Politique de certification des certificats d'AC

AC ChamberSign

-

ChamberSign France

Objet du document :	Ce document est lié à la hiérarchie d'autorités de certification ChamberSign France « AC ChamberSign ». Il constitue la politique de certification des certificats d'AC rattachés à cette hiérarchie.
Version	00
Date de diffusion	20/05/2011
Type de diffusion	Direction CSF

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

Liste de diffusion
Fonctions
Délégué Général
Directeur Technique
Responsable de la Sécurité du Système d'Information

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 » (dénommé IGC dans la suite du présent document).

Il constitue la Politique de Certification (PC) de cette IGC pour les certificats d'AC visant la conformité avec le référentiel générale de sécurité (cf. [RGS][1]) pour les quatre types de certificats suivant :

- certificats double usage signature / authentification niveau ** du [RGS],
- certificats de signature niveaux ** et *** du [RGS],
- certificats d'authentification niveaux ** du [RGS].

Cette hiérarchie est composée de deux niveaux :

- une AC Racine (ACR) « AC Racine – ChamberSign »,
- une AC fille (ACF) par type de certificats porteurs (double usage 2* RGS, authentification 2* RGS, signature 2* RGS, signature 3* RGS).

L'AC Racine comporte deux bi-clés : une bi-clé, dont le certificat correspondant est autosigné, qui correspond au sommet de la hiérarchie et qui est utilisée pour signer les autres certificats d'AC (ACR CertSign), une bi-clé, dont le certificat est signé par la bi-clé précédente, utilisée pour signer les LAR (liste des AC révoquées, ACR ARLSign).

Chaque AC fille comporte trois bi-clés : une bi-clé utilisée pour signer les certificats des porteurs de la classe correspondante (ACF CertSign), une bi-clé utilisée pour signer les LCR (listes de certificats révoqués) des certificats de la classe correspondante (ACF CRLSign) et une bi-clé utilisée pour signer les réponses OCSP pour les certificats de la classe correspondante (ACF OCSPResponder). Les certificats correspondants aux bi-clés de signature des certificats porteurs (ACF CertSign) et aux bi-clés de signature des LCR (ACF CRLSign) sont signés par l'ACR CertSign. Les certificats correspondants aux bi-clés de signature des réponses OCSP (ACF OCSPResponder) sont signés par l'ACF CertSign de la classe correspondante.

La structure de la présente PC 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 d'AC de l'IGC. Les certificats de porteurs, pour chacun des types identifiés ci-dessus, sont couverts par leur propre PC.

Ces politiques constituent le fondement des relations de l'IGC avec l'extérieur : utilisateurs (porteurs de certificats 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, notamment pour des utilisateurs non-spécialistes, ces politiques sont traduites dans des documents spécifiques à destination des

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

utilisateurs que sont les conditions générales d'utilisation. Ces conditions générales correspondent aux PKI Disclosure Statement décrit dans [RFC3647].

Les engagements arrêtés dans la présente 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 (porteurs et accepteurs) de ses certificats et d'être reconnu, si nécessaire, par les différents schémas d'évaluation / référencement en matière d'IGC.

La présente PC, comme les autres PC de CSF, sont des documents publics. La Déclaration des Pratiques de Certification correspondant à cette PC est un document accessible librement sur simple demande formulée auprès de CSF. Les autres documents qui découlent de cette 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.).

1.2. Identification

Ce document correspond à la PC suivante :

- Certificat d'AC

  {iso(1) member-body(2) france(250) type-org(1) chambersign(96) Travaux de certification(1) AC Chambersign(6) AC(0) Version(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 à la présente PC. Ces intervenants réalisent la mise en œuvre des fonctions suivantes :

- Fonctions de génération des certificats d'AC – Cette fonction génère les bi-clés d'AC (AC racine, AC filles) et les certificats correspondants. Les certificats sont ensuite mis à disposition des utilisateurs via la fonction de publication. Les clés privées d'AC sont ensuite mise en œuvre dans les modules cryptographiques d'IGC dans le cadre des fonctions de génération des certificats des porteurs et d'information sur l'état des certificats (génération des LCR, LAR et réponses OCSP). Au cours de ces cérémonies de clés sont également générées et remises aux personnes concernées les données de contrôles et d'activation des clés d'AC.
- 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.
- Fonction de gestion des révocations - Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à

[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.

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 (valides ou révoqués). S'agissant de certificats d'AC, cette fonction est mise en œuvre uniquement selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR).

