Politique de certification des certificats d'AC

ChamberSign France CA3 NG RGS

Objet du document :	Ce document décrit les exigences que respecte l'Autorité de Certification mis en œuvre par ChamberSign France dans le cadre de ses activités de services de confiance
Version	03
Date de diffusion	04/03/2021
Type de diffusion	Public

SOMMAIRE

Avertissement

1. Introduction

1.1. Présentation générale

Le présent document est lié à l'Infrastructure de Gestion de Clés (ci-après dénommée « IGC ») de ChamberSign France (ci-après dénommée « CSF »). Cette IGC est en charge de la gestion des certificats de la hiérarchie « AC ChamberSign France CA3 » (également dénommée « IGC »).

Sa structure est conforme au document [RFC3647].

L'objectif de ce document est de définir les engagements de CSF, via l'IGC, dans la délivrance et la gestion des certificats, pour le type mentionné ci-dessus, tout au long de leur cycle de vie.

Ces politiques constituent le fondement des relations de l'IGC avec l'extérieur : utilisateurs (porteurs et accepteurs de certificats), mais également partenaires (autres IGC que CSF souhaite reconnaître et desquelles il souhaite être reconnu), autorités publiques et organismes privés d'évaluation et de reconnaissance (qualification, référencement, etc.).

Cependant, compte tenu de la complexité des éléments à la fois techniques et juridiques contenus dans une Politique de Certification (ci-après dénommée « PC »), notamment pour des utilisateurs non-spécialistes, ces politiques sont traduites dans des documents spécifiques à destination des utilisateurs que sont les Conditions Générales d'Utilisation (ci-après dénommées « CGU »). Elles sont complétées par un PKI Disclosure Statement décrit dans le document [RFC3647] en langue anglaise.

Les engagements arrêtés dans les présentes PC correspondent :

- aux exigences imposées à CSF par la réglementation en vigueur ;
- aux objectifs que se fixe CSF en matière de services, de sécurité, de qualité et de performances afin de satisfaire les utilisateurs (porteurs et accepteurs) de ses certificats et d'être reconnue, si nécessaire, par les différents schémas d'évaluation / référencement en matière d'IGC.

Les présentes PC, comme les autres PC de CSF, sont des documents publics. La Déclaration des Pratiques de Certification (ci-après dénommée « DPC ») correspondant à ces PC est un document accessible librement sur simple demande formulée auprès de CSF. Les autres documents qui découlent de ces PC et de la DPC sont des documents internes à CSF qui peuvent être accessibles, si besoin, moyennant un accord de confidentialité (auditeurs externes, organismes de qualification, autorités publiques, etc.).

CSF est assujettie aux lois et règlements en vigueur en France.

Ce document constitue la Politique de Certification (PC) de cette IGC pour les certificats de personnes physiques et morales visant la conformité avec le Référentiel Général de Sécurité (ci-après RGS) selon les modalités de l'Agence Nationale de la Sécurité des Systèmes d'Information qui est l'autorité Française de supervision.

1.2. Identification

La désignation de numéro d'identification d'objet (OID) pour la présente PC :
- 1.2.250.1.96.1.8.1.1 : Certificats d'authentification ** RGS personne physique
- 1.2.250.1.96.1.8.1.2 : Certificats d'authentification *** RGS personne physique
- 1.2.250.1.96.1.8.1.3 : Certificats de signature ** RGS personne physique
- 1.2.250.1.96.1.8.1.4 : Certificats de signature *** RGS personne physique

- 1.2.250.1.96.1.8.1.5 : Certificats d'authentification et de signature * RGS personne physique
- 1.2.250.1.96.1.8.1.6 : Certificats d'authentification et de signature ** RGS personne physique
- 1.2.250.1.96.1.8.1.7 : Certificats de personne morale RGS 1*
- 1.2.250.1.96.1.8.1.8 : Certificats de personne morale RGS 2*
- 1.2.250.1.96.1.8.1.9 : Certificats d'authentification personne morale client/serveur RGS 1*

1.3. Entités intervenant dans l'IGC

Il est distingué les intervenants externes à l'IGC et les intervenants internes à l'IGC. Seuls les intervenants internes sont sous la responsabilité de CSF.

Les intervenants internes sont décrits dans la déclaration des pratiques de certification liée aux présentes PC. Ces intervenants réalisent la mise en œuvre des fonctions suivantes :

- **Fonction d'enregistrement des porteurs** - Cette fonction vérifie les informations d'identification du futur porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction de génération des certificats. Cette fonction a également en charge, lorsque cela est nécessaire, la re-vérification des informations du porteur lors du renouvellement du certificat de celui-ci.
- **Fonction de génération des certificats** - Cette fonction génère les certificats (création du format, signature électronique avec la clé privée de l'AC) à partir des informations transmises par la fonction d'enregistrement, y compris la clé publique du porteur.
- **Fonction de génération des éléments secrets du porteur** – L'IGC ne génère aucun des éléments secrets concernant le porteur (clé privée, code d'activation du support cryptographique, …), à l'exception du code de déblocage d'un support cryptographique lorsque celui-ci a été bloqué par le porteur après plusieurs essais du code d'activation.
- **Fonction de remise au porteur** - Cette fonction remet au porteur le support cryptographique ; qui doit conserver les clés secrètes et lui remet le ou les certificats correspondants.
- **Fonction de publication** - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'IGC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle met également à disposition les certificats valides des porteurs.
- **Fonction de gestion des révocations** - Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.
- **Fonction d'information sur l'état des certificats** - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR).

Les intervenants externes sont :

- **Porteur ou Porteurs de certificats** - désigne une personne physique identifiée dans un certificat de personne physique objet de la PC et fourni par l'IGC. Cette personne utilise sa clé privée et le certificat correspondant dans le cadre de ses activités professionnelles en relation avec l'entité identifiée dans le certificat et avec laquelle elle a un lien contractuel, hiérarchique ou réglementaire. Conformément aux CGU que le porteur signe, si l'entité ne l'interdit pas, le porteur peut utiliser son certificat pour des usages non professionnels et en ne revendiquant que la certification de ses nom et prénoms présents dans le certificat. Le Porteur peut également être désigné sous le nom de « demandeur de certificat » avant la délivrance du certificat.

- **Responsable de certificats (RCC)** - Désigne une personne physique qui représente l'entité au nom de laquelle le certificat de cachet a été délivré. Ce responsable est en charge de gérer le certificat généré conformément aux exigences de la PC. Il fait mettre en œuvre la clé privée et le certificat correspondant dans le cadre de ses activités en relation avec l'entité identifiée dans le certificat et avec laquelle le Responsable de Certificat a un lien contractuel, hiérarchique ou réglementaire.
- **Représentant légal** – Il s'agit d'un représentant légal de l'entité identifiée dans le certificat et à laquelle le porteur est rattaché.
- **Utilisateurs de certificats** - Un utilisateur de certificat est une personne physique ou une entité technique (application informatique, équipement réseau, …) qui se fie à un certificat objet des présentes PC pour mettre en œuvre le service de sécurité correspondant (vérification d'une authentification, vérification d'une signature électronique),
- **Entités d'audit / de qualification / de référencement** – Ces entités sont amenées à auditer tout ou partie de l'IGC, soit à la demande d'un client de CSF, soit à la demande de CSF (en vue de l'obtention d'une qualification ou d'un label), soit à la demande d'autorités publiques.
- **Autorités publiques** – Il s'agit d'entités administratives ou gouvernementales qui peuvent être amenées, en conformité avec les lois et règlementations applicables, à accéder à tout ou partie des systèmes et informations de l'IGC.

