Politique de certification des certificats cachets 1*

AC ChamberSign France

-

ChamberSign France

Objet du document :	Ce document est lié à la hiérarchie d'autorités de certification ChamberSign France « AC ChamberSign France ». Il constitue la politique de certification des certificats cachets (personnes morales) rattachés à cette hiérarchie pour les certificats correspondant au niveau RGS 1*.
Version	00
Date de diffusion	
Type de diffusion	Public

Rédigé par	Responsable Qualité ChamberSign
Vérifié par	Directeur Technique ChamberSign
Approuvé par	Délégué Général ChamberSign

Liste de diffusion
Fonctions
Public

Historique des versions	
Version	Nature de l'évolution
00	Création

SOMMAIRE

Avertissement

1. Introduction

1.1.Présentation générale

Le présent document est lié à l'Infrastructure de Gestion de Clés (IGC) de ChamberSign France (CSF), IGC en charge de la gestion des certificats de la hiérarchie « AC ChamberSign France » (dénommé IGC dans la suite du présent document).

Il constitue les Politiques de Certification (PC) de cette IGC pour les certificats cachets visant la conformité avec le référentiel général de sécurité au niveau * (cf. [RGS][1]).

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, 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, 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. Ces conditions générales correspondent aux PKI Disclosure Statement décrit dans [RFC3647].

Les engagements arrêtés dans les présentes PC correspondent :

- aux exigences imposées à CSF par la réglementation ;
- aux objectifs que se fixe CSF en matière de services, de sécurité, de qualité et de performances afin de satisfaire les utilisateurs de ses certificats et d'être reconnu, 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 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.).

[1] La liste des documents de référence est fournie en annexe 1, ces documents sont identifiés dans le texte entre « […] ».

1.2. Identification

La désignation de numéro d'identification d'objet (OID) pour les présentes PC est :

Certificat AC : ChamberSign France Cachet 1 étoile	
Politique de certification	
Authentification TLS	1.2.250.1.96.1.7.4.1.1
Authentification et Signature	1.2.250.1.96.1.7.4.2.1

{iso(1) member-body(2) france (250) type-org(1) chambersign (96) Arborescence AC ChamberSign France (1) AC Chambersign RGS LCR directe (7) Cachet 1* (4) Authentification et Signature (2) Version PC (1)}

1.3. Entités intervenant dans l'IGC

Il est distingué les intervenants externes[2] à l'IGC et les intervenants internes à l'IGC[3], qui sont sous la responsabilité de CSF vis-à-vis des intervenants externes.

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

- Fonction d'enregistrement - Cette fonction vérifie les informations d'identification du futur responsable du certificat du cachet (RCC) et du service applicatif auquel le certificat doit être rattaché, 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 RCC et/ou du service applicatif lors du renouvellement du certificat de celui-ci.
- Fonction de génération des certificats - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par la fonction d'enregistrement, y compris la clé publique du serveur.
- Fonction de génération des éléments secrets du serveur – L'IGC génère sous le contrôle exclusif du RCC des éléments secrets du service (clé privée et code d'activation de la clé privée).
- Fonction de remise au RCC - Cette fonction remet au RCC le ou les certificats correspondants ainsi que le code d'activation du cachet certificat.
- 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 RCC et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle met également à disposition les certificats valides des serveurs.
- 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

[2] Les intervenants externes sont des entités qui n'interviennent pas dans le fonctionnement de l'IGC mais qui sont amenés à interagir avec l'IGC.
[3] Les intervenants internes à l'IGC sont les entités qui interviennent dans le fonctionnement de l'IGC et qui peuvent être soit directement internes à CSF, soit externes à CSF avec un lien contractuel avec CSF.

fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR).

Les intervenants externes sont :

- Responsable du certificat de cachet (RCC) – La personne physique responsable du certificat de cachet, notamment de l'utilisation de ce certificat et de la bi-clé correspondante, pour le compte de l'entité dont dépend le serveur informatique identifié dans le certificat.
- Représentant légal – Il s'agit d'un représentant légal de l'entité identifiée dans le certificat et à laquelle le RCC 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.

