

# Certeurope

## Politique de Certification Racine

Référence	AC Racine Certeurope - Politique de Certification Racine 1.0.doc	Version	01
Date de création	26/04/2002	Date de mise à jour	14/10/2002

Ce document contient 43 pages

Etat du document	Officiel
Rédigé par	François RENO
Validé par	François RENO
Approuvé par	

**MODIFICATIONS**

Fichier	AC Racine Certeurope - Politique de Certification Racine 1.0.doc
Date	14/10/2002



**CertEurope**  
La Signature Electronique des  
Professions Réglementées

**CONFIDENTIEL CERTEUROPE**

**AC Certigrefe Classe 3Plus**  
**Procès-verbal d'initialisation de l'AC**

Exemplaire : Original

Date	Etat	Version	Commentaires
26/4/2002		0.1	Création du document

## DOCUMENTS REFERENCES

Référence	Version	Titre des documents

## SOMMAIRE

<b>MODIFICATIONS</b>	<b>2</b>
<b>DOCUMENTS REFERENCES</b>	<b>2</b>
<b>SOMMAIRE</b>	<b>3</b>
<b>1. INTRODUCTION</b>	<b>8</b>
1.1. PRESENTATION GENERALE	8
1.1.1. <i>Aperçu général</i>	8
1.1.2. <i>Aperçu de la politique</i>	8
1.2. DEFINITIONS	9
1.2.1. <i>Liste des acronymes</i>	9
1.2.2. <i>Définitions</i>	9
1.3. IDENTIFICATION (OID)	11
1.4. APPLICATIONS ET GROUPES D'UTILISATEURS CONCERNES	11
1.4.1. <i>Autorité de Certification Racine</i>	11
1.4.2. <i>Autorité d'Enregistrement (AE)</i>	11
1.4.3. <i>Autorité de Certification fille.</i>	12
1.4.4. <i>Parties utilisatrices</i>	12
1.5. ANNUAIRES	12
<b>2. DISPOSITIONS DE PORTÉE GÉNÉRALE</b>	<b>13</b>
2.1. OBLIGATIONS	13
2.1.1. <i>Obligations communes à toutes les composantes de l' AC et de l' AE.</i>	13
2.1.2. <i>Obligations de l'AC Racine</i>	13
2.1.3. <i>Gestion des supports et données d'activation.</i>	13
2.1.4. <i>Exactitude des informations</i>	13
2.1.5. <i>Délai entre la demande et l'émission du certificat</i>	14
2.1.6. <i>Protection des clés privées</i>	14
2.1.7. <i>Restriction quant à l'utilisation des clés privées de l'AC Racine</i>	14
2.1.8. <i>Fonction de séquestre.</i>	14
2.1.9. <i>Obligations d'une AE</i>	14
2.1.9.1. <i>Avis de génération et de révocation de certificats</i>	14
2.1.9.2. <i>Exactitude des informations</i>	14
2.1.9.3. <i>Protection des clés privées de l'AE</i>	14
2.1.9.4. <i>Restriction quant à l'utilisation des clés privées de l'AE</i>	14
2.1.10. <i>Obligations de l'AC Fille</i>	14
2.1.10.1. <i>Conformité à la PC</i>	14
2.1.10.2. <i>Propriété</i>	15
2.1.10.3. <i>Exactitude des informations</i>	15
2.1.10.4. <i>Protection des clés privées de l'AC Fille</i>	15
2.1.11. <i>Obligations des Utilisateurs de certificats</i>	15
2.1.11.1. <i>Utilisation des certificats à des fins pertinentes</i>	15
2.1.11.2. <i>Responsabilités en matière de vérification</i>	15
2.1.11.3. <i>Obligation de la vérification du statut des certificats</i>	15
2.2. RESPONSABILITES	15
2.2.1. <i>Limites de la responsabilité</i>	16
2.2.2. <i>Force majeure</i>	16
2.3. INTERPRETATION ET MISE EN APPLICATION	16
2.3.1. <i>Droit applicable</i>	16
2.3.2. <i>Intégralité, divisibilité, survie, avis</i>	16
2.3.3. <i>Règlement des différends</i>	16
2.3.4. <i>Permanence de la Politique de Certification</i>	17
2.4. TARIFS	17
2.4.1. <i>Frais d'émission et de renouvellement des Certificats</i>	17
2.4.2. <i>Frais d'accès au certificat</i>	17
2.4.3. <i>Frais de vérification de validité des certificats</i>	17
2.4.4. <i>Frais pour d'autres services</i>	17

**AC Certigrefre Classe 3Plus  
Procès-verbal d'initialisation de l'AC**

2.4.5.	<i>Politique de remboursement</i>	17
2.5.	PUBLICATION ET SERVICES ASSOCIES	17
2.5.1.	<i>Informations publiées</i>	17
2.5.2.	<i>Fréquence de publication</i>	17
2.5.3.	<i>Contrôles de l'accès</i>	18
2.6.	AUDIT DE CONFORMITE	18
2.6.1.	<i>Fréquence d'audit de conformité des entités</i>	18
2.6.2.	<i>Identité / qualité de l'auditeur</i>	18
2.6.3.	<i>Lien entre l'auditeur et la fonction vérifiée</i>	18
2.6.4.	<i>Objet de l'audit</i>	18
2.7.	CONFIDENTIALITE DES DONNEES A CARACTERE PERSONNEL ET DES INFORMATIONS	18
2.7.1.	<i>Types d'informations considérées comme confidentielles</i>	19
2.7.1.1.	<i>Données à caractère personnel</i>	19
2.7.1.2.	<i>Autres informations</i>	19
2.7.1.3.	<i>Types d'informations considérées comme non confidentielles</i>	19
2.7.1.4.	<i>Divulgence des causes de révocation / suspension de certificat</i>	19
2.8.	DROITS RELATIFS A LA PROPRIETE INTELLECTUELLE	19
<b>3.</b>	<b>IDENTIFICATION ET AUTHENTIFICATION</b>	<b>21</b>
3.1.	ENREGISTREMENT INITIAL	21
3.1.1.	<i>Conventions de noms</i>	21
3.1.2.	<i>Nécessité d'utilisation de noms explicites</i>	21
3.1.3.	<i>Règles d'interprétation des différentes formes de noms</i>	21
3.1.4.	<i>Unicité des noms</i>	21
3.1.5.	<i>Procédure de résolution de litige sur la déclaration de nom</i>	21
3.1.6.	<i>Reconnaissance, authentification et rôle des noms de marques de fabrique, de commerce et de services</i>	21
3.1.7.	<i>Preuve de possession d'une clé privée</i>	22
3.1.8.	<i>Vérification de l'identité de l'organisation</i>	22
3.1.9.	<i>Vérification de l'identité des Abonnés</i>	22
3.2.	RE-GENERATION DE CLES (HORS REVOCATION)	22
3.3.	RE-GENERATION DE CLES APRES REVOCATION	22
3.4.	DEMANDE DE REVOCATION	22
<b>4.</b>	<b>EXIGENCES OPERATIONNELLES</b>	<b>24</b>
4.1.	DEMANDE DE CERTIFICAT	24
4.1.1.	<i>Origine de la demande.</i>	24
4.1.2.	<i>Informations à fournir.</i>	24
4.1.3.	<i>Dossiers de demande de certificats.</i>	24
4.1.4.	<i>Archivage des dossiers.</i>	24
4.1.5.	<i>Opérations à effectuer.</i>	24
4.2.	EMISSION DU CERTIFICAT	25
4.3.	ACCEPTATION DU CERTIFICAT	25
4.4.	SUSPENSION ET REVOCATION DE CERTIFICAT	25
4.4.1.	<i>Causes possibles de révocation</i>	25
4.4.2.	<i>Personnes pouvant demander une révocation</i>	25
4.4.3.	<i>Procédure de demande de révocation</i>	25
4.4.4.	<i>Temps de traitement d'une demande de révocation</i>	26
4.4.5.	<i>Causes possibles de suspension</i>	26
4.4.6.	<i>Personne pouvant demander une suspension</i>	26
4.4.7.	<i>Procédure de demande de suspension</i>	26
4.4.8.	<i>Limites de la période de suspension</i>	26
4.4.9.	<i>Publication des causes de révocation</i>	26
4.4.10.	<i>Exigences de vérification en ligne de la révocation</i>	26
4.4.11.	<i>Autres formes de publication des avis de révocation</i>	26
4.5.	JOURNALISATION D'EVENEMENTS	27
4.5.1.	<i>Types d'événements enregistrés</i>	27
4.5.2.	<i>Fréquence des traitements de journalisation</i>	27