Les intervenants externes sont :

- Porteurs de certificats – Un porteur de certificat est une personne physique identifiée dans un certificat fourni par une des AC filles objet de la présente PC.
- 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 de la présente PC pour vérifier un certificat de porteur,
- 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 amenés, 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

La présente PC couvre les certificats suivants :

- le certificat de l'ACR de signature de certificats d'AC (certificat ACR CertSign, autosigné), utilisé pour signer les certificats de la hiérarchie d'AC (certificats des AC filles, certificat de signature de la Liste des certificats d'AC révoquées (LAR), certificats de signature des Listes de Certificats porteurs Révoqués (LCR)) ;
- le certificat de signature de la Liste des certificats d'AC Révoqués (LAR) des ACF rattachées à l'ACR (certificat ACR ARLSign, signé par l'ACR CertSign) ;
- les certificats des AC filles rattachées à l'ACR (certificats ACF CertSign, signés par l'ACR CertSign) ;
- les certificats de signature des Listes des Certificats porteurs Révoqués des porteurs pour chacune des ACF rattachées à l'ACR (certificats ACF CRLSign, signés par l'ACR CertSign) ;
- les certificats de signature des réponses OCSP pour les porteurs de chacune des ACF (un certificat ACF OCSPResponder par ACF, signé par l'ACF CertSign correspondante).

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 de la présente PC et des conditions générales d'utilisation (cf. CGU) 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 répond 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
ACF	Autorité de Certification Fille
ACR	Autorité de Certification Racine
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

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.

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
Toute entité (personne physique, personne morale ou process) détenant un certificat de clé généré par l'IGC.

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.

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.

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 HTTP à l'adresse www.chambersign.fr.

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

Ces services ont pour missions :

- de garantir les conditions de mise à jour et de disponibilité du site Web ;
- de gérer les droits d'accès correspondants.

Les engagements de disponibilité et de continuité d'activité de ces services (serveur Web, générateur de LAR / 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 :

- la présente PC ;
- les CGU ;
- les formats de certificats et de LAR / LCR objet de la présente PC ;
- les LAR / 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" (AC certifiée) correspondent à un Distinguished Name (DN).
Le contenu des DN est défini dans le document décrivant les profils de certificat [INF.INF.03].

3.1.2. Nécessité d'utilisation de noms explicites

Les noms utilisés dans les champs "issuer" et "subject" d'un certificat d'AC sont explicites dans le domaine de certification de CSF (utilisation des identifiants nationaux de structure SIREN/SIRET, identification du type de certificats couverts par l'AC,…).

3.1.3. Anonymisation ou pseudonymisation des porteurs

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 [INF.INF.03].

3.1.5. Unicité des noms

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

3.1.6. Identification, authentification et rôle des marques déposées

N/A s'agissant de certificats d'AC.

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.
De plus, pour tous les certificats d'AC objet de la présente PC, sauf les certificats d'ACF OCSPResponder, la génération d'une bi-clé d'AC et du certificat correspondant est réalisée au cours d'une seule et même « cérémonie de clés ».

3.2.2. Validation de l'identité d'un organisme

La présente PC couvre uniquement des certificats d'AC de CSF.

3.2.3. Validation de l'identité d'un individu

N/A.

3.2.4. Informations non vérifiées du porteur

N/A.

3.2.5. Validation de l'autorité du demandeur

Les cérémonies de clés sont ne peuvent être demandées que par la direction de CSF.

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

Le renouvellement des clés d'AC, courant ou après révocation, est réalisé au cours de cérémonies de clés identique aux cérémonies de clés initiales.

3.4. Identification et validation d'une demande de révocation

La révocation d'un certificat d'AC objet de la présente PC ne peut être demandée que par la direction de CSF.

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 d'AC ne proviennent que de la direction de CSF.

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

L'établissement d'une demande de certificat d'AC est de la responsabilité de la direction de CSF.

4.2. Traitement d'une demande de certificat

Suite à demande de génération formulée par la direction de CSF, le service de génération organise la ou les cérémonies de clés correspondantes (scripts, convocation des témoins, préparation des matériels et logiciels, etc.).

4.3. Délivrance du certificat

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

Les bi-clés et les certificats d'AC sont générés au cours de cérémonies de clés, suivant des scripts pré-définis et en présence de témoins, internes et/ou externes à l'IGC, attestant du déroulement effectif de chaque cérémonie par rapport au script correspondant, y compris, le cas échéant, la remise des « secrets d'IGC » aux porteurs désignés.

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

N/A.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

N/A.

4.4.2. Publication du certificat

Les certificats objet des présentes PC sont publiés sur le site Web de CSF.
Concernant le certificat d'AC Racine CertSign (autosigné), il est publié sur une page sécurisée et son empreinte peut-être vérifiée par téléphone auprès de 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'usage définies dans la présente PC (cf. § 1.4) et ceci conformément à l'utilisation spécifique décrite dans le contenu du certificat (attribut key usage et extended key usage, cf. [INF.INF.03]).

