# Politique de Certification

## AC ChamberSign Réseau de Confiance - CSF - Signature Numérique

## -

# ChamberSign France

| | |
|---|---|
| **Objet du document :** | Ce document constitue la politique de certification de l'autorité de certification ChamberSign France « AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE », c'est-à-dire l'ensemble des engagements de celle-ci concernant la délivrance de certificats numériques issue de cette hiérarchie |
| **Version** | Diffusion |
| **OID du document** | 1.2.250.1.96.16.1.5.5 |
| **Date de diffusion** | Novembre 2007 |

**SOMMAIRE**

**Avertissement**

La présente Politique de Certification est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de **CHAMBERSIGN FRANCE**. La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement par écrit par **CHAMBERSIGN FRANCE** ou ses ayants droit, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'article L.122-5, d'une part, que « *les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective* » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « *toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite* » (article L.122-4 du Code de la Propriété Intellectuelle).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

La Politique de Certification, propriété de **CHAMBERSIGN FRANCE,** peut être concédée par des accords de licence à toutes entités privées ou publiques qui souhaiteraient l'utiliser dans le cadre de leurs propres services de certification.

# 1 Préambule

**CHAMBERSIGN FRANCE** est une autorité de certification interopérable avec le réseau européen des Chambres de Commerce et d'Industrie.

Ce document constitue la politique de certification de l'autorité de certification « AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE », c'est-à-dire l'ensemble des engagements de celle-ci concernant la délivrance de certificats numériques issue de cette hiérarchie.

Le profil du certificat reprend les normes applicables en particulier les normes X.509V3 et la RFC 3280.

Le titulaire du certificat se voit préciser l'étendue de l'usage du certificat « AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE» par les conditions générales de vente de **CHAMBERSIGN FRANCE**.

Elle renforce le niveau de confiance de l'AC au moyen du certificat « AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE».

Les procédures de sécurité et de contrôle, à chaque niveau de la chaîne de fabrication, de validation et de délivrance des certificats électroniques, ont donc été revues en conséquence.

Elle prévoit la faculté d'avoir recours à un mandataire de certification.

Elle met en œuvre un mode de distribution des certificats afin de permettre l'installation du bi-clé de signature à partir du navigateur internet de l'abonné.

Elle garantit la qualité de son infrastructure de sécurité.

**CHAMBERSIGN FRANCE** assure par cette Politique de Certification la délivrance de certificats pour toute Autorité Utilisatrice (AU) susceptible d'intégrer l'usage de la signature électronique dans une ou plusieurs de ses applications informatiques.

La présente politique de certification est complétée par une Déclaration des Procédures de Certification (DPC) explicitant les différentes dispositions prises pour son respect et sa bonne exécution de la PC.

# 2 Présentation générale de la PC

Une politique de certification (PC) est identifiée par un nom unique (OID). Elle est composée d'un ensemble de règles décrivant les conditions d'émission d'un certificat.

Une PC est définie indépendamment des modalités de mise en œuvre de l'Infrastructure à Clés Publiques (ICP) à laquelle elle s'applique.

Elle décrit également les exigences auxquelles l'ICP doit se conformer pour l'enregistrement et la validation des demandes de certificats, et pour la gestion des certificats.

Les procédures de certification sont consignées dans un document appelé déclaration des procédures de certification (DPC), distinct de la PC, qui décrit comment ces exigences sont atteintes en pratique.

Cette PC est associée à la DPC relative à l'AC « AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE » . La DPC n'est pas diffusée de la même manière que la PC et sa consultation doit faire l'objet de demande argumentée auprès de l'AC.

La gestion des certificats couvre toutes les opérations relatives au cycle de vie d'un certificat, depuis son émission jusqu'à la fin de vie de ce certificat (péremption, révocation).

Cette PC vise la conformité aux normes suivantes :

- RFC 2527
- RFC 3280

Les travaux européens suivants ont également été suivis :

- TS 101 456
- TS 101 862
- ISS CWA 14167

Cette PC vise également la conformité à la politique type « PRIS V2.1 » de la DGME au niveau certificat de signature une étoile.

## 2.1 Liste des acronymes utilisés

| | |
|---|---|
| AA | Agence Autorité |
| AC | Autorité de Certification |
| AE | Autorité d'Enregistrement |
| AED | Autorité d'Enregistrement Déléguée |
| AGP | Autorité de Gestion de la Politique |
| AU | Autorité Utilisatrice |
| C | Country (Pays) |
| CCI | Chambre de Commerce et d'Industrie |
| CISSI | Commission Interministérielle pour la Sécurité des Systèmes d'Information |
| CN | Common Name |
| DDC | Dossier de Demande de Certificat |
| DGI | Direction Générale des Impôts |
| DGME | Direction Générale de la Modernisation de l'Etat |
| DN | Distinguished Name |
| DPC | Déclaration des Pratiques de Certification, ou EPC |
| DSA | Digital Signature Algorithm |
| EAR | Entité d'Audit et de Référencement |
| EPC | Enoncé des Pratiques de Certification, ou DPC |
| ICD | Identifiant d'organisation |
| ICP | Infrastructure à Clés Publiques |
| LCR | Liste des Certificats Révoqués |
| LDAP | Light Directory Access Protocol |
| MD2 | Message Digest n°2 |
| MD5 | Message Digest n°5 |
| MINEFI | Ministère de l'Économie, des Finances et de l'Industrie |
| O | Organisation |
| OC | Opérateur de Certification |
| OCSP | Online Certificat Service Provider |
| OID | Object Identifier |
| OU | Organisation Unit (Unité Organisationnelle) |
| PC | Politique de Certification |
| PC² | Procédures et Politiques de Certification de Clés |
| PC/SC | Dispositif standard de lecteur de carte à puce |
| PIN | Personal Identification Number |
| PKCS | Public Key Cryptographic Standard |
| PP | Profil de Protection |

| | |
|---|---|
| PP_OSM | Profil de Protection des Outils de Sécurisation de Messages |
| PRIS | Politique de Référencement Inter-Sectorielle de la DGME |
| RC | Responsabilité Civile |
| RSA | Rivest Shamir Adelman |
| S/MIME | Secure/Multipurpose Internet Mail Extensions |
| SHA-1 | Secure Hash Algorithm One |
| SMS | Abbreviation de Short Message Service |
| SSL | Secure Sockets Layer |
| TeleTVA | Procédure de déclaration de la TVA en ligne |
| TLS | Transport Layer Security |
| TMC | Tiers Moral de Confiance |
| UML | Unified Modeling Language |
| URL | Unique Resource Locator |
| USB | Universal Serial Bus |
| XML | Extensible Markup Language |

## 2.2 Terminologie

**Abonné :** Personne ayant signé un contrat d'abonnement aux services de ChamberSign France.

**Autorité Utilisatrice, AU :** Autorité détentrice d'applications qui référencent un certificat dans le cadre de ces applications.

**Autorité de Certification, AC** : entité responsable des certificats signés en son nom.

**Autorité d'Enregistrement, AE** : Entité qui vérifie, conformément à la politique de certification, que les demandeurs ou les porteurs de certificat sont identifiés, que leur identité est vraisemblable et que les contraintes liées à l'usage d'un certificat sont respectées. Cette entité effectue un contrôle de conformité, de cohérence et de vraisemblance des documents qu'elle reçoit. L'AE a des bureaux centraux et des bureaux de proximité également nommés AED .

**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 œuvre d'opérations de cryptographie basées sur des algorithmes asymétriques.

**Certificat :** clé publique d'un Porteur de Certificat, ainsi que certaines autres informations attestées par la signature numérique de l'Autorité de Certification qui l'a délivré. Un certificat contient des informations telles que :

- l'identité du Porteur de Certificat,
- la clé publique du Porteur de Certificat,
- la durée de vie du Certificat,
- l'identité de l'Autorité de Certification qui l'a émis,
- la signature de l'Autorité de Certification qui l'a émis,
- déclaration de qualification du certificat.

Un format standard de Certificat est normalisé dans la recommandation X.509V3 et la RFC 3039.

**Chaîne de confiance :** ensemble des certificats nécessaires pour valider la généalogie d'un certificat d'un titulaire du certificat. Dans une architecture horizontale simple, la chaîne se compose du certificat de l'Autorité de Certification qui a émis le certificat et de celui du titulaire du certificat.

**Common Name CN :** Identité du titulaire du certificat

**Composante de l'ICP :** entité indépendante jouant un rôle déterminé au sein de l'ICP.

**Déclaration des Procédures de Certification, DPC :** énoncé des procédures et pratiques respectées par une Autorité de Certification pour émettre des Certificats

**Distinguished Name, DN :** nom distinctif X.500 du titulaire pour lequel le certificat est émis.

**Données d'Accès :** Identifiant et mot de passe numériques propres à chaque titulaire communiqués par l'Autorité d'Enregistrement lors de l'enregistrement d'un titulaire.

**Données d'activation :** données privées associées à un titulaire de certificat permettant d'utiliser sa clé privée.

**Emission d'un Certificat :** fait d'exporter un certificat à l'extérieur d'une Autorité de Certification pour être remis au titulaire et faire l'objet d'une publication.

**Enregistrement d'un titulaire :** opération qui consiste pour une autorité d'enregistrement ou un mandataire de certification à constituer le profil d'un demandeur de certificat à partir de son dossier de demande de certificat, conformément à sa politique de certification.

**Format de signature :** structure de données et algorithmes utilisés pour créer une signature.

**Génération d'un certificat** : action réalisée par une autorité de certification et qui consiste à signer le type d'un certificat édité par une autorité d'enregistrement, après avoir vérifié la signature de l'autorité d'enregistrement.