**AC Certigreffe Classe 3Plus  
Procès-verbal d'initialisation de l'AC**

4.5.3.	<i>Durée de conservation des journaux d'événements</i>	27
4.5.4.	<i>Protection d'un journal d'événements</i>	28
4.5.5.	<i>Procédures de sauvegarde des journaux d'événements</i>	28
4.5.6.	<i>Système de collecte des journaux (interne ou externe)</i>	28
4.5.7.	<i>Imputabilité des événements</i>	28
4.5.8.	<i>Analyse des vulnérabilités</i>	28
4.6.	ARCHIVAGE DES DOSSIERS	28
4.6.1.	<i>Types de données à archiver</i>	28
4.6.2.	<i>Période de rétention des archives</i>	29
4.6.3.	<i>Protection des archives</i>	29
4.6.4.	<i>Besoins d'horodatage des enregistrements</i>	29
4.6.5.	<i>Procédures de récupération des archives</i>	29
4.7.	RECUPERATION EN CAS DE DESASTRE OU DE COMPROMISSION	29
4.7.1.	<i>Corruption des ressources informatiques, des logiciels et (ou) des données</i>	29
4.7.2.	<i>Compromission de la clé de signature de l'AC Racine</i>	29
4.8.	CESSATION D'ACTIVITE	29
<b>5.</b>	<b>CONTROLE DE SECURITE PHYSIQUE, CONTROLE DES PROCEDURES,</b>	
	<b>CONTROLE DU PERSONNEL</b>	<b>30</b>
5.1.	CONTROLES PHYSIQUES	30
5.1.1.	<i>Environnement physique</i>	30
5.1.2.	<i>Accès physique</i>	30
5.1.3.	<i>Energie et air conditionné</i>	30
5.1.4.	<i>Exposition aux liquides</i>	30
5.1.5.	<i>Prévention et protection incendie</i>	30
5.1.6.	<i>Conservation des médias</i>	30
5.1.7.	<i>Destruction des déchets</i>	30
5.2.	CONTROLES DES PROCEDURES	30
5.2.1.	<i>Rôles de confiance</i>	30
5.2.2.	<i>Nombre de personnes nécessaires à chaque tâche</i>	31
5.2.3.	<i>Identification et authentification des rôles</i>	31
5.3.	CONTROLES DU PERSONNEL	31
5.3.1.	<i>Qualifications, exigences d'habilitations</i>	31
5.3.2.	<i>Exigences de formation</i>	31
5.3.3.	<i>Sanctions pour des actions non autorisées</i>	31
5.3.4.	<i>Documentation fournie au personnel</i>	32
<b>6.</b>	<b>CONTROLES TECHNIQUES DE SECURITE</b>	<b>33</b>
6.1.	GENERATION ET INSTALLATION DE BI-CLE	33
6.1.1.	<i>Génération de bi-clé</i>	33
6.1.2.	<i>Transmission de la clé privée de confidentialité</i>	33
6.1.3.	<i>Transmission de la clé publique à l'AC</i>	33
6.1.4.	<i>Fourniture de la clé publique de validation de l'AC aux Utilisateurs</i>	33
6.1.5.	<i>Tailles de clés</i>	33
6.1.6.	<i>Paramètres de génération de clé</i>	33
6.1.7.	<i>Contrôle de qualité des paramètres de clés</i>	33
6.1.8.	<i>Mode de génération de clé</i>	34
6.1.9.	<i>Usage de la clé publique</i>	34
6.1.9.1.	<i>Clé publique de vérification (de signature)</i>	34
6.1.9.2.	<i>Clé publique de confidentialité</i>	34
6.2.	PROTECTION DE LA CLE PRIVEE	34
6.2.1.	<i>Normes pour les modules cryptographiques</i>	34
6.2.2.	<i>Contrôle de clé privée par plusieurs personnes</i>	34
6.2.3.	<i>Récupération de clé privée</i>	34
6.2.4.	<i>Sauvegarde de clé privée</i>	34
6.2.5.	<i>Archive de clé privée</i>	35
6.2.6.	<i>Méthode d'activation de clé privée</i>	35
6.2.7.	<i>Méthode de destruction de clé privée</i>	35

**AC Certigreffe Classe 3Plus  
Procès-verbal d'initialisation de l'AC**

6.3.	AUTRES ASPECTS DE LA GESTION DES BI-CLES	35
6.3.1.	<i>Archive des clés publiques</i>	35
6.3.2.	<i>Durée de vie des clés publiques et privées</i>	35
6.4.	DONNEES D'ACTIVATION	35
6.4.1.	<i>Génération et installation des données d'activation</i>	35
6.4.2.	<i>Protection des données d'activation</i>	35
6.5.	CONTROLES DE SECURITE DES POSTES DE TRAVAIL	35
6.5.1.	<i>Besoins de sécurité spécifiques sur les postes de travail</i>	35
6.6.	CONTROLES TECHNIQUES DU SYSTEME DURANT SON CYCLE DE VIE	36
6.6.1.	<i>Contrôles des développements des systèmes</i>	36
6.6.2.	<i>Contrôles de la gestion de la sécurité</i>	36
6.7.	CONTROLES DE LA SECURITE RESEAU	36
6.8.	CONTROLES DE LA GESTION DES MODULES CRYPTOGRAPHIQUES	36
<b>7.</b>	<b>PROFILS DE CERTIFICATS ET DE LCR</b>	<b>37</b>
7.1.	PROFIL DES CERTIFICATS	37
7.1.1.	<i>Champs de base</i>	37
7.1.2.	<i>Extensions des certificats</i>	37
7.1.2.1.	AuthorityKeyIdentifier	37
7.1.2.2.	SubjectKeyIdentifier	38
7.1.2.3.	KeyUsage	38
7.1.2.4.	CertificatePolicies	38
7.1.2.5.	basicConstraints	38
7.1.2.6.	cRLDistributionPoints.	38
7.1.3.	<i>Interprétation sémantique des champs critiques de la PC</i>	38
7.2.	PROFIL DE LCR	39
7.2.1.	<i>Champs de base</i>	39
7.2.2.	<i>Extensions des LCR et des entrées des LCR</i>	39
7.2.2.1.	AuthorityKeyIdentifier	39
<b>8.</b>	<b>ADMINISTRATION DES SPECIFICATIONS</b>	<b>40</b>
8.1.	PROCEDURES DE MODIFICATION DE LA PC	40
8.1.1.	<i>Articles pouvant être modifiés sans avis</i>	40
8.1.2.	<i>Articles dont la modification nécessite la formulation d'une nouvelle politique</i>	40
8.1.3.	<i>Changement avec avis</i>	40
8.1.4.	<i>Délai de préavis</i>	40
8.2.	PROCEDURES DE PUBLICATION ET DE NOTIFICATION	40
8.3.	PROCEDURES D'APPROBATION DE LA PC	41
<b>9.</b>	<b>ANNEXE 1 : DOCUMENTS DE RÉFÉRENCE</b>	<b>42</b>
<b>10.</b>	<b>ANNEXE 2: TEXTES LÉGISLATIFS ET RÉGLEMENTAIRES</b>	<b>43</b>
10.1.	CADRE GENERAL	43
10.2.	REGIME "DECLARATION - AUTORISATION"	43

## 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 œuvre 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).

### 1.1. PRESENTATION GENERALE

#### 1.1.1. APERÇU GENERAL

CERTEUROPE, Opérateur de Confiance et de Services de Certification, a pour vocation d'héberger et d'exploiter des ICP pour le compte d'autrui,

**AC Certigrefre Classe 3Plus  
Procès-verbal d'initialisation de l'AC**

notamment pour des professions réglementées telles que Greffiers des Tribunaux de Commerce, Experts-comptables.  
Au titre de ses services, CERTEUROPE offre la possibilité de certifier les clés de signature des Autorités de Certification clientes par son Autorité de Certification Racine CERTEUROPE. Cette possibilité offre :  
d'une part, la mutualisation d'une seule Autorité de Certification Racine entre les différentes AC,  
d'autre part, un vecteur de reconnaissance mutuelle de certificats d'abonné émis par les différentes AC hébergées.  
La Politique de Certification définie dans le présent document décrit les obligations des parties prenantes dans le cadre du service de certification des clés de signatures d'AC.