Dans le cadre de ses fonctions opérationnelles, les exigences qui incombent à CSF en tant que responsable de l'ensemble de l'IGC sont les suivantes :

- Être une entité légale au sens de la loi française.
- Rendre accessible l'ensemble des prestations déclarées dans les présentes PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux porteurs, aux utilisateurs de certificats, ceux qui mettent en œuvre ses certificats.
- S'assurer que les exigences des présentes PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans les présentes PC, correspondant au minimum aux fonctions obligatoires des présentes PC, notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats.
- Mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. La DPC est élaborée en fonction de cette analyse.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans les présentes PC, notamment en termes de fiabilité, de qualité et de sécurité.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats et de LCR), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux porteurs et utilisateurs de certificats.
- Être en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats des porteurs de cette entité.

1.4. Usage des certificats

1.4.1. Domaines d'utilisation applicables

OID applicables	Usage	Description
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.2	Authentification	L'usage est l'authentification des porteurs auprès de serveurs distants ou auprès d'autres personnes. Il peut s'agir d'authentification dans le cadre d'un contrôle d'accès à un serveur ou une application, ou de l'authentification de

		l'origine de données dans le cadre de la messagerie électronique. Nota : L'authentification ne constitue pas une signature au sens juridique du terme, car elle ne signifie pas que le porteur manifeste son consentement sur les données échangées (la garantie de non répudiation n'est donc pas offerte).
1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.4	Signature	L'usage est la signature électronique de données par le porteur du certificat (signataire). Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données..
1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.6	Double usage	Les usages sont : - la signature électronique de données par le porteur du certificat (signataire). Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données. - l'authentification des porteurs auprès de serveurs distants ou auprès d'autres personnes. Il peut s'agir d'authentification dans le cadre d'un contrôle d'accès à un serveur ou une application, ou de l'authentification de l'origine de données dans le cadre de la messagerie électronique. Nota : L'authentification ne constitue pas une signature au sens juridique du terme, car elle ne signifie pas que le porteur manifeste son consentement sur les données échangées (la garantie de non répudiation n'est donc pas offerte).
1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.8	Personne morale	L'usage est la signature au nom d'une entité morale ou d'une application. Le cachet permet d'attester de l'identité de l'entité légale pour laquelle le certificat a été émis. Il garantit également l'intégrité des données qui sont signées par le cachet.
1.2.250.1.96.1.8.1.9	Authentification serveur	L'usage est l'authentification d'un serveur sur la base de son nom de domaine. Le certificat d'authentification serveur permet à toute application utilisatrice de s'assurer de l'identité de l'entité légale et du nom de domaine pour lesquels le certificat a été émis. Il garantit également l'intégrité des données qui sont échangées entre l'application utilisatrice et le serveur.

Par ailleurs, CSF peut être amenée à émettre des certificats de test. Ces certificats de test sont identifiés comme tels dans leur DN par la mention explicite TEST. Ils ne sont couverts d'aucune garantie par CSF et ils ne doivent en aucun cas être utilisés à d'autres fins qu'à des fins de test. A la fin des phases de tests, ces certificats sont révoqués.

1.4.2. Domaines d'utilisation interdits

Toute utilisation d'un certificat autre que celles prévues dans le cadre de la présente PC et des CGU applicables est interdite. En cas de non-respect de cette interdiction, la responsabilité de CSF ne saurait être engagée.

1.5. Gestion de la PC

1.5.1. Entité gérant la PC

CSF, en tant que prestataire de services de certification, est responsable de la gestion de la présente PC.

Le processus d'évolution et d'amendements à la présente PC est précisé au chapitre 9.12 ci-dessous.

1.5.2. Point de contact

Toute question ou remarque concernant la présente PC peut être adressée par courriel à l'adresse suivante : qualite@chambersign.fr.

1.5.3. Entité déterminant la conformité d'une DPC avec cette PC

La détermination qu'une DPC réponde ou non aux exigences de la présente PC est prononcée par la Direction de CSF.

1.5.4. Procédures d'approbation de la conformité de la DPC

La procédure d'approbation de la conformité d'une DPC est identifiée dans la DPC concernée.

1.6. Définitions et acronymes

1.6.1. Acronymes

A
AC Autorité de Certification
ANSSI Agence Nationale de la Sécurité des Systèmes d'Information (Française)

C
CC Critères Communs
CCI Chambre de Commerce et d'Industrie
CGU Conditions Générales d'Utilisation
CODIR Comité de Direction de ChamberSign
CSF ChamberSign France

D
DPC Déclaration des Pratiques de Certification

I
IGC Infrastructure de Gestion de Clés.

L
LAR Liste des certificats d'AC Révoqués

LCR Liste des Certificats Révoqués

M
MC Mandataire de certification

O
OCSP Online Certificate Status Protocol
OID Object Identifier

P
PC Politique de Certification
PDS PKI (Public Key Infrastructure) Disclosure Statement
PIN Personnal Identification Number
PP Profil de Protection
PSCE Prestataire de Services de Certification Electronique

Q
QCP Qualified Certificate Policy
QSCD Qualified electronic Signature/Seal Creation Device

R
RCC Responsable de certificats
RGPD Règlement Général sur la Protection des Données du 14 avril 2016
RGS Référentiel Général de Sécurité
RL Représentant Légal
RSA Rivest Shamir Adelman

U
URL Uniform Resource Locator

1.6.2. Définitions

A

Accepteur
Toute entité (personne physique, personne morale ou application informatique) acceptant un certificat qui lui est soumis et qui doit en vérifier l'authenticité et la validité.

Autorité de Certification (AC)
Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ « issuer » du certificat), dans les certificats émis au titre de cette politique de certification.

Autorité de Certification racine
AC prise comme référence par une communauté d'utilisateurs (incluant d'autres AC). Elle est un élément essentiel de la confiance qui peut lui être accordée dans un contexte donné.

B

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

C

Certificat
Ensemble d'informations d'un utilisateur, y compris la clé publique, rendu infalsifiable par le chiffrement, avec la clé secrète de l'AC qui l'a délivré, d'un condensat calculé sur l'ensemble de ces informations. Un certificat contient des informations telles que :

- l'identité du porteur de certificat ;
- la clé publique du porteur de certificat ;
- usage(s) autorisé(s) de la clé ;
- la durée de vie du certificat ;
- l'identité de l'AC qui l'a émis ;
- la signature de l'AC qui l'a émis.

Un format standard de certificat est défini dans la recommandation X.509 v3.

Contrôle de conformité
Action qui consiste à réaliser un examen le plus exhaustif possible afin de vérifier l'application stricte des procédures et de la réglementation au sein d'un organisme.

D

Déclaration des Pratiques de Certification (DPC)
Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers afin de respecter la ou les politiques de certification qu'elle a promulguée(s).

Données d'activation
Données privées associées à un porteur permettant de mettre en œuvre sa clé privée.

E

Enregistrement
Action qui consiste pour une autorité à valider une demande de certificat, conformément à une politique de certification.

G

Génération (émission) d'un certificat
Action qui consiste pour l'AC à intégrer les éléments constitutifs d'un certificat, à les contrôler et à signer le certificat.