**Identificateur d'objet** : identificateur alpha numérique 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 composantes, fonctions et procédures dédiées à la gestion des clés et de Certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique.

**Liste de Certificats Révoqués, LCR :** liste comprenant les numéros de série des Certificats ayant fait l'objet d'une Révocation, signée par l'AC émettrice.

**Mandataire de certification ou mandataire :** personne désignée par l'abonné aux fins de recueillir les pièces des dossiers de demande de Certificats, de les vérifier, d'effectuer les demandes de révocation des certificats. Il est authentifié par ChamberSign France dans les conditions prévues par la DPC.

**MINEFI :** Ministère de l'Economie, des Finances et de l'Industrie.

**Module cryptographique :** un module cryptographique est un dispositif logiciel ou 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 œuvre ces éléments.

**Organisation :** entité juridique.

**Politique de Certification, PC :** ensemble de règles définissant les exigences auxquelles l'Autorité de Certification 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'Autorité de Certification.

**Pratique d'Enregistrement**, PE : Procédures d'identification d'organisation, de représentant légaux, d'individus respectés par les agents de l'AE et les mandataires de certification dans la délivrance de certificat à des usagers.

**Publication** : opération consistant à mettre un certificat à disposition d'une application utilisatrice pour lui permettre de vérifier une signature ou de chiffrer des informations.

**Référencement :** opération consistant à contrôler la conformité d'un type de Certificats émis par une Autorité de Certification afin que ceux-ci soient acceptés par une autorité utilisatrice. Si le résultat de cette opération est positif, ce type de Certificat est inscrit dans la liste tenue par l'autorité utilisatrice.

**Renouvellement d'un certificat :** opération effectuée, à la demande d'un titulaire de certificat, en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat.

**Révocation d'un Certificat :** opération effectuée sur demande du titulaire du certificat ou le mandataire de certification ou le représentant légal de l'organisation ou par une AC ou une AE dont le résultat est la suppression de la garantie de l'AC sur un certificat donné, avant la fin de sa période de validité .La demande peut être la conséquence de différents types d'événements tels que la compromission d'un bi-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.

**Titulaire :** personne physique identifiée de façon unique dans le certificat agissant pour le compte d'une entreprise et détentrice de la clé privée associée au certificat.
Avant d'avoir explicitement accepté le certificat et les informations qu'il contient et lorsqu'il vient solliciter les services de l'AC, il est appelé demandeur de certificat.

**Utilisateur de certificat :** toute entité qui utilise le certificat d'un titulaire pour s'assurer de son identité. La clé publique est utilisée, par exemple, aux fins exclusives de signature numérique.

**Validation de certificat :** opération de contrôle d'un certificat ou d'une chaîne de certification.

**Vérification de signature :** opération de contrôle d'une signature numérique.

**Viséo** : Nom commercial de l'applicatif de l'AE permettant notamment :

- La création des dossiers de demandes de certificats informatisés de l'AE par des agents de l'AE
- La gestion de la facturation des abonnés
- La gestion des flottes de certificats d'une organisation par un ou plusieurs mandataires

Les mandataires ainsi que les agents de l'AE (opérateurs de bureaux d'enregistrement) s'identifient et accèdent de manière sécurisée à cette plate forme avec leur certificat « CSF Class III Sign » ou équivalent grâce une gestion de rôle spécifique.

## 2.3 Type d'applications concernées par la PC

Les applications concernées sont celles qui supportent le certificat fabriqué selon la norme X.509V3, et dont le niveau d'exigence de qualification du porteur est élevé.

## 2.4 Type de certificat défini dans la PC

Le certificat visé par la présente PC est un certificat professionnel dont l'identifiant technique est «AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE».

Le certificat « AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE » délivré par **CHAMBERSIGN FRANCE** est commercialisé exclusivement sur des supports logiciels

La génération du certificat est sous la responsabilité du titulaire : la génération du bi-clé est faite sur le poste du titulaire à partir de son navigateur internet sous son propre contrôle.

Son identifiant commercial est « SIGNITIO » .

## 2.5 Modification de la PC

### 2.5.1 Organisme responsable de la modification et de la mise à jour

Cette politique de certification est sous la responsabilité de :

**CHAMBERSIGN FRANCE**
45, avenue d'IENA
75016 PARIS

**Personne responsable**

La responsabilité de la PC est portée par le Délégué Général de **CHAMBERSIGN FRANCE** pour le compte de l'AC. Il peut être contacté au siège de l'association à :

**CHAMBERSIGN FRANCE**
45, avenue d'IENA
75016 PARIS

Elle s'assure de la conformité de la PC aux règlements en vigueur, aux normes de sécurité et aux évolutions du marché.

### 2.5.2 Personne déterminant la conformité de la DPC avec la présente politique

**CHAMBERSIGN FRANCE** détermine la conformité de la DPC à la PC soit directement, soit par l'intermédiaire d'experts indépendants spécialisés dans les domaines des Infrastructures à Clé Publique et de la sécurité.

## 2.6 Identificateur numérique

La désignation de l'identification d'objet (OID) pour cette politique est : **1.2.250.1.96.16.1.5.5**

# 3 Dispositions de portée générale

Ce chapitre décrit les dispositions relatives aux obligations respectives de l'AC, de son personnel, des diverses entités composant l'ICP, des clients, des abonnés, des titulaires et des tiers utilisateurs. Elle contient également les dispositions juridiques s'appliquant à la résolution des litiges et aux lois en vigueur.

L'infrastructure à Clés Publiques repose sur les acteurs suivants :

- L'Autorité de Certification (AC), dont la fonction est de définir la Politique de Certification (PC) et de la faire appliquer, garantissant ainsi un certain niveau de confiance aux utilisateurs.
- L'Autorité d'Enregistrement (AE), dont la fonction est de vérifier que le demandeur est bien la personne qu'il prétend être, conformément aux règles définies par l'Autorité de Certification. Elle garantit la validité des informations contenues dans le certificat. L'Autorité d'Enregistrement est le lien entre l'Opérateur de Certification , l'abonné, le mandataire de certification et le titulaire.
- L'Opérateur de Certification (OC), dont la fonction est d'assurer la fourniture et la gestion du cycle de vie des certificats. Son rôle consiste à mettre en œuvre une plate-forme opérationnelle, fonctionnelle, sécurisée, dans le respect des exigences énoncées dans la Politique de Certification (PC) et dont les modalités sont détaillées dans la Déclaration des Pratiques de Certification (DPC).
- L'abonné est l'entreprise cocontractante de ChamberSign auprès de qui elle souscrit un abonnement aux services de certification
- Le titulaire de certificat est la personne physique détentrice d'un certificat.
- L'utilisateur tiers de certificat, dont la fonction est d'authentifier un porteur de certificat, de vérifier une signature numérique et/ou de chiffrer des messages à l'intention d'un porteur de certificat.

## 3.1 Contrôle de conformité à la PC type

### 3.1.1 Contrôle de conformité

L'AC référence la famille de certificats dans les conditions définies par l'AU, soit par référence à la loi du 13 mars 2000, soit par référence à une PC type.

Le principe des contrôles repose sur l'architecture du réseau et ses différents acteurs. Le contrôle est composé de trois parties :

- Les contrôles émanant des AU, AA, AGP,
- Les contrôles relatifs au réseau d'enregistrement,
- Les contrôles relatifs à la liaison entre le réseau d'enregistrement et le ou les opérateurs techniques.

Toute Autorité Utilisatrice peut diligenter chaque année un contrôle des différentes entités suivant son cahier des charges: en particulier, auprès de l'opérateur technique, pour s'assurer de la fiabilité technique du réseau et du respect des règles contractuelles ayant fait l'objet de l'agrément.

Chaque Autorité Utilisatrice fait siens ces contrôles en conformité avec les autres partenaires européens. L'AC donne libre accès aux contrôleurs désignés par une AGP, AU ou AA.

### 3.1.2 Identité du contrôleur

L'AU détermine l'identité du contrôleur et en informe **CHAMBERSIGN FRANCE** aux fins de référencement.

### 3.1.3 Modalités du contrôle de conformité

Le référencement de la famille de certificat est renouvelé selon la durée prévue par la PC type de l'AU.

L'audit de référencement suit les prescriptions prévues par la PC type en particulier les pratiques, procédures et moyens mis en œuvre pour émettre et gérer des familles de certificats à référencer. Les modalités de l'audit de référencement sont communiquées à l'AC.

L'AC laisse accès à ses locaux en tant que besoin et dans les conditions prévues dans le cadre du chapitre de la PC visant les « contrôles et accès physiques ».

Par défaut, en l'absence de PC type, un contrôle de conformité peut être effectué :

- par l'AC tous les trois ans par un expert indépendant
- lors du renouvellement d'un bi-clé d'AC avant toute émission et signature de certificat par cette dernière

### 3.1.4 Sujets couverts par le contrôle de conformité

Le contrôle de conformité porte sur les points suivants :

- les dispositions générales
- identification et authentification
- besoins opérationnels
- contrôles de sécurité physique, contrôle du personnel
- contrôles techniques de sécurité
- profil des certificats et LCR
- spécifications d'administration
- Annexes

### 3.1.5 Communication des résultats

Les résultats du contrôle de conformité des AU sont communiqués à l'AC par l'AU ou l'un de ses sous-traitants..

### 3.1.6 Mesures à prendre suivant les résultats

En cas de non-conformité, l'AC « AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE» décide de toute action corrective nécessaire.