**1.1.2. APERÇU DE LA POLITIQUE**

En vertu de la présente politique, les certificats ne seront délivrés qu'aux AC. La délivrance de certificats pour le compte d'abonné personne physique ou morale est exclue.  
L'AC Racine CERTEUROPE sera assujettie aux lois et règlements en vigueur sur le territoire de la République française, 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.  
L'AC Racine CERTEUROPE se réserve le droit de conclure des accords de certification croisée avec une ou des autorités de certification tierces. La présente Politique de Certification s'applique à la délivrance et l'utilisation de certificats de type Autorité de Certification  
Cette politique a été conçue pour être utilisée dans certaines situations, et indique les rôles et responsabilités spécifiques de l'AC Racine qui délivre ce type de certificat de l'autorité d'enregistrement..  
des AC filles  
CERTEUROPE décline toute responsabilité concernant l'utilisation de ces certificats pour tout usage autre que ceux qui 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 CERTEUROPE 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 du responsable de l'AC fille. L'identification se fera de la manière décrite dans cette politique.  
Aucun renseignement personnel recueilli par AC Racine CERTEUROPE ne sera divulgué sans le consentement du responsable de l'AC fille, à moins que la loi ne le prescrive.  
L'AC Racine CERTEUROPE garantit, au titre de la PC, le lien qui existe entre l'AC fille et son bi-clé

**1.2. DEFINITIONS**

**1.2.1. LISTE DES ACRONYMES**

AC	Autorité de Certification
AE	Autorité d'Enregistrement
C	Country (Pays)

**AC Certigreffe Classe 3Plus  
Procès-verbal d'initialisation de l'AC**

CISSI	Commission Interministérielle pour la Sécurité des Systèmes d'information
CN	Common Name
DN	Distinguished Name
DPC	Déclaration relative aux Pratiques de Certification
ICP	Infrastructure à Clé Publique
LCR	Liste des Certificats Révoqués
O	Organisation
OID	Object Identifier
OSC	Opérateur de Service de Certification
PC	Politique de Certification
PC2	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

**1.2.2. DEFINITIONS**

**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.

Dans la présente PC deux AC interviennent : l'AC racine qui délivre des certificats, l'AC fille qui reçoit de l'AC racine un certificat.

**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.

**Common Name (CN)** : identité réelle ou pseudonyme de l'AC fille 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 oeuvre 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'AC fille pour lequel le certificat est émis.



**AC Certigreffe Classe 3Plus**  
**Procès-verbal d'initialisation de l'AC**

**Données d'activation** : données privées associées à une AC permettant de mettre en oeuvre sa clé privée.

**Enregistrement (d'une AC fille)** : opération qui consiste pour l'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.

**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 l'AC racine et qui consiste à signer un proto-certificat émis par l'AC fille pour le transformer en certificat.

**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.

**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).

**Renouvellement (d'un certificat)** : opération effectuée à la demande d'une AC fille et qui consiste à générer un nouveau certificat pour l'AC fille sans régénérer de bi-clé.

**Révocation (d'un certificat)** : opération demandée par l'AC fille ou l'AE racine, et dont le résultat est la suppression de la caution de l'AC racine sur le certificat de l'AC fille, 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 des AC filles générées par l'AC racine, 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.

**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.

**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.

### 1.3. IDENTIFICATION (OID)

La présente Politique de Certification est enregistrée conformément à la norme d'enregistrement ISO par un identificateur numérique unique. Cet OID se rattache à l'identificateur unique de la société Certeuropa auteur du document. La désignation de l'identification objet (OID) pour la présente politique est :

#### 1.2.250.1.105.1.1

dont les champs sont définis comme suit :{iso(1) member-body(2) fr(250) type-org(1) certeuropa(105) pki-root(1) certificate-policy(1)}.

### 1.4. APPLICATIONS ET GROUPES D'UTILISATEURS CONCERNES

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

- AC racine
- Autorité d'Enregistrement racine
- AC fille
- Utilisateurs de certificats.

#### 1.4.1. AUTORITE DE CERTIFICATION RACINE

L'Autorité de Certification Racine 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 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, L'AC Racine CERTEUROPE est chargée:

- de créer et de signer des certificats liant les AC filles et leurs bi-clés
- de faire connaître l'état des certificats par l'intermédiaire des LCR
- de faire respecter la PC et la DPC par les différentes composantes de l'ACR, et les AC filles

La fonction d'enregistrement des certificats fait partie des fonctions indispensables d'une ICP.

La fonction d'enregistrement est assurée par l'Autorité d'Enregistrement.

#### 1.4.2. AUTORITE D'ENREGISTREMENT (AE)

L'Autorité d'Enregistrement est le lien entre l'Autorité de Certification racine et l'AC fille . En vertu de cette Politique de Certification, une AE est responsable de toutes les tâches qui lui sont assignées par l'AC. L'AE applique des procédures d'identification des personnes physiques et morales responsables de la composante AC fille à certifier, conformément aux règles définies par l'Autorité de Certification. Son but est :

- d'établir l'identité du demandeur,
- de distribuer le certificat au responsable de l'AC fille,
- de gérer et protéger les données personnelles et de sécurité des AC filles,
- 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'AE archive les dossiers de demande de certificat ou de révocation.  
Les fonctions de l'AE sont exécutées par des personnels désignés et agréés par le responsable de l'AC racine ; ces personnels ont connaissance et respectent les règles, principes et procédures énoncées dans la PC et la DPC.

**1.4.3. AUTORITE DE CERTIFICATION FILLE.**

En vertu de cette Politique de Certification, une AC Fille est une personne morale qui obtient un certificat d'AC des services de l'AC Racine CERTEUROPE.

L'AC fille 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 le ou les systèmes informatiques utilisés pour mettre en oeuvre le ou les certificats générés par l'AC ainsi que la ou les clés privées associées.
- de la protection, de l'intégrité et de la confidentialité de la clé privée de l'AC Fille, et des éventuelles données d'activations,
- 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.

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

**1.4.4. PARTIES UTILISATRICES**

En vertu de cette politique de certification, les Utilisateurs de certificats d'AC émis par l'AC racine sont les personnes ou organisations qui doivent vérifier la validité d'un certificat d'abonné émis par une AC fille

**1.5. ANNUAIRES**

La LCR de l'AC racine se présente sous la forme d'une entrée d'annuaire conforme aux normes X.500 et LDAP.

**2. DISPOSITIONS DE PORTÉE GÉNÉRALE**

**2.1. OBLIGATIONS**

**2.1.1. OBLIGATIONS COMMUNES A 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. Ces obligations 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
- respecter et appliquer leurs PC et DPC,
- se soumettre aux contrôles de conformité effectués par l'auditeur de CERTEUROPE, en respecter les conclusions et remédier aux non-conformités qu'ils révéleraient,
- respecter les accords ou contrats qui les lient entre elles,
- documenter les 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.

