SECURE TRANSACTIONS CERTIFICATION AUTHORITIES SHA-2

AUTORITÉS DE CERTIFICATION POUR LES ENVIRONNEMENTS DE TERMINAUX DE PAIEMENT EN MODE IP

===

POLITIQUE DE CERTIFICATION

DATE D'APPLICATION

Juin 2016

SUIVI DES MODIFICATIONS

DATE DE MISE A JOUR	PARTIE MODIFIEE (*chap. et page*)	NOUVEL INDICE DE REVISION	DESCRIPTION DES MODIFICATIONS
Juin 2016	-	V1.0	Création du document qui s'applique à l'AC *Secure Transactions CA SHA-2* qui permet la génération de certificats dans une architecture utilisant exclusivement l'algorithme de hachage SHA-256.

SOMMAIRE

1 PREAMBULE

1.1 PRESENTATION GENERALE

La présente politique de certification (PC) concerne « *les autorités de certification pour les environnements de terminaux de paiement en mode IP* ». Ces Autorité de Certification (AC) sont dénommées « *Secure Transactions Certification Authorities* SHA-2» ou « *Secure Transactions CA SHA-2* ». Elles sont dédiées à la délivrance de certificats aux serveurs, que ce soit des serveurs d'acquisition[1] ou des serveurs d'acceptation[2], et aux infrastructures de gestion de clés de délégataires dans la filière des terminaux de paiement en mode IP.

La finalité de l'*AC Secure Transactions CA SHA-2* pour les environnements de terminaux de paiement en mode IP est de simplifier l'usage des certificats nécessaires à l'authentification, éventuellement mutuelle, entre un équipement[3] de paiement électronique et un serveur d'acquisition lors de l'établissement d'une session sécurisée.

Les certificats délivrés par l'*AC Secure Transactions CA SHA-2* sont à destination d'entités du monde de la monétique pour une authentification de machine à machine.

Une PC est un ensemble de règles, identifié par un nom, qui définit les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et qui indique l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes.

Une PC décrit quelles sont les modalités de gestion et d'usage des certificats. Les pratiques mises en œuvre pour atteindre les garanties offertes sur ces certificats sont présentées dans un autre document : la « *Déclaration des Pratiques de Certification* », ci-après nommée DPC.

La gestion d'un certificat comprend toutes les phases du cycle de vie d'un certificat, de la demande d'attribution à la fin de vie de ce certificat. Le but de la présente PC est de fournir aux utilisateurs de certificats les informations relatives aux garanties offertes sur les certificats émis par celle-ci, ainsi que les conditions d'utilisation de ces certificats.

La présente PC fera l'objet de révisions périodiques afin de tenir compte de l'évolution des technologies et des recherches dans le domaine de la cryptographie[4].

1.2 IDENTIFICATION DU DOCUMENT

La présente PC est dénommée « *Politique de Certification de l'autorité de certification Secure Transactions CA SHA-2 pour les environnements de terminaux de paiement en mode IP*».

[1] Le présent document ne rentre pas dans le détail des différentes architectures existantes pour les serveurs d'acquisition (serveurs banques, passerelles, etc.).

[2] Un serveur d'acceptation est un serveur de monétique répartie auquel se connectent des terminaux ou points d'acceptation.

[3] Le présent document ne rentre pas dans le détail de l'implémentation des différents équipements terminaux pour le paiement électronique de proximité (TPE, passerelles, etc.).

[4] Voir en particulier les chapitres 4.2.3 et 6.1.4.

Elle est identifiée par l'Identifiant d'Objet (OID) suivant, déposé par l'Autorité de Certification *Secure Transactions CA SHA-2* auprès de l'AFNOR :

1.2.250.1.201.1.1.1

{iso(1) member-body(2) france(250) type-org(1) PAYCERT(201) STCA(1) pc(1) version(1)}

Cette PC est basée sur l'état de l'art constitué en France par le Référentiel Général de Sécurité pour les Certificats serveur.