I

Infrastructure de gestion de clés (IGC)
Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

J

Journalisation
Fait d'enregistrer dans un fichier dédié à cet effet certains types d'événements provenant d'une application ou d'un système d'exploitation d'un système informatique. Le fichier résultant facilite la traçabilité et l'imputabilité des opérations effectuées.

M

Mandataire de certification (MC)
Un MC est une personne physique qui est désignée par et placée sous la responsabilité d'une entité cliente afin de réaliser une grande partie du processus d'enregistrement des porteurs de cette entité cliente : constitution du dossier incluant le recueil des pièces justificatives, la signature du titulaire et sa propre signature de la commande au titre de l'entité puis la transmission au BE pour validation. Ensuite, réalisation du face-à-face et remise du support cryptographique personnalisé au titulaire (Porteur et RCC) le cas échéant.
Le MC est authentifié au moyen de son certificat électronique délivré en face à face auprès d'un BE ChamberSign. Il est habilité à effectuer la révocation des certificats concernant les titulaires de son entité.

O

Online Certificate Status Protocol (OCSP)
OCSP est un protocole Internet utilisé pour valider un certificat numérique X.509. OCSP est standardisé par l'IETF dans la RFC 6960.

Ce protocole est une alternative réglant certains des problèmes posés par les listes de révocation de certificats (CRL) dans une infrastructure à clés publiques (PKI). Les communications OCSP étant de la forme « requête/réponse », les serveurs OCSP sont appelés répondeurs OCSP.

P

Politique de certification (PC)
Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC déclare se conformer dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Porteur ou Porteurs de certificats
Désigne une personne physique identifiée dans un certificat de personne physique objet de la PC et fourni par l'IGC. Cette personne utilise sa clé privée et le certificat correspondant dans le cadre de ses activités professionnelles en relation avec l'entité identifiée dans le certificat et avec laquelle elle a un lien contractuel, hiérarchique ou réglementaire. Conformément aux CGU que le porteur signe, si l'entité ne l'interdit pas, le porteur peut utiliser son certificat pour des usages non professionnels et en ne revendiquant que la certification de ses nom et prénoms présents dans le certificat.
Le Porteur peut également être désigné sous le nom de « demandeur de certificat » avant la délivrance du certificat.
Ce terme peut aussi désigner la personne physique en charge d'un certificat de personne morale, notion de RCC.

Prestataire de Services de Certification Electronique (PSCE)
Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC

Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ « issuer » du certificat.

Publication d'un certificat
Fait d'inscrire un certificat dans un annuaire, à disposition d'utilisateurs susceptibles d'avoir à vérifier une signature ou à chiffrer des informations.

R

Renouvellement de certificat
Action effectuée à la demande d'un utilisateur ou en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat pour un porteur.

Responsable de certificats (RCC)
Désigne une personne physique qui représente l'entité au nom de laquelle le certificat de cachet a été délivré. Ce responsable est en charge de gérer le certificat généré conformément aux exigences de la PC. Il fait mettre en œuvre la clé privée et le certificat correspondant dans le cadre de ses activités en relation avec l'entité identifiée dans le certificat et avec laquelle le Responsable de Certificat a un lien contractuel, hiérarchique ou réglementaire.

Révocation de certificat
Action demandée par une entité autorisée (AC, MC, Porteur de certificat, etc.) et dont le résultat est la suppression de la caution de l'AC sur un certificat donné, avant la fin de sa période de validité. Cette action peut être la conséquence de différents types d'événements tels que la perte de la carte, la compromission d'une clé, le changement d'informations contenues dans un certificat, etc.

S

Service de Publication
Le Service de Publication rend disponible les certificats de clés publiques émis par une AC, à l'ensemble des utilisateurs potentiels de ces certificats. Il publie une liste de certificats reconnus comme valides et une liste de certificats révoqués (LCR). Ce service peut être rendu par un annuaire (par exemple de type X.500), un serveur d'information (Web), une délivrance de la main à la main, une application de messagerie, etc.

T

Titulaire
Désigne soit le porteur pour une personne physique, soit une personne morale, représentée par le RCC, au nom duquel un certificat cachet a été délivré.

U

Utilisateur Final
Porteur ou accepteur de certificat.

V

Vérification de certificat
La procédure de vérification d'un certificat consiste en un ensemble d'opérations destinées à s'assurer que les informations contenues dans le certificat ont été validées par une AC de confiance. La vérification d'un certificat inclut la vérification de sa période de validité, de son état (révoqué ou non), ainsi que de la signature de l'AC génératrice.

Vérification de signature

La vérification d'une signature consiste à déchiffrer la signature d'un message, en mettant en œuvre la clé publique du signataire supposé. Si le clair obtenu est identique à l'empreinte calculée à partir du message reçu, alors il est garanti que le message est intègre et qu'il a été signé par le porteur de la clé privée correspondante à la clé publique utilisée pour la vérification.

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

2.1. Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des utilisateurs (porteurs et accepteurs), CSF met en œuvre au sein de son IGC un service de diffusion et un service d'état des certificats.

Le service de diffusion s'appuie sur un serveur Web, accessible en HTTPs à l'adresse www.chambersign.fr.

Le service d'état des certificats s'appuie sur la génération de LCR et leur publication sur le site Web.

Les engagements de disponibilité et de continuité d'activité de ces services (serveur Web et générateur de LCR) sont précisés au chapitre 4.9 ci-dessous.

2.2. Informations devant être publiées

Les informations suivantes sont diffusées via le site Web de CSF :

- les présentes PC ;
- les CGU ;
- les formats de certificats et de LCR objet des présentes PC ;
- les LCR et LAR ;
- les certificats d'AC.

Les PC, CGU et les formats de certificats et de LCR sont validés par le Responsable de l'Autorité de Certification avant leur publication.

2.3. Délais et fréquences de publication

Les informations liées à l'IGC (PC, CGU, etc.) sont publiées dès leur validation par la direction de CSF.
La disponibilité des systèmes publiant ces informations est assurée pendant les jours ouvrés. La disponibilité des systèmes publiant les certificats d'AC est assurée 24h/24 et 7j/7.
Les LAR sont émises tous les ans. Elles sont signées par l'AC racine en Key Ceremony. Les LCR sont publiées au moins une fois par jour, dans la pratique une fois toutes les heures.

2.4. Contrôle d'accès aux informations publiées

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort (basé sur une authentification au moins à deux facteurs).