**AC Certigrefe Classe 3Plus  
Procès-verbal d'initialisation de l'AC**

Les membres du personnel de l'AC Racine CERTEUROPE, et les opérateurs mandatés, sont être personnellement responsables de leurs actes. L'expression « personnellement responsable » signifie que l'on puisse imputer une action à une personne.

**2.1.2. OBLIGATIONS DE L'AC RACINE**

L'AC racine doit :

- montrer qu'elle utilise une PC ;
- pouvoir démontrer, qu'elle a émis un certificat pour une AC Fille donnée et que le responsable de l'AC Fille a accepté le certificat ;
- tenir à disposition des Utilisateurs de certificats la notification de révocation du certificat d'une composante de l'AC Racine CERTEUROPE ou d'une AC Fille.
- prendre toutes les mesures raisonnables pour s'assurer que les responsables des AC Filles sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés et des certificats. La relation entre une AC Fille et l'AC Racine CERTEUROPE est formalisée par un contrat précisant les droits et obligations des parties et notamment les garanties apportées par l'AC Racine CERTEUROPE;

**2.1.3. GESTION DES SUPPORTS ET DONNEES D'ACTIVATION.**

Les éléments secrets d'une AC Fille 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.
- Etre protégé contre toute attaque physique ou logique, conformément à l'état de l'art du moment en la matière.

**2.1.4. EXACTITUDE DES INFORMATIONS**

Lorsque l'AC Racine génère un certificat, elle garantit qu'elle a délivré le certificat à une AC Fille et que les informations contenues dans le certificat en question ont été vérifiées conformément à la présente PC. L'AC Racine veille à ce que l'Autorité d'Enregistrement se conforme à toutes les modalités pertinentes de la présente Politique de Certification.

**2.1.5. DELAI ENTRE LA DEMANDE ET L'EMISSION DU CERTIFICAT**

Le certificat de l'AC Fille est émis dès réception de la demande lors de la cérémonie des clés de l'AC Fille.

Dans le cas d'une demande de révocation du certificat AC Fille, l'AE doit effectuer des vérifications avant d'accepter la révocation et d'introduire le certificat en cause dans la LCR. Ces procédures sont précisées au chapitre 4.4

L'AC Racine s'assure que toutes les procédures relatives à l'expiration, à la révocation et au renouvellement d'un certificat sont conformes aux dispositions de la présente PC et qu'elles ont été mentionnées à l'AC Fille, ou consignées dans tout autre document applicable décrivant les modalités d'utilisation du certificat.

**2.1.6. PROTECTION DES CLES PRIVEES**

L'AC s'engage à protéger et garantir l'intégrité et la confidentialité de sa clé privée ainsi que des données d'activation associées. Cette clé privée fait l'objet d'une sauvegarde sécurisée.

**2.1.7. RESTRICTION QUANT A L'UTILISATION DES CLES PRIVEES DE L'AC RACINE**

L'AC Racine 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 PC.

**2.1.8. FONCTION DE SEQUESTRE.**

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

**2.1.9. OBLIGATIONS D'UNE AE**

**2.1.9.1. Avis de génération et de révocation de certificats**

Une AE doit se conformer à toutes les exigences de la présente PC et de la DPC associée.

En outre, une AE doit :

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

**2.1.9.2. Exactitude des informations**

L'AE doit vérifier l'authenticité des pièces justificatives et l'exactitude des mentions qui établissent l'identité de l'AC Fille selon les procédures décrites au chapitre 4.1.

**2.1.9.3. 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 les données d'activation associées conformément au chapitre 6.4.2 du présent document.

**2.1.9.4. 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 PC.

**2.1.10. OBLIGATIONS DE L'AC FILLE**

**2.1.10.1. Conformité à la PC**

L'AC Fille doit se conformer à toutes les exigences de la présente PC la concernant.

L'AC Fille doit établir et faire respecter la présente PC sur les systèmes informatiques utilisés pour mettre en œuvre le certificat généré et la clé privée associée.

La relation entre l'AC Fille et l'AC Racine est formalisée par un engagement de l'AC Fille visant à certifier l'exactitude des renseignements et des documents fournis à l'AC Racine.

**2.1.10.2. Propriété**

En aucun cas l'AC Fille n'acquiert la propriété du certificat émis par l'AC Racine, il n'en acquiert que le droit d'usage. Tous les certificats demeurent la propriété de l'AC Racine qui les a émis.

**2.1.10.3. Exactitude des informations**

L'AC Fille a l'obligation contractuelle de communiquer des informations exactes lors de sa demande de certificat. Elle doit également notifier, au travers de l'AE, toute modification des informations fournies lors de la demande de certificat.

**2.1.10.4. Protection des clés privées de l'AC Fille**

L'AC Fille doit

- protéger en confidentialité et en intégrité sa clé privée et les données d'activation associées par des moyens appropriés à son environnement, conformément au chapitre 6.4.2,
- notamment en ce qui concerne l'initialisation des données d'activation; elle doit prendre toutes les mesures raisonnables pour en éviter la perte, la divulgation, la compromission, la modification ou l'utilisation non autorisée,
- informer dans les plus brefs délais l'AC Racine, en cas de compromission, ou de soupçon de compromission, de sa clé privée, selon les instructions prévues au chapitre 4.4,

- informer dans les plus brefs délais l'AC Racine, en cas de perte des données d'activation..

**2.1.11. OBLIGATIONS DES UTILISATEURS DE CERTIFICATS**

**2.1.11.1. Utilisation des certificats à des fins pertinentes**

Les Utilisateurs de certificats doivent respecter l'usage pour lequel le certificat a été émis lorsque cet usage est déclaré critique.

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.

**2.1.11.2. Responsabilités en matière de vérification**

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, et la validité de tout certificat sur l'itinéraire de confiance.

**2.1.11.3. Obligation de la vérification du statut des certificats**

Avant toute utilisation de certificats, notamment lorsque lesdits certificats créent des effets juridiques, l'Utilisateur doit vérifier la validité des certificats des différents AC de l'itinéraire de confiance en consultant les LCR appropriées. A défaut de remplir cette obligation, l'Utilisateur assume seul tous les risques de ses actions non conformes aux exigences de la présente politique, l'AC Racine ne garantissant aucune valeur juridique aux certificats qu'elle a émis et qui pourraient avoir été révoqués.

**2.2. RESPONSABILITES**

La responsabilité de l'un quelconque des intervenants dans la certification d'une AC et toute opération qui s'y rattache 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. Par conséquent, la responsabilité de l'AC ou du personnel de l'AC est dérogée dans la mesure où elle est capable de prouver n'avoir commis aucune négligence. 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.

**2.2.1. LIMITES DE LA RESPONSABILITE**

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, les documents contractuels ou la réglementation en vigueur.

Si la responsabilité de l'AC est établie, les conséquences financières de cette responsabilité n'excéderont pas les montants suivants : 30000 euros

**2.2.2. 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 PC 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 toute autre convention liant les parties.

**2.3. INTERPRETATION ET MISE EN APPLICATION**

**2.3.1. 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.

**2.3.2. INTEGRALITE, DIVISIBILITE, SURVIE, AVIS**

Sans objet dans le cadre de la présente PC.

**2.3.3. REGLEMENT DES DIFFERENDS**

En cas de litige relatif à l'émission d'un Certificat dans le cadre de la présente PC, la partie concernée adressera une notification à CERTEUROPE. CERTEUROPE et la partie concernée rechercheront une résolution amiable au litige dans un délai de quinze jours.

En l'absence de solution amiable à l'issue de cette période 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 chacun 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, cosigné par les parties, transactionnel et confidentiel, en cas de conciliation.
- soit par un procès verbal de non-conciliation cosigné par les parties.

En cas de litige qui ne trouverait pas de solution acceptable par les parties concernées 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.

**2.3.4. 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.

**2.4. TARIFS**

**2.4.1. FRAIS D'EMISSION 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.

**2.4.2. FRAIS D'ACCES AU CERTIFICAT**

Aucun frais ne sera facturé pour l'accès aux certificats de l'AC Racine ni des AC Filles.