L'utilisation par les AC de leurs bi-clés et de leurs certificats de signature de certificats est réservée à la génération des certificats d'AC, pour l'ACR, et des certificats de porteurs et de signature de réponses OCSP, pour les ACF.
L'utilisation par les AC de leurs bi-clés et de leurs certificats de signature de listes de révocation est réservée à la génération des LCR et LAR.
L'utilisation par les ACF de leurs bi-clés et de leurs certificats de signature OCSP est réservée à la génération de réponses OCSP.

L'utilisation d'une clé privée n'est autorisée que pendant la période de validité du certificat associé.

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'usage définies dans la présente PC (cf. § 1.4) et à l'usage prévu indiqué dans le certificat (attribut key usage et extended key usage, cf. [INF.INF.03]).

L'accepteur 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. Les durées de validité des certificats d'AC de CSF sont précisées dans le document [INF.INF.03]. 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 notamment la révocation d'un certificat d'AC.

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, lors d'une cérémonie de clés.

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. 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

Certificat d'ACR

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

- compromission ou suspicion de compromission de la clé privée correspondante ou des éléments secrets protégeant cette clé hors des boîtiers cryptographiques ;
- perte ou vol d'un boîtier cryptographique contenant les éléments secrets mentionnés à l'alinéa précédent ;
- cessation d'activité de l'AC racine ;
- par anticipation par exemple : en cas de risque de mise en péril de l'IGC suite à l'apparition d'une faiblesse au niveau des algorithmes ou des clés utilisés ;
- pour le certificat de l'ACR ARLSign, révocation du certificat ACR CertSign correspondant.

Certificat d'ACF

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

- pour les certificats ACF CertSign et ACF CRLSign, révocation du certificat de l'ACR CertSign correspondante ;
- pour un certificat d'ACF OCSPResponder, révocation du certificat ACF CertSign correspondant ;
- compromission ou suspicion de compromission de la clé privée de cette ACF ou des éléments secrets protégeant cette clé hors des boîtiers cryptographiques ;
- perte ou vol d'un boîtier cryptographique contenant les éléments secrets mentionnés à l'alinéa précédent ;
- par anticipation par exemple : en cas de risque de mise en péril de l'IGC suite à l'apparition d'une faiblesse au niveau de l'algorithme ou des clés utilisés.

Les causes de révocation ne sont jamais publiées.

4.9.2. Origine d'une demande de révocation

Seule la direction de CSF peut demander la révocation d'un certificat d'AC.

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 :

- pour les certificats révoqués d'ACF CertSign ou CRLSign, de déclencher la génération et la publication d'une nouvelle LAR contenant les n° de série de ces certificats,
- pour les certificats révoqués d'ACF OCSPResponder, d'ajouter les n° de série de ces certificats dans la ou les prochaines LCR à générer et publier, correspondant à la ou les ACF concernées,
- pour les certificats révoqués d'ACR et d'ACF, les retirer du serveur Web et informer explicitement sur le serveur Web de la révocation du ou des certificats concernés.

De plus, le cas échéant, l'ensemble des porteurs concernés sont avertis par messagerie électronique que leurs certificats ne sont plus valides compte-tenu de la révocation d'un des certificats de la chaine de certification.
Le cas échéant, les autorités publiques concernées sont également informées.

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

Le traitement d'une demande de révocation d'un certificat d'AC est réalisé immédiatement, dès réception de la demande par le service de gestion des révocations (7 jours / 7, week-ends et jours fériés compris).
La fonction de gestion des révocations est disponible 24heures su 24, 7jours sur 7. 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

Les accepteurs des certificats objet de la présente PC doivent vérifier la non-révocation des certificats d'AC sur lesquels ils vont baser leur confiance. Cette vérification se fait en consultant les LAR / LCR disponibles via le site Web de CSF.

4.9.7. Fréquence d'établissement des LCR

Dès révocations d'un certificat d'ACF CertSign ou CRLSign, une nouvelle LAR est générée et publiée par le service d'état des certificats.
La LAR a une durée de validité correspondant à la date de fin de validité du certificat ACR ARLSign.

Concernant les certificats ACF OCSPResponder, 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 2 jours ouvrés.

4.9.8. Délai maximum de publication d'une LCR

Le délai maximum de publication d'une LAR / 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

N/A (seul le mécanisme de LAR / LCR est mis en œuvre concernant les certificats d'AC).

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

N/A.