1.4. Usage des certificats

1.4.1. Domaines d'utilisation applicables

PC	Usages
[Authentification]	Les usages sont l'authentification des serveurs dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS.
[Signature et Authentification]	Les usages sont : • la signature électronique de données par l'organisation (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 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 l'organisation manifeste son consentement sur les données échangées (la garantie de non répudiation n'est donc pas offerte).

Par ailleurs, CSF peut être amené à émettre des certificats de test. Ces certificats de test sont identifiés comme tels dans leur DN. Ils ne sont couverts par aucune garantie par CSF et ils ne doivent en aucun cas être utilisés à d'autres fins qu'à des fins de test.

1.4.2. Domaines d'utilisation interdits

Toute utilisation d'un certificat autre que celles prévues dans le cadre des présentes PC et des conditions générales d'utilisation (cf. [PRO.ACC.41]) 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 des présentes PC.

Le processus d'évolution et d'amendements aux présentes PC est précisé au chapitre 9.12 ci-dessous.

1.5.2. Point de contact

Toute question ou remarque concernant les présentes 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 répond ou non aux exigences des présentes 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

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

O

OID	Object Identifier

P

PC	Politique de Certification
PIN	Personnal Identification Number
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Electronique

R

RCC	Responsable du Certificat de Cachet
RL	Représentant Légal
RSA	Rivest Shamir Adelman

U

URL	Uniform Resource Locator

1.6.2. Définitions

A

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 de l'organisation ;
- la clé publique du serveur ;
- 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 serveur 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.

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 RCC et les utilisateurs de certificats.

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 RCC 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 serveur.

Responsable du Certificat de Cachet
Cf. chapitre 1.3.

Révocation de certificat
Action demandée par une entité autorisée (AC, RCC, 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 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.

U

Utilisateur Final
Toute entité (personne physique ou personne morale) recevant un certificat et s'y fiant pour vérifier une valeur de cachet provenant du serveur auquel le certificat est rattaché.

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 RCC et des utilisateurs de certificats, 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 HTTP 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 ;
- les certificats d'AC

2.3. Délais et fréquences de publication

Les informations liées à l'IGC (PC, CGU, …) 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.

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

Les noms utilisés dans les certificats émis par CSF sont conformes aux spécifications de la norme X.500 et au [RGS].
Dans chaque certificat, le champ "issuer" (AC émettrice) et le champ "subject" (service de création de cachet) correspondent à un Distinguished Name (DN).
Le contenu des DN est défini dans le document décrivant les profils de certificat [GUI.ACC.11].

3.1.2. Nécessité d'utilisation de noms explicites

Les noms utilisés dans les champs "issuer" et "subject" d'un certificat de cachet sont explicites dans le domaine de certification de CSF (utilisation des identifiants nationaux de structure SIREN/SIRET, des noms officiels complets des entités,…).

3.1.3. Anonymisation ou pseudonymisation des services de création de cachet

N/A.

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 service de création de cachet) est unique sur le domaine de certification de CSF (cf. [GUI.ACC.11]).

3.1.6. Identification, authentification et rôle des marques déposées

Il n'y a pas 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,…).

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 RCC est rattaché font l'objet de vérification lors de l'enregistrement (existence, validité,…).

3.2.3. Validation de l'identité d'un individu

L'identité du RCC est vérifiée au travers de la vérification de documents officiels d'identité dont une copie certifiée conforme par le RCC est transmise par courrier.
Dans le cas d'un changement de RCC en cours de validité d'un certificat de cachet, le nouveau RCC est enregistré en tant que tel par l'AC en remplacement de l'ancien RCC.
L'identification du nouveau RCC (personne physique) représentant une entité nécessite l'identification de la personne physique et la vérification de son habilitation en tant que représentant de l'entité à laquelle le serveur est rattaché et en tant que RCC pour le serveur considéré.
Le titulaire retourné par le whois doit correspondre à la dénomination de l'organisme (entreprise ou administration) demandant le certificat.