**2.4.3. FRAIS DE VERIFICATION DE VALIDITE DES CERTIFICATS**

Des frais de vérification de validité des certificats peuvent être facturés par l'AC. Dans ce cas, les tarifs seront portés à la connaissance des Intervenants auxquels ils s'appliquent sous forme de publication électronique ou seront disponibles auprès de l'AC. Le statut des certificats est disponible gratuitement sous la forme de LCR.

**2.4.4. FRAIS POUR D'AUTRES SERVICES**

Aucun frais ne sera facturé pour l'accès à cette PC via le site Web de Certurope.

Tout autre accès à cette PC (copie papier, envoi par messagerie électronique) pourra faire l'objet d'une facturation.

**2.4.5. POLITIQUE DE REMBOURSEMENT**

Aucun remboursement ne sera effectué par l'AC.

**2.5. PUBLICATION ET SERVICES ASSOCIES**

**2.5.1. INFORMATIONS PUBLIEES**

Le service de publication fournit au minimum les informations suivantes, sachant que le moyen utilisé pour leur publication est libre :

- La Politique de Certification,
- la liste de certificats révoqués (LCR),
- Le certificat de l'AC Racine CERTEUROPE.

**2.5.2. FREQUENCE 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'AC Fille, l'événement déclencheur est l'acceptation, après vérifications, de la demande de révocation.
- dans le cas d'une révocation décidée par l'AC Racine l'événement déclencheur est la prise de décision par l'AC Racine CERTEUROPE.

L'AC doit également s'assurer de la publication d'informations (notamment la PC) ayant fait l'objet d'une révision.

**2.5.3. CONTROLES DE L'ACCES**

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.

**2.6. AUDIT DE CONFORMITE**

L'AC a la responsabilité du bon fonctionnement de ses composantes, 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'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.

**2.6.1. FREQUENCE D'AUDIT DE CONFORMITE DES ENTITES**

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.

**2.6.2. IDENTITE / QUALITE DE L'AUDITEUR**



CERTEUROPE peut déléguer les opérations de contrôle de conformité à une entité d'audit.

Cet auditeur doit pouvoir apporter la preuve de son expérience dans les ICP et technologies de cryptographie.

**2.6.3. LIEN ENTRE L'AUDITEUR ET LA FONCTION VERIFIEE**

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

**2.6.4. OBJET DE L'AUDIT**

Si l'audit de l'AC Racine se révèle nécessaire pour mener à bien les opérations de référencement des certificats d'une AC Fille, l'AC Fille et l'AC Racine CERTEUROPE détermineront les conditions et l'étendue des vérifications.

**2.7. CONFIDENTIALITE DES DONNEES A CARACTERE 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.

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.

**2.7.1. TYPES D'INFORMATIONS CONSIDEREES COMME CONFIDENTIELLES**

**2.7.1.1. 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 événements 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 sont considérés comme étant confidentiels, sauf :

- 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).

**2.7.1.2. Autres informations**

Les informations suivantes sont considérées comme confidentielles:

- les clés privées des entités propriétaires de certificats d'AC Filles,
- les données d'activation,
- les journaux d'événements des composantes de l'AC racine,

La clé privée de signature numérique ainsi que les données d'activation correspondantes, doivent demeurer confidentielles.

**AC Certigreffe Classe 3Plus  
Procès-verbal d'initialisation de l'AC**

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.

**2.7.1.3. Types d'informations considérées comme non confidentielles**

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

**2.7.1.4. Divulgation des causes de révocation / suspension de certificat**

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

- l'AE,
- au représentant légal de l'AC Fille
- à toute entité juridique dûment mandatée par les pouvoirs publics.

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.

**2.8. DROITS RELATIFS A LA PROPRIETE 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 1<sup>er</sup> 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 AC Serveur émis dans le cadre de la présente Politique de Certification seront décrits selon la norme ISO/IEC 9594 (Distinguished Names).

Un certificat AC Serveur émis dans le cadre de l'ICP ICP Racine CERTEUROPE doit contenir dans le champ **subject** : un Distinguished Name, nom distinctif facile à distinguer et obligatoire.

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. NECESSITE D'UTILISATION DE NOMS EXPLICITES**

Le nom distinctif (DN) X.501, porté dans le champ Subject du certificat AC Fille, doit être, non seulement facile à distinguer des autres noms, mais aussi unique.

Un nom distinctif (DN) d'AC Serveur doit se composer au moins des éléments :

- Nom de pays (C = FR).
- Nom d'organisation (O) : ce champ doit contenir le n°SIREN de l'AC Fille.
- Unité d'organisation (OU) : ce champ doit contenir la raison sociale de l'AC Fille.
- Nom usuel (CN) : ce champ doit contenir le nom distinctif de l'AC Serveur.

**3.1.3. REGLES D'INTERPRETATION DES DIFFERENTES FORMES DE NOMS**

Aucune exigence n'est stipulée.

**3.1.4. UNICITE DES NOMS**

L'unicité d'un certificat d'AC Serveur est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC Racine. Cependant, les noms distinctifs doivent être uniques au sein de l'ICP Racine CERTEUROPE.

L'unicité des noms est obtenue suivant les règles décrites au §3.1.2 de ce chapitre.

**3.1.5. PROCEDURE DE RESOLUTION DE LITIGE SUR LA DECLARATION DE NOM**

Une partie qui demande un certificat AC Fille 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 §3.1.4 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.

**3.1.6. RECONNAISSANCE, AUTHENTIFICATION ET ROLE 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 1<sup>er</sup> 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'AC Racine Certeuropé limite ses vérifications concernant le droit d'utiliser un nom à la consultation du Registre du Commerce et des Sociétés.

CERTEUROPE 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 CLE PRIVEE**

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. VERIFICATION DE L'IDENTITE 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 Racine Certeuropé 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 . celle-ci doit apporter la preuve de son existence, la preuve de l'identité de son représentant légal et le cas échéant la chaîne des mandats conférant leur pouvoir aux mandataires de sécurité. L'AC ou l'AE doit archiver toutes les informations pertinentes relatives à cet enregistrement. La DPC précisera les documents à fournir et les procédures d'enregistrement mise en œuvre par l'AE. L'AE limitera ses vérifications à la consultation du Registre du Commerce et des Sociétés.

### **3.1.9. VERIFICATION DE L'IDENTITE DES ABONNES**

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

Pour toute demande de certificat AC Fille faite au titre de l'appartenance à une organisation, il faut que ladite demande soit confirmée par écrit par le représentant légal de cette même organisation.

Le dossier doit comprendre les éléments listés au chapitre 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 AC Filles par l'AE doit se faire directement au 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.

### **3.2. RE-GENERATION DE CLES (HORS REVOCATION)**

Les bi-clés doivent être périodiquement renouvelés afin de minimiser les attaques cryptographiques. A cette occasion, l'AE doit vérifier à nouveau l'identité du responsable de l'AC Fille. Les bi-clés de signature des AC Serveur sont à renouveler au moins tous les douze ans.

Pour faciliter l'exploitation, un nouveau certificat peut être obtenu alors que le certificat courant est encore valide.

### **3.3. RE-GENERATION DE CLES APRES REVOCATION**

Si un certificat a été révoqué, il ne peut être réactivé. Il ne peut également jamais faire l'objet d'un renouvellement.

### **3.4. DEMANDE DE REVOCATION**

L'AC doit établir et rendre public la procédure le mécanisme qu'elle utilise pour traiter les demandes de révocation et en établir la validité.

L'AC 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 CERTEUROPE, 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 et doit être authentifiée par l'AE ou l'AC CERTEUROPEAC Racine CERTEUROPE.

Dans le cas où un certificat AC Serveur se doit d'être révoqué (voir chapitreXXXXXX 4.4), le responsable de l'AC Serveur doit informer au plus vite l'AC Racine CERTEUROPE.