1.3 ENTITES INTERVENANT DANS L'IGC

1.3.1 DECOUPAGE FONCTIONNEL DE L'IGC

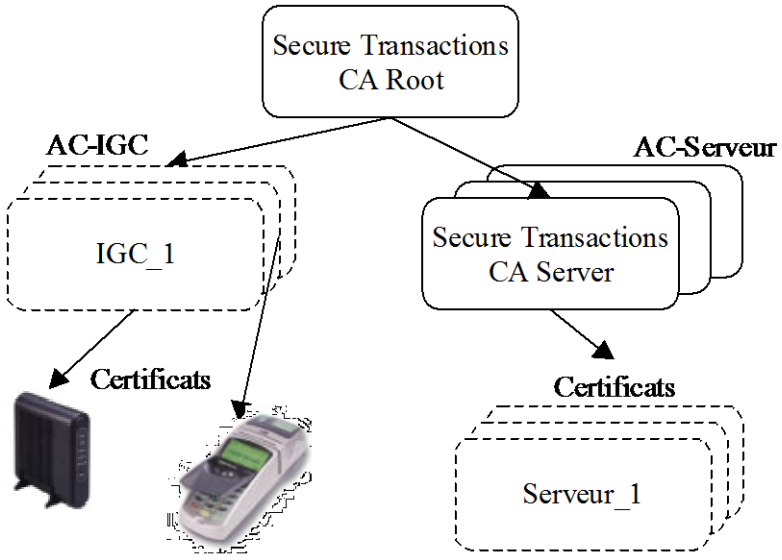
L'autorité de certification est le tiers de confiance de référence reconnu par l'ensemble de ses utilisateurs. A ce titre, l'AC engage sa responsabilité sur l'usage des certificats qu'elle délivre. Elle est donc directement ou indirectement responsable

- De l'autorité d'enregistrement (AE) des demandes de certificats ;
- De l'opérateur de certification (OC) pour la génération des certificats.

Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des biclés et des certificats (génération, diffusion, renouvellement, révocation,...) et s'appuient pour cela sur une infrastructure technique appelée « *infrastructure de gestion de clés (IGC)* ».

L'architecture de l'IGC est composée d'une AC racine et d'une AC fille (voir 1.4) :

- L'AC racine est l'AC « *Secure Transactions CA Root – SHA-2* ». Cette AC est auto-signée ;
- Une AC fille « *Secure Transactions CA Server – SHA-2* » signée par l'AC racine pour la production de certificats pour les serveurs[5] ;



Cette architecture se complète du côté des IGC de délégataires par leur architecture d'IGC.

La décomposition fonctionnelle d'une IGC qui est retenue dans le présent document est la suivante :

- **Fonction d'enregistrement** – Cette fonction vérifie les informations d'identification du futur responsable du certificat serveur informatique (RCSI) et des équipements auquel le certificat doit

[5] Le terme « serveur » couvre à la fois les serveurs d'acceptation et les serveurs d'acquisition

être rattaché avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC.

- **Fonction de génération des certificats** – Cette fonction génère (création du format, signature numérique avec la clé privée de l'AC *Secure Transactions CA SHA-2*) les certificats à partir des informations transmises par l'AE et de la clé publique de l'équipement provenant du RCSI.
- **Fonction de remise au RCSI** – Cette fonction remet au RCSI au minimum le certificat de l'équipement.
- **Fonction de publication** – Cette fonction met à disposition des différentes parties concernées, les conditions générales de services, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée au RCSI 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 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. Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR).

Un certain nombre d'entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

- **Responsable du certificat serveur informatique (RCSI)** – La personne physique responsable du certificat serveur ou de l'IGC du délégataire, notamment de l'utilisation de ce certificat et de la biclé correspondante, pour le compte de l'entité dont dépend le serveur informatique identifié dans le certificat.
- **Mandataire de certification (MC)** – Le mandataire de certification est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des RCSI et des serveurs informatiques de cette entité (il assure notamment le face-à-face pour l'identification des RCSI lorsque celui-ci est requis).
- **Utilisateur de certificat** – La machine (terminal ou serveur) qui reçoit un certificat et qui s'y fie pour vérifier une valeur d'authentification provenant d'une machine à laquelle le certificat est rattaché, ou pour établir une clé de session.
- **Personne autorisée** – Il s'agit d'une personne autre que le RCSI et le MC et qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du RCSI (demande de révocation, de renouvellement, …). Typiquement, dans une organisation, il peut s'agir d'un responsable hiérarchique du RCSI ou d'un responsable des ressources humaines.

La mise en œuvre opérationnelle de ces fonctions est effectuée par une ou plusieurs composante(s) de l'IGC, qui sont, dans la présente version de ce document, internes à l'AC.