En fonction du degré de non-conformité de la DPC à la PC, l'AC peut demander à toutes les composantes de l'ICP :

- la mise en place d'actions correctives dont la réalisation sera vérifiée dans les trois (3) mois
- la correction des non-conformités selon un calendrier précis à la suite de laquelle un contrôle de mise en conformité sera effectuée,
- la révocation du certificat de l'AC correspondante.

## 3.2 Respect et interprétation des dispositions juridiques

### 3.2.1 Dispositions juridiques

Les textes législatifs et réglementaires applicables à la présente PC sont indiqués en Annexe 1.
En cas de traduction, seule la version française du présent document fera foi.

Dispositions pénales :
Le fait d'accéder et de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 € d'amende (article L.323-1, alinéa 1 du Code Pénal).

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30 000 € d'amende (article L.323-1, alinéa 2 du Code Pénal).

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000 € d'amende (article L.323-2 du Code Pénal).

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 45 000 € d'amende (article L.323-3 du Code Pénal).

**CHAMBERSIGN**, **CHAMBERSIGN FRANCE** sont des marques déposées et enregistrées.

Sont interdits, sauf autorisation du propriétaire (article L.713-2 du Code de la Propriété Intellectuelle) :

- la reproduction, l'usage ou l'apposition de la marque **CHAMBERSIGN FRANCE**, même avec l'adjonction de mots tels que : "formule, façon, système, imitation, genre, méthode", ainsi que l'usage d'une marque reproduite, pour des produits ou services identiques à ceux désignés dans l'enregistrement de la marque **CHAMBERSIGN**,
- la suppression, ou la modification de la marque **CHAMBERSIGN** régulièrement apposée.

L'atteinte portée au droit du propriétaire de la marque **CHAMBERSIGN** constitue une contrefaçon engageant la responsabilité civile de son auteur.

Constitue une atteinte aux droits de la marque **CHAMBERSIGN** la violation des interdictions prévues aux articles L.713-2, L.713-3 et L.713-4 du Code de la Propriété Intellectuelle (article L.716-1 du Code de la Propriété Intellectuelle).

Les dispositions pénales mentionnées ci-avant ne sont pas exhaustives.

### 3.2.2 Séquestre

Pas d'exigence.

### 3.2.3 Arbitrage des litiges

Aucune exigence n'est stipulée.

En cas de contestation ou de litige, et avant toute saisie d'un tribunal, les parties tenteront, dans toute la mesure du possible, de régler leurs différends de façon amiable. Pour tout litige ou contestation, les parties font attribution de juridiction au Tribunal de grande instance de Paris.

## 3.3 Rôles et obligations de l'ICP et de ses composantes

### 3.3.1 Rôle de l'AC

**CHAMBERSIGN FRANCE** garantit en tant qu'AC le respect des exigences prévues dans la présente PC relatives à son activité de certification vis-à-vis des AU.
Elle garantit le respect de ces exigences par toutes les composantes de l'ICP.

### 3.3.2 Rôle de l'AE et du MC

L'AE a pour rôle de vérifier l'identité du demandeur du certificat ou l'authenticité d'une demande de révocation. Pour cela, l'AE assure les fonctions suivantes :

- La constitution du dossier d'enregistrement du titulaire
- la transmission de la demande à l'AC
- l'archivage des pièces du dossier ou l'envoi de pièces vers l'entité d'archivage de l'ICP

Le MC est choisi par l'organisation cliente qui est en relation directe avec l'AE ou l'AE déléguée.
Il assure pour elle la collecte des pièces nécessaires au dossier et les transmet à l'AE.

### 3.3.3 Obligations communes à toutes les composantes de l'ICP

Les différentes composantes de l'AC doivent :

- Protéger la clé privée et les éventuelles données d'activation en intégrité et en confidentialité,
- N'utiliser la clé privée d'AC qu'aux seules fins pour laquelle elle a été émise et avec les moyens appropriés,
- Mettre en œuvre les moyens techniques et employer les ressources humaines nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité,
- Documenter ses procédures internes de fonctionnement,
- Porter à la connaissance du responsable qualité toute non-conformité ou dysfonctionnement. Chaque entité documente des fiches de non-conformité.
- Respecter et appliquer les termes de la présente PC, et de la DPC qu'elles reconnaissent
- Accepter le résultat et les conséquences d'un contrôle de conformité, et en particulier remédier aux non-conformités qui pourraient être révélées,
- Respecter les conventions et contrats qui les lient aux autres entités composantes de l'AC.

### 3.3.4 Obligations relatives à la gestion des certificats

L'AC s'engage à :

- pouvoir démontrer aux autorités utilisatrices des certificats, qu'elle a émis un certificat pour un porteur donné.
- tenir à disposition des AU la notification de révocation du certificat d'une composante de l'ICP ou d'un titulaire
- assurer et maintenir la cohérence de la DPC avec la PC
- prendre toutes les mesures nécessaires et raisonnables pour s'assurer que l'abonné et les titulaires soient informé des droits et obligations concernant l'utilisation et la gestion des clés et des certificats.

### 3.3.5 Obligations relatives à la gestion des supports et des données d'activation

La distribution des certificats « AC ChamberSign Réseau de Confiance - CSF - Signature Numérique » est réalisé à partir du navigateur internet du titulaire. Les conditions de cette distribution sont précisées aux paragraphes 5.1 et suivants.

### 3.3.6 Obligations relatives à l'identification

L'AE et ses délégations (AED & MC) exécutent les obligations prévues aux fins d'identifications des titulaires de certificats, des mandataires de certificats et de leurs organisations de rattachement.

#### 3.3.6.1 Délivrance du certificat.

Suite au traitement administratif favorable d'un dossier, le titulaire reçoit par courriel le code PIN permettant de télécharger le certificat à partir de son navigateur internet et des informations secrètes qu'il a renseigner lors de l'élaboration de son dossier de demande de certificat.

#### 3.3.6.2 Révocation d'un certificat

Voir § 4.2

Les engagements spécifiques du MC font l'objet d'un contrat particulier avec l'autorité de certification joint lors de la contractualisation commerciale (Annexe 3 et Annexe 4).

Leur conformité est garantie par l'AC sur, en particulier, sur trois points :

- l'engagement à effectuer correctement et de façon indépendante les contrôles d'identité du demandeur
- le respect des parties de la PC et de la DPC qui lui incombent
- l'information par courriel ou par courrier, de son départ de la fonction de MC par lui-même ou par son représentant légal. Le cas échéant le représentant légal désignera le nouveau mandataire de certification et devra fournir les documents requis à l'identification du mandataire de certification.

### 3.3.7 Obligations relatives à la publication

Les informations suivantes sont publiées par l'AC sur son site Internet:

- La PC
- L'accès à LCR et aux répondeurs OCSP
- La liste des certificats auxquels la clé racine de l'ICP est subordonnée
- La liste des AC avec lesquelles l'AC est en certification croisée et l'empreinte de son certificat.

Les listes de certificats révoqués sont :

- protégées en intégrité ; seules les personnes habilitées dans les conditions prévues au § 6.3.1 « contrôle des personnels » disposent d'un droit d'accès ;
- accessibles gratuitement 24 heures sur 24 et 7 jours sur 7 sous réserve de justifier d'un abonnement régulièrement payé ou d'une relation en qualité d'AU, d'AGP, ou d'utilisateur ;
- mises à jour, avec une périodicité de 24 heures, à compter de l'émission du nouveau certificat du titulaire.

L'ensemble des opérations effectuées par l'AC découlant de :

- renouvellement du certificat après révocation
- émission d'un nouveau certificat

est exécuté au maximum dans les 24 heures à compter de la saisine de l'une des composantes de

l'AE (AE déléguée ou mandataire)

En cas d'indicent majeur tel que la perte, le vol, la suspicion de compromission ou la compromission des clés privée d'AC, l'AC met immédiatement en œuvre une procédure d'urgence diligentée par le responsable sécurité de l'AC. Elle informe les AU concernées des mesures spécifiques prises en fonction de la gravité de l'événement.

### 3.3.8 Obligations relatives à la journalisation

L' AC garantit la journalisation et les événements relatifs à son activité de certification en s'appuyant d'une part, sur son OC et, d'autre part, sur son AE.
Les modalités de journalisation des événements pour l'OC et l'AE concernent :

- l'accès aux systèmes physiques
- les modifications des systèmes et des applications
- les opérations traitées grâce aux applications.

Les modalités de renseignement de la journalisation des événements sont précisées au § 5.9 du présent document.

### 3.3.9 Obligations relatives à l'archivage

L'AC garantit les dispositions prises en matière d'archivage afin d'assurer la pérennité des journaux constitués par les différentes composantes de l'ICP.
La conservation de pièces papier est assurée par l'AE et l'AE déléguée.

### 3.3.10 Obligations relatives au séquestre

Les clés ne sont pas recouvrables.

## 3.4 Obligations du titulaire (porteur) du certificat

Des conditions générales de vente annexées à la DPC précisent les obligations de l'organisation abonnée et des titulaires.

Ces obligations recouvrent notamment:

- l'exactitude des informations communiquées à la date de la demande initiale ou de renouvellement du certificat
- la protection de la clé privée et des données d'activation
- la protection de l'accès au certificat
- l'obligation de demande de révocation effectuée auprès de l'AC en cas de vol, perte, compromission ou suspicion de compromission de sa clé privée, utilisation frauduleuse de sa clé, dès la découverte de cet incident par le titulaire.
- L'exactitude des informations du titulaire est validée par son représentant légal ou son mandataire de certification.