## **4. EXIGENCES OPERATIONNELLES**

Les certificats des AC Filles sont délivrées avec une vérification en face à face de l'identité du représentant légal., et de sa détention de la clé privée.

### **4.1. DEMANDE DE CERTIFICAT**

L'AE doit s'assurer que les demandeurs de certificats AC Serveur suivent et respectent les procédures et exigences publiées par l'AC.

**AC Certigrefre Classe 3Plus  
Procès-verbal d'initialisation de l'AC**

Chaque demande de certificat doit être accompagnée des pièces suivantes :

- Pièce d'identité du demandeur.
- Preuve de ses pouvoirs pour les attributs demandés.
- Le contrat client.

**4.1.1. ORIGINE DE LA DEMANDE.**

Un certificat est demandé par le représentant légal de l'AC Fille.

**4.1.2. INFORMATIONS A FOURNIR.**

Les informations suivantes doivent au moins figurer dans la demande de certificat AC Fille :

- une demande écrite, sur papier à entête portant le numéro SIREN de l'Abonné, signée par le représentant légal
- une déclaration de l'Abonné ( le responsable de l'AC Fille) , portant l'acceptation de ses engagements.
- une adresse postale de l'Abonné.
- le nom du responsable du Certificat d'AC Serveur,
- deux justificatifs d'identité de la personne physique mandatée sous la forme de copies
- la clé publique de l'AC Fille à certifier
- les données d'identification de l'organisation (DN X509),

**4.1.3. DOSSIERS DE DEMANDE DE CERTIFICATS.**

L'AE n'acceptera que les demandes de certificat d'AC Serveur qui seront appuyées par des dossiers constitués de pièces justificatives fiables tels que décrits ci dessus

**4.1.4. ARCHIVAGE DES DOSSIERS.**

Tout dossier de demande de certificat doit être archivé par l'AE pendant la durée d'opposabilité des documents.

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 de l'organisation ou de l'entreprise désignées responsables d'un certificat d'AC Fille émis par l'AC Racine Certurope.

**4.1.5. OPERATIONS A EFFECTUER.**

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

établir l'identité du demandeur, en vérifiant les pièces justificatives présentées par le représentant légal de l'Abonné  
s'assurer que le demandeur a pris connaissance des modalités applicables pour l'utilisation du certificat d'AC Fille. 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,  
obtenir la clé publique de l'AC Fille, et s'assurer que le demandeur détient bien la clé privée correspondante

**4.2. EMISSION DU CERTIFICAT**

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

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

L'AC doit s'assurer que la demande a bien été prise en compte et traitée par l'AE, et fournit une trace imputable de son avis,

L'AC doit générer le certificat,

L'AC 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'AC doit mettre le certificat à disposition de l'Abonné, c'est à dire rendre accessible par des moyens physiques 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'AC Racine.

#### **4.4. SUSPENSION ET REVOCATION DE CERTIFICAT**

##### **4.4.1. CAUSES POSSIBLES DE REVOCATION**

Lorsque la confiance dans un certificat (certificat d'AC Fille ou d'une composante de l'ICP CERTEUROPE) 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 :

- suspicion de compromission, compromission, perte ou vol de la clé privée ou des données d'activation,
- modification d'une information contenue 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 AC Fille.

Outre les cas de révocation de certificats mentionnés plus haut, l'AC Racine CERTEUROPE doit révoquer un certificat dès lors qu'elle est en possession d'informations de nature à indiquer une perte de confiance dans un certificat.

Plus généralement, l'AC Racine CERTEUROPE peut à sa discrétion, révoquer le certificat AC Serveur d'une entité identifiée lorsqu'elle ne respecte pas les obligations énoncées dans la présente PC et dans tous documents contractuels ainsi que dans toute loi et règlement applicable.

##### **4.4.2. PERSONNES POUVANT DEMANDER UNE REVOCATION**

Seuls peuvent demander la révocation d'un certificat d'AC Fille

- le responsable du certificat AC Fille,
- le représentant légal de l'AC Fille,
- l'AC Racine.

##### **4.4.3. PROCEDURE DE DEMANDE DE REVOCATION**

Dans le cas où son certificat se doit d'être révoqué (voir chapitre 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 Racine,
- soit selon la même procédure que pour l'enregistrement initial (cf. §4.1), c'est-à-dire par une procédure en face à face avec l'Abonné.

La demande de révocation doit contenir explicitement les informations d'identification de l'Abonné et de son certificat d'AC Fille.

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 demande comporte toutes les informations nécessaires à l'authentification du demandeur et si les motifs correspondent à l'un des motifs décrits au chapitre 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.

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.

**4.4.4. TEMPS DE TRAITEMENT D'UNE DEMANDE REVOCATION**

A la réception d'une demande de révocation, en provenance de l'Abonné ou du client, l'AE analyse cette demande en vérifiant l'authenticité du demandeur, puis la transmet sans délai à la composante de l'AC chargée d'analyser les causes et justificatifs éventuels de révocation.

Les demandes de révocation doivent être traitées immédiatement à réception de la demande.

La prise en compte des demandes de révocation par le service de révocation de l'AC doit pouvoir être effective a minima du lundi au vendredi de 9h à 18h sauf jours fériés.

**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. PROCEDURE DE DEMANDE DE SUSPENSION**

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

**4.4.8. LIMITES DE LA PERIODE DE SUSPENSION**

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

**4.4.9. PUBLICATION DES CAUSES DE REVOCATION**

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.

**4.4.10. EXIGENCES DE VERIFICATION EN LIGNE DE LA REVOCATION**

La validité des certificats AC Serveur est vérifiée en consultant la LCR la plus récente. Cette liste est publiée en ligne sur un annuaire.

Les LCR doivent être conformes à la norme X.509 V2.

L'annuaire de publication des LCR doit être conforme au protocole LDAP.

**4.4.11. AUTRES FORMES DE PUBLICATION DES AVIS DE REVOCATION**

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

**4.5. JOURNALISATION D'EVENEMENTS**

**4.5.1. TYPES D'EVENEMENTS ENREGISTRES**

Le personnel de l'ICP Racine CERTEUROPE doit pouvoir justifier les opérations effectuées, en particulier par la tenue d'un journal d'événements.

Les événements seront enregistrés sous forme manuelle 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 :

- 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 certificats,

**AC Certigrefre Classe 3Plus  
Procès-verbal d'initialisation de l'AC**

– opérations d'écriture dans les LCR,  
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. FREQUENCE 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. DUREE DE CONSERVATION DES JOURNAUX D'EVENEMENTS**

Les journaux doivent être archivés conformément aux instructions indiquées au §4.6.

**4.5.4. PROTECTION D'UN JOURNAL D'EVENEMENTS**

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 IP Racine CERTEUROPE doivent être protégés contre les tentatives non autorisées de modification et de destruction.

**4.5.5. PROCEDURES DE SAUVEGARDE DES JOURNAUX D'EVENEMENTS**

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.

**4.5.6. SYSTEME 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. IMPUTABILITE DES EVENEMENTS**

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 VULNERABILITES**

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 régulièrement. 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 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.

#### **4.6. ARCHIVAGE DES DOSSIERS**

##### **4.6.1. TYPES DE DONNEES A ARCHIVER**

Les données à archiver sont au moins les suivantes :

- les logiciels et les fichiers de configuration des équipements informatiques de l'ICP Racine CERTEUROPE
- la PC,
- la DPC,
- les agréments contractuels ou les conventions,
- les journaux d'événements,
- les LCR telles qu'é émises
- les notifications de révocation,
- les justificatifs d'identité des Abonnés (responsable d'AC Serveur),
- le contrat signé par les Abonnés,
- les données d'enregistrement/renouvellement :
- les type et n° des documents présentés,
- le lieu du dépôt des copies des documents (ou copie de ces documents) incluant le contrat signé par l'abonné,
- les options du contrat (par ex : consentement pour publication),
- l'identité signataire du contrat,
- la méthode de vérification des documents,

##### **4.6.2. PERIODE DE RETENTION DES ARCHIVES**

Les certificats de clés de signature AC Serveur, ainsi que les LCR produites par l'AC Racine doivent être archivés pendant au moins cinq 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. 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.

