.
**Zone d'enregistrement** : zone utilisée pour les opérations d'enregistrement en mode ~~face-~~face-~~à~~ à-face dont l'accès est contrôlé par le personnel habilité des Greffes des Tribunaux de commerce.
~~**Zone réservée :** zone dont l'accès est restreint aux personnes qui y ont leur emploi, habilitées ou en cours d'habilitation, titulaires d'un code d'accès délivré par l'Agent de sécurité du site.~~
**Zone ~~à haute sécurité~~sécurisée** : zone dont l'accès est restreint aux personnes habilitées à effectuer des opérations très sensibles liés à la sécurité de l'~~ICP INFOGREFFE~~ICP CERTIGREFFE et de ses infrastructures (ex : gestion des clés de l'~~AC INFOGREFFE~~AC CERTIGREFFE, Opération de recouvrement, etc.). ~~La Zone à haute sécurité est incluse dans la zone réservée.~~
Identification (OID)
La présente Politique de Certification est dénommée :
«PC INFOGREFFE : Politique de Certification D'INFOGREFFE *En support aux Services de Certification de classe 3+ »*

La personne responsable de cette PC est
M. Jean-Marc Bahans
Adresse 33 Cours de l'Argonne
CP 33000
Localité Bordeaux

La présente Politique de Certification est parallèlement enregistrée conformément à la norme d'enregistrement ISO par un identificateur numérique unique. Cet OID se rattache à l'identificateur unique de la société auteur du document.
Tout lecteur a donc les moyens de vérifier l'appartenance du document à INFOGREFFE
La désignation de l'identification objet (OID) pour la présente politique est : 1.2.250.1.106.1.1
dont les champs sont définis comme suit :(iso(1) member-body(2) fr(250) type-org(1) infogreffe(106) pki(1) certificate-policy(1).

## ~~1.3~~1.2 *Applications et groupes d'Utilisateurs concernés*

Le processus de certification et la gestion du cycle de vie du certificat font appel à une grande diversité d'intervenants dans la chaîne de la confiance :

- Autorité de Certification et ses propres composantes ou services,
- Autorité d'Enregistrement,
- Abonnés de l'Autorité de Certification,
- Utilisateurs de certificats,
- Mandataires de sécurité d'entreprise.

### ~~1.3.1~~1.2.1 Autorité de Certification (AC)

L'Autorité de Certification est responsable vis-à-vis de ses clients, mais aussi de toute personne se fiant à un certificat qu'elle a émis, de l'ensemble du processus de certification, et donc de la validité des certificats qu'elle émet. A ce titre, elle édicte la Politique de Certification et valide les Déclarations de Pratique de Certification qui doivent identifier les obligations de toutes les entités externes participant aux services de l'AC.
La garantie apportée par l'Autorité de Certification vient de la qualité de la technologie mise en oeuvre, mais aussi du cadre réglementaire et contractuel qu'elle définit et s'engage à respecter.
En vertu de cette politique, une ~~AC INFOGREFFE~~AC CERTIGREFFE est chargée:

- ✓ de créer et de signer des certificats liant les Abonnés et le personnel de l'ICP à leurs clés de vérification de signature,
- ✓ de faire connaître l'état des certificats par l'intermédiaire des LCR,
- ✓ de faire respecter la PC par les différentes composantes de l'ICP, les clients et les Abonnés,
- ✓ de faire respecter la DPC par les différentes composantes de l'ICP.

La fonction d'enregistrement des certificats fait partie des fonctions indispensables d'une ICP.
L'AC doit s'assurer qu'elle est remplie par une Autorité d'Enregistrement, distincte de l'AC avec laquelle elle collabore ou qui lui est rattachée.
L'Autorité de Certification a un devoir de contrôle et d'audit des Autorités d'Enregistrement.
Les fonctions de l'AC doivent être exécutées par des personnels désignés par le responsable de l'AC, connaissant et respectant les règles, principes et procédures énoncés dans la PC et la DPC liés au fonctionnement de l'AC ;

### ~~1.3.2~~1.2.2 Autorité d'Enregistrement (AE)

L'Autorité d'Enregistrement applique des procédures d'identification des personnes physiques ou morales, conformément aux règles définies par l'Autorité de Certification. Son but est :

- de coordonner les demandes d'identification électronique,
- d'établir que le demandeur a bien l'identité et les droits qui seront indiqués dans le certificat selon la classe du certificat envisagé,
- de distribuer à l'Abonné, en cas de besoin, un support physique (carte à puce, papier…) nécessaire à l'acquisition ou l'utilisation de son certificat,
- de gérer et protéger les données personnelles et de sécurité des Abonnés,
- de maintenir, administrer, exploiter et protéger les machines et logiciels utilisés pour remplir ces fonctions.

L'AE a également pour tâche de réceptionner les demandes de révocation de certificats et doit les traiter.

L'Autorité d'Enregistrement est le lien entre l'Autorité de Certification et l'Abonné. En vertu de cette Politique de Certification, une AE est responsable de toutes les tâches qui lui sont assignées par l'AC.
L'AE archive les dossiers de demande de certificats ou de révocation.
L'AE peut être constituée d'une seule unité ou d'unités distinctes coopérant entre elles ou hiérarchiquement dépendantes. Diverses structures sont acceptables du moment qu'elles soient adaptées aux exigences de la PC en matière d'enregistrement des Abonnés. Ainsi, l'AE peut déléguer tout ou partie de ses fonctions à des unités de proximité (AE locales).
Les fonctions de l'AE doivent être exécutées par des personnels désignés par le responsable de l'AE et agréés par le responsable de l'AC, ayant connaissance et respectant les règles, principes et procédures énoncées dans la PC et la DPC.

### ~~1.3.3~~1.2.3 Abonné

En vertu de cette Politique de Certification, un Abonné peut être une entité, personne morale, personne physique ou entreprise, qui obtient un certificat des services de l'AC.
L'Abonné est responsable :

- de l'authenticité, de l'exactitude, et de la complétude des données d'identification fournies à l'AE lors de l'enregistrement,
- d'établir et de faire respecter la politique de sécurité sur les postes informatiques utilisés pour mettre en oeuvre les certificats.

L'Abonné en tant que personne physique, est responsable :

- de la protection, de l'intégrité et de la confidentialité de sa clé privée, et des éventuelles données d'activation,
- de la sécurité de ses équipements matériels, logiciels et de ses réseaux impliqués dans l'utilisation de ses certificats,
- de l'utilisation de sa clé privée et de son certificat, qui doit être conforme à la présente Politique de Certification.

Il doit communiquer à l'AC, par les canaux qu'elle aura désignés, définis dans la DPC, toute information ayant pour conséquence la révocation de son certificat.

### ~~1.3.4~~1.2.4 Opérateur de Service de Certification (OSC) :

L'Opérateur de Service de Certification assure les prestations techniques, en particulier cryptographiques, nécessaires au processus de certification. Il est en charge du bon fonctionnement et de la sécurité des moyens informatiques et techniques. Il est en charge de la sécurité des personnels, des locaux et plus généralement du bon respect des procédures.
Il est techniquement dépositaire de la clé privée de l'Autorité de Certification utilisée pour la signature des certificats. Une de ses premières missions et de la protéger contre toute compromission.
Sa responsabilité ne peut être engagée que par l'Autorité de Certification et se limite au respect des procédures établies dans la Déclaration des Pratiques de Certification, approuvée par l'Autorité de Certification. L'Autorité de Certification a un devoir de contrôle et d'audit de l'Opérateur de Service de Certification.
En tant qu'expert, l'Opérateur de Service de Certification a un devoir de conseil auprès de l'Autorité de Certification.

### ~~1.3.5~~1.2.5 Annuaires

Le dépôt de LCR se présente sous la forme d'une entrée d'annuaire conforme aux normes X.500 et LDAP.

### ~~1.3.6~~1.2.6 Parties utilisatrices

En vertu de cette Politique de Certification, les principaux Utilisateurs de certificats émis sont les Greffes des Tribunaux de Commerce, ainsi que les services du MINEFI gestionnaires des téléprocédures.

### ~~1.3.7~~1.2.7 Mandataires de sécurité

Le mandataire de sécurité est l'Autorité d'Enregistrement déléguée auprès des greffiers dans le cadre de la procédure d'enregistrement. Cette personne doit être désignée par le représentant légal de l'entreprise cliente. Son rôle et ses obligations doivent être définies dans un contrat.

### ~~1.3.8~~1.2.8 Applicabilité de la Politique

Cette Politique de Certification convient pour assurer l'intégrité et l'authentification des téléprocédures qui, si elles étaient falsifiées, pourraient causer des pertes financières appréciables ou exiger des correctifs de nature administrative à l'Abonné.
Les applications concernées par cette PC sont celles qui permettent le support des téléprocédures, par exemple en mode messagerie sécurisée, web avec authentification, ou par échange de documents signés électroniquement.

# 2 DISPOSITIONS DE PORTÉE GÉNÉRALE

## *2.1 Obligations*

Si elle veut faire référencer une ou plusieurs de ses catégories de certificats, l'AC doit s'assurer que les fonctions qu'elle met en oeuvre ou auxquelles elle fait appel (cas de l'AE) sont conformes à la PC-Type. Elle doit garantir qu'elles en respectent les exigences de sécurité.
Les obligations de l'AC et de l'AE sont décrites ci-après.

### 2.1.1 Obligations communes à toutes les composantes de l'AC et de l AE.

Certaines des obligations sont communes à toutes les composantes qui concourent à l'accomplissement des fonctions de l'ICP, d'autres leurs sont spécifiques. Les obligations communes à toutes les composantes de l'ICP sont les suivantes :

- protéger et garantir l' intégrité et la confidentialité de leurs clés privées,
- n'utiliser leurs clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés, selon la présente Politique de Certification,
- respecter et appliquer la présente PC et la DPC associée, pour ce qui les concerne,
- se soumettre aux contrôles de conformité effectués par l'Entité d'Audit et de Référencement du MINEFI, et par l'auditeur du Conseil National des Greffiers (CNG), en respecter les conclusions et remédier aux non-conformités qu'ils révèleraient,
- définir les relations contractuelles avec les sous-traitants et l'OSC,
- respecter les accords ou contrats qui les lient entre elles ou aux Abonnés,
- documenter leurs procédures internes de fonctionnement,
- mettre en oeuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent, dans des conditions garantissant qualité et sécurité.

Les membres du personnel de l'ICP, et les opérateurs mandatés, à qui sont assignés des rôles relatifs à l'ICP (cf. §5.2.1) doivent être personnellement responsables de leurs actes. L'expression « personnellement responsable » signifie que l'on puisse imputer une action à une personne (Cf §4.5.7).

### 2.1.2 Obligations de l'AC

#### 2.1.2.1 Fonctions de gestion des certificats

L'AC doit :

- vérifier que l'AC à laquelle elle est subordonnée utilise une PC se conformant à la PC-type du MINEFI;
- pouvoir démontrer aux Utilisateurs de ses certificats, qu'elle a émis un certificat pour un Abonné donné et que cet Abonné a accepté le certificat ;
- tenir à disposition des Abonnés et des Utilisateurs de certificats la notification de révocation du certificat d'une composante de l'ICP ou d'un Abonné;
- prendre toutes les mesures raisonnables pour s'assurer que ses Abonnés sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats. La relation entre un Abonné et l'AC est formalisée par un abonnement ou un lien contractuel précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.
- fournir à chaque Abonné un énoncé de ses droits et obligations en vertu de cette Politique de Certification

#### 2.1.2.2 Gestion des supports et données d'activation

Si les éléments secrets d'un Abonné sont gérés sur un support matériel dont la mise en œuvre est conditionnée par l'utilisation d'un code personnel, ce support matériel doit :

- disposer d'un contrôle d'accès lors de la personnalisation,
- pouvoir être désactivé.

La fourniture du support doit faire l'objet d'une distribution sécurisée ainsi que le transport du code personnel.

#### 2.1.2.3 Exactitude des informations

Lorsque l'AC émet un certificat, l'AC garantit qu'elle a délivré le certificat à un Abonné et que les informations contenues dans le certificat en question ont été vérifiées conformément à cette PC. L'AC veillera à ce que les AE qui fonctionnent en son nom, se conforment à toutes les modalités pertinentes de la présente Politique de Certification, concernant le fonctionnement des AE.

#### 2.1.2.4 Délai entre la demande et l'émission du certificat

Il n'y a pas d'exigence sur le délai entre la demande d'un certificat et sa fabrication. L'émission d'un certificat est subordonnée au respect de la procédure de traitement des demandes.

#### 2.1.2.5 Révocation et renouvellement des certificats

Dans le cas d'une demande de révocation du certificat d'un Abonné, l'AE qui reçoit la demande doit effectuer des vérifications avant d'accepter la révocation et d'introduire le certificat en cause dans la LCR protégée en intégrité et authenticité. Ces procédures sont précisées au §4.4.
L'AC émettrice doit s'assurer que toutes les procédures relatives à l'expiration et à la révocation d'un certificat sont conformes aux dispositions de cette PC et qu'elles ont été mentionnées à l'Abonné, ou consignées dans tout autre document applicable décrivant les modalités d'utilisation du certificat.
Les demandes de renouvellement sont traitées au §3.2.

#### 2.1.2.6 Protection des clés privées

L'AC s'engage à protéger et garantir l'intégrité et la confidentialité de sa clé privée et les données d'activation de clé associé conformément à la section 6 du présent document. Cette clé privée doit faire l'objet d'une sauvegarde sécurisée.
L'AC s'engage à transmettre en toute confidentialité les données d'activation aux Abonnés.
L'AC s'engage à ce que les clés privées et les codes d'activation qu'elle pourrait avoir en sa possession pour le compte d'autrui sont protégés conformément à la section 4 et 5.3 du présent document.

Le support matériel des éléments secrets d'un Abonné (type carte à puce) et le code d'activation de ce support devront être fournis par des moyens de distribution différents (Poste, retrait au guichet, …).

#### 2.1.2.7 Restriction quant à l'utilisation des clés privées de l'AC émettrice

L'AC s'engage à n'utiliser ses clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés, selon la présente Politique de Certification.

#### 2.1.2.8 Fonction de séquestre

Il n'y a pas de fonction de séquestre mise en œuvre dans le cadre de cette PC

### 2.1.3 Obligations d'une AE

#### 2.1.3.1 Avis d'émission et de révocation de certificats

Une AE doit se conformer à toutes les exigences de la présente Politique de Certification et de la DPC associée.
En outre, une AE doit :

- traiter les demandes de certificat ;
- transmettre à l'AC une trace imputable de la validité de la vérification ;
- transmettre en toute confidentialité des supports physiques aux Abonnés ;
- conserver et protéger en confidentialité et en intégrité toutes les données à caractère personnel et d'identification collectées lors des procédures d'enregistrement.

#### 2.1.3.2 Exactitude des informations

L'AE doit vérifier l'authenticité des pièces justificatives et l'exactitude des mentions qui établissent l'identité de l'Abonné ou de l'entreprise selon les procédures décrites au chapitre 3.

#### 2.1.3.3 Protection des clés privées de l'AE

L'AE s'engage à protéger et garantir l'intégrité et la confidentialité de sa clé privée et des données d'activation conformément à la section 6 du présent document.

#### 2.1.3.4 Restriction quant à l'utilisation des clés privées de l'AE

L'AE s'engage à n'utiliser ses clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés, selon la présente Politique de Certification.