3.2.4. Informations non vérifiées du RCC et/ou du serveur informatique

Toutes les informations concernant les RCC figurant 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. Certification croisée d'AC

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

Le premier renouvellement est réalisé en ligne s'il a lieu avant la date d'expiration du certificat à renouveler. Le RCC 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 demandes de certificats proviennent soit directement du futur RCC, soit du représentant légal de l'entité concernée.

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 RCC.

4.2. Traitement d'une demande de certificat

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).
Ensuite, si aucun problème n'est détecté, il formate et transmet la demande au service de génération des certificats.

4.3. Délivrance du certificat

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

Suite à validation du dossier de demande de certificat par la fonction d'enregistrement de l'IGC, le processus consiste à remettre au RCC la clé publique certifiée : génération de la bi-clé, sous le contrôle et la responsabilité du RCC, dans un dispositif cryptographique (logiciel ou matériel) choisi par le RCC (moyennant le respect des exigences définies au chapitre 6.2 ci-dessous), envoie 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 RCC

L'URL permettant de télécharger le certificat est envoyé au RCC.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

Le certificat fait l'objet d'une acceptation explicite par le RCC suite à son téléchargement.

4.4.2. Publication du certificat

Les certificats objet 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 le RCC

L'utilisation de la clé privée et du certificat associé est limitée aux conditions d'usage 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'usage par le RCC.

4.5.2. Utilisation de la clé publique et du certificat par l'utilisateur 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]).

L'utilisateur est tenu de vérifier la validité du certificat et la conformité de son utilisation.

La responsabilité de CSF ne peut être engagée pour une utilisation ne correspondant pas aux conditions d'usage.

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 3 ans. Les bi-clés doivent être en effet périodiquement renouvelées afin de minimiser les risques d'attaque 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 RCC 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. Une modification sans renouvellement est interdite.

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.

4.9.1. Causes possibles d'une révocation

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

- la clé privée du serveur est perdue, volée, inutilisable, compromise ou suspectée de compromission (demande du RCC lui-même) ;
- les informations du serveur figurant dans le certificat ne sont plus valides ou plus en cohérence avec l'utilisation prévue du certificat, ceci avant l'expiration normale du certificat ;
- il a été démontré que le RCC 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) ;
- l'arrêt définitif du serveur ou la cessation d'activité de l'entité du RCC.

Les causes de révocation ne sont jamais publiées.

4.9.2. Origine d'une demande de révocation

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

- le RCC pour le serveur considéré ;
- l'entité dont dépend le RCC ;
- 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 formate et 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 RCC 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 72h (délai maximum) suivant la réception de la demande, pendant les heures ouvrées.
La fonction de gestion des révocations est disponible 24 heures sur 24, 7 jours sur 7. 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).

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

Les utilisateurs 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.

4.9.7. Fréquence d'établissement des LCR

Le service d'état des certificats publie une mise à jour au plus tous les jours 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 72 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

Un système de vérification en ligne (OCSP) n'est pas proposé.

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

Cf. chapitre 4.9.6.

4.9.11. Autres moyens disponibles d'information sur les révocations

N/A (seul le mécanisme de LCR 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 certificats de cachet, autres que la révocation des certificats correspondants.

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. Fonction d'information sur l'état des certificats

4.10.1. Caractéristiques opérationnelles

Les LCR sont mises à disposition librement et gratuitement via le site Web de CSF.

4.10.2. Disponibilité du service

Le service est disponible 24 heures / 24 et 7 jours / 7 via le site Web de CSF.

La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction d'information sur l'état des certificats est de 4 heures (jours ouvrés).
La durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des certificats est de 32 heures (jours ouvrés).

4.10.3. Dispositifs optionnels

N/A.

4.11. Fin de la relation entre le RCC et l'AC

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et l'entité de rattachement du serveur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué. De plus, l'AC doit révoquer un certificat de cachet pour lequel il n'y a plus de RCC explicitement identifié.