La Déclaration des Pratiques de Certification (DPC) de l'AC *Secure Transactions CA SHA-2* décrit l'organisation opérationnelle de l'IGC et la répartition des rôles entre les différentes composantes en fonction de l'organisation fonctionnelle et de la définition des rôles décrites dans cette PC.

L'AC reste in fine responsable vis-à-vis de toute partie externe à l'IGC des prestations fournies et doit garantir le respect des engagements pris dans sa PC et sa DPC, relatifs à son activité de certification. Le cadre contractuel entre l'AC et ses différentes composantes est régi globalement par les missions respectives des différentes directions de *l'AC Secure Transactions CA SHA-2.*

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

- Etre en relation par voie contractuelle et/ou hiérarchique avec le propriétaire de l'équipement pour la gestion de ses certificats ;
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux maîtrises d'ouvrage d'application, aux utilisateurs de certificats, etc. qui mettent en œuvre ses certificats ;
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur ;
- Mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. La DPC est élaborée en fonction de cette analyse ;
- Mettre en œuvre les différentes fonctions identifiées dans la PC notamment en matière de génération des certificats, de remise au propriétaire de l'équipement, de gestion des révocations et d'information sur l'état des certificats ;
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans la PC notamment en termes de fiabilité, de qualité et de sécurité ;
- Générer, et renouveler lorsque nécessaire, ses biclés et les certificats correspondants (signature de certificats et de LCR), ou faire renouveler ses certificats dans le cadre de la hiérarchie supérieure. Diffuser ses certificats d'AC aux RCSI et utilisateurs de certificats.

1.3.2 AUTORITE D'ENREGISTREMENT

Le service interne de l'AC Secure Transactions CA SHA-2 qui joue le rôle d'AE a pour rôle de vérifier l'identité du futur RCSI et du serveur informatique. Pour cela, l'AE assure les tâches suivantes :

- La prise en compte et la vérification des informations du futur RCSI et du serveur informatique et de leur organisation de rattachement et la constitution du dossier d'enregistrement correspondant ;
- Le cas échéant, la prise en compte et la vérification des informations du futur MC et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- L'archivage des pièces du dossier ;
- L'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC en fonction de l'organisation décrite ci-après ;
- La conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du RCSI ou, le cas échéant, du MC, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

1.3.3 RESPONSABLES DE CERTIFICATS SERVEURS

Dans le cadre de la présente PC, un RCSI est une personne physique qui est responsable de l'utilisation de la clé privée et du certificat du serveur ou de l'IGC du délégataire qui est identifié dans ce certificat, pour le compte de l'entité également identifié dans ce certificat. Le RCSI a un lien contractuel / hiérarchique / réglementaire avec cette entité. Il doit respecter les conditions qui lui incombent définies dans la présente PC.

A noter que le certificat étant rattaché au serveur et non au RCSI, ce dernier peut être amené à changer en cours de validité du certificat : départ du RCSI de l'entité, changement d'affectation et de responsabilité au sein de l'entité, etc.

L'entité doit signaler à l'AC préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RCSI de ses fonctions et lui désigner un successeur. Une AC doit révoquer un certificat serveur pour lequel il n'y a plus de RCSI explicitement identifié.

1.3.4 UTILISATEURS DE CERTIFICATS

Dans le contexte de la présente PC, les utilisateurs de certificat sont les équipements informatiques de l'autre extrémité de la liaison devant être sécurisée par le certificat serveur.

1.3.5 AUTRES ACTEURS DE L'IGC

Administrateur de l'AC : responsable du bon fonctionnement de l'ensemble des services rendus par l'autorité de certification, notamment de l'organisation et du bon déroulement des séances nécessitant la mise en œuvre d'un outil cryptographique par un opérateur. Il est responsable de l'ensemble des services rendus par l'AC.

Auditeur : personne désignée par la Direction de l'AC Secure Transactions CA SHA-2 et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre de la politique de certification et des services effectivement fournis par l'AC.

Ingénieur système : il est chargé de l'installation, de la mise en route, de la configuration et de la maintenance technique des équipements informatique de l'AC. Il assure technique des systèmes et des réseaux de cette plate-forme.

Opérateur (de certification) : l'opérateur de l'AC réalise l'exploitation des services offerts par l'autorité, dans le cadre de ses attributions. Il est chargé de lancer l'exécution des fonctions cryptographiques.