Les clés privées utilisées par les responsables et les exploitants de l'AE pour accéder aux applications de l'AE ne doivent pas être utilisées à d'autres fins.

### 2.1.4 Obligations du Client et de l'Abonné

Le client et l'Abonné doivent se conformer à toutes les exigences de la présente Politique de Certification et de la partie publiée de la DPC associée.
Les engagements du client sur l'usage du certificat doivent être portés à sa connaissance avant souscription du contrat qui le lie à l'AC.
Lorsqu'une société demande un certificat pour un de ses salariés, le partage des rôles entre client et Abonné est effectué comme suit :

- la société est "cliente", car elle contracte,
- le salarié est "Abonné", car le certificat est émis à son nom.

La relation entre le client et l'AC est formalisée par un engagement du client visant à certifier l'exactitude des renseignements et des documents fournis par les Abonnés bénéficiant des services de l'ICP pour le compte de ce client. Il s'engage à respecter le contrat qui le lie à l'AC.
Si le client est une organisation, il doit établir et faire respecter la PC sur les postes informatiques utilisés pour mettre en œuvre les certificats.
En aucun cas le client n'acquiert la propriété du certificat émis par l'AC, il n'en acquiert que le droit d'usage. Tous les certificats demeurent la propriété de l'AC qui les a émis.

#### 2.1.4.1 Exactitude des informations

Le client et l'Abonné ont l'obligation contractuelle de communiquer des informations exactes lors de la demande de certificat. Ils ont également l'obligation de notifier l'AC, au travers de l'AE, de toute modification des informations fournies lors de la demande de certificat.
Le contrat entre le client et INFOGREFFE doit comporter au moins les informations suivantes :

- l'accord sur les obligations,
- l'accord, le cas échéant, sur l'utilisation de carte à puce,
- l'accord sur l'archivage des données d'enregistrement,
- l'accord sur les règles de révocation,
- l'accord optionnel sur la publication du certificat,
- la mention de garantie de l'exactitude et de la complétude des informations fournies ainsi que la validité des documents transmis ou présentés,
- la durée de l'archivage du dossier.

#### 2.1.4.2 Protection des clés privées de l'Abonné

L'Abonné s'engage à suivre toute prescription en matière de politique de sécurité dans le cadre de l'usage du certificat.
L'Abonné doit:

- protéger en confidentialité et en intégrité sa clé privée et les données d'activation par des moyens appropriés à son environnement, conformément au §6 ; il doit prendre toutes les mesures raisonnables pour en éviter la perte, la divulgation, la compromission, la modification ou l'utilisation non autorisée,
- respecter les restrictions sur l'utilisation de sa clé privée et du certificat correspondant,
- informer dans les plus brefs délais l'AE, en cas de compromission, ou de soupçon de compromission, de sa clé privée, selon les instructions prévues au §4.4.3,
- informer dans les plus brefs délais l'AE, en cas de perte des données d'activation (mot de passe ou code PIN).

Le mandataire de sécurité doit, en ce qui concerne la protection du pli scellé qui lui a été confié lors de l'enregistrement :

- s'engager à ne pas utiliser la carte à puce de l'Abonné,
- assurer les obligations de l'Abonné mentionnées ci-dessus jusqu'à ce qu'il lui ait remis le pli.

#### 2.1.4.3 Restriction quant à l'utilisation des clés privées de l'Abonné

L'Abonné doit exclusivement utiliser ses clés privées et certificats à des fins autorisées par la présente Politique de Certification, ainsi que dans le respect des lois et règlements en vigueur.

### 2.1.5 Obligations des Utilisateurs de certificats

#### 2.1.5.1 Utilisation des certificats à des fins pertinentes

Les Utilisateurs de certificats doivent respecter l'usage pour lequel un certificat a été émis lorsque cet usage a été déclaré critique. (voir §6.1.8)
Un Utilisateur de certificat ne doit utiliser les certificats que conformément à la procédure de validation de l'itinéraire de certification, procédure qui est spécifiée dans les normes X. 509 et PKIX et déterminée par la recommandation ISO/IEC 9594-8.

#### 2.1.5.2 Responsabilités en matière de vérification

Les Utilisateurs de certificat doivent vérifier la validité du certificat de l'AC qui a émis le certificat qu'ils vont utiliser.
Les Utilisateurs de certificat doivent contrôler la validité des certificats qu'ils vont utiliser (dates de validité et statut de révocation potentiel), ainsi que leur validité intrinsèque, en particulier la signature de l'AC, et la validité de tout certificat sur l'itinéraire de confiance
En outre, l'Utilisateur de certificat doit utiliser la clé publique extraite du certificat de l'émetteur pour vérifier une signature électronique.

#### 2.1.5.3 Responsabilité de la vérification de la révocation

Avant toute utilisation de certificats, notamment lorsque lesdits certificats créent des effets juridiques, l'Utilisateur de certificat doit impérativement vérifier la validité des certificats auxquels il entend se fier auprès de l'AC en consultant les Listes des Certificats Révoqués appropriées les plus récentes. A défaut de remplir cette obligation, l'Utilisateur de certificat assume seul tous les risques de ses actions non conformes aux exigences de la présente politique, l'AC ne garantissant aucune valeur juridique aux certificats qu'elle a émis et qui pourraient avoir été révoqués ou qui ne serait pas valides.

### 2.1.6 Obligations du service de publication

Les LCR doivent être disponibles pour les Utilisateurs de certificat conformément aux exigences décrites au §4.4.9.

## *2.2 Responsabilités*

La responsabilité de l'un quelconque des intervenants dans la certification d'une transaction et toute opération qui s'y rattache (AC, prestataire de l'AC, client, Abonné, Utilisateur de certificat, …) ne pourra être mise en jeu que si cet intervenant a commis une faute ou une négligence, ou s'il est responsable en vertu d'une clause contractuelle qui lui est applicable.

Le contrat à établir entre l'AC et chaque client définira les limites d'utilisation des certificats émis par l'AC dans le cadre de celui-ci.

### 2.2.1 Responsabilité de l'AC et du personnel de l'AC

Les dispositions ci-dessous s'appliquent à l'égard des clients de l'AC : ceux-ci déclarent y adhérer et faire leur affaire de leur acceptation par les Abonnés et les Utilisateurs concernés.

#### 2.2.1.1 Exigences

Toutes les obligations de l'AC découlant de la présente PC sont des obligations de moyens. En outre, l'AC ne pourra pas être tenue pour responsable d'un fait dommageable qui lui serait imputable si ce fait a été causé par un événement quelconque hors du contrôle raisonnable de l'AC.
L'AC est responsable des fautes ou négligences imputables aux membres de son personnel.
Au titre des exigences de la présente PC, l'AC a une obligation de moyens. Dans l'hypothèse où la responsabilité de l'AC serait mise en cause, celle-ci pourra être engagée selon les règles du droit commun.
La responsabilité de l'AC et du personnel de l'AC n'est engagée que dans le cas où elle fait une erreur et que cette erreur résulte d'une négligence de la part de l'AC ou du personnel de l'AC. Par conséquent, la responsabilité de l'AC ou du personnel de l'AC est dégagée dans la mesure où elle est capable de prouver n'avoir commis aucune négligence (cf §4.5)

#### 2.2.1.2 Limites de la responsabilité

L'AC n'est en aucun cas responsable de l'utilisation de certificats -par les clients, les Abonnés ou tous autres tiers- dans des conditions autres ou à des fins autres que celles définies par la présente PC, la DPC associée, les certificats eux-mêmes, les documents contractuels ou la réglementation en vigueur.
L'AC n'assume aucune responsabilité en ce qui concerne :
- l'exactitude, l'authenticité ou la valeur juridique de l'ensemble des documents remis lors de la demande de certificat. En particulier en cas de présentation d'une pièce d'identité falsifiée.
- les retards, erreurs, altérations ou omissions qui pourraient affecter les messages à l'occasion de leur transmission par des moyens indépendants de ceux mis en œuvre dans l'ICP.

Si la responsabilité de l'AC est établie, les conséquences financières de cette responsabilité n'excéderont pas les montants définis dans le contrat avec l'Abonné:

#### 2.2.1.3 Autres modalités

- **Exonération de responsabilité**

L'AC n'assume aucun engagement ni responsabilité quant à la forme, la suffisance, l'exactitude, l'authenticité, la falsification ou l'effet juridique des documents remis lors de l'enregistrement.
L'AC n'assume aucun engagement ni responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, ni quant aux retards, à la mutilation ou autres erreurs pouvant se produire dans la transmission de toute télécommunication, indépendants des moyens mis en œuvre au sein de l'ICP.
Les exonérations de responsabilité mentionnées dans le cadre des contrats entre l'~~AC INFOGREFFE~~AC CERTIGREFFE et ses Abonnés s'imposent aux clients et aux Abonnés.

- **Force majeure**

Une partie ne saurait être tenue responsable pour tout retard ou interruption dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente Politique de Certification lorsque les circonstances y donnant lieu relèvent de la force majeure au sens de l'article 1148 du Code civil, de la jurisprudence des tribunaux français et des clauses contractuelles contenues dans la DPC et toutes autres conventions liant les parties (par exemple le contrat d'abonnement).

### 2.2.2 Responsabilité de l'AE

L'AC et l'AE conviendront des conditions et limites de la responsabilité éventuelle de l'AE dans le cadre de la mise en œuvre de l'ICP. Tant les clients que les Abonnés et Utilisateurs seront liés par les conditions et limites de responsabilité ainsi fixées.

## *2.3 Indépendance des parties et absence de rôle de représentation*

Dans le cadre de la certification d'une transaction et de toute opération qui s'y rattache, l'AC, l'AE et chaque client agissent en toute indépendance et pour leur propre compte : aucune de ces personnes n'est réputée agir au nom ou pour le compte d'une autre personne, ni assumer les obligations ou responsabilités d'une autre personne.

## *2.4 Interprétation et mise en application*

### 2.4.1 Droit applicable

La présente PC est régie par le droit français, et ce même si les activités qui en découlent peuvent comporter des éléments de localisation hors de France.
En cas de litige sur l'interprétation ou l'exécution d'un contrat faisant référence à la présente PC, les parties à ce contrat conviennent que le litige sera soumis au Tribunal de Commerce de Paris.
Si une disposition de la présente PC s'avérait inapplicable ou incompatible avec une loi ou un règlement en vigueur, elle sera considérée comme nulle, mais cette nullité n'affectera en aucune manière la validité des autres dispositions de la présente PC.

### 2.4.2 Intégralité, divisibilité, survie, avis

Sans objet dans le cadre de la présente PC.

### 2.4.3 Règlement des différends

En cas de litige relatif à l'émission d'un certificat dans le cadre de la présente PC, l'Intervenant concerné adressera une notification à INFOGREFFE. INFOGREFFE et l'Intervenant concerné rechercheront une résolution amiable au litige dans un délai de quinze jours.
En l'absence de solution amiable dans un délai pré-cité, les litiges seront soumis à une procédure d'expertise amiable auprès d'un expert agréé auprès de la cour d'appel de Paris dont la durée sera fixée par l'expert saisi.
L'expert amiable doit tenter de concilier les intervenants dans un délai de deux (2) mois à compter de sa saisie. Il propose un rapport en vue de concilier chacune des intervenants. Ce rapport a un caractère confidentiel et ne peut servir que dans le cadre de la procédure d'expertise amiable.
Cette procédure doit être soldée :

- soit par la production d'un accord transactionnel et confidentiel, en cas de conciliation, co-signé par les intervenants,
- soit par un procès verbal de non-conciliation co-signé par les intervenants.

En cas de litige qui ne trouverait pas de solution acceptable par les Intervenants concernés dans les conditions définies aux deux alinéas précédents, les parties à ce contrat conviennent que le litige sera soumis au Tribunal de Commerce de Paris.

Si une disposition de la présente PC s'avérait inapplicable ou incompatible avec une loi ou un règlement en vigueur, elle sera considérée comme nulle, mais cette nullité n'affectera en aucune manière la validité des autres dispositions de la présente PC.

### 2.4.4 Permanence de la Politique de Certification

Le caractère inapplicable dans un contexte donné d'une disposition de la Politique de Certification n'affecte en rien la validité des autres dispositions, ni de cette disposition hors du dit contexte. La Politique de Certification continue à s'appliquer en l'absence de la disposition inapplicable et ce tout en respectant l'intention des parties.

## *2.5 Tarifs*

### 2.5.1 Frais d'émission et de renouvellement des Certificats

Des frais d'émission de certificat seront facturés selon une échelle de tarifs diffusés par l'AC, ou négociés dans le cadre d'un contrat d'abonnement.

### 2.5.2 Frais d'accès au certificat

Aucun frais ne sera facturé pour l'accès aux certificats inclus dans la Chaîne de certification.

### 2.5.3 Frais de vérification de validité des certificats

Un moyen gratuit de contrôle du statut des certificats abonnés (sous la forme d'une LCR) ainsi que l'accès aux certificats des Autorités de Certification impliquées dans la chaîne de certification de l'~~AC INFOGREFFE~~AC CERTIGREFFE est mis à disposition des Utilisateurs de certificat. Par contre l'~~AC INFOGREFFE~~AC CERTIGREFFE se réserve de rendre payant l'accès à un annuaire des certificats effectivement valides.

### 2.5.4 Frais pour d'autres services

Aucun frais ne sera facturé pour l'accès à cette PC via le site Web de l'AC. Tout autre accès à cette PC (copie papier, envoi par messagerie électronique) pourra faire l'objet d'une facturation.

Tout autre frais demandé à un Abonné ou une partie utilisatrice doit être facturé selon une échelle de tarifs définie par l'AC, ou négociés dans le cadre d'un contrat d'abonnement.

### 2.5.5 Politique de remboursement

Aucun remboursement ne sera effectué par l'AC.

## *2.6 Publication et services associés*

### 2.6.1 Informations publiées

La Politique de Certification, certains éléments de la DPC, les formulaires de demande de certificat, les contrats client type, et les conventions d'usage Abonné type en vertu desquels les certificats sont émis, sont disponibles sur le site WEB d'INFOGREFFE (http://www.~~infogreffe~~certigreffe.fr). Les éléments suivants doivent être inclus dans les informations publiées, notamment via la présente PC :

- l'obligation d'utiliser un support carte à puce dans le cas du choix de certificats de classe 3+,
- les limites d'usage du certificat,
- les limites de responsabilité,
- les durées d'archivage,

- la procédure de règlement de litige,
- les lois applicables,
- le référencement MINEFI de l'AC,
- les informations sur les moyens disponibles pour vérifier les certificats.

La DPC, qui donne, entre autres, le détail des procédures et des moyens mis en oeuvre pour assurer la protection des installations de l'AC, n'est pas publiée dans son intégralité pour des raisons de sécurité évidentes. Les éléments publiés de la DPC doivent permettre de vérifier la conformité des pratiques de certification avec la PC.
Toutefois l'AC doit fournir, en cas de besoin, la version complète de sa DPC, lors d'une demande d'un organisme habilité à en connaître à des fins de vérification, d'audit ou de contrôle, prévu à cet effet dans la présente politique, ainsi que dans le cadre du respect de la loi.
Le service de publication fournit au minimum les informations suivantes, sachant que le moyen utilisé pour leur publication est libre :

- la liste des certificats dont la publication a été explicitement autorisée par le client,
- la liste de certificats révoqués (LCR) la plus récente,
- la liste des certificats de l'AC à laquelle l'~~AC INFOGREFFE~~AC CERTIGREFFE est subordonnée,
- le certificat de l'~~AC INFOGREFFE~~AC CERTIGREFFE,

La LCR doit être accessible 24 heures sur 24 et 7 jours sur 7.