4.12. Séquestre de clé et recouvrement

N/A (les clés privées objet des présentes PC ne font l'objet d'aucun séquestre).

5. Mesures de sécurité non techniques

5.1.Mesures de sécurité physiques

CSF met en œuvre les mesures de sécurité physique, au sein des différentes composantes de l'IGC, nécessaires 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.

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 autorisée 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 [PRO.ACC.41].

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.

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 RCC 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

Les bi-clés des serveurs sont générées dans les dispositifs cryptographiques des RCC sous le contrôle et la responsabilité de ceux-ci. 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

Chaque RCC peut choisir librement son support cryptographique. Ce support doit cependant être conforme aux exigences correspondantes du [RGS] pour le niveau 1* (cf. exigences sur les dispositifs de création de cachet des serveurs). Le RCC s'engage contractuellement auprès de CSF sur cette conformité.

Les clés privées des serveurs ne font l'objet d'aucun séquestre et d'aucune sauvegarde par CSF.

6.3.Autres aspects de la gestion des bi-clés

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

6.4.Données d'activation

La PC ne stipule aucune exigence, la bi-clé étant mise en œuvre par les RCC eux-mêmes et sous leur entière responsabilité.

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 / Système de datation

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 et des LCR

Les profils de certificats, de LCR sont définis dans le document [GUI.ACC.11].

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 trois 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. [PRO.ACC.41] et la politique tarifaire 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. [PRO.ACC.41] et la politique tarifaire de CSF.

9.1.5. Politique de remboursement

N/A.

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

Cf. [PRO.ACC.41].

9.2.2. Autres ressources

Cf. [PRO.ACC.41].

9.2.3. Couverture et garantie concernant les entités utilisatrices

Cf. [PRO.ACC.41].

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 serveurs,
- les données d'activation associées aux clés privées d'AC et des serveurs,
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- les dossiers d'enregistrement des RCC,
- les causes de révocations, sauf accord explicite du RCC.

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 serveurs), 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. [PRO.ACC.41].

9.4.2. Informations à caractère personnel

Toutes les données d'enregistrement des RCC sont considérées comme personnelles.

9.4.3. Informations à caractère non personnel

N/A.

9.4.4. Responsabilité en termes de protection des données personnelles

Cf. législations et réglementations en vigueur. Sur le territoire français, voir notamment les déclarations de traitement de données à caractère personnel faîtes auprès de la CNIL.

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 RCC à CSF ne sont ni divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du RCC, 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.

9.4.7. Autres circonstances de divulgation d'informations personnelles

N/A

9.5.Droits sur la propriété intellectuelle et industrielle

Cf. [PRO.ACC.41].

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 [PRO.ACC.41].

9.6.2. Service d'enregistrement

Cf. chapitre 9.6.1.

9.6.3. RCC

Cf. [PRO.ACC.41].

9.6.4. Utilisateurs de certificats

Cf. [PRO.ACC.41].

9.6.5. Autres participants

Cf. [PRO.ACC.41].

9.7.Limite de garantie

Cf. [PRO.ACC.41].

9.8.Limite de responsabilité

Cf. [PRO.ACC.41].

9.9.Indemnités

Cf. [PRO.ACC.41].

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. [PRO.ACC.41].

9.14. Juridictions compétentes

Cf. [PRO.ACC.41].

9.15. Conformité aux législations et réglementations

Cf. [PRO.ACC.41].

9.16. Dispositions diverses

9.16.1. Accord global

Cf. [PRO.ACC.41].

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. [PRO.ACC.41].

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

Cf. [PRO.ACC.41].

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.
[DIRSIG]	Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.
[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
[DécretRGS]	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
[ArrêtéRGS]	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
[SIG]	Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.

11. Documents externes de nature technique

[RGS]	Référentiel Général de Sécurité – Version 1.0
[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
[PRO.ACC.41]	ChamberSign France – Conditions Générales d'Utilisation Cachet