Officier de sécurité de l'AC : il est responsable de l'application de la politique de sécurité physique, logique et fonctionnelle de l'AC. Il gère les habilitations et les contrôles d'accès physiques à la plate-forme informatique et est chargé de mettre en œuvre la politique de sécurité.

1.4 USAGE DES CERTIFICATS

1.4.1 DOMAINES D'UTILISATION APPLICABLES

La présente PC traite des biclés et des certificats à destination d'entités du monde de la monétique :

- Un serveur : soit un serveur d'acquisition de transactions de paiement électronique avec lequel un équipement terminal demande à établir une session sécurisée, soit un serveur d'acceptation demandant l'établissement d'une session sécurisée avec un serveur d'acquisition ;
- Une IGC d'un délégataire dans la filière des terminaux de paiement électronique.

Dans la suite de ce document, sauf mention explicite, les deux équipements destination seront dénommés « *serveur* ».

Les applications utilisatrices de ces certificats peuvent les utiliser :

- A des fins de l'établissement d'une connexion sécurisée par SSL pour les serveurs ;
- A des fins de signature de certificats destinés à être rattachés à des équipements terminaux pour l'IGC d'un délégataire.

1.4.2 DOMAINES D'UTILISATION INTERDITS

Les applications utilisatrices de ces certificats ne doivent pas les utiliser à des fins :

- De signature électronique au sens de la manifestation du consentement selon l'article 1316-4 du code civil ;
- Tout autre usage que ceux prévus au chapitre précédent.

L'AC doit respecter ces restrictions, faire connaître et imposer leur respect par les RCSI et les utilisateurs de certificats.

1.5 GESTION DE LA PC

1.5.1 ENTITE GERANT LA PC

L'AC est responsable de la gestion de la présente PC. Le présent document doit être validé par une instance interne désignée par la Direction de l'AC Secure Transactions CA SHA-2.

1.5.2 POINT DE CONTACT

Tout envoi adressé à l'autorité de certification concernant la diffusion du présent document doit être adressée à :

Secure Transactions CA
PayCert
153 rue Saint Honoré
75001 Paris

1.5.3 ENTITE DETERMINANT LA CONFORMITE D'UNE DPC AVEC CETTE PC

Les personnes responsables des audits de l'AC sont désignées par la direction de l'AC Secure Transactions CA SHA-2 qui prononce la conformité ou non de la DPC à la présente PC.

1.5.4 PROCEDURES D'APPROBATION DE LA CONFORMITE DE LA DPC

Les modalités d'approbation de la conformité de la DPC seront déterminées par la direction de l'AC Secure Transactions CA SHA-2.

1.6 DEFINITIONS ET ACRONYMES

1.6.1 ACRONYMES UTILISES

AC	Autorité de Certification
AE	Autorité d'Enregistrement
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
IGC	Infrastructure de Gestion de Clés.
LCR	Liste des Certificats Révoqués
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de Certification
RCSI	Responsable du certificat serveur informatique
RSA	Rivest Shamir Adelman
RSSI	Responsable de la Sécurité des Systèmes d'Information
URL	Uniform Resource Locator

IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunications Union
PKIX	Public Key Infrastructure Working Group (Groupe de travail de l'IETF)

1.6.2 TERMES UTILISES DANS LE PRESENT DOCUMENT

Applications utilisatrices : services exploitant les certificats émis par l'AC Secure Transactions CA SHA-2 pour des besoins d'établissement d'une session sécurisée.

Biclé : une biclé est un couple de deux clés, une clé privée (devant être conservée secrète) et la clé publique correspondante, nécessaire à la mise en œuvre d'une prestation cryptographique basée sur des algorithmes asymétriques.

Certificat : clé publique d'un utilisateur, ainsi que certaines autres informations rendue infalsifiable par chiffrement avec la clé secrète de l'autorité de certification qui l'a délivré. Le format de certificat utilisé dans le cadre de la présente PC est le format X.509 v3 [9594-8].

Composante : plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC.

Déclaration des Pratiques de Certification (DPC) : énoncé des pratiques de certification (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 et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Délégataire : AC ayant reçu de la part de l'AC Secure Transactions CA SHA-2 le droit de générer des certificats pour serveur ou système d'acceptation en conformité avec la politique de certification de l'AC Secure Transactions CA SHA-2

Dispositif de protection de clés privées : Il s'agit du dispositif matériel et/ou logiciel utilisé par le serveur pour stocker et mettre en œuvre sa clé privée.