### 2.6.2 Fréquence de publication

L'écriture d'un événement donnant lieu à mise à jour et publication de la LCR doit se faire dans un délai inférieur à un jour ouvré, s'il n'est pas possible de le faire en temps réel après validation de l'événement. Le délai est compté à partir du moment où a lieu l'événement déclencheur de l'action et ne prend pas en compte les jours non ouvrés (samedi, dimanche et jours fériés). La nouvelle LCR publiée est complète et n'est pas définie comme un delta de la LCR précédente.
Les éléments déclencheurs pour la mise à jour et la publication de la LCR dépendent de l'opération à effectuer :

- dans le cas d'une demande de révocation du certificat d'un Abonné, l'événement déclencheur est l'acceptation, après vérification, de la demande de révocation.
- dans le cas d'un incident majeur tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de la clé racine, l'événement déclencheur est la constatation de cet incident par l'AC.

L'AC doit également s'assurer de la publication d'informations (notamment la PC) ayant fait l'objet d'une révision suite à modification, dans un délai précisé dans la DPC.

### 2.6.3 Contrôles de l'accès

L'accès aux informations publiées, pour création ou modification, ne sera autorisé qu'au seul personnel habilité par l'AC, et ce à travers des contrôles d'accès appropriés.
Les conditions de mise en œuvre de mesures de sécurité aux fins de contrôler l'accès aux informations publiées sont du ressort du service de publication.

### 2.6.4 Bases documentaires

L'AC est tenue de diffuser les informations identifiées au §2.6.1.

## *2.7 Audit de conformité*

L'AC a la responsabilité du bon fonctionnement des composantes de l'ICP, conformément aux dispositions énoncées dans le présent document. L'AC effectuera en ce sens des contrôles réguliers de conformité et de bon fonctionnement des composantes de cette ICP.
L'audit de conformité est fait sur demande de l'AP ou de l'AC elle-même, selon les conditions précisées dans la DPC.

L’audit comprend entre autres:

- l'examen de la validité du processus de vérification que l'AC a mis en place pour valider la qualité de ses services ;
- une comparaison entre les pratiques de l’AC, et des composantes de l'ICP, décrites dans la DPC et la conformité à ces déclarations ;
- une comparaison entre les pratiques de l’AC, et des composantes de l'ICP, et les exigences des différentes Politiques de Certification a priori supportées.

Le contrôle de conformité à la PC-Type a pour but de vérifier la recevabilité de catégories de certificats délivrés par une AC. Les contrôles sur le fonctionnement des composantes de l’AC se feront dans ce seul but. Il ne s’agit en aucun cas d’accréditation d’AC au sens de la Directive Européenne sur la signature électronique (DIR_EU_SIGN), non plus que de qualification au sens du Décret n°2001-272.

### 2.7.1 Fréquence d’audit de conformité des entités

L’EAR peut également être amenée à procéder à l’audit d’une composante de l’AC dans le cadre du fonctionnement régulier de l’AC. Cet audit s’effectuera sur préavis, à une fréquence à définir, ou de façon exceptionnelle.

### 2.7.2 Identité / qualité de l’auditeur

Le MINEFI et le Conseil National des Greffiers peuvent déléguer les opérations de contrôle de conformité aux clauses de la PC-Type à une entité d’audit (par exemple une EAR) qu’ils désignent. Cet auditeur doit pouvoir apporter la preuve de son expérience dans les ICP et technologies de cryptographie.

### 2.7.3 Lien entre l’auditeur et la fonction vérifiée

Le contrôleur ne doit être lié en aucune façon aux parties auditées (AC, OSC..) et au commanditaire en dehors du contrat d'audit.

### 2.7.4 Objet de l’audit

Si l’audit d’une composante de l’AC se révèle nécessaire pour mener à bien les opérations de référencement des certificats, l’AP et l’AC candidate déterminent les conditions et l’étendue des vérifications.
Le contrôle de conformité portera parmi les points suivants:

- dispositions générales (cf. chapitre 2 : §2.2 et suivants)
- identification et authentification (cf. chapitre 3),
- besoins opérationnels (cf. chapitre 4),
- contrôle de sécurité physique, contrôle des procédures, contrôle du personnel (cf. chapitre 5),
- contrôles techniques de sécurité (cf. chapitre 6),
- profil des certificats et LCR (cf. chapitre 7),
- spécifications d'administration (cf. chapitre 8).

### 2.7.5 Mesures à prendre à la suite de l’audit

La réception par INFOGREFFE des rapports d'audit ainsi établis par des tiers ne constitue ni l'entérinement ni l'approbation par INFOGREFFE du contenu, des conclusions ou des recommandations de ces rapports. INFOGREFFE n'est pas l'auteur des rapports d'audit et n'est donc pas responsable de leur contenu.
A l’issue d’un contrôle de conformité, le contrôleur rend au commanditaire de l’audit un avis parmi les suivants :
« Réussite », « Échec », « A confirmer ».

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

- en cas de réussite, le commanditaire remet à l'ICP contrôlée un avis de référencement MINEFI des certificats, ou de labellisation CNG,
- en cas d'échec, et selon l'importance des non-conformités, le contrôleur peut proposer au commanditaire le déréférencement ou le retrait du label des certificats émis par l'AC défaillante.
- en cas de résultat « A confirmer », le commanditaire peut remettre à l'AC défaillante un avis précisant sous quel délai les non-conformités doivent être réparées. Au terme du délai, un contrôle de « Confirmation » permet de vérifier que tous les points critiques ont bien été résolus.

### 2.7.6 Communication des résultats

La communication des résultat des contrôles de conformité est laissée à l'appréciation des Autorités de Politique.

## *2.8 Confidentialité des données à caractère personnel et des informations*

Il est rappelé que l'AC, en tant que gestionnaire de données à caractère personnel, est soumise à la loi n°78-17 du 6 janvier 1978 « Informatique et Libertés ». Conformément à cette loi, toute personne concernée –en l'occurrence tout client, Abonné ou Utilisateur- a le droit notamment d'accéder aux informations qui se rapportent à elle et, le cas échéant, à les faire rectifier.
L'AC prendra toutes les mesures nécessaires pour que les obligations résultant de cette loi soient scrupuleusement respectées, et elle définira en conséquence la teneur de ses relations avec l'AE.
Plus généralement, la présente PC est établie dans un contexte légal qui est fixé non seulement par la loi n°78-17, mais aussi par la directive européenne du 24 octobre 1995 et par toute convention internationale entrée en vigueur.
Les fichiers contenant des données nominatives font l'objet d'une déclaration ordinaire à la CNIL.

### 2.8.1 Types d'informations considérées comme confidentielles

#### 2.8.1.1 Données à caractère personnel

Toutes les données collectées et détenues par l'AC ou une AE sur une personne physique ou morale (par exemple : contrats du Client, procédure d'enregistrement, révocation, autres évènements consignés, correspondances échangées entre l'Abonné et l'AC ou l'AE, etc…) sont considérées comme confidentielles et ne doivent pas être divulguées sans avoir obtenu le consentement préalable de l'Abonné ou du client.
Les renseignements concernant l'identification ou d'autres données à caractère personnel, du client ou de l'Abonné, apparaissant sur les certificats bien que considérés comme non confidentiels (puisque ayant pour vocation d'être diffusés en clair et à large échelle),ne feront l'objet d'une publication systématique que :

- si le client ou l'Abonné a donné son consentement exprès et préalable à toute diffusion,
- si leur publication a été demandée sur décision judiciaire ou administrative (Ex : fourniture de preuve d'authenticité et validité du certificat -lien entre le certificat et l'Abonné- à un tiers).

#### 2.8.1.2 Autres informations

Les informations suivantes sont considérées comme confidentielles:

- les clés privées des Abonnés,
- les données d'activation des Abonnés,
- les journaux d'événements des composantes de l'ICP,

La divulgation de ces informations secrètes par l'Abonné s'effectuera à ses risques et périls, l'AC se dégageant alors de tout préjudice pouvant en résulter.
Les résultats des contrôles de conformité sont considérés comme confidentiels et ne peuvent être diffusés, sauf si leur publication a été demandée sur décision judiciaire ou administrative.

### 2.8.2 Types d'informations considérées comme non confidentielles

Les Listes des Certificats Révoqués ne contiennent que les numéros d'enregistrement des certificats, et leur date de révocation. Ces informations ne sont pas confidentielles

### 2.8.3 Divulgation des causes de révocation / suspension de certificat

Les causes de révocation de certificat ne peuvent être communiquées qu'aux entités suivantes :

- l'AE,
- l'AP en cas de litiges,
- à l'Abonné, au mandataire de sécurité et/ou au représentant légal.

Les causes de révocation ne devront contenir aucune information sur les personnes allant à l'encontre des lois nationales.
Les causes de révocation sont considérées comme confidentielles et protégées en conséquence.

## *2.9 Droits relatifs à la propriété intellectuelle*

Tous les droits de propriété intellectuelle détenus par l'AC sont protégés par la loi, règlement et autres conventions internationales applicables. Ils sont susceptibles d'entraîner la responsabilité civile et pénale en cas de leur non respect. Par exemple, conformément à la loi n°98-536 du 1er juillet 1998 (Journal officiel du 2 juillet , p.10075) et à la directive européenne 96/6/CE du 11 mars 1996, les bases de données réalisées par l'AC sont protégées. Le texte de la loi peut être consulté sur le site suivant : http://www.legifrance.gouv.fr.
En vertu des articles 323-1 à 323-7 du Code pénal, applicables lorsque une infraction est commise sur le territoire français, les atteintes et les tentatives d'atteintes aux systèmes de traitement automatisé de données sont sanctionnées, notamment l'accès et le maintien frauduleux, les modifications, les altérations et le piratage de données, etc.
Les peines encourues varient de 1 à 3 ans d'emprisonnement et d'une amende allant de 100.000 à 15.000.000 francs pour les personnes morales.
La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctifs, droits d'auteur (par exemple : logiciels, pages WEB, bases de données, textes originaux, etc.) est sanctionnée par les articles L 716-1 et suivants du Code de la propriété intellectuelle.

# 3 IDENTIFICATION ET AUTHENTIFICATION

## *3.1 Enregistrement initial*

### 3.1.1 Conventions de noms

Les noms utilisés dans un certificat émis dans le cadre de la présente Politique de Certification seront décrits selon la norme IS0/IEC 9594 (Distinguished Names).
Un certificat émis dans le cadre de l' ICP doit contenir dans le champ **subject :** un Distinguished Name, nom distinctif facile à distinguer et obligatoire pour l' Abonné.
Ces noms doivent être sous la forme d'une chaîne imprimable (printableString) X. 501 et doivent être conformes à la partie 1 de la norme PKIX. Le nom distinctif (DN) X.501, porté dans le champ Subject du certificat ne doit pas être vide.

### 3.1.2 Nécessité d'utilisation de noms explicites

Le nom distinctif (DN) X.501, porté dans le champ Subject du certificat, doit être, non seulement facile à distinguer des autres noms, mais aussi unique pour une AC donnée.
Le contenu des champs de nom Subject et Issuer doit avoir un lien explicite avec l'entité authentifiée.
Un nom distinctif (DN) doit se composer au moins des éléments :

- Nom de pays (C = FR),
- Nom d'organisation (O) : ce champ doit contenir le ~~n°SIREN~~ numéro d'identification de l'entreprise,
- Unité d'organisation (OU) : ce champ doit contenir la raison sociale de l'entreprise
- Nom usuel (CN = CommonName),

Dans le cas de personnes physiques, le nom distinctif doit contenir soit une combinaison du nom de famille, du prénom, et facultativement d'initiales, soit un pseudonyme identifié comme tel. Il peut aussi contenir une fonction ou un rôle organisationnel. Dans le cas d'un autre type d'entité identifiée, le nom distinctif doit refléter son nom légal authentifié.
Pour exemple, le nom distinctif sera le suivant :
DN = {C=FR, O = 243516879, OU=MA SOCIETE, CN = Dupont Jean PA},

### 3.1.3 Règles d'interprétation des différentes formes de noms

Aucune exigence n'est stipulée.

### 3.1.4 Unicité des noms

L'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC. Cependant, les noms distinctifs doivent être uniques au sein de l'ICP.
L'unicité des noms est obtenue suivant les règles décrites au §3.1.2.

### 3.1.5 Procédure de résolution de litige sur la déclaration de nom

Une partie qui demande un certificat doit avoir le droit d'utiliser le nom qu'elle souhaite y voir figurer. Elle doit également être en mesure de prouver qu'elle a le droit d'utiliser ce nom en particulier.
L'AC s'engage quant à l'unicité des noms de ses porteurs définie dans sa politique de nommage, conformément aux § 3.1.1 et §3.1.2. Elle proposera des procédures de résolution amiable des litiges portant sur la revendication d'utilisation d'un nom, portant sur la demande d'informations complémentaires qui devront être consignées dans le dossier d'enregistrement. Ces informations sont les prénoms de l'état civil ainsi que la date et lieu de naissance du demandeur.

### 3.1.6 Reconnaissance, authentification et rôle des noms de marques de fabrique, de commerce et de services

Le droit d'utiliser un nom qui est une marque de fabrique, de commerce ou de services ou un autre signe distinctif (nom commercial, enseigne, dénomination sociale) au sens des articles L.711-1 et suivants du Code de la Propriété intellectuelle (codifié par la loi n°92-957 du 1er juillet 1992 et ses modifications ultérieures) appartient au titulaire légitime de cette marque de fabrique, de commerce ou de services, ou de ce signe distinctif ou encore à ses licenciés ou cessionnaires.
L'AE limite ses vérifications concernant le droit d'utiliser un nom à la consultation du Registre du Commerce et des Sociétés.
INFOGREFFE dégage toute responsabilité en cas d'utilisation illicite par les clients et Abonnés des marques déposées, des marques notoires et des signes distinctifs, ainsi que les noms de domaine.

### 3.1.7 Preuve de possession d'une clé privée

L'AC doit vérifier que le demandeur est véritablement en possession de la clé privée associée à la clé publique de vérification de signature qui a été inscrite dans son certificat.

### 3.1.8 Vérification de l'identité de l'organisation

L'AE vérifie l'identification de l'organisation, de son représentant légal et de toutes personnes désignées par ce dernier, directement ou indirectement, pour le représenter vis-à-vis de l'AC ou de l'AE. A défaut de désignation d'un mandataire de sécurité, le représentant légal est l'unique représentant de l'organisation.
Lors de l'enregistrement, l'AE doit vérifier l'existence de l'organisation, l'identité de son représentant légal. L'organisation doit apporter pour sa part la chaîne des mandats conférant leur pouvoir aux mandataires de sécurité.
L'AE doit archiver toutes les informations pertinentes relatives à cet enregistrement. La DPC précisera les documents à fournir et les procédures d'enregistrement mises en oeuvre par l'AE.

### 3.1.9 Vérification de l'identité des Abonnés

L'AE acceptera seulement les demandes de certificat appuyées par des dossiers constitués de pièces justificatives fiables tels que décrits dans les paragraphes suivants.