## 3.5 Obligations des applications utilisatrices

Les applications des AU qui utilisent les certificats doivent :

- vérifier et respecter l'usage pour lequel un certificat a été émis
- vérifier la signature numérique de l'AC émettrice du certificat en parcourant la chaîne de certification jusqu'à la racine référencée
- contrôler la validité des certificats (la date de validité et l'état du certificat)

## 3.6 Responsabilités de l'AC

L'AC a la responsabilité de l'élaboration et de la mise en œuvre de la politique de certification et par conséquence, du choix des opérateurs. Elle est seule responsable au regard d'AGP, AA et AU, qui ont référencée le certificat. Elle délègue une partie de cette responsabilité à un ou plusieurs opérateurs techniques et à une ou plusieurs autorités d'enregistrement.

L'AC fait son affaire personnelle de toute conséquence dommageable qui lui serait imputable résultant du non respect du présent document par elle-même ou l'une de ses composantes.

Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou de négligence, l'AC et l'ensemble de ses composantes sont responsables de tout préjudice causé à toute personne physique ou morale qui s'est fié raisonnablement aux certificats qu'elle délivre.

En tout état de cause, la responsabilité de l'AC se conformera strictement au titre de cette famille de certificat référencée par cette PC, aux prescriptions de la loi du 13 mars 2000 sur le nouveau régime de la preuve, en particulier les chapitres afférents à la signature électronique sécurisée.

L'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des titulaires à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.
Elle exerce son devoir général de surveillance par les moyens appropriés afin de garantir la sécurité et l'intégrité des certificats délivrés par elle-même

## 3.7 Politique de confidentialité de l'AC

### 3.7.1 Types d'informations considérées comme confidentielles

Les informations suivantes sont considérées comme confidentielles :

- La DPC de l'AC
- Les clés privées de porteurs de certificats
- Les données d'activation associées aux clés privées des porteurs
- Les journaux d'événements des composantes de l'AC et de l'AE
- Le dossier d'enregistrement de l'abonné et des titulaires et notamment les données personnelles

### 3.7.2 Divulgation des causes de révocation et de suspension des certificats

Aucune exigence n'est stipulée pour les causes de suspension du certificat.
Les causes de révocation du certificat sont précisées dans le cadre des conditions générales de vente de l'AC.

### 3.7.3 Remise sur demande de l'organisation abonnée ou du titulaire

La clé privée de signature numérique et ses données d'activation sont considérées comme des informations confidentielles. En cas de divulgation par le titulaire de ces informations secrètes, cela s'effectuera à ses propres risques et périls.

Elles ne peuvent donc être divulguées qu'au titulaire préalablement identifié et à sa demande expresse. Elles pourront, avec son accord, être remises temporairement soit à l'AE, soit au mandataire, afin de faciliter l'installation et le confinement convenable du certificat.

### 3.7.4 Délivrance aux autorités habilitées

Les procédures de l'AC relatives au traitement de la confidentialité sont conformes à la législation en vigueur.

### 3.7.5 Droits de propriété intellectuelle

Tous les développements liés à la délivrance des certificats sont propriétés de l'AC.
Les certificats eux-mêmes sont propriétés de l'AC, l'utilisateur en acquérant le droit d'usage.

L'AC peut, de sa propre autorité, révoquer un certificat et les services qui y sont rattachés si son titulaire ou son abonné venait à en faire un usage contraire aux dispositions en vigueur en matière de propriété intellectuelle.
Cf. l'Avertissement en introduction de la présente PC.

### 3.7.6 Données à caractère personnel détenues par une AC

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique au contenu de tous les documents détenus ou transmis par l'AC ou par un de ses représentants.

Les abonnés et les titulaires de certificats disposent d'un droit d'accès, de rectification et d'opposition à la cession de toute information qui les concerne. Ce droit peut s'exercer par l'intermédiaire de l'AE ayant recueilli ces informations.
Toutes les données collectées et détenues par l'AC ou une AE sur une personne physique ou morale (par exemple : procédure d'enregistrement, révocation, autres événements consignés, correspondances échangées entre l'abonné et l'AC ou l'AE, etc.…) sont confidentielles.

# 4 Identification et Authentification

## 4.1 Enregistrement initial

### 4.1.1 Convention de noms

Cette section et la suivante sont basées sur la RFC 3280 « Internet X.509 Public Key Infrastructure Certificate and CRL Profile ».

Le « subject name » utilisé pour le certificat est unique et les informations qu'il contient sont décrits dans la DPC 04.01.01.

### 4.1.2 Nécessité de noms significatifs

Les informations portées dans le champ « Subject name » du certificat sont explicites :

- le nom et prénom du demandeur (rubrique CN, tel que décrit au § 4.1.1),
- l'adresse électronique du demandeur,
- la dénomination sociale de l'organisation représentée par le demandeur, telle que figurant au K-Bis ou tout autre document attestant du nom de l'organisation (ex : extrait du répertoire SIRENE)
- L'identifiant ISO 6523 de l'organisation (En France le n° SIRET, précédé de son ICD (0002 pour la France) et suivi de la dénomination sociale de l'organisation)
- le nom de la commune de l'unité organisationnelle représentée par le demandeur, tel que figurant au K-Bis ou tout autre document attestant du nom de l'organisation ( ex : extrait du répertoire SIRENE )
- le nom de pays du siège social de l'unité organisationnelle représentée par le demandeur, tel que figurant au K-Bis ou tout autre document attestant du nom de l'organisation ( ex : extrait du répertoire SIRENE ) et formulé selon la convention internationale de nommage.

### 4.1.3 Règles d'interprétation

Aucune interprétation particulière n'est à faire des informations portées dans le champ "Objet" des certificats.

### 4.1.4 Unicité des noms

L'unicité d'un certificat est établie par celle du numéro de série, au sein de l'Autorité de Certification « AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE ». L'AC s'engage également à ce que le champ "Objet" présente aussi un caractère d'unicité, obtenu par la présence de l'adresse électronique du demandeur, à l'exception du renouvellement de certificat ou le champ « objet » est alors réutilisé.

### 4.1.5 Procédure de résolution de dualité sur les noms

Le « subject name » contenu dans le certificat doit être unique et sans équivoque pour les certificats issus d'une hiérarchie de l'AC et conforme au standard X.500 pour l'unicité des noms.

Quand un demandeur demande un certificat, remplace un certificat précédemment acquis, les attributs obligatoires spécifiés au § 4.1.1, hormis le numéro de série du certificat, doivent être maintenus dans le but de préserver l'unicité et la persistance des noms.

### 4.1.6 Reconnaissance, authentification et droit des marques

Pas d'exigence

### 4.1.7 Authentification du mandataire de certification

Toute organisation ayant recours à la fonction de mandataire de certification doit préalablement constituer un dossier d'enregistrement du mandataire.

Ce dossier d'enregistrement du mandataire comprend :

- une demande écrite signée du représentant légal de l'organisation. Le cas échéant cette demande pourra être signée électroniquement.
- Un mandat signé par le représentant légal et le mandataire de certification. Ce mandat porte également les engagements suivants :
    - le contrôle préalable, correct et indépendant des dossiers des demandeurs
    - le départ de l'organisation à signaler à l'AE
- Justificatif d'identité du mandataire de certification selon les règles de la législation française

### 4.1.8 Authentification du demandeur

L' organisation s'abonne par l'intermédiaire d'un MC.

L'AE et ses délégations constituent un dossier d'enregistrement unique pour chaque organisation abonnée.

Seul le représentant légal est habilité à engager l'organisation abonnée pour le premier DDC, en particulier lorsque l'organisation a recours aux services d'un MC. Les conditions d'enregistrement du MC sont précisées au § 4.1.8.2.

Le demandeur est authentifié par le MC.

L'organisation abonnée à laquelle est rattaché le demandeur par contrat est identifiée par l'AE déléguée dans les conditions prévues au § 4.1.8.1.

#### 4.1.8.1 Dossier déposé auprès d'une AE

Les éléments du dossier sont déposés auprès de l'AE :

- Un formulaire d'abonnement tamponnée et signé du représentant légal de l'organisation. Le formulaire intègre un mandat signé par le représentant légal et le demandeur du certificat.
- La copie d'un justificatif d'identité du demandeur de certificat, selon la législation en vigueur (CNI, passeport), certifiée conforme.

Le dossier d'enregistrement du demandeur est valable quatre ans.

#### 4.1.8.2 Dossier déposé auprès d'un MC

Dans le cadre d'un abonnement où l'organisation a recours à la fonction de MC, il constitue les dossiers de demandes de certificats (DDC) pour les demandeurs au sein de l'organisation.

Les éléments du DDC sont les suivants :

- La copie d'un justificatif d'identité du demandeur de certificat, selon la législation en vigueur (ex : CNI, passeport), certifiée.
- La lettre d'autorisation de délivrance d'un certificat, signée du MC et du demandeur.

Le dossier d'enregistrement du demandeur est valable trois ans.

Les éléments des dossiers sont transmis par le MC à l'AE déléguée pour validation, journalisation et archivage.

## 4.2 Authentification d'une demande de révocation

Il existe trois méthodes de révocation :

- En ligne, par le titulaire sur le site public de l'AC,
- En ligne, par l'application de gestion de certificats,
- Hors ligne, par téléphone à l'AE ou l'une de ses délégations.