3. Identification et authentification

3.1. Nommage

3.1.1. Convention de noms

Pour les personnes physiques :

Champ	Description
DN	encodé en UTF8String
countryName	code ISO sur 2 lettres (cf. ISO3166-1) du pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère, …)
organizationName	nom officiel de l'entité (dénomination sociale du siège social)
organizationalUnitName	identifiant national de la structure parmi : • Pour les entités basées en France Métropolitaine et les DOM : 0002 <<N° SIRET sur 14 caractères>> • Pour les entités basées en Nouvelle-Calédonie : S540 <<N° RIDET sur 9 caractères maximum>> • Pour les autres entités basées dans un pays de la communauté européenne : S<<code ISO3166-1 du pays sur 3 chiffres>> <<n° de TVA intracommunautaire sur 14 caractères maximum>> Le champ peut être itéré 3 fois
organizationIdentifier	Numéro d'immatriculation officiel du prestataire conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « SI:FR- » suivi du numéro SIREN ou SIRET Identifiant de l'entité avec laquelle le porteur est en lien • VAT<code pays>-<numéro de TVA intracommunautaire> • NTR<code pays>-<numéro de SIREN>
locality	ville où se trouve l'établissement du porteur
surName	Nom du porteur
givenName	Prénom1(,Prénom2,Prénom3,…) Les différents prénoms sont mentionnés dans l'ordre indiqué sur la pièce d'identité présentée lors de l'enregistrement et dont la copie est conservée dans le dossier d'enregistrement.
commonName	Prénom1(,Prénom2,Prénom3,…) NOM Les différents prénoms sont mentionnés dans l'ordre indiqué sur la pièce d'identité présentée lors de l'enregistrement et dont la copie est conservée dans le dossier d'enregistrement.
title	le cas échéant, fonction du porteur au sein de sa structure
serialNumber	numéro séquentiel de 4 chiffres permettant de traiter les cas d'homonymie Par défaut, la valeur de cet attribut est « 0001 ». Si un porteur dont tous les autres attributs du DN sont identiques (countryName, organizationName, organizationIdentifier, organizationalUnitName et commonName) a déjà été enregistré, la valeur de l'attribut serialNumber pour le nouveau porteur passe à « 0002 » et ainsi de suite.

Pour les personnes morales :

Champ	Description
DN	encodé en UTF8String
countryName	code ISO sur 2 lettres (cf. ISO3166-1) du pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère,…)
organizationName	nom officiel de l'entité (dénomination sociale du siège social)
organizationalUnitName	identifiant national de la structure parmi : • Pour les entités basées en France Métropolitaine et les DOM : 0002 <<N° SIRET sur 14 caractères>> • Pour les entités basées en Nouvelle-Calédonie : S540 <<N° RIDET sur 9 caractères maximum>> • Pour les autres entités basées dans un pays de la communauté européenne : S<<code ISO3166-1 du pays sur 3 chiffres>> <<n° de TVA intracommunautaire sur 14 caractères maximum>> Le champ peut être itéré 3 fois
organizationIdentifier	Numéro d'immatriculation officiel du prestataire conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « SI:FR- » suivi du numéro SIREN ou SIRET Identifiant de l'entité avec laquelle le porteur est en lien • VAT<code pays>-<numéro de TVA intracommunautaire> • NTR<code pays>-<numéro de SIREN>
locality	ville où se trouve l'établissement du porteur
commonName	FQDN du service ou nom du cachet
serialNumber	numéro séquentiel de 4 chiffres permettant de traiter les cas d'homonymie Par défaut, la valeur de cet attribut est « 0001 ». Si un porteur dont tous les autres attributs du DN sont identiques (countryName, organizationName, organizationIdentifier, organizationalUnitName et commonName) a déjà été enregistré, la valeur de l'attribut serialNumber pour le nouveau porteur passe à « 0002 » et ainsi de suite.

3.1.2. Nécessité d'utilisation de noms explicites

Les noms utilisés dans les champs "issuer" et "subject" d'un certificat de porteur sont explicites dans le domaine de certification de CSF (utilisation des identifiants nationaux de structure SIREN/SIRET, utilisation des noms et prénoms des porteurs, etc.).

3.1.3. Anonymisation ou pseudonymisation des porteurs

L'anonymisation ou la pseudonymisation ne sont pas autorisées dans le cadre de la présente PC.

3.1.4. Règles d'interprétation des différentes formes de nom

Les significations des différents champs du DN, aussi bien de l'"issuer" que du "subject", sont décrites dans [GUI.ACC.11].

3.1.5. Unicité des noms

Dans chaque certificat produit, le DN du champ "issuer" (AC émettrice) et du champ "subject" (AC ou porteur) est unique sur le domaine de certification de CSF.

3.1.6. Identification, authentification et rôle des marques déposées

Il n'y a pas d'utilisation dans un certificat de nom de marque autres que le nom de l'organisme correspondant, tel que mentionné sur les documents officiels faisant l'objet d'une vérification lors des procédures d'enregistrement (Kbis, etc.).

3.2. Validation initiale de l'identité

3.2.1. Méthode pour prouver la possession de la clé privée

Les fichiers de demande de certificat, contenant la clé publique à certifier, sont scellés à l'aide de la clé privée correspondante.

3.2.2. Validation de l'identité d'un organisme

Les informations concernant la structure à laquelle le porteur est rattaché font l'objet de vérification lors de l'enregistrement (existence, validité, etc.).

3.2.3. Validation de l'identité d'un individu

OID applicables	Description
1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.9	L'identité du porteur ou du responsable de certificat est vérifiée au travers de la vérification de documents, dont une copie certifiée conforme par le porteur est transmise par courrier.
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.2 1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.4 1.2.250.1.96.1.8.1.6 1.2.250.1.96.1.8.1.8	L'identité du porteur ou du responsable de certificats est vérifiée au travers de la vérification de documents officiels d'identité effectuée lors d'un face-à-face.

3.2.4. Informations non vérifiées du porteur

Toutes les informations concernant les informations du champ sujet dans ces certificats font l'objet de vérifications.

3.2.5. Validation de l'autorité du demandeur

Cette étape est effectuée en même temps que la validation de l'identité de l'organisme.

3.2.6. Critères d'interopérabilité

La décision que l'IGC de CSF reconnaisse et/ou soit reconnue par une autre IGC est du ressort du Conseil d'Administration de CSF.

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

OID applicables	Description
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.6 1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.8 1.2.250.1.96.1.8.1.9	Le premier renouvellement, s'il est autorisé par la réglementation au moment de l'expiration du certificat à renouveler, est réalisé en ligne s'il a lieu avant la date d'expiration du présent certificat. Le porteur valide en ligne que les informations liées au certificat à renouveler sont toujours exactes. Le renouvellement suivant est réalisé suivant la procédure d'enregistrement initial. Le renouvellement suite à révocation est réalisé suivant la procédure d'enregistrement initial.
1.2.250.1.96.1.8.1.2 1.2.250.1.96.1.8.1.4	Le premier renouvellement, s'il est autorisé par la réglementation au moment de l'expiration du certificat à renouveler, est réalisé en ligne s'il a lieu avant la date d'expiration du présent certificat. Le porteur valide en ligne que les informations liées au certificat à renouveler sont toujours exactes. Le

	renouvellement suivant est réalisé suivant la procédure d'enregistrement initial. Le renouvellement suite à révocation est réalisé suivant la procédure d'enregistrement initial.

3.4. Identification et validation d'une demande de révocation

Toute demande de révocation fait l'objet d'une authentification du demandeur et d'une vérification de son autorité pour une telle demande.

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

Les dossiers de demandes de certificats proviennent soit :

- du futur porteur,
- du responsable de certificat,
- du représentant légal de l'entité concernée,
- d'un mandataire de certification de cette entité.

4.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat

L'établissement d'une demande de certificat est de la responsabilité de l'entité dont dépend le futur porteur ou le responsable de certificat.

4.2. Traitement d'une demande de certificat

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

Le service d'enregistrement de l'IGC s'assure de l'origine, de l'intégrité et de la cohérence de la demande transmise (cf. chapitre 3.2).

4.2.2. Acceptation ou rejet de la demande

Ensuite, si aucun problème n'est détecté, il valide les informations contenues dans la demande et transmet cette dernière au service de génération des certificats.

4.2.3. Durée d'établissement du certificat

Dès la demande de certificat reçue par le service de génération des certificats, le certificat est établi.