#### 3.1.9.1 Vérification de l'identité des individus agissant pour le compte d'une organisation

Le certificat doit toujours contenir le nom et éventuellement toutes les informations complémentaires permettant d'identifier son titulaire sans ambiguïté.
Pour toute demande de certificat faite au titre de l'appartenance à une organisation, il faut que ladite demande soit confirmée par écrit par un mandataire de sécurité ou le représentant légal.
Le dossier doit comprendre les éléments listés au §4.1.2.
L'AE doit conserver les pièces reçues pour l'enregistrement de l'Abonné, examiner les pièces et documents remis avec un soin raisonnable et vérifier s'ils présentent ou non l'apparence de conformité et de validité.
La distribution des certificats par l'AE peut se faire directement au demandeur ou au mandataire de sécurité :

- S'il s'agit du demandeur, avant la distribution, l'AE vérifie en face à face, c'est-à-dire en présence du demandeur, un original d'une pièce d'identité officielle du demandeur comportant sa photo et sa signature.
- S'il s'agit du mandataire de sécurité, avant la distribution, l'AE vérifie en face à face, c'est-à-dire en présence du mandataire de sécurité, un original d'une pièce d'identité officielle du mandataire de sécurité comportant sa photo et sa signature. Le mandataire de sécurité a par la suite la charge de distribuer les éléments qui lui ont été remis au demandeur.

## *3.2 Ré-génération de clés (hors révocation)*

Les bi-clés doivent être périodiquement renouvelés afin de minimiser les attaques cryptographiques. Pour cela il est nécessaire que l'abonné renouvelle son bi- clés de signature. A cette occasion, l'AE doit vérifier à nouveau l'identité de l'Abonné. Les bi-clés de signature des Abonnés sont à renouveler au moins tous les trois ans.
Pour faciliter l'exploitation, un nouveau certificat peut être obtenu alors que le certificat courant est encore valide les modalités permettant d'assurer tout de même l'unicité du DN sont précisées dans la PC.

Pour les clés de signature, la demande de certificat qui suit le renouvellement de clé est signée par la clé privée courante de l'Abonné dans la limite de la durée de vie de la clé courante et en absence de révocation.

Etant donnée l'obligation de l'AC de garantir la conformité des informations remises lors de l'enregistrement, telle qu'énoncée dans l'article 6.1 de la Directive Européenne du 13/12/99 sur le cadre communautaire pour les signatures électroniques, il ne peut y avoir de renouvellement purement technique. La vérification lors d'un renouvellement ou lors de la modification d'informations faisant partie du dossier, doit être la même que lors d'un enregistrement initial, avec la présentation de toutes les pièces demandées pour ce dernier.

## *3.3 Ré-génération de clés après révocation*

Si un certificat a été révoqué, il ne peut être ré-activé. Il ne peut également jamais faire l'objet d'un renouvellement. Il faut procéder à la certification de nouvelles clés de la même façon que pour un enregistrement initial.
Après une révocation, l'attribution et la certification de nouvelles clés suivent la procédure d'enregistrement initial (cf. §3.1). Selon le type de révocation (compromission de la clé, compromission de l'autorité signataire du certificat) il appartient à l'Abonné de formuler une nouvelle demande de génération de certificat.

## *3.4 Demande de révocation*

L'AC doit établir et rendre public la procédure qu'elle utilise pour traiter les demandes de révocation et en établir la validité.
L'AC ou l'AE doit s'assurer du bon droit de la personne qui fait une demande de révocation. Elle vérifie la validité de la demande soit en vérifiant un ensemble d'informations déposées lors de l'enregistrement initial, soit au moyen d'une signature numérique valide reconnue par l'AC, soit de toute autre façon non équivoque.
Par nature une demande de révocation doit être traitée en urgence.
Une demande de révocation ne peut être présentée que par une entité habilitée (cf. §4.4.2) et doit être authentifiée par l'AE ou l'AC.
Dans le cas où son certificat se doit d'être révoqué (voir causes §4.4.1), l'Abonné doit informer au plus vite l'AE ou l'AC.

# 4 EXIGENCES OPERATIONNELLES

Les certificats proposés sont de classe 3+ avec une procédure d'enregistrement complète en face à face avec la personne morale et distribution de la clé privé/certificat sur une carte à puce.

## *4.1 Demande de Certificat*

L'AE doit s'assurer que les demandeurs de certificat suivent et respectent les procédures et exigences publiées par l'AC.
Chaque demande de certificat doit être accompagnée des pièces décrites au §4.1.2 qui permettent de prouver l'identité et les pouvoirs des futurs Abonnés conformément aux procédures applicables notamment :

- la preuve de l'identité du demandeur ;
- la preuve des pouvoirs pour les attributs demandés, par exemple d'appartenance à un organisme ou une société ;
- le contrat client ou la référence à un contrat client préexistant

Le cas échéant, il doit exister une autorisation et un contrat signés d'un mandataire de sécurité identifié. Ce contrat doit faire mention des obligations d'information du mandataire de sécurité sur ses obligations.

### 4.1.1 Origine de la demande

Un certificat est demandé par le représentant légal ou le mandataire de sécurité.

### 4.1.2 Informations à fournir

**Pour les certificats de Classe 3+, objet de cette PC**

Les informations suivantes doivent au moins figurer dans la demande de certificat d'Abonnés :

- une demande écrite, sur papier à entête portant le numéro SIREN de l'entreprise, signée par le chef d'entreprise ou le mandataire de sécurité, un modèle est proposé sur le site www.~~infogreffe~~certigreffe.fr
- une déclaration de l'Abonné décrite dans la DPC associée, portant l'acceptation des engagements de l'Abonné et désignant éventuellement le mandataire de sécurité pour le représenter auprès du greffier et lui remettre le certificat,
- une pièce portant le numéro ~~SIREN~~ d'identification de l'entreprise (extrait Kbis) si la demande est faite dans un greffe autre que celui territorialement compétent,
- une adresse postale professionnelle de l'Abonné,
- deux justificatifs d'identité de l'Abonné sous la forme de copies de documents d'identification (photocopie du permis de conduire, photocopie de la carte d'identité nationale etc.).
- le nom d'Abonné à utiliser dans le certificat,
- l'adresse de courrier électronique du demandeur,

Lorsqu'elles transitent sur un réseau, ces informations doivent être protégées en intégrité (notamment la clé publique de l'Abonné) et en confidentialité, afin de respecter les dispositions du §2.8.

### 4.1.3 Dossiers de demande de certificats.

L'AE acceptera seulement les demandes de certificat entreprise appuyées par des dossiers constitués de pièces justificatives fiables tels que décrits au §4.1.2 ci-dessus.

### 4.1.4 Archivage des dossiers.

Tout dossier de demande de certificat doit être archivé par les AE pendant la durée d'opposabilité des documents, définie au §4.6.2.
Durant cette durée d'opposabilité des documents, le dossier de demande de certificat doit pouvoir être présenté par l'AE sur demande de l'AC. Ce dossier, complété par les mentions que l'AE sera amenée à y consigner doit permettre de retrouver l'identité réelle des personnes physiques qui ont été désignées par un pseudonyme dans le certificat émis par l'AC.

### 4.1.5 Opérations à effectuer.

Lors d'une demande de certificat, l'AE doit effectuer les opérations suivantes:

- établir l'identité du demandeur (réelle dans le cas où le nom est un pseudonyme), en vérifiant les pièces justificatrices présentées par l'abonné ou le mandataire de sécurité ; quand le demandeur utilise un pseudonyme, le lien avec le nom d'état civil doit être établi,
- vérifier l'autorisation des attributs demandés (lorsque cela est approprié),
- s'assurer que le demandeur a pris connaissance des modalités applicables pour l'utilisation du certificat ; l'AE vérifie la date et la signature par l'Abonné du contrat ou de la déclaration indiquant qu'il a pris connaissance de ses droits et obligations,
- attribuer une carte à puce à l'Abonné, et faire générer par cette carte le bi-clé de l'Abonné

## *4.2 Emission du Certificat*

Une demande de certificat n'oblige en aucune façon l'AC à émettre un certificat.

L'émission d'un certificat par une AC indique que celle-ci a définitivement et complètement approuvé la demande de certificat selon les procédures décrites dans la DPC. Le certificat est considéré comme valable dès le moment où il est accepté par l'Abonné.

A la réception d'une demande de certificat :

- L'AC doit s'assurer que la demande a bien été prise en compte par une AE qu'elle a reconnue et que l'AE a traité la demande, et fournit une trace imputable de son avis,
- L'AC doit générer le certificat en y appliquant sa signature,
- L'AE doit notifier à l'Abonné la mise à disposition de son certificat et l'ensemble des procédures à suivre pour être en mesure de l'obtenir et de l'utiliser en cas d'acceptation,
- L'AE doit mettre le certificat à disposition de l'Abonné, c'est à dire rendre accessible par des moyens physiques ou logiques les informations permettant l'obtention du certificat.

## *4.3 Acceptation du certificat*

Le face à face de l'Abonné avec l'AE vaut acceptation de sa part du certificat et des obligations qui le lient à l'ICP.

## *4.4 Suspension et révocation de certificat*

### 4.4.1 Causes possibles de révocation

Lorsque la confiance dans un certificat (certificat d'Abonné ou d'une composante de l'ICP) est remise en cause, le certificat concerné doit d'être révoqué et placé dans une liste de certificats révoqués (LCR).
Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat :

- fin du contrat de travail de l'Abonné (ex : démission, licenciement, décès)
- suspicion de compromission, compromission, perte ou vol de la clé privée ou des données d'activation,
- modification de la situation de l'Abonné remettant en cause l'exactitude des informations contenues dans le certificat,
- suspicion de compromission, compromission, perte ou vol de la clé privée de l'AC, ou plus généralement, révocation du certificat de l'AC,
- décision de changement de composante de l'AC ou de l'AE suite à non-conformité des procédures de la DPC,
- cessation d'activité de l'organisme porteur du certificat.

Outre les cas de révocation de certificats mentionnés plus haut, l'AC et l'AE doivent révoquer un certificat dès lors qu'elles sont en possession d'informations de nature à indiquer une perte de confiance dans un certificat. Plus généralement, l'AC et l'AE peuvent, à leur discrétion, révoquer le certificat d'une entité identifiée lorsqu'elle ne respecte pas les obligations énoncées dans la présente Politique de Certification et dans tous documents contractuels ainsi que dans toute loi et règlement applicable.

### 4.4.2 Personnes pouvant demander une révocation

Seuls peuvent demander la révocation d'un certificat (certificat d'Abonné ou d'une composante de l'ICP) :

- l'Abonné, responsable du certificat,
- le mandataire de sécurité,
- le représentant légal,
- l'AC émettrice,
- une AE.

### 4.4.3 Procédure de demande de révocation

L'AE ou l'AC doit s'assurer que lors de la demande de révocation, toutes les procédures et exigences publiées par l'AC sont respectées.

Dans le cas où son certificat se doit d'être révoqué (voir causes §4.4.1), l'Abonné doit informer au plus vite l'AE ou l'AC. L' Abonné ne pouvant plus s'authentifier par signature, l'AC ou l'AE authentifieront la demande de révocation :

- soit au moyen d'une signature numérique valide reconnue par l'AC (par exemple, celle du mandataire de sécurité pour le certificat d'Abonné agissant pour le compte d'une organisation),
- soit selon la même procédure que pour l'enregistrement initial (cf. §3.1), c'est-à-dire par une procédure en face à face avec l'Abonné ou son mandataire de sécurité,
- soit par une autre procédure manuelle prévue à cet effet (par exemple en vérifiant un ensemble d'informations déposées lors de l'enregistrement initial).
- l'AC découvre et établit que le certificat n'a pas été délivré conformément aux procédures imposées par la présente DPC.

La demande de révocation doit contenir explicitement les informations d'identification de l'Abonné et de son certificat. La demande doit également contenir quand c'est possible la cause de révocation et le cas échéant, les éléments justificatifs de cette cause.
Les causes de révocation mentionnées dans les certificats révoqués ne doivent en aucun cas contenir d'informations privées sur les personnes et ce conformément aux lois nationales.
Si la procédure de demande de révocation d'un certificat est justifiée et acceptée, la révocation est déclenchée. L'ensemble des opérations et des mesures prises par l'AC doit être consigné et archivé.
Dans tous les cas de révocation d'un certificat, l'Abonné et le mandataire de sécurité doivent être informés de la révocation de son certificat. Cette notification doit indiquer la date à laquelle la révocation du certificat a pris effet et peut être effectuée par messagerie électronique.

### 4.4.4 Temps de traitement d'une demande révocation

A la réception d'une demande de révocation, en provenance de l'Abonné ou du mandataire de sécurité, l'AE analyse cette demande en vérifiant l'authenticité du demandeur, puis la transmet à la composante de l'AC chargée d'analyser les causes et justificatifs éventuels de révocation. Si la demande comporte toutes les informations nécessaires à l'authentification du demandeur et si les motifs correspondent à l'un des motifs décrits au §4.4.1, l'AC révoque le certificat en faisant introduire le numéro de série du certificat et éventuellement d'autres informations dans une liste de révocation.
Les demandes de révocation doivent être traitées immédiatement à réception de la demande.
L'AC sera immédiatement informée en cas de compromission avérée ou soupçonnée de la clé d'une des composantes de l'~~ICP INFOGREFFE~~ICP CERTIGREFFECERTIGREFFE. Pour tous les autres cas de révocation, un temps minimal de traitement, incluant la publication, garanti devra figurer dans la DPC qui ne devra pas dépasser un jour ouvré. La prise en compte des demandes de révocation par le service de révocation de l'AC doit pouvoir être effective au moins du lundi au vendredi de 9h à 18h sauf jours fériés, et si possible 24h/24 et 7j/7.

### 4.4.5 Causes possibles de suspension

La présente PC n'est pas concernée par la suspension de certificats.

### 4.4.6 Personne pouvant demander une suspension

La présente PC n'est pas concernée par la suspension de certificats.

### 4.4.7 Procédure de demande de suspension

La présente PC n'est pas concernée par la suspension de certificats.

### 4.4.8 Limites de la période de suspension

La présente PC n'est pas concernée par la suspension de certificats.

### 4.4.9 Fréquence de publication des LCR

L'AC doit garantir aux Utilisateurs de certificats qu'elle délivre, la mise à disposition d'une LCR à jour. Un délai minimum de mise à jour des listes de certificats révoqués sera fixé dans la DPC en fonction des objectifs opérationnels (cf. §2.6.2) et du délai de traitement d'une révocation (cf §4.4.4).

### 4.4.10 Exigences de vérification des LCR

Avant toute utilisation de certificats, tout Utilisateur de certificat doit, outre la vérification de la validité intrinsèque du certificat auquel il entend se fier, en particulier sa signature, impérativement vérifier auprès de l'AC le statut de révocation de ce certificat, en consultant les Listes des Certificats Révoqués (LCR) les plus récentes.
Il appartient aussi à l'Utilisateur de certificat de vérifier la validité des LCR. La validité d'une LCR est contrôlée par vérification de sa signature et vérification de la validité du certificat de l'AC l'ayant publiée.
En particulier le statut de révocation du certificat de l'~~AC INFOGREFFE~~AC CERTIGREFFE doit être vérifié, en consultant la LCR la plus récente de l'AC à laquelle l'~~AC INFOGREFFE~~AC CERTIGREFFE est subordonnée.
En cas d'indisponibilité temporaire des LCR nécessaires à la vérification d'un certificat, l'Utilisateur du certificat doit considérer le certificat comme potentiellement non valide. Il doit, si possible, différer le traitement du document signé par le certificat, ou en cas d'impossibilité d'attente, considérer la signature comme invalide, sauf à engager sa propre responsabilité (cf. §2.1.5.3).