##### **4.6.5. PROCEDURES DE RECUPERATION DES ARCHIVES**

Une composante de l'ICP Racine CERTEUROPE ne peut récupérer et consulter que ses propres archives.

#### **4.7. RECUPERATION EN CAS DE DESASTRE OU DE COMPROMISSION**

##### **4.7.1. CORRUPTION DES RESSOURCES INFORMATIQUES, DES LOGICIELS ET (OU) DES DONNEES**

L'ICP Racine CERTEUROPE 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 Racine) 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,

##### **4.7.2. COMPROMISSION DE LA CLE DE SIGNATURE DE L'AC RACINE**

En cas de compromission de la clé de signature de l'AC Racine, celle ci doit en avvertir l'ensemble des AC Filles qu'elle a générées ainsi que toute entité utilisant son certificat dans un chemin de certification.

**4.8. CESSATION D'ACTIVITE**

Si l'AC Racine 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.

**5. CONTROLE DE SECURITE PHYSIQUE, CONTROLE DES PROCEDURES, CONTROLE DU PERSONNEL**

**5.1. CONTROLES PHYSIQUES**

**5.1.1. ENVIRONNEMENT PHYSIQUE**

La DPC précisera 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,

**5.1.2. ACCES PHYSIQUE**

L'accès physique à une composante de l'ICP AC Racine CERTEUROPE 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.

**5.1.3. ENERGIE ET AIR CONDITIONNE**

Les installations électriques et de conditionnement d'air doivent être suffisantes pour le bon fonctionnement des systèmes informatiques de l'ICP Racine.

**5.1.4. EXPOSITION AUX LIQUIDES**

Les systèmes ne doivent pas être situés en zone inondable.

**5.1.5. PREVENTION ET PROTECTION INCENDIE**

Les systèmes doivent être protégés contre les incendies grâce à un système de protection incendie.

**5.1.6. CONSERVATION DES MEDIAS**

Les supports de stockage utilisés par le système doivent être protégés contre un excès de température, d'humidité et de magnétisme et autres variables ambiantes.

**5.1.7. DESTRUCTION DES DECHETS**

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

**5.2. CONTROLES DES PROCEDURES**

**5.2.1. ROLES DE CONFIANCE**

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

- opérateurs,
- administrateurs,
- responsable de sécurité.

**L'Opérateur** d'une composante réalise l'exploitation des services offerts par la composante, dans le cadre de ses attributions. Il est chargé entre autres du démarrage des services et de leur arrêt

**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 de l'ensemble des composantes de l'ICP Certurope et de leur environnement. A ce titre il est a accès à l'ensemble des journaux des composantes de l'ICP. 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 NECESSAIRES A CHAQUE TACHE**

Toute opération relative aux certificats (génération, modification, révocation...) requiert l'autorisation ou la présence d'au moins un membre du personnel de l'ICP Racine CERTEUROPE.

**5.2.3. IDENTIFICATION ET AUTHENTIFICATION DES ROLES**

Toutes les personnes amenées à œuvrer sur les composantes de l'AC doivent être nommées personnellement et le Responsable de Sécurité doit donner son accord) avant que l'accès ne leur soit donné.

**5.3. CONTROLES DU PERSONNEL**

**5.3.1. QUALIFICATIONS, EXIGENCES D'HABILITATIONS**

Les personnes qui accomplissent des tâches relatives à l'exploitation de l'AC :

- Doivent être nommées à leur poste par écrit ;
- Doivent être tenus par contrat ou par la loi de respecter les obligations, notamment de confidentialité, du poste qu'ils occupent ;
- Doivent posséder les qualifications pertinentes et ont reçu toute la formation nécessaire pour accomplir leurs tâches ;
- Ne doivent pas avoir de tâches ou d'intérêts susceptibles d'entrer en conflit d'intérêt avec les tâches qui leur incombent à l'égard de l'AC Racine Certurope.

**5.3.2. EXIGENCES DE FORMATION**

L'AC doit s'assurer que tous les membres du personnel qui accomplissent des tâches touchant l'exploitation de l' AC Racine ont reçu une formation adaptée aux tâches leur incombant ;

**5.3.3. SANCTIONS POUR DES ACTIONS NON AUTORISEES**

Sur faute avérée ou soupçonnée d'un membre exploitant l'ICP Racine CERTEUROPE dans l'accomplissement de ses tâches en rapport avec l'exploitation de l'AC, l'AC lui interdira l'accès au système et, le cas échéant, prendra toutes sanctions disciplinaires adéquates.

**5.3.4. DOCUMENTATION FOURNIE AU PERSONNEL**

L'AC doit mettre à la disposition du personnel de l'ICP Racine CERTEUROPE la présente Politique de Certification, et s'assurer qu'ils disposent de l'accès à toute loi, toute politique ou tout contrat qui s'applique au poste qu'ils occupent.

**6. CONTROLES TECHNIQUES DE SECURITE**

**6.1. GENERATION ET INSTALLATION DE BI-CLE**

**6.1.1. GENERATION DE BI-CLE**

L'AC doit produire son propre bi-clé de signature numérique au moyen d'un algorithme cryptographique sûr et selon une procédure impliquant plusieurs personnes. La clé privée de l'AC Racine est dédiée à la signature des certificats d'AC Filles.

Les ACs Filles doivent également produire leur propre le bi-clé de signature numérique au moyen d'un algorithme cryptographique sûr et selon une procédure impliquant plusieurs personnes.

L'objectif est d'obtenir un secret sûr et non duplicable, dont la création nécessite plus d'une personne.

**6.1.2. TRANSMISSION DE LA CLE PRIVEE DE CONFIDENTIALITE**

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

**6.1.3. TRANSMISSION DE LA CLE PUBLIQUE A L'AC**

La clé publique d'AC Serveur du client 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.

**6.1.4. FOURNITURE DE LA CLE PUBLIQUE DE VALIDATION DE L'AC AUX UTILISATEURS**

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

**6.1.5. TAILLES DE CLES**

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

- Les bi-clés de l'AC Racine sont d'une complexité au moins équivalente à 2048 bits pour l'algorithme RSA,
- Les bi-clés d'une AC Fille sont d'une complexité au moins équivalente à 2048 bits pour l'algorithme RSA.

Les opérateurs de l'ICP Racine CERTEUROPE n'ont que des certificats avec une clé d'au moins 1024 bits.

**6.1.6. PARAMETRES DE GENERATION DE CLE**

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 Electronics 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.

**6.1.7. CONTROLE DE QUALITE DES PARAMETRES DE CLES**

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

**6.1.8. MODE DE GENERATION DE CLE**

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

**6.1.9. USAGE DE LA CLE 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"

**6.1.9.1. 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.

**AC Certigrefre Classe 3Plus  
Procès-verbal d'initialisation de l'AC**

La clé publique de vérification de l'AC Racine est la seule clé utilisable pour vérifier la signature des certificats AC Serveur 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 de signature AC Racine et AC Serveur:

– **keyCertSign** et/ou **cRLSign** (aucune autre valeur autorisée).

**6.1.9.2. Clé publique de confidentialité**

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

**6.2. PROTECTION DE LA CLE PRIVEE**

**6.2.1. NORMES POUR LES MODULES CRYPTOGRAPHIQUES**

L'Abonné doit protéger les clés privées de l'AC Fille dont il en a la responsabilité afin qu'elles ne soient pas divulguées. 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 cadre de certificats de classe AC Serveur, l'utilisation de module cryptographique est imposé.

Concernant le module cryptographique de l'AC Racine, celui-ci doit être en conformité avec les recommandations de la norme FIPS140-1 niveau 3 au minimum.