4.3. Délivrance du certificat

4.3.1. Actions de l'AC concernant la délivrance du certificat

OID applicables	Description
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.2 1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.4 1.2.250.1.96.1.8.1.6 1.2.250.1.96.1.8.1.8	Suite à validation du dossier de demande de certificat par la fonction d'enregistrement de l'IGC, le processus consiste à remettre au porteur ou au responsable de certificat en mains propres, un support cryptographique vierge, identifié de façon unique et lié au porteur, qui fera l'objet d'une personnalisation sous le contrôle du porteur : personnalisation du code d'activation (code PIN), génération de la bi-clé dans le support, envoi de la clé publique à la fonction de génération

	des certificats, téléchargement sur le support du certificat généré.
1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.9	Suite à validation du dossier de demande de certificat par la fonction d'enregistrement de l'IGC, le processus consiste à remettre au porteur ou au responsable de certificat la clé publique certifiée par l'AC : génération de la bi-clé, sous le contrôle et la responsabilité du porteur, dans un support cryptographique (logiciel ou matériel) choisi par le porteur ou le responsable de certificat (moyennant le respect des exigences définies au chapitre 6.2 ci-dessous), envoi de la clé publique à la fonction de génération des certificats, téléchargement sur le support du certificat généré.

4.3.2. Notification par l'AC de la délivrance du certificat au porteur

Le certificat est remis au porteur ou au responsable de certificat au moment de la personnalisation de son support.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

OID applicables	Description
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.2 1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.4 1.2.250.1.96.1.8.1.6 1.2.250.1.96.1.8.1.8	Le certificat fait l'objet d'une acceptation explicite par le porteur ou le responsable de certificats au moment de sa remise. Le porteur est amené à valider le contenu de son certificat en signant électroniquement l'attestation de délivrance via la saisie de son code PIN protégeant l'accès à la clé privée du certificat qui vient de lui être généré.
1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.9	Le certificat fait l'objet d'une acceptation implicite par le porteur ou le responsable de certificats suite à son téléchargement.

4.4.2. Publication du certificat

Les certificats objets des présentes PC ne font pas l'objet de publication par CSF.

4.4.3. Notification par l'AC aux autres entités de la délivrance du certificat

Les différentes composantes concernées de l'IGC sont informées de la délivrance du certificat via le système d'information de l'IGC.

4.5. Usages de la bi-clé et du certificat

4.5.1. Utilisation de la clé privée et du certificat par l'AC

L'utilisation de la clé privée et du certificat associé est limitée aux conditions d'usages définies dans les présentes PC (cf. § 1.4) et ceci conformément à l'utilisation spécifique décrite dans le contenu du certificat (attribut key usage et/ou extended key usage, cf. [GUI.ACC.11]).

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

L'utilisation d'une clé privée n'est autorisée que pendant la période de validité du certificat associé et vaut acceptation des conditions d'usages par le porteur.

4.5.2. Utilisation de la clé publique et du certificat par l'accepteur du certificat

L'utilisation du certificat et de la clé publique associée est limitée aux conditions d'usages définies dans les présentes PC (cf. § 1.4) et à l'usage prévu indiqué dans le certificat (attribut key usage et/ou extended key usage, cf. [GUI.ACC.11]).

Le porteur ou le responsable de certificat est tenu de vérifier la validité du certificat et la conformité de son utilisation.

4.6. Renouvellement d'un certificat

Un renouvellement de certificat sans renouvellement de la bi-clé correspondante est impossible. Une demande de renouvellement s'accompagne donc forcément de la génération d'une nouvelle bi-clé (cf. chapitre 4.7 ci-dessous). Ce chapitre n'est donc pas applicable.

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

4.7.1. Causes possibles de changement d'une bi-clé

La cause principale de la délivrance d'un nouveau certificat et de la bi-clé correspondante est l'arrivée à la date de fin de validité du certificat. La durée de validité des certificats CSF est de trois (3) ans. Les bi-clés doivent être en effet périodiquement renouvelées afin de minimiser les risques d'attaque cryptographique.

Un renouvellement peut être aussi réalisé de manière anticipée, suite à un événement ou un incident déclaré par le porteur, les plus fréquents étant la perte, le vol ou le dysfonctionnement du support cryptographique.

Une modification des informations contenues dans le certificat entraîne également la délivrance d'un nouveau certificat (avec renouvellement de la bi-clé).

La délivrance d'un nouveau certificat est réalisée de manière identique au processus de délivrance initiale. Seule la phase d'enregistrement peut différer pour un renouvellement (cf. chapitre 3.3).

4.7.2. Origine d'une demande d'un nouveau certificat

Cf. chapitres 4.1 à 4.4.

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

Cf. chapitres 4.1 à 4.4.

4.7.4. Notification au porteur de l'établissement du nouveau certificat

Cf. chapitres 4.1 à 4.4.

4.7.5. Démarche d'acceptation du nouveau certificat

Cf. chapitres 4.1 à 4.4.

4.7.6. Publication du nouveau certificat

Cf. chapitres 4.1 à 4.4.

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

Cf. chapitres 4.1 à 4.4.

4.8. Modification du certificat

La modification d'un certificat entraîne obligatoirement le renouvellement du certificat et de la bi-clé correspondante : cf. chapitre 4.7.

4.9. Révocation et suspension des certificats

Il n'y a pas de suspension possible de certificat. Seule la révocation définitive des certificats peut être réalisée.

OID applicables	Description
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.6 1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.8 1.2.250.1.96.1.8.1.9	CSF assure la disponibilité du statut de révocation à tout moment et au-delà de la période de validité du certificat en mettant en œuvre les mesures suivantes : • Publication sans limite de temps des certificats révoqués dans les LCR publiées.
1.2.250.1.96.1.8.1.2 1.2.250.1.96.1.8.1.4	CSF assure la disponibilité du statut de révocation à tout moment et au-delà de la période de validité du certificat en mettant en œuvre les mesures suivantes : • Publication sans limite de temps des certificats révoqués dans les LCR publiées ; • Conformité de la réponse OCSP, révoqué, en cas de sollicitation après la date de fin de vie du certificat.

4.9.1. Causes possibles d'une révocation

OID applicables	Description
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.2 1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.4 1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.6	Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat objet des présentes PC : • la clé privée du certificat est perdue, volée, inutilisable (dysfonctionnement du support), compromise ou suspectée de compromission (demande du porteur lui-même) ; • les informations ou les attributs du porteur figurant dans son certificat ne sont plus valides ou plus en cohérence avec l'utilisation prévue du certificat, ceci avant l'expiration normale du certificat ; • les algorithmes cryptographiques mis en œuvre sont obsolètes et ne sont plus considérés sûrs ; • il a été démontré que le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ; • le certificat d'AC est révoqué (ce qui entraîne la révocation des certificats signés par la clé privée correspondante) ; • le porteur ne satisfait plus aux conditions professionnelles requises (cessation d'activité, décès). • le porteur et/ou, le cas échéant, le MC / l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC ; • une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur. Les causes de révocation ne sont jamais publiées.