### 4.4.11 Publication des causes de révocation en ligne

Les motifs de la révocation d'un certificat donné ne sont jamais divulgués à des tiers sauf en cas d'accord écrit de l'Abonné ou du client, ou de requête administrative ou judiciaire.
Dans le cadre des audits et contrôles auxquels l'AC est soumise en vertu de la présente Politique de Certification (par exemple, audit par une EAR), des éléments sur les motifs de révocation, non nominatifs et non liés à un certificat, pourront être utilisés. D'une manière plus générale, ces éléments pourront être utilisés à des fins statistiques.

### 4.4.12 Exigences de vérification en ligne de la révocation

La validité des certificats est vérifiée en consultant les Listes des Certificats Révoqués valides les plus récentes. Cette liste est publiée en ligne sur un annuaire.

Les LCR doivent être des listes de certificats révoqués conformes à la norme X.509 V2.
L'annuaire de publication des LCR doit être conforme au protocole LDAP V2.

### 4.4.13 Autres formes de publication des avis de révocation

Aucune autre forme de publication des avis de révocation que la LCR n'est proposée aux Utilisateurs de certificat.

### 4.4.14 Autres formes de publication des avis de révocation – Exigences de vérification

Aucune autre forme de publication des avis de révocation que la LCR n'est proposée aux Utilisateurs de certificat.

### 4.4.15 Exigences spéciales en cas de révocation pour compromission des clés

En cas de compromission avérée ou soupçonnée de la clé de signature de l'AC, INFOGREFFE doit dès qu'elle en a connaissance en aviser :

- les AC auxquelles elle est liée,
- toutes les autorités qui l'accréditent,
- toutes les AE rattachées,
- l'Autorité de Politique,
- tous les Abonnés,
- le CNG,
- le MINEFI.

L'~~AC INFOGREFFE~~AC CERTIGREFFE doit par ailleurs révoquer sans délai l'ensemble des certificats qu'elle aura pu émettre.
Dans le cas où le client, l'Abonné ou une composante de l'ICP a connaissance d'une perte de confiance dans un certificat (cf. §4.4.1), réelle ou soupçonnée, il a l'obligation de procéder sans délais à la vérification de la révocation du certificat associé ou de la demander dans les plus brefs délais si celle-ci n'a pas été faite.

## *4.5 Journalisation d'événements*

### 4.5.1 Types d'événements enregistrés

Le personnel de l'ICP doit pouvoir justifier les opérations effectuées, en particulier par la tenue d'un journal d'événements.
Les événements seront enregistrés sous forme papier ou sous forme électronique par saisie ou par génération automatique. Les différentes composantes liées à la gestion des certificats doivent tenir à jour une liste d'événements qui les concernent. La liste des événements et données à conserver doit être documentée.
L'AC doit consigner au moins les événements suivants :

- tous les événements ayant trait à la sécurité des systèmes informatiques impliqués dans l'ICP,
- démarrage et arrêt des systèmes informatiques,
- démarrage et arrêt des applications,
- Opérations échouées ou réussies pour créer, extraire, établir des mots de passe ou modifier les privilèges système d'exploitants privilégiés,
- génération des clés de ses composantes,
- la génération et la révocation de certificat,
- changements des caractéristiques et (ou) de ses composantes,
- création et révocation de certificats,
- opérations pour initialiser, extraire, valider et invalider des Abonnés
- opérations d'écriture dans les LCR,
- événements relatifs au support carte à puce (génération des données d'activation à enregistrer).

Ces enregistrements d'événements devront contenir au minimum les champs suivants, s'ils sont pertinents :

- type d'opération,
- destinataire de l'opération,
- nom du demandeur de l'opération,
- nom de l'exécutant
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes),
- date et heure de l'opération,
- cause de l'événement,
- résultat de l'événement (échec ou réussite).

L'AC devra recueillir, par des moyens automatiques ou manuels, d'autres événements. Ce sont ceux concernant la sécurité et qui ne sont pas produits par les systèmes informatiques, notamment :

- les accès physiques,
- les actions de maintenance et de changements de la configuration du système,
- les changements apportés au personnel,
- les actions de destruction : des supports contenant des clés, des données d'activation ou des renseignements personnels sur les Abonnés.

### 4.5.2 Fréquence des traitements de journalisation

Le processus de journalisation doit être effectué en tâche de fond et permettre un enregistrement en temps réel des opérations effectuées. Le processus de journalisation doit être conçu de façon à être incontournable.
En cas de saisie manuelle l'écriture doit se faire dans le même jour ouvré que l'événement.

### 4.5.3 Durée de conservation des journaux d'événements

Les journaux doivent être conservés par la composante sur le site pour une période minimale de un mois. Ces journaux doivent ensuite être archivés conformément aux instructions indiquées au §4.6.2

### 4.5.4 Protection d'un journal d'événements

L'écriture dans les journaux d'événements doit être conditionnée par des contrôles de droits d'accès. Les enregistrements et l'horloge des composantes de l'ICP doivent être protégés contre les tentatives non autorisées de modification et de destruction.

### 4.5.5 Procédures de sauvegarde des journaux d'événements

Les journaux d'événements seront sauvegardés. L'ensemble des copies de sauvegarde des journaux d'événements devront être protégées au même niveau que les originaux (voir §4.5.4).
Les précisions sont fournies dans la DPC.

### 4.5.6 Système de collecte des journaux (interne ou externe)

L'enregistrement des événements doit commencer au démarrage des systèmes concernés par les événements à enregistrer et se terminer à l'arrêt de ces systèmes.

### 4.5.7 Imputabilité des événements

L'imputabilité d'une action revient à la personne, l'organisme ou le système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer dans l'un des champs du journal d'événements.

### 4.5.8 Analyse des vulnérabilités

Les composantes de l'AC responsables de la fonction de journalisation doivent être en mesure de détecter toute tentative de violation de l'intégrité du système de gestion des certificats, y compris les équipements physiques, l'environnement d'exploitation et le personnel.
Les journaux d'événements journaliers doivent être contrôlés pour identifier des anomalies liées à des tentatives en échec.
Les journaux doivent être revus avec une fréquence hebdomadaire. Cette révision donnera lieu à un résumé dans lequel les éléments importants sont analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.
Il est souhaitable qu'un rapprochement mensuel soit fait entre les journaux de l'AE et ceux des composantes de l'AC pour vérifier la concordance entre événements dépendants et contribuer ainsi à révéler toute anomalie.
La DPC doit documenter les mesures à prendre à la suite de ces analyses.

## *4.6 Archive des dossiers*

### 4.6.1 Types de données à archiver

Les données à archiver sont au moins les suivantes :

- les logiciels et les fichiers de configuration des équipements informatiques de l'ICP,
- la PC,
- la DPC,
- les agréments contractuels ou les conventions avec d'autres AC,
- les journaux d'événements,
- les certificats tels qu'émis ,
- les LCR telles qu'émises ou publiées,
- les notifications de révocation,
- les justificatifs d'identité des Abonnés,
- le contrat signé par les Abonnés,
- les données d'enregistrement/renouvellement :
    1. les type et n° des documents présentés,
    2. le lieu du dépôt des copies des documents (ou copie de ces documents) incluant le contrat signé par l'abonné,
    3. les options du contrat (par ex : consentement pour publication),
    4. l'identité signataire du contrat (par ex : mandataire de sécurité),
    5. la méthode de vérification des documents,
    6. l'identité de l'AC et de l'AE émettant le certificat.

### 4.6.2 Période de rétention des archives

Les certificats de clés de signature, ainsi que les LCR produites par l'AC doivent être archivés pendant au moins cinq ans après l'expiration des clés.
Tout dossier de demande de certificat doit être archivé pendant la durée d'opposabilité des documents, c'est-à-dire cinq (5) ans après l'expiration des clés.

### 4.6.3 Protection des archives

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

- être protégées en intégrité,
- être disponibles,
- pouvoir être relues et exploitées.

### 4.6.4 Procédures de copie des archives

Il appartient contractuellement aux AE de s'assurer de la disponibilité des archives les concernant, par une procédure de copie des archives ou tout autre moyen à leur convenance.
Les procédures de copie des archives de l'AC seront fournies dans la DPC.

### 4.6.5 Besoins d'horodatage des enregistrements

Les enregistrements des certificats et des LCR sont horodatées conformément à la politique de sécurité de l'AC en matière d'archivage.

### 4.6.6 Système de collecte des archives (interne ou externe)

Aucune exigence n'est stipulée. Les précisions seront fournies dans la DPC.

### 4.6.7 Procédures de récupération des archives

Une composante de l'ICP ne peut récupérer et consulter que ses propres archives.
Le processus de récupération doit faire l'objet d'une procédure et figurer dans la DPC.
Une archive doit être récupérée sous un délai inférieur à 2 jours ouvrés.

## *4.7 Changement de clé d'une composante*

L'AC possède une clé privée de signature unique avec laquelle sont effectuées toutes les opérations de certification. Le certificat portant la clé publique associée à la clé privée unique de l'AC est le certificat « courant » de l'AC.
La durée de validité du certificat courant de l'~~AC INFOGREFFE~~AC CERTIGREFFE est de 10 ans à compter du 27/09/2001
L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration de son certificat courant de l'AC. Pour cela la date de fin de validité du certificat courant de l'AC doit être postérieure à la date de fin de validité des certificats d'Abonnés émis sous ce certificat d'AC.
Par conséquent, pour garantir une durée de validité identique pour tous les certificats d'Abonnés, le certificat courant de l'AC doit être renouvelé avant que sa durée de validité restant à courir ne devienne inférieure à la durée de validité des certificats d'Abonnés.
L'AC doit demander le renouvellement de son bi-clé dans les trois mois précédant cette date.
Lorsqu'un nouveau bi-clé d'AC est généré, seule la nouvelle clé privée correspondante doit être utilisée pour générer des certificats. Le certificat portant la clé publique précédente peut toujours être utilisé pour valider les certificats émis sous ce certificat et ce jusqu'à ce que ces certificats d'Abonnés aient expiré.
Lorsqu'une composante renouvelle ses clés, le nouveau certificat est mis à disposition des Abonnés dans les délais indiqués au §2.6.2. L'Autorité de Politique INFOGREFFE est notifiée dans le même délai que celui de publication du nouveau certificat.
L'AE doit demander le renouvellement de son certificat dans les trois mois précédant son expiration.
Selon la nature du changement (fin de période de validité de clés, renouvellement de clé suite à une révocation, etc.), les mesures prises doivent respecter les procédures de traitement énoncées dans les chapitres correspondants.

## *4.8 Récupération en cas de désastre ou de compromission*

L'ICP doit disposer d'un plan de reprise d'activités en cas de sinistre (comprenant notamment la compromission ou la suspicion de compromission de la clé de l'AC) qui prend en compte les paramètres suivants :

- services de révocation et de publication de la LCR et de la chaîne de certification, à remettre en service en priorité,
- délai minimum de recouvrement de ces services,
- procédures de secours ( détection de sinistre, contact des équipes de secours, etc.),

- politique de sécurité et de protection des secrets,
- tests pratiques, formation et entraînement des personnels,

Ce plan est testé à une fréquence qui sera définie dans la DPC.

A l'issue de la mise en œuvre du plan de secours, ce document peut faire l'objet d'une mise à jour afin d'affiner les procédures.

### 4.8.1 Corruption des ressources informatiques, des logiciels et (ou) des données

L'AC doit établir des procédures visant à assurer le maintien des activités et décrire, dans ces procédures, les étapes prévues en cas de corruption ou de perte de ressources informatiques, de logiciels et (ou) de données.

Cette rubrique doit être renseignée et apparaître dans la DPC .

### 4.8.2 Révocation de la clé publique d'une composante de l'AC

Après avoir corrigé les problèmes ayant motivé la révocation, et avoir publié le numéro de série du certificat dans la LCR appropriée, l'AC peut :

- produire un nouveau bi-clé de signature de l'AC,
- émettre de nouveaux certificats à toutes les entités et s'assurer que toutes les LCR sont signées au moyen de la nouvelle clé.

L'Autorité de Politique pourra proposer un contrôle préalable à la remise en service de toute composante de l'AC.

### 4.8.3 Compromission des clés d'une composante de l'ICP

En cas de compromission de la clé de signature numérique d'une AC, celle-ci doit, avant de redéfinir un certificat au sein de l'ICP révoquer sa clé publique suivant les procédures décrites au §4.4 et au §4.8.2.

### 4.8.4 Sécurisation d'une installation après une catastrophe naturelle ou un autre sinistre

L'AC doit établir des procédures visant à assurer le maintien des activités et décrire, dans ces procédures, les étapes prévues après une catastrophe naturelle ou un autre sinistre.

## *4.9 Cessation d'activité d'une composante*

Si l'AC interrompt ses activités :

- elle doit immédiatement en aviser ses Abonnés et prendre des dispositions pour que les clés et l'information de l'AC continuent d'être archivées,
- elle doit également aviser tous les AC avec lesquels il a un lien de hiérarchie,
- elle doit mettre fin aux contrats de sous-traitance,
- sa clé doit être détruite, ou le module cryptographique qui la supporte.

De même , en cas de changements dans la gestion des activités de l'AC, celle-ci doit en aviser toutes les entités auxquelles il a émis des certificats et l'AC racine.
Si les opérations d'une AC sont transférées à une autre AC, celle-ci devra avoir le même niveau d'assurance.
Les archives de l'AC doivent être conservées selon les indications et la période stipulées au chapitre 4.6.
En conséquence, l'AC en fin de vie s'engage à:

- communiquer dans un délai de préavis de 6 mois son intention de cesser son activité,
- mettre en œuvre tous les moyens dont elle dispose pour informer ses partenaires de ses intentions,
- révoquer son certificat,
- révoquer tous les certificats valides qu'elle a signés,
- remettre ses archives ainsi que l'ensemble des données dont elle dispose à l'AP.

Dans le cas où une composante de l'ICP autre que l'AC interrompt ses activités, l'AC doit reprendre à sa charge ou faire porter sur une autre entité les obligations de cette composante.

# 5 CONTROLE DE SECURITE PHYSIQUE, CONTROLE DES PROCEDURES, CONTROLE DU PERSONNEL

## *5.1 Contrôles physiques*

### 5.1.1 Situation géographique et construction de sites

Le site d'hébergement de l'AC se trouve sur le territoire national , dispose de locaux à accès contrôlé, et est inspecté régulièrement par les services de l'Etat compétents.
La DPC précise les conditions de sécurité physique et les règles appliquées aux et dans les locaux, en particulier sur les sujets suivants :

- Emplacement, construction et accès physique,
- Système électrique et système de conditionnement d'air,
- Dégâts causés par l'eau,
- Prévention et protection-incendie,
- Stockage et archivage des supports,
- Retrait du matériel, destruction,
- Duplication des supports de sauvegarde à l'extérieur des locaux.

### 5.1.2 Accès physique

L'accès physique à une composante de l'~~ICP INFOGREFFE~~ICP CERTIGREFFE doit être protégé contre tout accès non autorisé.
Les zones à accès contrôlé doivent être physiquement protégées contre un accès extérieur non autorisé. La liste des personnels autorisés à y accéder doit exister et être limitée au strict besoin du bon fonctionnement du service. L'accès des personnels autorisés doit être contrôlé par un moyen physique et enregistré.
En dehors des heures ouvrables, la sécurité doit être renforcée par la mise en oeuvre de moyens de détection d'intrusion physique.