Dispositif d'établissement de session : Il s'agit du dispositif mis en œuvre par l'utilisateur pour établir une session sécurisée avec un serveur, notamment générer la clé symétrique de session et la chiffrer avec la clé publique du serveur contenue dans le certificat correspondant.

Données d'enregistrement d'un utilisateur : ensemble d'informations nécessaires à l'enregistrement.

Empreinte : dans le contexte de cette PC, le terme empreinte est utilisé pour représenter le résultat d'une fonction de hachage, c'est-à-dire d'une fonction calculant le condensat d'informations de telle sorte que toute modification du message entraîne la modification de l'empreinte.

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.

Paramètres de clés publiques : données publiques relatives à l'algorithme utilisé, pour la mise en œuvre de clés privées, comme par exemple l'exposant, etc.

Politique de certification (PC) : ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme 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 RCSI et les utilisateurs de certificats.

Produit de sécurité : un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Serveur : sauf mention contraire, il s'agit d'un équipement informatique disposant d'un certificat fourni par l'AC et qui est rattaché à l'entité identifiée dans le certificat.

2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

2.1 ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

Pour la mise à disposition des informations devant être publiées à destination des RCSI et des utilisateurs de certificats, l'AC Secure Transactions CA SHA-2 met en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats.

2.2 INFORMATIONS DEVANT ETRE PUBLIEES

L'AC a pour obligation de publier au minimum les informations suivantes à destination des RCSI et utilisateurs de certificats :

- Sa politique de certification, couvrant l'ensemble des rubriques du [RFC3647], ainsi que les éventuels documents complémentaires ;
- La liste des certificats révoqués ;
- Les certificats en cours de validité de l'AC ;
- Pour les certificats d'AC autosignés (AC Racine), les informations permettant aux utilisateurs de certificats de s'assurer de l'origine de ces certificats (cf. chapitre 6.1.3).

L'AC a également pour obligation de publier, à destination des RCSI les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.).

Les moyens utilisés pour la publication de ces informations sont décrits dans la DPC correspondant à la présente PC.

2.3 DELAIS ET FREQUENCES DE PUBLICATION

Les délais et les fréquences de publication dépendent des informations concernées :

- Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), l'information est publiée dès que nécessaire afin que soient assurés à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC ;
- Pour les certificats d'AC, ils doivent être diffusés préalablement à toute diffusion de LCR correspondants sous délai 24 h.
- Pour les informations d'état des certificats voir le chapitre 4.10.

Les exigences de disponibilité des systèmes publiant ces informations dépendent des informations concernées :

- Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), les systèmes doivent être disponibles pendant les jours ouvrés avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 8h (jours ouvrés) et une durée totale maximale d'indisponibilité par mois de 32h (jours ouvrés), ceci hors cas de force majeure.
- Pour les informations d'état des certificats voir le chapitre 4.10.

2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'ensemble des informations publiées à destination des utilisateurs de certificats doit être libre d'accès en lecture.

L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort.

L'accès en modification aux systèmes de publication des autres informations doit être strictement limité aux fonctions internes habilitées de l'IGC, au moins au travers d'un contrôle d'accès de type mots de passe basé sur une politique de gestion stricte des mots de passe.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 NOMMAGE

3.1.1 TYPES DE NOMS

Les noms utilisés doivent être conformes aux spécifications de la norme X.500.

La convention de nommage utilisée par l'AC Secure Transactions CA SHA-2 consiste à désigner un équipement par un nom distinctif (DN=Distinguished Name) construit de la façon suivante :

C= pays

O= organisation

OU=division / serveur / autre

CN= nom distinctif de l'équipement

Le champ d'extension SubjectAlternativeName du certificat serveur peut contenir l'adresse IP du serveur.

3.1.2 NECESSITE D'UTILISATION DE NOMS EXPLICITES

Les noms choisis pour désigner les serveurs dans les certificats doivent être explicites.

3.1.3 ANONYMISATION OU PSEUDONYMISATION

S'agissant de certificats serveurs, les notions d'anonymisation ou de pseudonymisation sont sans objet.

3.1.4 REGLES D'INTERPRETATION DES DIFFERENTES FORMES DE NOM

Sans objet.