Elles ont décrites dans la DPC

# 5 Exigences opérationnelles

## 5.1 Demande de certificat

### 5.1.1 Origine de la demande

Un certificat « AC ChamberSign Réseau de Confiance - CSF - Signature Numérique » peut être demandé par le représentant légal de l'organisation ou un représentant dûment mandaté.

### 5.1.2 Informations à fournir

Les informations à fournir figurent sur le site Internet dans le formulaire d'enregistrement à remplir par le demandeur, le MC ou le représentant légal pour le compte du demandeur.

Les opérateurs d'AE ne traitent que des DDC constitués de l'ensemble des pièces justificatives suivantes :

- Nom et prénom du titulaire
- Adresse mail du titulaire
- Numéro Siret de l'établissement
- Copie de Carte d'identité des titulaires* certifié conforme

**Dossier Mandataire de certification (Facultatif)**

Il est constitué des pièces suivantes :

- Nom et prénom du titulaire
- Adresse mail du titulaire
- Numéro de Siret de l'établissement
- Copie de Carte d'identité des titulaires* certifiés conforme par le titulaire
- Un mandat signé par le représentant légal et le mandataire de certification.

### 5.1.3 Procédure de demande d'un certificat

La demande de certificat se fait en quatres (4) étapes :

1. Constitution d'un Dossier de Demande Certificat par l'abonné ou le MC
2. Traitement du DDC par l'AE
3. Envoi par courriel et/ou SMS du code de retrait
4. Saisie par le titualire :
   - des réponses aux questions secrètes renseignées lors de la constitution du DDC,
   - du n° de dossier
   - code de retrait

   La correspondance des informations renseignées avec les informations du dossier déclenche le processus de génération de paires de clés dans le navigateur internet du titualire, l'envoi de la clé privée, la signature de la clé privée transmise par l'AC et l'installation de la clé publique certifiée dans le navigateur du titulaire.

La preuve de la possession de la clé privée par le titulaire est garantie le processus.

### 5.1.4 Acceptation d'un certificat

L'Autorité de Certification est informée du retrait de chaque certificat par le demandeur correspondant. Le titulaire est tenu d'avertir l'AC de toute inexactitude ou défection d'un certificat dans les sept jours ouvrés consécutifs au retrait du certificat, afin que celui-ci soit révoqué et qu'un autre certificat puisse lui être fourni.

Le titulaire est réputé avoir accepté son certificat lorsque ce délai est dépassé.

En outre, l'acceptation d'un certificat vaut acceptation de la PC en référence (OID unique stocké dans le certificat).

## 5.2 Révocation d'un certificat

Un certificat « AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE » est dans l'un des trois états suivants : valide, expiré ou révoqué.

L'Autorité de Certification « AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE » ne permet pas la suspension des certificats.

### 5.2.1 Cas de révocation

Lorsque l'une des circonstances ci-dessous se réalise, le certificat concerné doit être révoqué. Le numéro de série est alors placé dans la liste des certificats révoqués (LCR).

#### 5.2.1.1 Révocation d'un certificat d'AC

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

- compromission possible, probable ou certaine de la clé privée de l'AC,
- non-conformité de la DPC par rapport à la PC,
- cessation ou cession d'activité de l'AC.

#### 5.2.1.2 Révocation d'un certificat

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

- les informations figurant dans le certificat ne sont plus exactes, ceci avant l'expiration normale du certificat,
- non respect des règles d'utilisation du certificat
- non-paiement du prix du certificat
- résiliation du contrat d'abonnement
- fraude dans le DDC
- la clé privée du titulaire du certificat est suspectée de compromission, est compromise, est perdue ou est volée,
- le titulaire, le mandataire ou représentant légal de l'organisation en fait la demande,
- le certificat de l'AC est révoqué (ce qui entraîne la révocation de tous les certificats signés par la clé privée correspondante),
- le décès du titulaire, la cessation ou la cession d'activité de l'organisation,
- le licenciement, départ ou la démission du titulaire du certificat

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a eu connaissance, le certificat concerné doit être révoqué et le numéro de série placé dans la Liste de Certificats Révoqués (LCR).

### 5.2.2 Origine des demandes de révocation

La révocation d'un certificat peut émaner :

- du titulaire du certificat,
- du MC,
- du représentant légal du titulaire,
- de l'AC émettrice du certificat,
- de l'AE ayant autorisé l'émission du certificat.

### 5.2.3 Informations à fournir

Elle doit contenir explicitement les informations d'identification du certificat et de son titulaire.

Chaque personne habilitée à la révocation du certificat (cf § 5.2.4) dispose de moyens propres communiqués lors de l'inscription au service pour effectuer l'acte de révocation d'un certificat

### 5.2.4 Procédure de révocation

La demande de révocation est faite auprès de l'AE.
A la réception d'une demande de révocation, en provenance du titulaire ou de l'AC, l'AE analyse cette demande en vérifiant l'authenticité du demandeur et le droit à révoquer le certificat.

Si la demande est recevable, l'AE demande à l'AC de révoquer le certificat en faisant introduire le numéro de série du certificat dans la Liste de Révocation des Certificats.
Le titulaire du certificat est informé de la révocation par un récépissé (courriel).
L'opération est enregistrée dans le journal des événements de l'AC.

#### 5.2.4.1 En ligne

Le service en ligne est mis à disposition des personnes mentionnées au § 5.2.2, afin de révoquer un certificat dans les meilleurs délais.

Le demandeur de révocation d'un certificat se connecte sur le site de l'AC http://www.chambersign.fr/revocation/ac_csf_reseau_de_confiance/sn/ et peut révoquer un certificat.

- Le titulaire : à l'aide des questions/réponses secrètes transmissent lors du dossier d'inscription,
- Le mandataire et/ou le représentant légal : à l'aide de leur certificat d'identité numérique « AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE » en signant numériquement la révocation du certificat du titulaire concerné dans l'application de l'AE.

#### 5.2.4.2 Hors ligne

Le service de révocation téléphonique et électronique est mis à disposition du titulaire du certificat, du mandataire de certification ou du responsable légal, de 9h à 17h, pendant les jours ouvrés.

La révocation se fait :

- par un agent de l'AE qui rappelle le demandeur de révocation. L'agent de l'AE lui pose des questions/réponses permettant de vérifier sa qualité et l'identité de l'organisation.
- par la réception d'un courriel signé du mandataire de certification ou du responsable légal contenant :
    - le nom du titulaire de certificat à révoquer
    - le courriel du titulaire
    - et éventuellement le numéro de série du certificat

### 5.2.5 Délai de traitement d'une révocation

5.2.5.1 Certificat d'une des composantes de l'AC ou de l'AE

En cas de compromission du certificat d'une des composantes de l'AC (comme décrit au §5.2.1.1.a), l'ensemble des certificats signés par la clé privée correspondante est révoqué. Les abonnés, les titulaires et les Autorités Utilisatrices sont prévenus de cette compromission dans les 12h.

5.2.5.2 Certificat du titulaire

La demande de révocation et la vérification des droits de la personne qui en fait la demande se font de manière synchrone et la LCR en ligne est alimentée et rafraîchie toutes les 24 heures. Le délai de publication de la révocation d'un certificat n'excède donc jamais 24 heures.

## 5.3 Renouvellement de certificat (hors révocation)

Les bi-clés sont périodiquement renouvelés afin de minimiser les attaques cryptographiques.
Les bi-clés de signature des demandeurs sont renouvelés tous les deux ans.

## 5.4 Emission de nouveaux certificats après révocation

Le porteur de certificat suit le processus normal de demande de certificat décrit au § 5.1.3, si celle-ci intervient après une révocation. Une nouvelle paire de clé est alors générée.

## 5.5 Suspension du certificat

Sans objet.

L'Autorité de Certification « AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE » ne permet pas la suspension des certificats.

Un certificat « AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE » est dans l'un des trois états suivants : valide, expiré ou révoqué.

## 5.6 Vérification de la validité des certificats

### 5.6.1 Contrôle en ligne du statut des certificats

Le niveau de contrôle en ligne de l'état d'un certificat et les protocoles utilisés correspondent à l'état de l'art.

### 5.6.2 Forme de publication de LCR

Les LCR sont disponibles sur le site de l'AC :

- au format « LCR V2 » au format binaire,
- au format RFC 2560 sur le répondeur OCSP.

## 5.7 Renouvellement d'une clé d'une composante de l'ICP

### 5.7.1 Clé de signature de l'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du bi-clé de l'AC. Pour cela la période de validité de la clé de l'AC doit être supérieure à celle des certificats qu'elle signe.

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

Dès qu'un nouveau bi-clé d'AC est généré, seule la nouvelle clé privée doit être utilisée pour générer des certificats.

Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que ces certificats signés avec la clé privée correspondante aient expiré.

### 5.7.2 Clé de signature des autres composantes

Une composante de l'ICP demandera le renouvellement de son bi-clé et de son certificat de signature dans les trois mois précédant l'expiration de sa clé, à condition que le certificat correspondant n'ait pas été révoqué.

## 5.8 Révocation d'une clé d'une composante de l'ICP

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

### 5.8.1 Causes de révocation d'un certificat d'une composante de l'ICP

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

- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante,
- décision de changement de composante de l'ICP suite à la détection d'une non-conformité des procédures appliquées par la composante avec celles annoncées dans la DPC,
- cessation d'activité de la composante.

### 5.8.2 Révocation d'un certificat d'une composante de l'ICP

L'AC précisera dans sa DPC les procédures à mettre en oeuvre en cas de révocation d'un certificat d'une composante de l'ICP.