### 5.1.3 Energie et air conditionné

Les administrateurs des composantes de l'~~ICP INFOGREFFE~~ICP CERTIGREFFE doivent s'assurer que les installations électriques et de conditionnement d'air sont suffisantes pour le bon fonctionnement de leur système.

### 5.1.4 Exposition aux liquides

Les administrateurs des composantes de l'~~ICP INFOGREFFE~~ICP CERTIGREFFE doivent s'assurer que leur système n'est pas situé en zone inondable.

### 5.1.5 Prévention et protection incendie

Les administrateurs des composantes de l'~~ICP INFOGREFFE~~ICP CERTIGREFFE doivent s'assurer que leur système est protégé contre les incendies grâce à un système de protection incendie.

### 5.1.6 Conservation des médias

Les administrateurs des composantes de l'~~ICP INFOGREFFE~~ICP CERTIGREFFE doivent s'assurer que les supports de stockage utilisés par leur système sont protégés contre un excès de température, d'humidité et de magnétisme et autres variables ambiantes.

### 5.1.7 Destruction des déchets

Tous les supports servant au stockage de l'information sensible doivent être effacés ou détruits avant leur mise au rebut.

### 5.1.8 Sauvegarde hors site

Les administrateurs des composantes de l'~~ICP INFOGREFFE~~ICP CERTIGREFFE doivent s'assurer que les installations de sauvegarde à l'extérieur de leurs locaux offrent le même niveau de sécurité que leurs locaux principaux.
Toute sortie d'équipement, d'information ou de médias relatif à l'~~ICP INFOGREFFE~~ICP CERTIGREFFE fait l'objet d'une autorisation.

## *5.2 Contrôles des procédures*

### 5.2.1 Rôles de confiance

Afin de veiller à la séparation des tâches critiques, on distingue les rôles suivants au sein des composantes de l'ICP :

- opérateurs,
- ingénieurs systèmes,
- administrateurs,
- responsables de sécurité,
- auditeur du système.

**L'Opérateur** d'une composante réalise l'exploitation des services offerts par la composante, dans le cadre de ses attributions. Il est chargé de lancer l'exécution des fonctions cryptographiques.
**L'Ingénieur Système** est chargé de la mise en route, de la configuration et de la maintenance technique de la plate-forme supportant la composante. Il assure l'administration du système et du réseau de cette plate-forme.

**L'Administrateur** met en œuvre les politiques de certification et déclarations relatives aux procédures de certification de l'ICP au sein de la composante qu'il administre. Il est responsable de l'ensemble des services rendus par cette composante.
**Le Responsable de Sécurité** est chargé de contrôler la sécurité physique et fonctionnelle d'une composante de l'ICP et de son environnement. Il gère les contrôles d'accès physique à la plate-forme de la composante, et est chargé de mettre en œuvre la politique de sécurité régissant la composante.
**L'Auditeur du système** est autorisé à consulter et maintenir les archives et le journaux d'audit.
**Administrateur** et **responsable de sécurité** sont confondus dans le cadre de la présente PC.
Les attributions associées à chaque rôle doivent être décrites dans la DPC. Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où cela ne dégrade pas la sécurité des services offerts.

### 5.2.2 Nombre de personnes nécessaires à chaque tâche

Toute opération relative aux certificats requiert l'autorisation ou la présence d'au moins un membre du personnel de l'ICP.
Le nombre de personnes dont la présence ou l'autorisation sont nécessaires à chaque tâche doivent être décrites dans la DPC.

### 5.2.3 Identification et authentification des rôles

Tous les membres du personnel de l'AC doivent être nommés formellement par le responsable de sécurité. Ils doivent faire vérifier leur identité et leurs autorisations avant :

- que leur nom soit ajouté à la liste d'accès aux locaux de l'AC,
- que leur nom soit ajouté à la liste des personnes autorisées à accéder physiquement au système de l'AC.

Tous les intervenants sur le système de l'AC, ou d'une autre composante de l'ICP, doivent faire vérifier leur identité et leur autorisation avant :

- qu'un certificat leur soit délivré pour accomplir le rôle qui leur est dévolu,
- qu'un compte soit ouvert en leur nom dans le système.

L'AC ne doit donner l'accès au rôle de l'intervenant qu'après contrôle positif de l'identification/authentification.

## *5.3 Contrôles du personnel*

### 5.3.1 Passé professionnel, qualifications, exigences d'habilitations

Le responsable de l'AC doit s'assurer que tous les membres du personnel qui accomplissent des tâches relatives à l'exploitation d'une AC ou d'une AE, ainsi que les dirigeants de la société :

- sont nommés à leur poste par écrit ;
- sont tenus par contrat ou par la loi de respecter les obligations, notamment de confidentialité, du poste qu'ils occupent ;
- possèdent les qualifications pertinentes et ont reçu la formation nécessaire pour accomplir leurs tâches ;

- n’ont pas de tâches ou d’intérêts susceptibles d’entrer en conflit avec les obligations qui leur incombent à l’égard de l’AC ou de l’AE ;

### 5.3.2 Procédures de contrôle du passé professionnel

Des contrôles du passé professionnel doivent être faits afin de déterminer dans la mesure du raisonnable le caractère digne de confiance et la compétence des postulants à un emploi auprès de l’AC.

### 5.3.3 Exigences de formation

L’AC doit s’assurer que tous les membres du personnel qui accomplissent des tâches touchant l’exploitation d’une AC ou d’une AE ont reçu une formation adaptée concernant les principes de fonctionnement et des mécanismes de sécurité de l’AC ou de l'AE, et sont familiarisés aux règles de sécurité en vigueur.

### 5.3.4 Fréquence des formations

Le contenu des formations décrites au §5.3.3 doit être mis à jour en fonction des changements apportés à l’ICP, et les personnels de l’AC doivent bénéficier de la formation professionnelle en fonction des besoins.
En outre, le personnel exploitant l’AC doit participer à des séances de formation sur la sécurité au moins une (1) fois par année.

### 5.3.5 Gestion des métiers

Aucune exigence n'est stipulée.

### 5.3.6 Sanctions pour des actions non autorisées

Sur faute avérée ou soupçonnée d’un membre de l’ICP dans l’accomplissement de ses tâches en rapport avec l’exploitation d’une AC ou d’une AE, l’AC doit lui interdire l’accès au système et, le cas échéant, prendre toutes sanctions disciplinaires adéquates.

### 5.3.7 Contrôle des personnels des entreprises contractantes

L’AC doit s’assurer que les personnels des entreprises contractantes respectent l’accès aux locaux conformément aux indications du §5.1.2
Les exigences relatives au personnel des entreprises contractantes sont identiques à celles relatives aux employés, en particulier à celles décrites au §5.3.

### 5.3.8 Documentation fournie au personnel

L’AC doit mettre à la disposition des membres de l’ICP la présente Politique de Certification, et s’assurer qu’ils disposent de l’accès à toute loi, ou tout contrat qui s’applique au poste qu’ils occupent.
Les documents dont doit également disposer le personnel sont notamment les suivants :

- la PC supportée par la composante à laquelle il appartient,
- la DPC propre au domaine de certification,
- les procédures internes de fonctionnement,
- les documents constructeurs des matériels et logiciels utilisés.

# 6 CONTROLES TECHNIQUES DE SECURITE

## *6.1 Génération et installation de bi-clé*

### 6.1.1 Génération de bi-clé

L'AC doit produire son propre bi-clé de signature numérique au moyen d'un algorithme de cryptographie et selon une procédure impliquant plusieurs personnes conformément aux dispositions du §5.2.2. La clé privée de l'AC est dédiée à la signature des certificats INFOGREFFE.

~~Certificat de classe 3+ :~~

Le bi-clé de signature numérique de l'Abonné est produit par la carte à puce de l'Abonné lors de la procédure d'enregistrement en face à face avec l'AE.

L'AC ne gère pas de bi-clé de confidentialité pour le compte des Abonnés.

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

La clé publique d'un Abonné doit être remise à l'AC sous la forme d'un paquet attestant de la possession de la clé privée correspondante. La transmission doit assurer l'intégrité de bout en bout.

### 6.1.3 Fourniture de la clé publique de validation de l'AC aux Utilisateurs

La clé publique de vérification de l'AC est diffusée sous la forme d'un certificat numérique X509 V3 protégé en intégrité avec authentification d'origine (certificat signé par l'AC à laquelle l'~~AC INFOGREFFE~~AC CERTIGREFFE est subordonnée) qui est en particulier téléchargeable à partir du site de l'AC.

### 6.1.4 Tailles de clés

Afin de respecter les durées de vie définies au §6.3.2, les tailles de clés sont définies de la façon suivante :

- les bi-clés d'une AC sont d'une complexité au moins équivalente à 2048 bits pour l'algorithme RSA.
- les bi-clés d'un Abonné sont d'une complexité au moins équivalente à 1024 bits pour l'algorithme RSA.

Les bi-clés des entités identifiées sont d'une complexité au moins équivalente à 1024 bits pour l'algorithme RSA. En particulier tous les opérateurs de l'ICP n'ont que des certificats avec une clé d'au moins 1024 bits.

### 6.1.5 Paramètres de génération de clé

L'équipement de génération de bi-clé doit utiliser des paramètres respectant les normes internationales de sécurité propre à l'algorithme considéré (RSA).

Les recommandations décrites dans le document suivant doivent être appliquées pour la génération des bi-clés RSA :

*IEEE P1363 / D9 (Draft Version 9). Standard Specifications for Public Key Cryptography - Annex A (Informative) - Number-Theoretic Background. (Copyright 0 1997, 1998, 1999 by*

*the Institute of Electrical and Etectronics Engineers, Inc., 345 East 47th Street New York, NY 10017, USA, All rights reserved.)*
Les choix suivants seront retenus :

- l'exposant public sera 65537 ;
- le choix des premiers p et q peut être aléatoire ou fort, sous réserve d'appliquer les recommandations applicables du document cité en référence.

### 6.1.6 Contrôle de qualité des paramètres de clés

Le contrôle de la qualité des paramètres doit être effectué conformité avec le §6.1.5.

### 6.1.7 Mode de génération de clé (matériel ou logiciel)

Les bi-clés de l'AC doivent être produits par un module cryptographique matériel.

### 6.1.8 Usage de la clé publique

Les différents usages possibles des clés publiques sont définis et contraints par l'utilisation d'une extension de certificat X.509 v3 (champ « keyUsage »).
Le champ « keyUsage » est marqué comme "critique".
Le champ « keyUsage » des certificats d'AE est défini dans la DPC.

#### 6.1.8.1 Clé publique de vérification (de signature)

Une clé publique de vérification doit être utilisée à des fins d'identification, d'authentification, d'intégrité et/ou de non - répudiation.
La clé publique de vérification de l'AC est la seule clé utilisable pour vérifier la signature des certificats et des LCR.
Le champ « keyUsage » du certificat doit être utilisé conformément au profil des certificats et des LCR. Ce champ doit comporter l'une des valeurs suivantes :
Pour les certificats de clés d'Abonnés :
**digitalSignature** et **nonRepudiation**
Pour les certificats de clés de signature de certificats de l'AC :
**keyCertSign** et **cRLSign** (aucune autre valeur autorisée)

#### 6.1.8.2 Clé publique de confidentialité

L'AC ne gère pas de bi-clé de confidentialité pour le compte des Abonnés.

## *6.2 Protection de la clé privée*

### 6.2.1 Normes pour les modules cryptographiques

L'Abonné doit protéger sa clé privée afin qu'elle ne soit pas divulguée. Il lui appartiendra de s'assurer qu'une maintenance particulière est réalisée sur le poste utilisé ; en particulier de la stabilité du système, de l'absence de virus, vers et chevaux de Troyes. Il lui appartiendra également de choisir le matériel et les logiciels offrant une sécurité suffisante pour la protection et l'utilisation de ses clés privées conformément aux dispositions du présent paragraphe.

Dans le présent cadre de certificats de classe 3+, l'utilisation de module cryptographique de type carte à puce est imposé.
Concernant le module cryptographique de l'AC, celui-ci doit être en conformité avec les recommandations de la norme FIPS140-1 niveau 3 au moins.

### 6.2.2 Contrôle de clé privée par plusieurs personnes

Plusieurs personnes doivent contrôler les opérations de production des clés de l'AC. Les données utilisées pour leur création doivent être partagées par plusieurs personnes. Le partage du secret permettant la génération ou la regénération de la clé de l'AC doit être fait entre deux (2) personnes au minimum.

### 6.2.3 Récupération de clé privée

Les clés privées de signature numérique des Abonnés ne doivent jamais se trouver en main tierce et leur recouvrement est donc impossible.
L'AC ne gère pas de bi-clé de confidentialité pour le compte des Abonnés.

### 6.2.4 Sauvegarde de clé privée

Une entité identifiée peut sauvegarder ses propres clés de signature numérique . Le cas échéant, les clés sauvegardées doivent être enregistrées sous forme chiffrée et être protégées logiquement ou physiquement contre tout accès illicite. Les mesures de protection prises sur la clé sauvegardée doivent être au moins du même niveau que celles prises pour la clé d'origine.
Concernant l'AC, sa clé privée est stockée dans le module cryptographique. Ce module cryptographique doit disposer :

- d'une détection d'intrusion lorsque la clé privée est active,
- d'un autotest.

### 6.2.5 Archive de clé privée

Les mesures et les contraintes relatives à l'archivage des clés privées sont identiques à celles qui sont prises en matière de sauvegarde (cf §6.2.4).

### 6.2.6 Initialisation de clé privée dans un module cryptographique

La procédure d'initialisation de clé privée et la procédure de mise sous contrôle des secrets sont spécifiés comme suit :
Les clés privées de l'AC sont générées dans le module cryptographique; elles sont conservées chiffrées, n'étant en clair qu'au moment requis pour leur utilisation.
Les clés privées des entités identifiées sont tant que possible générées par un moyen local. Dans le cas de certificats de classe 3+, ces clés sont générées dans le module cryptographique de type carte à puceLes clés privées des entités identifiées sont tant que possible conservées chiffrées, n'étant en clair qu'au moment requis pour leur utilisation.

### 6.2.7 Méthode d'activation de clé privée

L'Abonné doit être identifié avant que la clé privée ne soit activée. Cette authentification peut se faire sous forme de données d'activation (code PIN ou mot de passe). Une fois désactivées, les clés privées doivent être conservées tant que possible sous une forme chiffrée.

L’activation de la clé privée de l’AC est décrite dans la DPC.

### 6.2.8 Méthode de désactivation de clé privée

L'Abonné s’engage à ne jamais quitter son poste de travail en le laissant dans un état qui permette d'utiliser sa clé privée sans utiliser un secret approprié.
La désactivation de la clé privée de l’AC est décrite dans la DPC.

### 6.2.9 Méthode de destruction de clé privée

Lorsque le certificat de signature numérique arrive à expiration ou s’il est révoqué, la clé privée ne doit plus servir à aucune opération et doit être détruite.
Lorsque l’AC doit détruire sa clé privée, elle doit réinitialiser le module cryptographique ce qui implique la réécriture complète de toute forme de mémoire dans le module cryptographique. Elle doit aussi détruire tous les secrets de génération qui ont été partagés.
Pour détruire une clé privée, il faut écraser toutes les copies des clés privées quel qu’en soit le support. Les procédures de destruction des clés privées sont décrites dans la DPC.