**6.2.2. CONTROLE DE CLE PRIVEE PAR PLUSIEURS PERSONNES**

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

**6.2.3. RECUPERATION DE CLE PRIVEE**

Les clés privées de signature numérique ne doivent jamais se trouver en main tierce : leur recouvrement est par conséquent impossible.

**6.2.4. SAUVEGARDE DE CLE PRIVEE**

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.

**6.2.5. ARCHIVE DE CLE PRIVEE**

Les mesures et les contraintes relatives à l'archivage des clés privées sont identiques à celles qui sont prises en matière de sauvegarde

**6.2.6. METHODE D'ACTIVATION DE CLE PRIVEE**

La méthode d'activation de clé privée d'une AC Fille est du ressort du Client. Celui-ci doit assurer que son personnel habilité à activer la clé privée de l'AC Serveur, soit identifié par le système.

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

**6.2.7. METHODE DE DESTRUCTION DE CLE PRIVEE**

Lorsque le certificat AC Fille arrive à expiration ou s'il est révoqué, la clé privée ne **doit** plus servir à aucune opération et doit être détruite.

L'Abonné doit alors réinitialiser le module cryptographique et détruire tous les secrets de génération qui ont été partagés.

**6.3. AUTRES ASPECTS DE LA GESTION DES BI-CLES**

**6.3.1. ARCHIVE DES CLES PUBLIQUES**

L'AC Racine doit archiver toutes les clés publiques de vérification conformément au §XXXXXXX

**6.3.2. DUREE DE VIE DES CLES PUBLIQUES ET PRIVEES**

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.

**6.4. DONNEES D'ACTIVATION**

**6.4.1. GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION**

Les cartes à puce fournies sont protégés avec des données d'activation.. 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 DONNEES D'ACTIVATION**

Les données d'activation doivent être protégées en confidentialité par les AC Filles et les composantes de l'ICP.

**6.5. CONTROLES DE SECURITE DES POSTES DE TRAVAIL**

**6.5.1. BESOINS DE SECURITE SPECIFIQUES 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 Racine CERTEUROPE :

- 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 poste de travail AC, associé au module cryptographique contenant la clé privée de l'AC Racine CERTEUROPE, doit être hors ligne.

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. Pour les AC Filles le niveau minimal d'assurance recherché pour les Abonnés de l'ICP Racine CERTEUROPE doit répondre aux mêmes objectifs de sécurité suivants :

- 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.

**6.6. CONTROLES TECHNIQUES DU SYSTEME DURANT SON CYCLE DE VIE**

**6.6.1. CONTROLES DES DEVELOPPEMENTS DES SYSTEMES**

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'ICP Racine CERTEUROPE doit être documentée et respecter dans la mesure du possible des normes de modélisation et d'implémentation. 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. CONTROLES DE LA GESTION DE LA SECURITE**

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. CONTROLES DE LA SECURITE RESEAU**

L'AC Racine CERTEUROPE doit être isolée physiquement de tout réseau de communication.

#### **6.8. CONTROLES 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 §0
- « **signatureAlgorithm** » : l'identifiant de l'algorithme utilisé pour produire la signature du certificat.
- « **signatureValue** » : le résultat de cet algorithme 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 Racine CERTEUROPE
- **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, Identifiant for SHA-1checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc.) ;
- **issuer** : nom de l'AC, complété avec le nom distinctif (Distinguished Name) de X.500 de l'AC qui a créé le certificat (AC Racine Certeuropé)
- **countryName** : pays d'établissement : Ce champ doit être renseigné pour l'issuer avec le pays d'établissement de l'ICP Racine CERTEUROPE (FR)
- **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 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, Identifiant for RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc.)
- **SubjectPublicKey** : clé publique de l'AC (Racine ou Fille).

#### **7.1.2. EXTENSIONS DES CERTIFICATS**

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 ni 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

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'une même AC. Ce champ contiendra l'empreinte numérique SHA-1 de la clé publique de l'AC Fille.

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 chapitre 6.1.9,
- gérer la criticité comme défini au chapitre 6.1.9.

**7.1.2.4. CertificatePolicies**

Cette extension non critique définit la politique 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 d'AC Racine et Fille ;
- inclure le champ « **policyInformation** » en renseignant le champ « **policyIdentifier** » avec l'OID de la PC ; cf § 1.3

**7.1.2.5. basicConstraints**

Cette extension critique indique si l'entité destinataire du certificat peut agir comme une AC en utilisant la clé privée correspondant à la clé publique certifiée pour signer des certificats.

L'AC Racine doivent utiliser la valeur CA « TRUE » pour les certificats AC Filles.

Le nombre d'ACs Fille subordonnées sous l'AC Racine n'est pas limité. Par conséquent, le pathLenConstraint doit être renseigné à 0 pour l'AC Racine.

Pour les AC Filles cette valeur sera précisée à chaque cas.

**7.1.2.6. cRLDistributionPoints.**

Cette extension non critique identifie le ou les emplacements où l'Utilisateur de certificat peut trouver une LCR.

L'AC doit :

- inclure cette extension dans les certificats AC Serveur ;



**AC Certigrefre Classe 3Plus  
Procès-verbal d'initialisation de l'AC**

- renseigner le champ « **uniformRessourceldentifier** » : l'AC indiquera l'adresse d'annuaire (nom distinctif) contenant la LCR.

**7.1.3. INTERPRETATION SEMANTIQUE DES CHAMPS CRITIQUES DE LA PC**

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**

La LCR dans sa forme finale est l'ensemble des éléments suivants :

- « **tbsCertList** » : l'ensemble des champs décrits aux chapitres 7.1.1 et 7.1.2; 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 CRL, 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.509 v2. 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 CRL, 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

**7.2.2. EXTENSIONS DES LCR ET DES ENTREES DES LCR**

La version 2 de CRL X.509 permet de rajouter des informations additionnelles.

Pour les LCR émises par l'AC Racine, 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 ni 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

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 ;

## **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. PROCEDURES DE MODIFICATION DE LA PC**

#### **8.1.1. ARTICLES POUVANT ETRE MODIFIES 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 NECESSITE LA FORMULATION D'UNE NOUVELLE POLITIQUE**

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

- la composition de l'AC Racine ou de l'AE,
- à chaque modification des documents de référence de l'AP (ex : PC-Type du MINEFI) ainsi que chaque année pour assurer sa conformité aux normes de sécurité et à l'évolution des mises en œuvre du marché. CERTEUROPE 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 chapitre 8.1.4.

#### **8.1.3. CHANGEMENT AVEC AVIS**

L'AC préviendra qui de droit (par exemple le MINEFI, éventuellement les Abonnés et tiers Utilisateurs de tout projet de modification de la PC ou de la DPC concernant :

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

#### **8.1.4. DELAI DE PREAVIS**

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.

## **8.2. PROCEDURES DE PUBLICATION ET DE NOTIFICATION**

La PC est disponible depuis trois sources différentes :

- Par courrier, adresser la demande à :  
CERTEUROPE  
23 rue Ballu  
75009 Paris
- Par téléchargement, sur le site Web de CERTEUROPE : URL :  
<http://www.certeurope.fr/reference/pc-root.pdf>

Toute remarque sur la présente PC est à adresser soit par courrier à,  
CERTEUROPE  
23 rue Ballu  
75009 Paris  
soit par e-mail à : [info@certeurope.fr](mailto:info@certeurope.fr)

## **8.3. PROCEDURES D'APPROBATION DE LA PC**

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, Information Technology - Open Systems Interconnection – ISO/IEC 9594-8 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 Internet X509 Public Key Infrastructure, Certificate and CRL 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: TEXTES LÉGISLATIFS ET RÉGLEMENTAIRES**

### **10.1. CADRE GENERAL**

- 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

### **10.2. REGIME "DECLARATION - 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.

**AC Certigrefe Classe 3Plus  
Procès-verbal d'initialisation de l'AC**

- 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.