### 5.8.3 Révocation d'un certificat de signature de l'AC

L'AC doit révoquer l'ensemble des certificats des porteurs en cours de validité. L'AC doit indiquer aux titulaires que leur certificat est révoqué.

L'AC envoie une information aux AE et aux MC. Ces derniers devront informer les titulaires de certificats en leur indiquant explicitement que leur certificat a été révoqué car la clé de signature de l'AC n'est plus valide.

L'Autorité responsable du référencement doit être immédiatement informée en cas de compromission de la clé de signature de l'AC. Elle retransmettra l'information aux différentes applications utilisatrices.

L'AC informe les autres applications utilisatrices de ces certificats par courriel.

### 5.8.4 Délai de traitement

La révocation d'un certificat d'AE ou d'une composante de l'ICP doit être effectuée dès la détection d'un événement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat.
La révocation du certificat de signature de l'AC doit être effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

## 5.9 Journalisation des événements

La journalisation des événements est opérée manuellement ou par génération automatique. Elle permet de garantir l'auditabilité, la traçabilité, l'imputabilité et que de s'assurer que la séparation des fonctions est effective.
La journalisation des évènements permet également de prouver le respect des dispositions énoncées dans la PC et la DPC.

### 5.9.1 Informations enregistrées pour chaque évènement :

Ces enregistrements d'événements contiennent au minimum les champs suivants :

- 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).

### 5.9.2 Imputabilité

Les différentes composantes liées à la gestion des certificats sont tenues à jour dans une liste d'événements qui les concernent.

### 5.9.3 Evènements enregistrés par l'AE

L'AE consigne au moins les événements suivants :

- les demandes de certificat,
- les demandes de révocation,
- les sollicitations et accusés de réception de l'OC (quand le lien est automatique),
- toutes les actions des AED pour l'enregistrement et la révocation,
- toutes les actions des administrateurs de l'AE,
- les tests de bon fonctionnement des applications de l'AE.

### 5.9.4 Evènements enregistrés par l'OC :

L'OC consigne au moins les événements suivants :

- tous les événements ayant trait à la sécurité de son système,
- démarrage et arrêt du système,
- démarrage et arrêt de l'application de l'OC,
- opérations échouées ou réussies pour créer, extraire, établir des mots de passe ou modifier les privilèges système de l'utilisateur maître de l'AC, du responsable de sécurité de l'AC ou du gestionnaire de l'AC,
- génération des clés de l'OC,
- changements des caractéristiques et (ou) des clés de l'OC,
- création et révocation de certificats,
- opérations pour initialiser, extraire, valider et invalider des titulaires, des abonnés et pour mettre à jour ou récupérer leurs clés,
- opérations de lecture et d'écriture dans l'annuaire des certificats et des LCR.

### 5.9.5 Evènements divers

L'OC recueille aussi, par des moyens électroniques ou manuels, de l'information sur la sécurité qui n'est pas produite par le système automatique de l'OC, notamment :

- journaux des accès physiques,
- maintenance et changement de la configuration du système,
- changements apportés au personnel,
- registres sur la destruction des supports contenant des clés, des données d'activation ou des renseignements personnels sur les titulaires

### 5.9.6 Processus de journalisation

L'ensemble des données du cycle de vie des certificats est journalisé des fichiers de traces (Log)

### 5.9.7 Protection d'un journal des évènements

Les fichiers de traces sont signés numériquement toutes les heures, puis archivés

### 5.9.8 Copies de sauvegarde des journaux des évènements

Les serveurs d'archives de ChamberSign se trouvent dans 2 lieux différents. En outre, un DVDRom est gravé tous les mois

### 5.9.9 Procédures de collecte de journaux

Des déclencheurs de logs sont intégrés dans le code de l'application de l'AC.

### 5.9.10 Anomalies et audit

Chaque anomalie détectée, déclenche un enregistrement dans le logiciel de « Suivi de code de l'application ». Le traitement des anomalies donne lieu à un correctif logiciel.

## 5.10 Archives

L'archivage est réalisé par l'AC dans le but d'assurer la continuité de service, l'auditabilité et la non répudiation des opérations.

Les mesures nécessaires sont mises en place par l'AC afin que ces archives soient disponibles, ré exploitables, protégées en intégrité et qu'elles fassent l'objet de règles strictes d'exploitation et de protection contre la destruction.

L'AC décrit précisément dans ses procédures internes, et notamment la DPC, les points suivants :

### 5.10.1 Types de données archivées

PC, PE, DPC, LCR, Journaux d'événements, Audit, Dossier de Demande de Certificat, récépissés, notifications et justificatifs d'identité.

### 5.10.2 Protection des archives

Les médias d'archives sont protégés physiquement contre l'effacement et par des moyens cryptographiques. Ils sont stockés dans un coffre situé dans un lieu différent du site d'exploitation.

### 5.10.3 Période de rétention des archives

| | |
|---|---|
| PC, DPC et annexes | Pendant le fonctionnement de l'AC |
| Dossier de Demande de Certificat, récépissés, notifications et justificatifs d'identité | 10 ans après la fin de validité du certificat |
| LCR et journaux d'événements et Audit | 10 ans |

### 5.10.4 Procédures de copie des archives

Cf. DPC

### 5.10.5 Besoins d'horodatage des enregistrements

Cf. DPC

### 5.10.6 Procédures de collecte des archives

Cf. DPC

### 5.10.7 Procédure de sauvegarde des archives

Des procédures adéquates sont mises en œuvre par l'AC afin de prévenir les destructions ou les pertes des archives primaires. Les jeux de sauvegardes sont renouvelés tous les trimestres.

## 5.11 Cessation d'activité de l'AC

### 5.11.1 Arrêt de l'AC

Si l'AC interrompt ses activités, elle en avise immédiatement ses abonnés et clients et prend des dispositions pour que les clés et l'information de l'AC continuent d'être archivées.

L'AC avise également tous les AC avec lesquelles il est en certification croisée et de reconnaissance mutuelle, ainsi que les AU auprès desquelles les certificats sont référencés.

Dans le cas où une des composantes de l'ICP, autre que l'AC, interrompt ses activités, l'AC doit faire

porter à une autre entité la charge de cette composante ou l'opérer elle-même.
En cas de transfert d'activité vers une autre entité, l'AC est garante du respect de sa PC par la nouvelle composante.

Les archives de l'AC doivent être conservées selon les indications et la période stipulée au § 5.10

### 5.11.2 Changement de la clé de l'AC

Avant que la période d'usage de la clé d'AC expire (Voir §7.1), un changement de clé peut être opéré. La « vieille clé logique de l'AC» et la clé privée correspondante doivent être désactivées et une « nouvelle paire de clés d'AC » doit être générée avec le même DN.

### 5.11.3 Compromission et recouvrement après désastre

L'AC s'efforcera de remettre en œuvre un service opérationnel dans les meilleurs délais en particulier :

#### 5.11.3.1 Compromission de la clé privée de l'AC

Le plan de continuité de l'AC pour ce cas est mis en œuvre. Il comprend :
s'il y a lieu :

- La révocation de la clé de l'AC
- Aviser :
    - AU, AA, AGP qui l'accréditent,
    - Toutes les AC avec lesquelles des accords de participations croisés ont été opérés,
    - L'AE,
    - Tous les titulaires et les abonnés
- Produire une nouvelle paire de clé,
- Emettre des nouveaux certificats à toutes les entités.

#### 5.11.3.2 Recouvrement après désastre

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

Lorsque le dépôt de documents ne relève pas de l'OC, celui-ci s'assure que toute entente avec ce dépôt prévoit la mise en place, par celui-ci, de ces procédures.

# 6 Contrôles

Ce chapitre définit les mesures de sécurité physique, logique, les procédures et les exigences en matière de management, ressources humaines pour atteindre cette politique

## 6.1 Contrôles physiques

Des contrôles de sécurité physique sont mis en place par l'AC et sont détaillés dans la DPC correspondant à cette PC, autour des thèmes suivants :

- situation géographique,
- contrôle d'accès physique,
- énergie et air conditionné,
- exposition aux liquides,
- sécurité incendie,
- conservation des médias,
- destruction des supports,
- sauvegarde hors site.

### 6.1.1 Situation géographique et construction de sites

Cf. la DPC

### 6.1.2 Accès physique

Cf. la DPC

### 6.1.3 Energie et air conditionné

Cf. DPC

### 6.1.4 Exposition aux liquides

Cf. DPC

### 6.1.5 Sécurité incendie

Cf. DPC

### 6.1.6 Site de secours

Cf. DPC

### 6.1.7 Conservation de médias

Cf. DPC

### 6.1.8 Destruction des supports

Cf. DPC

### 6.1.9 Sauvegarde hors site

Cf. DPC

## 6.2 Contrôles des procédures

Des contrôles des procédures sont mis en place par l'AC et sont détaillés dans la DPC correspondant à cette PC, autour des thèmes suivants :

### 6.2.1 Rôles de confiance

Les rôles sont clairement identifiés :

- Responsable de la sécurité : Assure la sécurité physique et logique des moyens de l'AC. Optionnellement, il approuve la génération et la révocation des certificats
- Administrateurs systèmes : Ils sont autorisés à installer, configurer et à maintenir les systèmes informatiques de l'AC
- Opérateurs systèmes : Administrent au quotidien les systèmes et applications de l'AC. Ils sont également autorisés à faire les sauvegardes et restaurations.
- Auditeurs systèmes : Autorisés à voir et maintenir les archives et les fichiers d'audit.
- Responsable qualité : Assure la cohérence des actions des différents rôles de confiance et la qualité des services rendus aux utilisateurs

### 6.2.2 Nombre de personnes nécessaires à l'exécution de tâches sensibles

Selon le type d'opération effectuée, le nombre et le type de personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différent. La DPC indique le nombre d'exploitants minimum nécessaire par type d'opération.