1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.8 1.2.250.1.96.1.8.1.9	Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat objet des présentes PC : • la clé privée du certificat est perdue, volée, inutilisable (dysfonctionnement du support), compromise ou suspectée de compromission (demande du responsable de certificat lui-même) ; • les informations figurant dans son certificat ne sont plus valides ou plus en cohérence avec l'utilisation prévue du certificat, ceci avant l'expiration normale du certificat ; • les algorithmes cryptographiques mis en oeuvre sont obsolètes et ne sont plus considérés sûrs ; • il a été démontré que le responsable du certificat n'a pas respecté les modalités applicables d'utilisation du certificat ; • le certificat d'AC est révoqué (ce qui entraîne la révocation des certificats signés par la clé privée correspondante) ; • le responsable du certificat a changé et n'a pas été remplacé. • le responsable du certificat et/ou, le cas échéant, le MC / l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC ; • une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du responsable du certificat. Les causes de révocation ne sont jamais publiées.

4.9.2. Origine d'une demande de révocation

Les entités qui peuvent demander la révocation d'un certificat objet des présentes PC sont les suivantes :

- le porteur au nom duquel le certificat a été émis ou le responsable de certificats associé ;
- le représentant légal ou le mandataire de l'entité dont dépend le porteur ;
- CSF.

4.9.3. Procédure de traitement d'une demande de révocation

La validation de la demande inclut la vérification de l'origine de la demande et de l'applicabilité de la cause invoquée. Après cette validation, le service de gestion des révocations transmet la demande au service d'état des certificats chargé d'ajouter les n° de série de certificats à révoquer dans les prochaines LCR à générer et à publier.

4.9.4. Délai accordé au porteur pour formuler la demande de révocation

La demande de révocation doit être formulée dès connaissance de l'évènement correspondant.

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

Les demandes de révocation sont traitées dans les 24h suivant la réception de la demande, 7 jours / 7 (week-ends et jours fériés compris), hors révocations consécutives à des demandes de modification des données du porteur.

La fonction de gestion des révocations est disponible 24 heures sur 24, 7 jours sur 7.

OID applicables	Description
1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.9	La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations est de 2h (jours ouvrés). La durée maximale totale d'indisponibilité

	par mois de la fonction de gestion des révocations est de 16h (jours ouvrés).
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.6 1.2.250.1.96.1.8.1.8	La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations est de 2h. La durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations est de 8h.
1.2.250.1.96.1.8.1.2 1.2.250.1.96.1.8.1.4	La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations est de 1h. La durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations est de 4h.

4.9.6. Exigences de vérification de la révocation par les accepteurs de certificats

OID applicables	Description
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.6 1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.8 1.2.250.1.96.1.8.1.9	Les accepteurs des certificats doivent vérifier la non-révocation des certificats sur lesquels ils vont baser leur confiance. Cette vérification se fait en consultant les LCR disponibles via le site Web de CSF. Les certificats révoqués restent présents dans la LCR même après leur date d'expiration d'origine.
1.2.250.1.96.1.8.1.2 1.2.250.1.96.1.8.1.4	Les accepteurs des certificats doivent vérifier la non-révocation des certificats sur lesquels ils vont baser leur confiance. Cette vérification se fait en consultant les LCR disponibles via le site Web de CSF, ou en interrogeant le service en ligne d'état des certificats (OCSP) qui intègre une réponse "certificat révoqué" après la date de fin de vie du certificat. Les certificats révoqués restent présents dans la LCR même après leur date d'expiration d'origine.

4.9.7. Fréquence d'établissement des LCR et des LAR et durée de validité des LCR et des LAR

Le service d'état des certificats publie une mise à jour quotidienne des LCR. Chaque LCR contient la date et l'heure prévisionnelles de publication de la LCR suivante.

Par mesure de sécurité, les LCR ont une durée de validité de 96 heures.

4.9.8. Délai maximum de publication d'une LCR

Le délai maximum de publication d'une LCR après sa génération est de 30 minutes.

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

Le service est disponible 24 heures / 24 et 7 jours / 7.

OID applicables	Description
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.6 1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.8 1.2.250.1.96.1.8.1.9	Un système de vérification en ligne (OCSP) n'est pas proposé.
1.2.250.1.96.1.8.1.2 1.2.250.1.96.1.8.1.4	Un système de vérification en ligne (OCSP) est mis en œuvre et répond aux mêmes exigences de sécurité, notamment en

	terme de disponibilité, que le système de publication des LCR.

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

Cf. chapitre 4.9.6.

4.9.11. Autres moyens disponibles d'information sur les révocations

Aucun autre moyen n'est mis en œuvre.

4.9.12. Exigences spécifiques en cas de compromission de la clé privée

Il n'y a pas de mesures particulières, concernant les clés privées des porteurs, autres que la révocation des certificats correspondants.

En cas de compromission de sa clé privée ou de connaissance de compromission de la clé privée de l'AC ayant émis son certificat, le porteur doit interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

4.9.13. Causes possibles d'une suspension

Les certificats ne peuvent être révoqués que de façon définitive. Il n'est pas envisagé de possibilité de révocation temporaire (suspension).

4.9.14. Origine d'une demande de suspension

N/A

4.9.15. Procédure de traitement d'une demande de suspension

N/A

4.9.16. Limites de la période de suspension d'un certificat

N/A

4.10. Service d'état des certificats

4.10.1. Caractéristiques opérationnelles

Les services permettant de connaître le statut des certificats sont mises à disposition librement et gratuitement via le site Web de CSF.

4.10.2. Disponibilité du service

OID applicables	Description
1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.9	La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction d'information sur l'état des certificats est de 8 heures. La durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des certificats est de 32 heures.
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.6 1.2.250.1.96.1.8.1.8	La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction d'information sur l'état des certificats est de 4 heures. La durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des certificats est de 16

	heures.
1.2.250.1.96.1.8.1.2 1.2.250.1.96.1.8.1.4	La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction d'information sur l'état des certificats est de 2 heures. La durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des certificats est de 8 heures. Le temps de réponse maximum du service OCSP à une requête reçue portant sur l'état d'un certificat est de 10 secondes à partir de la réception de la requête par le serveur.

4.10.3. Dispositifs optionnels

N/A.

4.11. Expiration de l'abonnement des porteurs

A l'expiration de l'abonnement des porteurs (notamment fin de l'activité ayant justifié l'attribution d'un certificat), le certificat est révoqué.

4.12. Séquestre de clé et recouvrement

N/A (les clés privées objets des présentes PC ne font l'objet d'aucun séquestre, elles ne sont pas exportables des dispositifs cryptographiques).

5. Mesures de sécurité non techniques

5.1. Mesures de sécurité physiques

CSF met en œuvre les mesures de sécurité physiques, au sein des différentes composantes de l'IGC, nécessaire pour assurer le fonctionnement sécurisé de ses services conformément aux engagements pris dans le présent document, notamment en termes de disponibilité (contrôle d'accès physique, services supports (alimentation électrique, climatisation, …), protection contre les dégâts des eaux, protection contre les incendies et protection des supports).

5.2. Mesures de sécurité procédurales

Au sein de chaque composante de l'IGC, des rôles fonctionnels de confiance sont identifiés et formellement attribués, en respectant des règles strictes de séparation des attributions.
Toute attribution d'un rôle et des droits correspondants fait l'objet d'une vérification préalable de l'identité et des autorisations correspondantes.
Pour la réalisation d'opérations, l'intervention de plusieurs personnes peut être requise.
CSF met en œuvre des rôles de porteurs de secrets qui ont pour responsabilité de recevoir, et conserver de manière sécurisée une part du secret nécessaire à la mise en œuvre de la chaîne d'AC.