3.1.5 UNICITE DES NOMS

Afin d'assurer la continuité d'une identification unique au sein du domaine de l'AC dans ses certificats successifs (renouvellement) et pour éviter toute ambiguïté, le DN du champ "subject" de chaque certificat serveur doit permettre d'identifier de façon unique le serveur correspondant au sein du domaine de l'AC.

Ce DN doit pour cela respecter les exigences correspondantes définies au chapitre 7, notamment pour le traitement des cas d'homonymie au sein du domaine de l'AC.

Durant toute la durée de vie de l'AC, un DN attribué à un serveur ne peut être attribué à un autre serveur.

A noter que l'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC, mais que ce numéro est propre au certificat et non pas au serveur et ne permet donc pas d'assurer une continuité de l'identification dans les certificats successifs d'un serveur donné.

3.1.6 PROCEDURES DE RESOLUTION DES LITIGES SUR LA REVENDICATION D'UN IDENTIFIANT

Tout litige sur l'attribution d'un nom sera résolu par l'examen par l'AE des preuves permettant de garantir l'identité réelle d'un serveur.

3.2 VALIDATION INITIALE DE L'IDENTITE

L'enregistrement d'un serveur auquel un certificat doit être délivré se fait via l'enregistrement du MC et du RCSI correspondant. Ce dernier devra notamment démontrer que le serveur appartient bien à l'entité qu'il représente.

Dans la suite de ce document il sera considéré que l'organisation dispose toujours d'un MC, celui-ci pouvant le cas échéant être le RCSI lui-même.

Un porteur peut être amené à changer en cours de validité du certificat serveur correspondant (cf. chapitre 1.3.3), dans ce cas, tout nouveau RCSI doit également faire l'objet d'une procédure d'enregistrement.

L'enregistrement d'un serveur informatique, peut se faire soit directement auprès de l'AE, soit via un mandataire de certification de l'entité. Dans ce dernier cas, le MC doit être préalablement enregistré par l'AE.

La validation initiale de l'identité d'une entité ou d'une personne physique est ainsi réalisée dans les cas suivants :

- Enregistrement d'un MC : validation de l'identité "personne morale" de l'entité pour lequel le MC interviendra et de l'identité "personne physique" du futur MC.
- Enregistrement d'un RCSI via un MC pour un certificat à émettre ou d'un nouveau RCSI pour un certificat déjà émis : validation par le MC de l'identité "personne physique" du futur RCSI, de son habilitation à être RCSI pour le serveur considéré et pour l'entité considérée, ainsi que du nom de domaine du serveur.

Pour des raisons de simplicité de présentation, ces différents cas sont regroupés dans le chapitre 3.2.3.

3.2.1 METHODE POUR PROUVER LA POSSESSION DE LA CLE PRIVEE

Lors de l'enregistrement, le RCSI doit fournir à l'AC, via le MC le cas échéant, une preuve de possession de sa clé privée correspondant à la clé publique contenue dans la demande de certificat serveur.

3.2.2 VALIDATION DE L'IDENTITE D'UN ORGANISME

Cf. chapitre suivant.

3.2.3 VALIDATION DE L'IDENTITE D'UN INDIVIDU

3.2.3.1 ENREGISTREMENT D'UN MANDATAIRE DE CERTIFICATION

Une AE est amenée à constituer un dossier d'enregistrement pour un Mandataire de Certification pour répondre aux besoins suivants :

- Utilisation du dossier du MC comme référence pour les données d'identification de l'entité de tous les RCSI présentés par le MC.

L'authentification du MC par l'AE est réalisée lors d'un face-à-face physique[6] ou par une méthode apportant un degré d'assurance équivalent.

Ensuite, lors de la transmission des dossiers d'enregistrement des serveurs, le MC devra être authentifié de façon forte au cours d'un face à face et/ou par le paraphe du MC apposé sur les différentes pages du dossier de demande, complété par sa signature sur les principales pages.

Le dossier d'enregistrement d'un MC doit comprendre :

- une demande écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité,
- un mandat, daté de moins de 3 mois, désignant le MC. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le MC,
- un engagement signé, et daté de moins de 3 mois, du MC, auprès de l'AC, à effectuer correctement et de façon indépendante les contrôles des dossiers des demandeurs,
- un engagement signé, et daté de moins de 3 mois, du MC à signaler à l'AE son départ de l'entité,
- un exemplaire des statuts de l'entreprise, en cours de validité, portant la signature de ses représentants, ou pour une association un procès-verbal de l'assemblée générale portant la signature de ses représentants,
- une pièce, valide au moment de l'enregistrement, portant le numéro SIREN de l'entreprise (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements) ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat,
- un document officiel d'identité en cours de validité du MC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie.