### 6.2.3 Identification et authentification des rôles

Cf. DPC

## 6.3 Contrôle du personnel

Des contrôles effectués sur le personnel sont mis en place par l'AC et sont détaillés dans la DPC correspondant à cette PC, autour des thèmes suivants :

### 6.3.1 Antécédents professionnels, qualifications, expériences et exigences d'habilitations

Le responsable de l'AC doit s'assurer que tous les membres du personnel qui accomplissent des tâches relatives à l'exploitation de l'AC ou de l'AE :

- sont nommés à leur poste par écrit,
- sont liés par contrat ou par la loi aux modalités du poste qu'ils occupent,
- ont reçu toute la formation nécessaire pour accomplir leurs tâches,
- sont tenus par contrat ou par la loi de ne pas divulguer de renseignements ayant trait à la sécurité de l'AC, aux clients ou aux abonnés ; une clause de confidentialité doit être expressément inscrite dans les contrats de travail des membres du personnel de l'AC,
- n'ont pas de tâches qui risquent de causer un conflit d'intérêt avec les tâches qui leur incombent à l'égard de l'AC ou de l'AE.

### 6.3.2 Procédure de contrôle des antécédents professionnels

Les composantes de l'AC s'assurent que les membres du personnel qui accomplissent des tâches associées à l'exploitation de l'AC ont fait l'objet d'une vérification de leur passé professionnel.

Les composantes de l'AC s'engagent à vérifier l'honnêteté de leurs personnels par tous les moyens légaux dont elles disposent. Une enquête adaptée est conduite auprès des personnels appelés à remettre ou mettre en œuvre des conventions secrètes.

### 6.3.3 Exigences de formation

L'AC s'assure que tous les membres du personnel qui accomplissent des tâches touchant l'exploitation de l'AC ou de l'AE ont reçu une formation complète sur le fonctionnement et la sécurité mise en œuvre sur l'AC ou sur l'AE.

Le personnel de l'AC suit un programme de formation pour accomplir correctement leurs fonctions et qui porte :

- sur les différentes applications et versions d'applications auxquelles il pourrait avoir accès dans le cadre de leur fonction au sein du système de l'AC,
- sur toutes les tâches qu'il accomplit dans le cadre de l'ICP,
- sur le matériel et les systèmes d'exploitation formant l'environnement opérationnel de l'AC,
- sur le plan de secours de l'AC après un sinistre et les procédures de maintien des activités.

Le personnel d'AE suit un programme de formation pour accomplir correctement les tâches d'exploitation et de vérification d'identité et d'enregistrement.

### 6.3.4 Fréquence des formations

Cf. DPC

### 6.3.5 Gestions des métiers

Cf. DPC

### 6.3.6 Sanctions pur des actions non autorisées

Cf. DPC

### 6.3.7 Contrôle des personnels contractants

Cf. DPC

### 6.3.8 Documentation fournie au personnel

Les documents dont dispose le personnel sont les suivants :

- les PC supportées par la composante à laquelle il appartient,
- les DPC propres au domaine de certification,
- les procédures internes de fonctionnement.

# 7 Contrôles techniques de sécurité

Ce chapitre définit les dispositions de gestion des clés de l'AC et des clients.

## 7.1 Génération des clés, installation et protection

### 7.1.1 Génération des bi-clés

Les clés gérées dans le cadre de l'AC sont des clés dont le champ usage est critique : le bi-clé de signature du titulaire est généré à partir du navigateur internet par le titulaire lui-même et sous sa propre responsabilité.

Le certificat ne se génère ou ne transite en aucun cas sur le poste de l'opérateur de l'AE ou du MC.

### 7.1.2 Import et export de la clé privée

L'ensemble des processus appelés lors de la génération du bi-clé (CSP et PKCS 11) autorisent la génération des clés dans le navigateur internet du titulaire.

Aucun paquet cryptographique de type PKCS#12 ne transite sur le poste informatique du MC ou de l'opérateur de l'AE.

Cf. la DPC

### 7.1.3 Publication de la clé publique de signature à l'émetteur du certificat

La clé publique est transmise chiffrée en SSL afin d'assurer son intégrité avant que le certificat ne soit produit.

### 7.1.4 Fourniture d'un certificat d'AC

La clé publique de l'AC est accessible sur le site Internet de l'AC.

L'empreinte (Thumbprint) du certificat de la clé publique de l'AC permet d'en établir l'authenticité. Il est vérifiable par téléphone auprès de l'AC.

### 7.1.5 Taille des clés

Le titulaire d'un certificat générant lui-même son bi-clé à partir de son navigateur internet. La taille des clés est imposée est de 2048 bits.

L'AC se réserve le droit de forcer la taille à une valeur supérieure en cas de nécessité.

### 7.1.6 Paramètres de génération des clés publiques

Les clés sont générées à partir du navigateur internet du titulaire. L'algorithme du navigateur internet du dispositif respecte les normes internationales de sécurité.

### 7.1.7 Contrôle de la qualité des paramètres des clés

Le contrôle des paramètres de bi-clé est effectué en respect du § 7.1.6

### 7.1.8 Mode de génération de clé de l'ICP

L'AC s'assure que les clés demeurent confidentielles et conservent leur intégrité, en particulier :

a) La clé privée de signature de l'AC est contenue dans un dispositif cryptographique :
   - o de type FIPS 140-1 niveau 3 ou supérieur,
   - o EAL4 ou supérieur – conforme aux normes ISO 15408.

b) La clé privée de l'AC n'est pas sauvegardée, stockée. Elle ne peut être recouvrée que par des personnels dûment autorisés à cette tâche, suite à la convocation de 5 des 8 porteurs de secrets afin de régénérer la clé privée le l'AC.

c) Si des copies de la clé privée d'AC existent, elles ne sont opérées que dans des matériels ayant le même niveau ou supérieur que ceux en production,

d) Quand la clé est stockée dans un dispositif matériel dédié, il n'est pas possible de l'exécuter en dehors.

### 7.1.9 Usage de la clé publique

L'usage de la clé publique est défini et restreint par l'extension du certificat X.509V3.

## 7.2 Protection de la clé privée

Le titulaire doit protéger sa clé privée afin qu'elle ne soit pas divulguée.

### 7.2.1 Dispositifs de gestion des éléments secrets du porteur

Le porteur charge sa clé privée sur le dispositif physique externe fournit par l'AC. Il est également responsable de l'intégrité et de la confidentialité des données d'activation liées à sa clé privée ainsi que de la sécurité physique et logique du dispositif physique externe.

### 7.2.2 Contrôle de la clé privée de signature de l'AC

Un système de secrets partagés (où « n » exploitants parmi « m » doivent s'authentifier pour mettre en œuvre les clés privées de signature de l'AC) est mis en place.

### 7.2.3 Récupération de la clé privée

Ce service n'est pas disponible.

### 7.2.4 Sauvegarde de la clé privée

La clé privée est confinée dans un dispositif physique externe. L'export est impossible.

### 7.2.5 Archivage de la clé privée

Voir le § 7.2.4

### 7.2.6 Initialisation et conservation de la clé privée dans un module cryptographique

La clé privée de l'AC est gérée dans un dispositif cryptographique qui utilise des données fixes et/ou aléatoires introduites depuis l'extérieur.

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

L'utilisation de la clé privée requiert si le titulaire l'a souhaité lors de la génération de la paire de clés à partir de son navigateur internet. Il est possible lors de cette génération de choisir un niveau d'accès aux clés privées par l'intermédiaire d'un code d'activation (PIN) connu seulement du titulaire.

#### 7.2.8 Méthode désactivation de la clé privée

Sans objet, il s'agit d'un certificat logiciel.

#### 7.2.9 Méthode de destruction de la clé privée

Lorsque le certificat est révoqué ou est arrivé à expiration la clé privée doit être détruite. Le titulaire utilise la fonction d'effacement.

### 7.3 Autres aspects de la gestion des clés

#### 7.3.1 Archivage des clés publiques des abonnés

Les clés publiques des titulaires sont archivées pendant 10 ans après leur expiration.

#### 7.3.2 Durée de vie des certificats

La durée de vie des certificats est de 3 ans.

### 7.4 Données d'activation

#### 7.4.1 Données d'activation et installation

Les titulaires gèrent eux-mêmes leurs bi-clés dans leur module cryptographique. Ils génèrent leurs bi-clés de manière autonome et sous leur seule et entière responsabilité.

#### 7.4.2 Protection des données d'activation

Les données d'activation doivent être considérées par le titulaire comme confidentielles.

#### 7.4.3 Autres aspects liés aux données d'activation

Le code confidentiel (PIN) a une longueur fixée par le titlaire.

### 7.5 Sécurité des postes de travail des composantes de l'ICP

Les besoins de sécurité suivants permettent d'évaluer le niveau de sécurité des postes de travail des composantes de l'AC :

- identification et authentification des utilisateurs du poste de travail,
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlés par rôle et nom d'utilisateur),
- protection contre les virus informatiques,
- fonctions d'audits (imputabilité et nature des actions effectuées),
- gestion des reprises sur erreur.

Le niveau minimal d'assurance recherché répond au moins à ces objectifs de sécurité. Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires, à prendre en compte dans la recherche du niveau minimal d'assurance offert par les postes de travail.