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

Tous les personnels, internes et externes à CSF, amenés à travailler au sein de composantes de l'IGC sont soumis à des obligations de qualifications, de compétences, de formations initiales et continues et d'habilitations en fonction de leurs rôles.

L'honnêteté de ces personnels est vérifiée conformément à ce qui est autorisé par la loi.

5.4. Procédures de constitution des données d'audit

Les différents évènements liés au fonctionnement de l'IGC font l'objet d'une journalisation d'évènements enregistrée de façon manuelle ou automatique. Les fichiers résultants, sous forme papier ou électronique, rendent possible la traçabilité et l'imputabilité des opérations effectuées.
Ces journaux d'évènements sont datés, protégés et font l'objet d'un archivage. Ils sont régulièrement contrôlés afin d'évaluer les éventuelles vulnérabilités pesant sur l'IGC.

5.5. Archivage des données

Des dispositions en matière d'archivage, papier et électronique, sont prises afin d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC et d'autres données (dossier d'enregistrement, PC, DPC, certificats et LCR émis, …).
Les durées de conservation des archives sont précisées dans l'ensemble des CGU de CSF.

5.6. Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela, la période de validité de ce certificat de l'AC est supérieure à celle des certificats qu'elle signe.

5.7. Reprise suite à compromission et sinistre

Chaque entité opérant une composante de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements, y compris dans le cas d'incidents majeurs (compromission de clés privées, faiblesse des algorithmes utilisés, …). Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.
Chaque composante de l'IGC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant des engagements de CSF dans les présentes PC notamment en ce qui concerne les fonctions liées à la publication et à la révocation des certificats.
Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les engagements des présentes PC.
En cas de détection d'un incident de sécurité sur l'infrastructure de confiance, CSF s'engage à fournir les informations liées à cet incident en envoyant un message à l'adresse cert-fr.cossi@ssi.gouv.fr

5.8. Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC, ou la totalité de l'IGC, peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.
CSF mettra en œuvre les mesures requises pour assurer au minimum la continuité de l'archivage des informations et la continuité des services de révocation.
CSF a pris les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où CSF serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.
Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats, CSF les en avisera aussitôt que nécessaire et, au moins, sous le délai d'un mois. De même, CSF informera les autorités publiques concernées.

6. Mesures de sécurité techniques

6.1. Génération et installation de bi clés

OID applicables	Description
1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.9	Les bi-clés des porteurs sont générées sous forme logicielle.
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.2 1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.4 1.2.250.1.96.1.8.1.6 1.2.250.1.96.1.8.1.8	Les bi-clés des porteurs sont générées dans les supports cryptographiques matériels, remis par ChamberSign France, sous leur contrôle. Les clés publiques à certifier sont transmises protégées à l'IGC de manière à en garantir l'origine et à en assurer l'intégrité.

Le certificat racine de l'IGC est téléchargeable sur le site Web de ChamberSign.
L'utilisateur peut vérifier l'empreinte du certificat racine sur le site sécurisé https://www.keymanagement.chambersign.fr ou en contactant CSF par téléphone.

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

OID applicables	Description
1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.9	Le support utilisé doit être conforme aux exigences correspondantes du RGS pour le niveau 1*. Le porteur ou le responsable du certificat s'engage contractuellement auprès de CSF sur cette conformité. Les clés privées ne font l'objet d'aucun séquestre et d'aucune sauvegarde par CSF. Les supports cryptographiques contenant les clés privées doivent assurer la fonction de signature pour le porteur ou le serveur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers.
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.2 1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.4 1.2.250.1.96.1.8.1.6 1.2.250.1.96.1.8.1.8	Les supports cryptographiques font l'objet d'une qualification par l'ANSSI au niveau requis par le RGS. Les clés privées ne font l'objet d'aucun séquestre et d'aucune sauvegarde. Les supports cryptographiques contenant les clés privées ne sont activés que suite à la saisie d'un code d'activation (code PIN) entièrement maîtrisé par le porteur ou le responsable de certificat, qu'il doit garder secret.

6.3. Autres aspects de la gestion des bi-clés

Les clés publiques des porteurs sont archivées dans le cadre de l'archivage des certificats correspondants.
Les bi-clés et les certificats des porteurs ont une durée de vie de trois (3) ans.

6.4. Données d'activation

OID applicables	Description
1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.9	La PC ne prévoit aucune exigence, la bi-clé étant mise en œuvre par les responsables de certificats eux-mêmes et sous leur entière responsabilité.
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.2 1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.4 1.2.250.1.96.1.8.1.6 1.2.250.1.96.1.8.1.8	Les données d'activation correspondent aux codes PIN des supports cryptographiques, qui sont personnalisés par les porteurs lors de la personnalisation de leur support et qu'ils ne doivent communiquer à personne. Les différentes composantes de l'IGC n'ont à aucun moment connaissance de ce code.

6.5. Mesures de sécurité des systèmes informatiques

Au sein des différentes composantes de l'IGC, les mesures de sécurité relatives aux systèmes informatiques satisfont aux objectifs de sécurité qui découlent d'analyses de risques menées au niveau de chaque composante.

6.6. Mesures de sécurité des systèmes durant leur cycle de vie

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC est documentée. La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau sont documentées et contrôlées.
Les objectifs de sécurité sont définis lors des phases de spécification et de conception. Les systèmes et les produits utilisés sont fiables et sont protégés contre toute modification.

6.7. Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC. Les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et les configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par CSF.

6.8. Horodatage

La datation des évènements au sein de l'IGC utilise l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près. Pour les opérations faites hors ligne (ex : administration d'une AC Racine), cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système peut toutefois ordonner les évènements avec une précision suffisante.

7. Profils des certificats, OCSP et des LCR

OID applicables	Description
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.1.2 1.2.250.1.96.1.8.1.3 1.2.250.1.96.1.8.1.5 1.2.250.1.96.1.8.1.6 1.2.250.1.96.1.8.1.7 1.2.250.1.96.1.8.1.8 1.2.250.1.96.1.8.1.9	Les profils de certificats, de LCR sont définis dans le document [GUI.ACC.11].
1.2.250.1.96.1.8.1.4	Les profils de certificats, de LCR sont définis dans le document

	[GUI.ACC.11]. Les certificats produits contiennent les extensions qualifiées suivantes : - id-etsi-qcs-QcCompliance - id-etsi-qcs-QcSSCD - QcEuPDS

Les jetons OCSP sont signés par un certificat de la Sub : ChamberSign France CA3 NG RGS

8. Audit de conformité et autres évaluations

Le présent chapitre ne traite que les audits et évaluation de la responsabilité de CSF afin de s'assurer du bon fonctionnement de son IGC et ne traite pas des audits de qualification régis par les textes règlementaires.

8.1. Fréquences et / ou circonstances des évaluations

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, CSF procède à un contrôle de conformité de cette composante. CSF procède également régulièrement à un contrôle de conformité de l'ensemble de son IGC, au moins une fois tous les deux ans.

8.2. Identités / qualifications des évaluateurs

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

8.3. Relations entre évaluateurs et entités évaluées

L'équipe d'audit ne peut pas appartenir à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et est dûment autorisée à pratiquer les contrôles visés.

8.4. Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans les présentes PC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

8.5. Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à CSF un avis parmi les suivants : "réussite", "échec", "à confirmer". CSF prend alors, et fait prendre, les mesures requises en fonction des conclusions du contrôle.