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

### 6.3.1 Archive des clés publiques

L’AC émettrice doit archiver toutes les clés publiques de vérification conformément au §4.6.

### 6.3.2 Durée de vie des clés publiques et privées

La période de validité de toutes les clés de 1024 bits est d’au plus quatre (4) ans.
La période de validité des clés 2048 bits est d’au plus douze (12) ans.
L’utilisation d’une longueur particulière de clé doit être déterminée conformément à l’évaluation de la menace et des risques prenant en compte l’évolution des technologies d’attaque.
Les durées de validité des certificats sont définies dans la DPC.

## *6.4 Données d'activation*

### 6.4.1 Génération et installation des données d'activation

Les cartes à puce sont fournies aux Abonnés protégés avec des données d’activation. Les données d’activation sont définies par l'AC de façon à les rendre imprévisibles. Les mécanismes cryptographiques et de contrôle de l’accès utilisant ces données doivent être suffisamment robustes pour protéger les clés et les données elles-mêmes.

### 6.4.2 Protection des données d'activation

Les données d’activation doivent être protégées en confidentialité par les Abonnés et les composantes de l’ICP. Celles-ci doivent être mémorisées et en aucun cas ne doivent être transcrites sur un support.

### 6.4.3 Autres aspects des données d'activation

Les données d'activation sont transmises par l'AC aux Abonnés par un canal différent de celui des cartes à puce.
Certificat de classe 3+ :
L'utilisation de code PIN requiert une longueur d'au moins quatre (4) caractères.

## *6.5 Contrôles de sécurité des postes de travail*

### 6.5.1 Exigences de sécurité spécifiques sur les postes de travail

Les besoins de sécurité suivants doivent permettre d'évaluer le niveau de sécurité des postes de travail des composantes de l'ICP :

- identification et authentification des Utilisateurs du poste de travail,
- 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,

Le niveau minimal d'assurance recherché doit au moins répondre à ces objectifs de sécurité. Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires, à prendre en compte dans la recherche du niveau minimal d'assurance offert par les postes de travail.
Aucune exigence n'est stipulée pour le poste de travail de l'Utilisateur d'un certificat INFOGREFFE. Cependant, les Abonnés et les Utilisateurs de certificats devront prendre toutes les mesures leur permettant de satisfaire à leurs obligations du §2.1.4 et §2.1.5.

### 6.5.2 Niveau de sécurité des postes de travail

Un niveau minimal d'assurance dans le niveau de sécurité offert doit être défini dans la DPC pour tous les systèmes de l'ICP.
Si on utilise un système de mots de passe réutilisables, un mécanisme permettant de bloquer temporairement le compte après un nombre limité et fixé au préalable de tentatives est souhaitable. Cette mesure de protection est obligatoire pour les systèmes de l'AC.

## *6.6 Contrôles techniques du système durant son cycle de vie*

### 6.6.1 Contrôles des développements des systèmes

L'implémentation d'un système permettant de mettre en oeuvre les composantes de l'~~ICP INFOGREFFE~~ICP CERTIGREFFE doit être documentée et respecter dans la mesure du possible des normes de modélisation et d'implémentation. Les composantes de l'ICP doivent faire l'objet d'un suivi d'activité afin d'anticiper les modifications nécessaires notamment en termes de capacité de traitement et de stockage. La configuration du système, des composantes, doit être documentée et contrôlée. De même, toute modification ou mise à niveau de composantes du système doit être documentée et contrôlée et suivre la procédure pour la gestion des évolutions du système (changement de version, « patch »).

### 6.6.2 Contrôles de la gestion de la sécurité

Toute évolution du système doit être documentée et doit apparaître 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 Contrôles de la sécurité réseau*

L'interconnexion vers des réseaux publics doit être protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'~~ICP INFOGREFFE~~ICP CERTIGREFFE.
L'AC doit s'assurer que les réseaux internes de l'ICP sont dans un environnement sécurisé et doit contrôler régulièrement leur configuration.

## *6.8 Contrôles de la gestion des modules cryptographiques*

Les modules cryptographiques utilisés par l'AC doit présenter un label d'évaluation correspondant à une évaluation faite selon une méthode internationale d'assurance du niveau de sécurité (ex : ITSEC, Critères Communs).

# 7 PROFILS DE CERTIFICATS ET DE LCR

## *7.1 Profil des certificats*

Les certificats sont conformes à la norme X.509 v3 et au document RFC 2459.
Le certificat dans sa forme identifiée est l'ensemble des éléments suivants :

- « **tbsCertificate** » : l'ensemble des champs décrits aux §7.1.1 et §7.1.2 et signés par l'AC avec sa clé privée ;
- « **signatureAlgorithm** » : l'identifiant de l'algorithme utilisé pour produire la signature du certificat ; et
- « **signatureValue** » : le résultat de la signature sur l'ensemble des champs de « **tbsCertificate** ».

### 7.1.1 Champs de base

Selon la version 3 de la norme X.509 des certificats, les champs suivants doivent être complétés par le logiciel de l'AC :
**version** : version du certificat X. 509, complété avec une valeur entière de 2 pour indiquer que le certificat est un certificat X.509 version 3

**serialNumber** : numéro de série unique du certificat, complété avec une valeur entière. Cette valeur doit être unique pour chaque certificat émis par l'ICP

**signature** : ce champ est une structure composée du champ « algorithmIdentifier », elle-même composée du champ « **algorithm** », complété avec l'identifiant (OID) de l'algorithme utilisée par l'AC pour signer le certificat, . L'algorithme utilisé est le RSA avec l'OID 1.2.840.113549.1.1.5 (sha-1WithRSAEncryption, Identifier for SHA-1checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc.) ;

Remarque : le champ « **parameters** » n'est pas utilisé pour le RSA.

**issuer** : nom de l'AC, complété avec le nom distinctif (Distinguished Name) de X.500 de l'AC qui a créé le certificat

**countryName** : pays d'établissement : Ce champ doit être renseigné pour l'issuer avec le pays d'établissement de l'ICP

**validity** : dates d'activation et d'expiration du certificat
**notBefore** : date d'activation du certificat
**notAfter** : date d'expiration du certificat

**subject** : nom distinctif X.500 de l'Abonné pour lequel le certificat est émis ;

**subjectPublicKeyinfo**
**algorithmIdentifier** : ce champ est une structure composée du champ « **algorithm** », qui définit l'identifiant de l'algorithme(OID) pour lequel le certificat est émis, complété avec l'OID 1.2.840.113549.1.1.1 (OID description: rsaEncryption, Identifier for RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc.)
Remarque : le champ « **parameters** » n'est pas utilisé pour le RSA.
**subjectPublicKey** : clé de l'Abonné

### 7.1.2 Extensions des certificats

La version 3 de certificat X.509 permet de rajouter des informations additionnelles sur la clé publique de l'Abonné, la clé publique de l'émetteur, et sur les LCR.
Pour les certificats émis par l'AC, les champs d'extensions standards de X.509v3 seront considérés de la façon suivante (les champs non listés dans les paragraphes suivants ne sont pas utilisés et inclus dans les certificats générés par l'AC) :

#### 7.1.2.1 AuthorityKeyIdentifier

Cette extension non critique identifie la clé publique utilisée pour vérifier la signature sur un certificat. Elle est utilisée lorsqu'un émetteur a plusieurs clés de certification.
L'AC doit:

- inclure l'extension dans tous les certificats qu'elle émet ;
- ne pas renseigner les champs « **authorityCertIssuer** » et « **authorityCertSerialNumber** » ;
- inclure le champ « **authorityKeyIdentIfier** » avec un identifiant unique de la clé de l'AC utilisée.

#### 7.1.2.2 SubjectKeyIdentifier

Cette extension non critique identifie la clé publique qui est certifiée. Cela permet de différencier plusieurs clés d'un même Abonné. Ce champ contiendra l'empreinte numérique SHA-1 de la clé publique de l'Abonné. L'AC doit:

- inclure l'extension dans tous les certificats;
- remplir le champ « SubjectKeyIdentifier » avec les 160 bits de l'empreinte numérique SHA-1 de la valeur binaire de la clé publique de l'Abonné (sans l'étiquette, la longueur et le nombre de bits non utilisés),

#### 7.1.2.3 KeyUsage

Cette extension définit l' utilisation prévue de la clé contenue dans le certificat.

L'AC doit :

- inclure l'extension dans tous les certificats des Abonnés,
- indiquer l'usage prévu de la clé comme défini au §6.1.8,
- gérer la criticité comme défini au §6.1.8.

#### 7.1.2.4 CertificatePolicies

Cette extension non critique définit les politiques de certification que le certificat reconnaît supporter. Ce champ est traité pendant la validation du chemin de confiance.
L'AC doit :

- inclure l' extension dans tous les certificats des Abonnés ;
- inclure le champ « **policyInformation** » en renseignant le champ « **policyIdentifier** » avec l' OID de la PC ; cf §01.2 ;

#### 7.1.2.5 subjectAltName

Cette extension donne une information complémentaire sur l'Abonné. Cette extension est non critique et contient :

- pour les certificats de serveur, l'adresse de messagerie correspondant au responsable du serveur d'application concerné.
- pour un abonné individuel, son adresse de messagerie.

L'AC doit:

- mettre le champ Critique à « FALSE » ( NON);
- renseigner le champ « **generalName** » avec l'adresse de messagerie au format RFC822

#### 7.1.2.6 basicConstraints

Cette extension critique indique si l'entité destinataire du certificat peut agir comme une Autorité de Certification en utilisant la clé privée correspondant à la clé publique certifiée pour signer des certificats.
L'~~AC INFOGREFFE~~AC CERTIGREFFE doit utiliser la valeur CA « FALSE » pour les certificats d'Abonnés.
Le certificat de l'~~AC INFOGREFFE~~AC CERTIGREFFE doit utiliser la valeur CA à « TRUE »

#### 7.1.2.7 cRLDistributionPoints.

Cette extension non critique identifie l'emplacement où l'Utilisateur de certificat peut trouver une LCR.
L'AC doit :

- inclure cette extension dans les certificats d' Abonnés ;
- renseigner les champs ~~« **directoryName** »~~ et « **uniformRessourceIdentifier** » : l'AC indiquera l'~~-~~adresse d'annuaire ~~(nom distinctif)~~ contenant les LCR.

### 7.1.3 Interprétation sémantique des champs critiques de la Politique de Certification

Conformément à la norme X.509v3, le caractère critique doit être traité de la façon suivante selon que l'extension est critique ou non :

- si l'extension est non - critique, alors:
  - si l'application ne sait pas la traiter, l'extension est abandonnée mais le certificat est accepté.
  - si l'application sait la traiter, alors:
    - si l'extension est conforme avec l'usage que l'application veut en faire, l'extension est traitée.
    - si l'extension n'est pas conforme avec l'usage que l'application veut en faire, l'extension est abandonnée, mais le certificat est accepté.
- si l'extension est critique, alors :
  - si l'application ne sait pas la traiter, le certificat est rejeté.
  - si l'application sait la traiter, alors :
    - si l'extension est conforme avec l'usage que l'application veut en faire, l'extension est traitée.
    - si l'extension n'est pas conforme avec l'usage que l'application veut en faire, le certificat est rejeté.

## *7.2 Profil de LCR*

Les certificats sont conformes à la norme X.509 v2 et au document RFC 2459.
Une LCR dans sa forme finale est l'ensemble des éléments suivants :

- « **tbsCertList** » : l'ensemble des champs décrits aux §7.2.1 et §7.2.2 ; L'AC doit apposer avec sa clé privée un sceau sur le certificat. Ce sceau est le résultat d'une fonction mathématique appliquée sur ce champ
- « **signatureAlgorithm** » : l'identifiant de l'algorithme utilisé pour produire le sceau d'intégrité de la liste; et
- « **signatureValue** » : le résultat de cet algorithme sur l'ensemble des champs de « **tbsCertList** ».

### 7.2.1 Champs de base

Selon la version 2 de la norme X.509 des LCR, les champs suivants doivent être complétés par le logiciel de l'AC :
Les LCR doivent au moins inclure les champs de base spécifiés dans la recommandation X.509v2. Ces champs sont les suivants:
**version** : version de la LCR, version 2 complété avec une valeur entière de 1 pour indiquer que le certificat est un certificat X.509 version 2
**signature** : signature de l'AC pour authentifier la LCR, complétée avec l'identifiant (OID) de l'algorithme utilisé pour signer le certificat.
**issuer** : nom de l'AC, complété avec le nom distinctif (Distinguished Name) de X.500 de l'AC qui a créé le certificat
**thisUpdate** : complété avec la date indiquant quand la LCR a été générée
**nextUpdate** : complété avec la date indiquant quand la prochaine mise à jour de la LCR sera générée

**revokedCertificates** : complété avec la séquence des certificats révoqués avec les champs suivants :

**userCertificate** : complété avec le numéro de série de certificat révoqué
**revocationDate** : complété avec la date de révocation du certificat

Remarque : le champ « **crlEntryExtensions** » n'est pas utilisé par l'AC

### 7.2.2 Extensions des LCR et des entrées des LCR

La version 2 de LCR X.509 permet de rajouter des informations additionnelles.
Pour les LCR émises par l'AC, les champs d'extensions standards de X.509v2 seront considérés de la façon suivante (les champs non listés dans les paragraphes suivants ne sont pas utilisés et inclus dans les certificats générés par l'AC) :

#### 7.2.2.1 AuthorityKeyIdentifier

Cette extension non critique identifie la clé publique à utiliser pour vérifier la signature sur la LCR. Elle est utilisée lorsqu'un émetteur a plusieurs clés de certification.
L'AC doit :

- inclure cette extension dans toutes les LCR qu'elle émet ;
- ne pas renseigner les champs « **authorityCertIssuer** » et « **authorityCertSerialNumber** ».
- renseigner le champ « **authorityKeyIdentifier** » avec un identifiant unique de la clé de l'AC utilisée ;

~~**7.2.2.2CRLNumber**~~

~~Cette extension permet à un utilisateur de LCR de déterminer s'il a déjà vu et traité les LCR générées avant celle-ci, et que celle qu'il reçoit est postérieure à celle dont il dispose. L'AC doit :~~

~~- inclure cette extension dans toutes les LCR qu'elle émet ;~~
~~- renseigner le champ avec un nombre croissant séquentiel pour chaque LCR émise par l'AC ;~~

# 8 ADMINISTRATION DES SPECIFICATIONS

Le présent chapitre définit les exigences en matière d'administration et de gestion de la présente Politique de Certification.

## *8.1 Procédures de modification de la PC*

### 8.1.1 Articles pouvant être modifiés sans avis

Le responsable de l'AC peut modifier la présente politique sans préavis aux Abonnés et aux tiers Utilisateurs lorsque, selon l'évaluation du responsable de la politique, ces modifications n'ont aucun impact sur eux.

### 8.1.2 Articles dont la modification nécessite la formulation d'une nouvelle politique

Cette PC devra être revue en raison de projets de modifications suivants :

- les certificats référencés,
- la composition de l'AC ou de l'AE,
- à chaque modification des documents de référence de l'AP (ex : PSE du CNG, PC-Type du MINEFI) ainsi que chaque année pour assurer sa conformité aux normes de sécurité et à l'évolution des mises en oeuvre du marché.