4.9.11. Autres moyens disponibles d'information sur les révocations

La révocation de certificats d'AC fait l'objet, en plus de la LAR / LCR, d'une information diffusée au moins sur le site Web de CSF et, le cas échéant, relayée par d'autres sites administratifs ou professionnels, ainsi que sur appel téléphonique à CSF.

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

Il n'y a pas d'autres mesures, concernant les clés privées d'AC, que celles présentées dans les chapitres précédents.

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 LAR / 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 2 heures.
La durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des certificats est de 8h.

4.10.3. Dispositifs optionnels

N/A.

4.11. Expiration de l'abonnement des porteurs

N/A.

4.12. Séquestre de clé et recouvrement

N/A (les clés privées objet de la présente 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, 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.

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 / LAR émis,…).
Les durées de conservation des archives sont précisées dans les Conditions Générales d'Utilisation.

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 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

Les bi-clés d'AC sont générées dans des modules cryptographiques sécurisés au cours de cérémonies de clés. Des modules cryptographiques assurent également la génération des certificats correspondants.
Les longueurs des clés d'AC sont précisées dans le document [INF.INF.03].

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

Les modules cryptographiques des AC font l'objet d'une qualification par l'ANSSI au niveau requis par le RGS.
Les clés privées d'AC ne font l'objet d'aucun séquestre et d'aucun archivage.
Le contrôle des clés privées d'AC est assuré par du personnel de confiance (porteurs de secrets d'IGC), suivant un schéma de partage de secret nécessitant n intervenant parmi m.
L'activation des clés privées d'AC dans les modules cryptographiques nécessite l'intervention d'au moins deux personnes dans des rôles de confiance.
Les clés privées d'AC peuvent faire l'objet d'une copie de secours, soit dans un module cryptographique faisant l'objet d'une qualification par l'ANSSI au niveau requis par le RGS,

soit sous forme chiffrée, suivant les exigences requises par le RGS et de telle manière que les clé privées d'AC ne soient jamais en clair en dehors d'un module cryptographique.

6.3. Autres aspects de la gestion des bi-clés

Les clés publiques des AC sont archivées dans le cadre de l'archivage des certificats correspondants.
Les durées de vie des clés et certificats d'AC sont précisées dans le document [INF.INF.03].

6.4. Données d'activation

La génération et l'installation des données d'activation des modules cryptographiques d'AC sont réalisées par du personnel de confiance lors des phases d'initialisation et de personnalisation de ces modules.
Ces données d'activation sont protégées en confidentialité, intégrité et disponibilité.

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, OSCP et des LCR

Les profils de certificats et de LCR / LAR sont définis dans le document [INF.INF.03].

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 par an.

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. les [CGU] 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. les Conditions Générales d'Utilisation 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. les Conditions Générales d'Utilisation.

9.2.2. Autres ressources

Cf. les Conditions Générales d'Utilisation.

9.2.3. Couverture et garantie concernant les entités utilisatrices

Cf. les Conditions Générales d'Utilisation.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations suivantes sont considérées comme confidentielles 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. les Conditions Générales d'Utilisation.

9.4.2. Informations à caractère personnel

Toutes les données d'enregistrement des porteurs 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 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. les Conditions Générales d'Utilisation.

9.6. Interprétations contractuelles et garanties

9.6.1. Autorités de Certification

Au titre de la présente 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 les Conditions Générales d'Utilisation.

9.6.2. Service d'enregistrement

Cf. chapitre 9.6.1.

9.6.3. Porteurs de certificats

Cf. les Conditions Générales d'Utilisation.

9.6.4. Utilisateurs de certificats

Cf. les Conditions Générales d'Utilisation.

9.6.5. Autres participants

Cf. les Conditions Générales d'Utilisation.

9.7. Limite de garantie

Cf. les Conditions Générales d'Utilisation.

9.8. Limite de responsabilité

Cf. les Conditions Générales d'Utilisation.

9.9. Indemnités

Cf. les Conditions Générales d'Utilisation.

9.10. Durée et fin anticipée de validité de la PC

9.10.1. Durée de validité

Cette PC reste en application jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2. Fin anticipée de validité

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

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

La fin de validité de la présente 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

La PC est revue régulièrement afin d'assurer sa 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 cette 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. les Conditions Générales d'Utilisation.

9.14. Juridictions compétentes

Cf. les Conditions Générales d'Utilisation.

9.15. Conformité aux législations et réglementations

Cf. les Conditions Générales d'Utilisation.

9.16. Dispositions diverses

9.16.1. Accord global

Cf. les Conditions Générales d'Utilisation.

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. les Conditions Générales d'Utilisation.

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. les Conditions Générales d'Utilisation.

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

[INF.INF.03] ChamberSign France – Profils de Certificats et de LCR