8.6. Communication des résultats

Les résultats des audits de conformité sont tenus à la disposition de l'organisme de qualification en charge de la qualification de CSF.

9. Autres problématiques métiers et légales

9.1. Tarifs

9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

Cf. l'ensemble des CGU de CSF

9.1.2. Tarifs pour accéder aux certificats

N/A.

9.1.3. Tarifs pour accéder aux informations d'état et de révocation des certificats

L'accès aux informations d'état des certificats est libre et gratuit.

9.1.4. Tarifs pour d'autres services

Cf. l'ensemble des CGU de CSF

9.1.5. Politique de remboursement

N/A.

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

Cf. l'ensemble des CGU de CSF

9.2.2. Autres ressources

Cf. l'ensemble des CGU de CSF

9.2.3. Couverture et garantie concernant les entités utilisatrices

Cf. l'ensemble des CGU de CSF

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations suivantes sont considérées comme confidentielles et font l'objet de procédures de protection adéquates :

- la partie non-publique de la DPC de l'AC,
- les clés privées de l'AC, des composantes et des porteurs de certificats,
- les données d'activation associées aux clés privées d'AC et des porteurs,
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- les dossiers d'enregistrement des porteurs,
- les causes de révocations, sauf accord explicite du porteur.

9.3.2. Informations hors du périmètre des informations confidentielles

N/A.

9.3.3. Responsabilités en termes de protection des informations confidentielles

Les informations confidentielles soit ne sont pas accessibles (par exemple, clés privées des porteurs qui ne sont sous forme déchiffrée qu'à l'intérieur des cartes supports cryptographiques), soit sont accessibles uniquement aux personnes justifiant du besoin d'en connaître et dûment autorisées (par exemple, parties de "secrets d'IGC").

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

Les informations à caractère personnel sont explicitement identifiées et font l'objet de procédures de protection adéquates, en conformité avec les exigences légales et règlementaires applicables.

Cf. l'ensemble des CGU de CSF.

9.4.2. Informations à caractère personnel

Toutes les données d'enregistrement des porteurs sont considérées comme personnelles. Les données personnelles inhérentes au porteur sont les suivantes : nom, prénom, qualité (Représentant Légal ou non), service, fonction, email professionnel, téléphone professionnel, preuve de l'identité.

9.4.3. Informations à caractère non personnel

N/A.

9.4.4. Responsabilité en termes de protection des données personnelles

Conformément au Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (« RGPD ») et à la règlementation française en vigueur, les traitements de CSF sont inscrits au registre des traitements et font l'objet de mesures de sécurité techniques et organisationnelles appropriées afin de garantir la conformité à la législation.

9.4.5. Notification et consentement d'utilisation des données personnelles

Conformément aux législations et réglementations en vigueur, en particulier sur le territoire français, les informations personnelles remises par les porteurs à CSF ne sont ni divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

Cf. législations et réglementations en vigueur.

9.5. Droits sur la propriété intellectuelle et industrielle

Cf. l'ensemble des CGU de CSF

9.6. Interprétations contractuelles et garanties

9.6.1. Autorités de Certification

Au titre des présentes PC, et pour le domaine qu'elles couvrent (cf. chapitres 1.3 et 1.4 ci-dessus), CSF garantit le respect des engagements décrits dans le présent document et dans l'ensemble des CGU de CSF

.

9.6.2. Service d'enregistrement

Cf. chapitre 9.6.1.

9.6.3. Porteurs de certificats

Cf. l'ensemble des CGU de CSF

9.6.4. Utilisateurs de certificats

Cf. l'ensemble des CGU de CSF

9.6.5. Autres participants

Cf. l'ensemble des CGU de CSF

9.7. Limite de garantie

Cf. l'ensemble des CGU de CSF

9.8. Limite de responsabilité

Cf. l'ensemble des CGU de CSF

9.9. Indemnités

Cf. l'ensemble des CGU de CSF

9.10. Durée et fin anticipée de validité de la PC

9.10.1. Durée de validité

Chacune de ces PC reste en application jusqu'à la fin de vie du dernier certificat émis au titre de la PC considérée.

9.10.2. Fin anticipée de validité

La cessation d'activité de l'IGC, programmée ou suite à sinistre, entraîne la fin de validité des présentes PC.

9.10.3. Effets de la fin de validité et clauses restant applicables

La fin de validité des présentes PC rend caduques les engagements de CSF qui y sont portés, à l'exception des clauses traitant de la fin de vie de l'IGC, de l'archivage et du transfert d'activité.

9.11. Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, CSF s'engage à :

- au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'IGC et de ses différentes composantes.
- au plus tard un mois après la fin de l'opération, en informer, le cas échéant, l'organisme de qualification.

9.12. Amendements à la PC

9.12.1. Procédures d'amendements

Les PC sont revues régulièrement afin d'assurer leur conformité avec les évolutions à la fois techniques (normes, référentiels, …) et juridiques (lois, règlements, …).

9.12.2. Mécanisme et période d'information sur les amendements

Toute nouvelle version est disponible en format électronique sur le site Internet de CSF dès son approbation par la Direction de CSF.
Elle prend effet dès sa publication.

9.12.3. Circonstances selon lesquelles l'OID doit être changé

L'OID de chacune des PC comporte le numéro de version principale. Toute évolution significative de la PC, notamment les évolutions ayant un impact sur les certificats déjà émis, entraîne une évolution du numéro de version principale et donc, une évolution de l'OID.

9.13. Dispositions concernant la résolution de conflits

Cf. l'ensemble des CGU de CSF

9.14. Juridictions compétentes

Cf. l'ensemble des CGU de CSF

9.15. Conformité aux législations et réglementations

Cf. l'ensemble des CGU de CSF

9.16. Dispositions diverses

9.16.1. Accord global

Cf. l'ensemble des CGU de CSF

9.16.2. Transfert d'activités

Cf. chapitre 5.8 ci-dessus.

9.16.3. Conséquences d'une clause non valide

Au cas où une clause des présentes PC s'avèrerait être non valide au regard de la loi applicable, ceci ne remettrait pas en cause la validité et l'applicabilité des autres clauses.

9.16.4. Application et renonciation

Cf. l'ensemble des CGU de CSF

9.16.5. Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français ainsi que toutes autres conventions pouvant lier les parties.

9.17. Autres dispositions

Les politiques et procédures de l'AC sont non-discriminatoires.
Cf. l'ensemble des CGU de CSF

ANNEXE 1 - DOCUMENTS DE REFERENCE

10. Documents externes de nature juridique

[CNIL] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.

[eSIGN] Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

[LCEN] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.

[ORDONNANCE] Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

[Décret RGS] Décret n° 2010-112 du 02/02/2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005

[Arrêté RGS] Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques, lui-même pris pour l'application des articles 9, 10 et 12 de de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

[Arrêté RGS v2.0] Arrêté du Premier ministre du 13 juin 2014, portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques.

[Décret eSIGN] Décret N° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, pris pour l'application de l'article 1367 du code civil dans sa rédaction issue de l'article 4 de l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations

[RGPD] Règlement (UE) n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

11. Documents externes de nature technique

[RGS] Référentiel Général de Sécurité – Version 2.0

[RFC3647] IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003

12. Documents internes ChamberSign France

[GUI.ACC.11] ChamberSign France – Profils de Certificats et de LCR