INFOGREFFE reçoit très volontiers les corrections d'erreurs ou changements suggérés à lecture de ce document et qui seront communiqués au point de contact référencé au chapitre 8.2. Ces demandes de corrections doivent faire parvenir leurs commentaires au responsable de la politique dans des délais inférieurs à la moitié des délais de préavis fixés au §8.1.4.

### 8.1.3 Changement avec avis

L'AC doit prévenir le CNG et le MINEFI, éventuellement les Abonnés et les Utilisateurs de certificats (voir §8.1.4) de tout projet de modification de la PC ou de la DPC concernant :

- les certificats référencés,
- la composition de l' AC ou de l' AE,
- les pratiques de certification.

Le processus de revue pour la modification et l'approbation de la PC et de la DPC doit être documenté et mis en œuvre.

### 8.1.4 Délai de préavis

Le responsable de l'AC doit donner un préavis de trente (30) jours aux Abonnés et aux tiers Utilisateurs avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, ont un impact majeur sur eux.

Le responsable de l'AC doit donner un préavis de quinze (15) jours aux Abonnés et aux tiers Utilisateurs avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, ont un impact mineur sur eux.

Le responsable de l'AC doit donner un préavis aux Abonnés et aux tiers Utilisateurs dans les sept (7) jours d'un changement de la présente politique qui résulte d'une situation hors du contrôle du responsable de la politique, à condition que ce changement ait un impact sur eux.

En cas de changement intervenant dans la composition de l'AC ou de l'AE, l'AC doit prévenir le CNG et le MINEFI :

- au plus tard un mois avant le début de l' opération si elle a un impact sur le niveau de qualité et de sécurité des fonctions de l' AC et de l' AE vis à vis des certificats référencés,

- au plus tard un mois après la fin de l'opération s' il n' y a pas d' impact.

## *8.2 Procédures de publication et de notification*

La PC est disponible depuis les sources suivantes :
- Par courrier, adresser la demande à :

INFOGREFFE

~~108 rue Damremont~~

~~75018 Paris~~4 Place Félix Eboué

75012 PARIS

- Par téléchargement, sur le site Web d'INFOGREFFE :

URL : http://www.~~info~~certigreffe.fr

Toute remarque sur la présente PC ou la DPC associée est à adresser soit par courrier à INFOGREFFE, soit par e-mail à :

info@~~infogreffe~~certigreffe.fr

## *8.3 Procédures d'approbation de la PC*

L'approbation de la PC de l'AC est réalisée par l'AP qui notamment vérifie son adéquation aux documents de référence de l'AP, suivant une procédure de revue documentée.
La décision de l'Abonné de ne pas demander la révocation de son certificat suite à la notification d'un changement proposé constitue l'acceptation du changement.

# 9 ANNEXE 1 : DOCUMENTS DE RÉFÉRENCE

| | |
|---|---|
| ITU-T X.509v3, ISO/IEC 9594-8 | Information Technology - Open Systems Interconnection – The Directory :Authentication Framework, Recommendation X.509, June 97 |
| P1363 | IEEE P1363 / D9 (Draft Version 9). Standard Specifications for Public Key Cryptography - Annex A (informative) - NumberTheoretic Background. |
| PC2 | Procédures et politiques de certification de clés,. CISSI, version 2.0 du 28 avril 1999. |
| PKCS#10 | Certification Request Syntax Standard (PKCS#10), RSA Lab. Version 1.0, November 1, 1993. |
| RFC 2459 | Intemet X509 Public Key Infrastructure, Certificate and LCR Profile, RFC 2459, January 1999 |
| RFC 2527 | Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, S. Chokhani and W. Ford, March 1999. |
| ROLES-IGC | Rôles des exploitants d'une infrastructure de gestion de clés, CISSI, version 1.0 du 7 mars 1999 |

# 10 ANNEXE 2: FORMAT D'UN CERTIFICAT X.509

La recommandation de l'ITU-T X.509v3 ou ISO/IEC 9594-8 spécifie le format d'un certificat de clé publique. Le code ASN1 suivant précise quelles sont les informations contenues dans un certificat X.509v3.

*-basic certificate definition*

Certificate : := SIGNED { SEQUENCE {
version [0] Version DEFAULT vl,
seriaINumber CertificateSerialNumber,
signature AlgorithmIdentIfier,
issuer Narne, - *nom de l'AA du MINEFI,*
validity validity,
subject Name,
subjectPublicKeyInfo SubjectPublIcKeyinfo,
IssuerUniqueIdentifler [1] IMPLICIT UniqueIdentifier OPTIONAL,
-si présent, version doit être v3
subjectUniqueIdentifler [2] IMPLICIT UnIqueIdentifier OPTIONAL
- si présent, version doit être v3
extensions [3] Extensions OPTIONAL
-si présent, version doit être v3-1 1

Version : := INTEGER ( vl (0). v2(l), v3(2) )

CertificateSerialNumber ::= INTEGER

AlgorithmIdentifier ::= SEQUENCE {
algorithm ALGORITHM.&id ({Supported Algorithms}) ,
parameters ALGORITHM.&Type({Supported Algorithms}{@algorithm}) OPTIONAL }

Definition of the following information object set is deferred perhaps to standardized profiles or to protocol implementation conformance staternents. The set is required to specify a table constraint on the pararneters component of AlgorithmIdentIlier.

SupportedAlgorithme ALGORITHM ::= {…}

Validity ::= SEQUENCE {
notfbefore Time,
notAfter Time }

SubjectPublicKeyInfo ::= SEQUENCE {
Algorithm AlgorithmIdentifier,
subjectPublIcKey BIT STRING}

Time ::= CHOICE {
utcTime UTCTIme,
generalizedTime GeneralizedTime}

Extensions ::=SEQUENCE OF Extension

- For those extensions where ordering of individuel extensions within the SEQUENCE is significant, the specification of those individuel extensions shall include the rules for the significance of the order therein
-

**Extension** ::= SEQUENCE {
extnId EXTENSION.&id ({ExtensionSet}),
critical BOOLEAN DEFAULT FALSE,
extnValue OCTET STRING
- contains a DER encoding of a value of type &Extn Type
- for the extension object identified by extnId - )
-

**ExtensionSet** EXTENSION ::= {…}

# 11 ANNEXE 3: PROFILS DE CERTIFICAT ET LCR

Profil pour les extensions des certificats X.509v3 de classe Télé – Procédures.

**Introduction**

Le profil décrit dans cette annexe fournit une implémentation recommandée pour les certificats X.509 version 3 et les listes de révocation Version 2 pour les relations de Télé - Procédures avec les Administrations Françaises en applications des exigences définies dans le PC-type du MINEFI.

**Tables décrivant le profil**

Dans les tables suivantes, les colonnes « Elém. » et « Table » permettent d'établir une référence croisée avec les éléments des autres tables. Le numéro dans la colonne table indique le numéro de la table et le numéro qui suit le caractère 1 indique l'élément dans cette table.

La colonne « Champ » indique le nom ASN1 du champ X.509.

La colonne « Trai » indique si le traitement de ce champ est obligatoire ou optionnel en conformité avec la PC-Type du MINEFI (Politique de Certification type).

La colonne « Génération » précise le niveau d'utilisation requis pour chaque champ. Le niveau d'utilisation indique quelle entité doit utiliser le champ dans ses traitements. La colonne « Génération » est divisée en deux types de certificats « Signature » et « GC » pour gestion de clé. La colonne « Signature » traite du certificat du porteur du certificat (Abonné).

**Classification d'utilisation**

Chaque champ listé est indiqué comme étant obligatoire ou optionnel. Lorsqu'un champ est encapsulé dans un autre champ, l'exigence sur le champ encapsulé n'est effective que si le champ le contenant (parent) est lui-même supporté.

**Capacités statiques**

Les classifications suivantes sont utilisées pour spécifier des conformités statiques (capacités).

**Obligatoire (m)2**

Les applications générant des certificats et des LCR doivent être capables de générer le champ concerné. Les applications traitant les certificats doivent être capables de recevoir ce champ et d'effectuer les traitements associés.

2 Pour éviter des erreurs de lecture entre des documents anglais et français, nous avons choisi d'utiliser la lettre m de 'mandatory' pour désigner la caractéristique obligatoire, tout en gardant le V pour optionnel.

**Optionnel (o)**

Les applications générant des certificats et des LCR ne sont pas tenus de générer le champ concerné. Si le champ est présent, il doit être traité comme un champ obligatoire, et les champs encapsulés doivent être traités comme indiqués. Les applications traitant les certificats peuvent ignorer ce champ, à moins qu'il soit indiqué comme « critique ».

**Non applicable H**

Le champ n'est pas applicable.

**Comportement dynamique**

Les classifications suivantes sont utilisées pour spécifier des conformités dynamiques (comportements).

**Interdit (x)**

Les applications générant des certificats et des LCR doivent s'assurer que le champ concerné n'est jamais généré. Les applications traitant les certificats doivent générer et retourner une erreur appropriée si un champ interdit est rencontré.

**Critique (k)**

Si le champ est présent dans un certificat et que l'application qui doit le traiter ne le reconnaît pas, ce système doit considérer le certificat comme invalide. Si le champ est présent dans une LCR et n'est pas reconnu par l'application qui doit le traiter, il doit indiquer à l'Utilisateur que la LCR n'est peut-être pas au bon niveau.

**Requis (r)**

L'information pour ce champ doit être rempli au moment de la génération du certificat.

| Elém | Champ | traitement | Signature Porteur | GC | Notes | Table |
|---|---|---|---|---|---|---|
| 1. | certificate | m | mr | mr | | |
| 2. | version | m | mr | mr | | |
| 3. | serialNumber | m | mr | mr | | |
| 4. | signature | m | mr | mr | | |
| 5. | Issuer | m | mr | mr | | |
| 6. | validity | m | mr | mr | | |
| 7. | notBefore | m | mr | mr | | |
| 8. | notAfter | m | mr | mr | | |
| 9 | subject | m | mr | mr | | |
| 10. | subjectPublicKeyInfo | m | mr | mr | | |
| 11. | algorithmIdentifier | m | mr | mr | | T2/1 |
| 12. | subjectPublicKey | m | mr | mr | | |
| 13. | issuerUniqueIdentifier | o | o | O | 1 | |
| 14. | subjectUniqueIdentifier | o | o | O | 1 | |
| 15. | extensions | m | mr | mr | | T3/1 |
| 1. Ce champ ne doit pas être renseigné par l'~~AC INFOGREFFE~~AC CERTIGREFFE | | | | | | |

**Tableau 1 : Certificat de base**

| Elém | Champ | trai | Signature Porteur | GC | Notes | Table |
|---|---|---|---|---|---|---|
| 1. | algorithmIdentifier | m | mr | mr | | |
| 2. | Algorithm | m | mr | mr | | |
| 3. | Parameters | m | o | o | 1 | |
| 1. Ce champ n'est pas renseigné pour l'algorithme RSA | | | | | | |

**Tableau 2 : Identifiant d'algorithme**

| Elém | Champ | trai | Signature Porteur | GC | Notes | Table |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| 1. | extensions | m | mr | mr | | |
| 2. | Extension | | | | | |
| 3. | extnID | m | mr | mr | | |
| 4. | critical | m | mr | mr | | |
| 5. | extnValue | m | mr | mr | | |

**Tableau 3 : Extensions**

| Elém | Champ | trai | Signature Porteur | GC | Notes | Table |
|---|---|---|---|---|---|---|
| 1. | AuthorityKeyIdentifier | o | mr | mr | 1 | |
| 2. | SubjectKeyIdentifier | o | mr | mr | 2 | |
| 3. | KeyUsage | o | kmr | kmr | | |
| 4. | ExtendedKeyUsage | o | o | o | 3 | |
| 5. | PrivateKeyUsagePeriod | o | o | o | 3 | |
| 6. | CertificatePolicies | o | kmr | kmr | | |
| 7. | policyMappings | o | o | o | | |
| 8. | subjectAltName | o | - | - | | |
| 9. | issuerAltName | o | o | o | | |
| 10. | subjectDlrectoryAttributes | o | o | o | | |
| 11. | basicConstraints | m | kmr | kmr | | |
| 12. | nameConstraints | o | - | - | | |
| 13. | policyConstraints | o | - | - | | |
| 14. | cRLDistributionPoints | m | mr | mr | | |

1. Ce champ est recommandé pour la génération et le traitement des certificats
2. Contient l'empreinte numérique de la clé publique de l'Abonné
3. Ce champ ne doit pas être renseigné par l'~~AC INFOGREFFE~~AC CERTIGREFFE

**Tableau 4 : Extensions standard**

| Elém | Champ | traitement | Génération | Notes | Table |
|---|---|---|---|---|---|
| | | | | | |
| 1. | CertificateRevocationList | m | mr | | |
| 2. | version | m | mr | | |
| 3. | signature | m | mr | | T2/1 |
| 4. | issuer | m | mr | | |
| 5. | thisUpdate | m | mr | | |
| 6. | nextupdate | m | mr | | |
| 7. | revokedcertificates | m | mr | | |
| 8. | usercertificate | m | mr | | |
| 9 | revocationDate | m | mr | | |

| | | | | | |
|---|---|---|---|---|---|
| 10. | crlEntryExtensions | o | o | 1 | |
| 11. | crlExtensions | m | mr | | |
| 1. Ce champ ne doit pas être renseigné par l'~~AC INFOGREFFE~~AC CERTIGREFFE | | | | | |

**Tableau 5 : Liste de certificats révoqués**

| Elém | Champ | traitement | Génération | Notes | Table |
|---|---|---|---|---|---|
| | | | | | |
| 1. | AuthorityKeyIdentifier | o | mr | | |
| 2. | issuerAltName | o | o | | |
| 3. | cRLNumber | o | o | 1 | |
| 4. | lssuingDistributionPolnt | o | o | | |
| 5. | deltaCRLIndicator | o | o | | |
| 1. Ce champ ne doit pas être renseigné par l'~~AC INFOGREFFE~~AC CERTIGREFFE | | | | | |

**Tableau 6 : Extensions LCR**

| Elém | Champ | traitement | Génération | Notes | Table |
|---|---|---|---|---|---|
| 1. | reasonCode | o | o | 1 | |
| 2. | holdlnstructionCode | o | o | 1 | |
| 3. | invalidityDate | o | o | 1 | |
| 4. | certificatelssuer | o | o | 1 | |
| 1. Ce champ ne doit pas être renseigné par l'~~AC INFOGREFFE~~AC CERTIGREFFE | | | | | |

**Tableau 7 : Extensions d'entrées de LCR**

# 12 ANNEXE 4: TEXTES LÉGISLATIFS ET RÉGLEMENTAIRES

**Cadre général**

- Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Article 28 de la loi no 90-1170 du 29 décembre 1990, modifié par l'article 17 de la loi de réglementation des télécommunications no 96-659 du 26 juillet 1996.
- Loi no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
- Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique
- Article 1148 du code civil relatif à la Force Majeure

**Régime "déclaration - autorisation"**

- Décret no 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptographie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.
- Décret no 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptographie dispensées de toute formalité préalable.

- Arrêté du 17 mars 1999 définissant la tome et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptographie.
- Arrêté définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fournitures d'un moyen ou d'une prestation de cryptographie, no PRMX9802730A du 13 mars 1998
- Arrêté définissant le modèle de notification préalable par le fournisseur des identités des intermédiaires utilisés pour la fourniture des moyens ou prestations de cryptographie soumis à autorisation, no PRMX9802732A du 13 mars 1998.