Un niveau minimal d'assurance dans la sécurité offerte est défini dans la DPC pour les postes des agents de l'AE et des MC.

Aucune exigence n'est stipulée pour le poste de travail des titulaires.

## 7.6 Contrôles techniques du système durant son cycle de vie

### 7.6.1 Contrôle des développements des systèmes

Les applications de l'ICP respectent les normes de modélisation, de contrôle et d'implémentation conforme aux standards UML. La configuration du système, toutes les modifications et mises à niveau sont documentées et contrôlées.

### 7.6.2 Contrôle de gestion de la sécurité

L'AC met en œuvre des procédures administratives et managériales correspondant à l'état de l'art.

## 7.7 Contrôle de la sécurité réseau

Le réseau de l'OC fait l'objet de règles de sécurité informatique correspondant à l'état de l'art en la matière qui sont définies par l'AC dans la DPC.

## 7.8 Contrôle de la gestion des modules cryptographiques

Les modules cryptographiques sont évalués à minima selon les critères FIPS 140-1 au niveau 3 ou supérieur et selon les Critères Communs au niveau EAL 4.

# 8 Profils des certificats utilisateurs et de la liste de révocation

## 8.1 Profil du certificat

Les certificats de l'AC "AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE" :

- respectent les exigences de la norme X.509 V3,
- sont conforme à la RFC 3280 : « Internet X.509 Public Key Infrastruture Certificate and Profile CRL »
- ne contiennent pas les champs « Issuer Unique Identifer » or « Subject Unique Identifier »

### 8.1.1 Numéro de la version

Le champ version est fixé à 2 indiquant qu'il s'agit d'une version V3.

### 8.1.2 Numéro de série

Le numéro de série unique du certificat attribué par le module cryptographique de l'AC exprimé sous la forme d'un nombre hexadécimal.

### 8.1.3 Extension du certificat

8.1.3.1 Extension courante

| Extension | Critique | Valeur |
|---|---|---|
| Authority Key Identifier | | KeyIdentifier, valeur SHA-1 du hash de la clé publique de l'AC – RFC 3280 |
| Subject Key Identifier | | KeyIdentifier, valeur SHA-1 du hash de la clé publique du titulaire - RFC 3280<br>Identifiant de l'algorithme |
| Key Usage | X | Non-Repudiation |
| Certificate Policies<br>policy Identifier<br>policy Qualifier<br>CPS URI<br>User Notice | | **1.2.250.1.96.16.1.5.5**<br>http://www.chambersign.fr/telechargement/pc/AC_Chambersign_France_Reseau_de_confiance/pc_Signature.html<br>C'est un certificat de signature.<br>Il est délivré après validation de pièces officielles. |
| Authority Info Access | | OCSP;URI:http://ocsp.chambersign.fr/ |
| CRL Distribution Points | | http://www.chambersign.fr/telechargement/lcr/Signature.crl |
| Basic Constraints | | CA=FALSE |
| Subject AltName<br>RFC Name | | Le courriel du titulaire |
| Issuer AltName<br>RFC Name<br>URI | | autorite@chambersign.fr<br>http://www.chambersign.fr |

### 8.1.4 Identifiant de l'algorithme

L'identifiant d'algorithme des certificats est défini comme suit :

id-sha1-width-RSAEncryption 1.2.840.113549.1.1.5

L'algorithme identifiant le champ "subject" de la clé publique est défini comme suit :

RsaEncryption 1.2.840.113549.1.1.1

### 8.1.5 Noms

#### a) Champs noms de l'émetteur

Les noms suivants sont obligatoires dans le DN des titulaires.

| Attribut | Valeur |
|---|---|
| Country | FR |
| Organization | AC ChamberSign Réseau de Confiance |
| OrganizationUnit | Certificat pour les professionnels |
| OrganizationUnit | 0002 433702479 |
| Common Name | Signature numérique |

#### b) Champs Noms du certificat

Les noms suivants sont obligatoires dans le DN des titulaires.

| Attribut | Valeur |
|---|---|
| Country | Code ISO du pays de l'organisation de l'abonné |
| Locality | Ville de l'organisation |
| Organization | Dénomination légale de l'organisation |
| Common Name | Prénom et nom du titulaire |
| E.Mail | Adresse mail de l'abonné |
| Title | Position du titulaire dans l'organisation |
| OrganizationUnit | Service fonctionnel du titulaire |
| OrganizationUnit | <ICD> <N° d'identification de l'entreprise> |

(*) En cas d'absence d'ICD pour un pays donné, ChamberSign France utilise un substitut d'ICD, construit comme suit :

- **G+Code GS1**

La liste des codes GS1 peut-être obtenu sur le site de GS1 à l'adresse suivante :

- http://www.gs1.org/productssolutions/idkeys/support/prefix_list.html

Exemple : le substitut d'ICD pour la Belgique est **G540**

Les noms suivants sont optionnels dans le DN des titulaires.

| Attribut | Valeur |
|---|---|
| givenName | Nom propre du titulaire |
| surName | Nom d'usage du titulaire |

#### 8.1.6 Contrainte de noms

Pas d'exigence

#### 8.1.7 Politique d'OID du certificat

Tous les certificats contiennent l'OID défini au § 2.6

### 8.2 Profil de la Liste des Certificats Révoqués (LCR)

#### 8.2.1 CRL binaire

Les LCR de l'AC « AC CHAMBERSIGN RESEAU DE CONFIANCE - CSF - SIGNATURE NUMERIQUE» sont conforme à la RFC 3280 – « Internet X.509 Public Key Infrastucture Certiticate and CRL Profile » et contiennent les champs suivants :

- Version : la version de la LCR,
- SerialNumber : numéro de série de la LCR,
- Signature : l'identifiant de l'algorithme de signature de l'AC soit MD5RSA,
- Issuer : le nom de l'AC émettrice qui signe les certificats soit "Autorité consulaire",
- Validity : validité de LCR
- ThisUpdate : date de génération de la LCR,
- NextUpdate : prochaine date à laquelle cette LCR sera mise à jour,
- RevokedCertificates : liste des numéros de série des certificats révoqués,
  - UserCertificate : numéro de série de certificat révoqué,
  - RevocationDate : date à laquelle un certificat donné a été révoqué.

#### 8.2.2 OCSP

Les serveurs OCSP de l'AC fabriquent des jetons conformes à la RFC 2560.

# 9 Politique Administrative

Ce chapitre décrit les exigences en matière d'administration et de gestion de la Politique de Certification

## 9.1 Modification des spécifications

Les seuls changements qui ne requièrent pas d'informations sont éditoriaux, corrections typographiques ou de changement des détails des contacts.

### 9.1.1 Liste des items

a) Tous les items de cette PC peuvent être changés avec une information avec un préavis de trois mois
b) Les changements d'items qui n'ont pas d'impact substantiel sur les abonnés, les titulaires et/ou les Tiers utilisateurs peuvent être changés avec un préavis de 30 jours

### 9.1.2 Méthode de diffusion des avis

L'AC avertit les titulaires des modifications par courrier électronique.

Les spécifications modifiées sont publiées sur le site Internet de l'AC.

### 9.1.3 Période de commentaire

Les personnes souhaitant commenter sur les modifications doivent faire parvenir leurs commentaires au responsable de la politique dans des délais inférieurs à la moitié des délais de préavis fixés au § 9.1.2.

### 9.1.4 Traitement des commentaires

Aucune exigence particulière.

### 9.1.5 Modifications nécessitant l'adoption d'une nouvelle politique

Si un changement de politique a, selon l'évaluation du responsable de la politique, un impact majeur sur un nombre important de titulaires et/ou des Tiers utilisateurs, le responsable de la politique peut, à sa discrétion, instituer une nouvelle politique avec un nouvel identificateur d'objet (OID).

## 9.2 Publication et procédures de notification

### 9.2.1 Copie de la politique de certification

Une copie de PC est disponible sous forme électronique sur le site de **CHAMBERSIGN FRANCE** :
http://www.chambersign.tm.fr/pc/ac_csf_reseau_de_confiance/sn/

## 9.3 Procédure d'approbation de la DPC

Ces points sont précisés au § 3.6.

# 10 ANNEXES

## 10.1 Annexe 1 : Documents de référence

| | |
|---|---|
| DIR_EU_SIGN | Directive 1999/93/EC du parlement européen et du conseil du 13 décembre 1999 sur un cadre commun pour les signatures électroniques. |
| Textes français | • Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de signature électronique,<br>• Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique,<br>• Projet de loi Informatiques et Libertés du 18 juillet 2001 |
| DIR_EU_PRIV | Directive 95/46/EC du parlement européen et du conseil du 24 octobre 1995 sur la protection des individus en ce qui concerne le traitement des données personnelles et leur libre circulation. |
| CNIL | Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ETSI TS 101 862 V1.1.1 (2000-12) Qualified certificate Profile |
| ISO 6523 | La norme ISO 6523 est relative aux technologies de l'information et à la structure pour l'identification des organisations et des parties d'organisations. |
| ITU-T X.509v3, ISO/IEC 9594-8 | Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, Recommendation X.509. |
| PC² | Procédures et politiques de certification de clés, CISSI, version 2.2 de Janvier 2001. |
| RFC 2459 | Internet X.509 Public Key Infrastructure Certificate and CRL Profile |
| RFC 2527 | Certificate Policy and Certification Practices Framework |
| RFC 2560 | X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP |
| RFC 3280 | Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, RFC 3280 April 2002 |
| RFC 822 | Standard for the format of Arpa internet text messages, August 13, 1982, Revised by David H. Crocker |