Nota - Le MC doit être informé que les informations personnelles d'identité pourront être utilisées comme élément d'authentification lors de la demande de révocation. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

3.2.3.2 ENREGISTREMENT D'UN RCSI VIA UN MC POUR UN CERTIFICAT SERVEUR A EMETTRE

Le dossier d'enregistrement, déposé auprès d'un MC, doit au moins comprendre :

- un mandat, daté de moins de 3 mois, désignant le futur RCSI comme étant habilité à être RCSI pour le serveur auquel le certificat doit être délivré. Ce mandat doit être signé par le MC et co-signé, pour acceptation, par le futur RCSI bénéficiaire,
- un document officiel d'identité en cours de validité du RCSI comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté au MC qui en transmet une copie à l'AE pour conservation.
- un engagement sur la possession par l'entité du serveur devant recevoir un certificat.

Nota - Le RCSI doit être informé que les informations personnelles d'identité pourront être utilisées comme élément d'authentification lors de la demande de révocation. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

L'authentification du RCSI par le MC est réalisée lors d'un face-à-face physique ou par une méthode apportant un degré d'assurance équivalent.

[6] Si c'est le face-à-face qui est mis en œuvre comme méthode d'authentification, il peut avoir lieu soit au moment de l'enregistrement, soit lors de la remise du certificat.

3.2.3.3 ENREGISTREMENT D'UN NOUVEAU RCSI VIA UN MC POUR UN CERTIFICAT SERVEUR DEJA EMIS

Dans le cas de changement d'un RCSI d'un certificat serveur en cours de validité de ce certificat, le nouveau RCSI doit être enregistré en tant que tel par l'AC en remplacement de l'ancien RCSI.

Le dossier d'enregistrement, déposé auprès d'un MC, doit au moins comprendre :

- un mandat, daté de moins de 3 mois, désignant le futur RCSI comme étant habilité à être le nouveau RCSI pour le serveur auquel le certificat a été délivré, en remplacement du RCSI précédent. Ce mandat doit être signé par le MC et co-signé, pour acceptation, par le futur RCSI,
- un document officiel d'identité en cours de validité du RCSI comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté au MC qui en transmet une copie à l'AE pour conservation.

Nota - Le RCSI doit être informé que les informations personnelles d'identité pourront être utilisées comme élément d'authentification lors de la demande de révocation. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

L'authentification du RCSI par le MC est réalisée lors d'un face-à-face physique ou par une méthode apportant un degré d'assurance équivalent.

3.2.3.4 REMPLACEMENT D'UN MC

En cas de remplacement d'un MC, le nouveau MC doit déposer un dossier d'enregistrement tel que décrit en 3.2.3.1.

3.2.4 INFORMATIONS NON VERIFIEES DU RCSI

La présente PC ne formule pas d'exigence spécifique sur le sujet.

3.2.5 VALIDATION DE L'AUTORITE DU DEMANDEUR

Cette étape est effectuée en même temps que la validation de l'identité de la personne physique (directement par l'AE ou par le MC).

3.2.6 CRITERES D'INTEROPERABILITE

Le cas échéant, l'AC gère et documente les demandes d'accords et les accords de reconnaissance avec des AC extérieures au domaine de sécurité auquel l'AC appartient.

3.3 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLES

Le renouvellement de la biclé d'un serveur entraîne automatiquement la génération et la fourniture d'un nouveau certificat.

3.3.1 IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT COURANT

Lors du renouvellement, la vérification de l'identité du RCSI et des informations du serveur informatique correspondant est optionnelle. Elle est laissée à l'appréciation de l'AC qui engage sa responsabilité quant à la validité des informations contenues dans le certificat renouvelé.

Lors du renouvellement suivant, l'AE, saisie de la demande, identifiera le RCSI et vérifiera les informations du serveur informatique selon la même procédure que pour l'enregistrement initial ou une procédure offrant un niveau de garantie équivalent. Une demande de renouvellement de clé peut être signée à l'aide d'un outil et d'un certificat de signature à un niveau de sécurité au moins équivalent au niveau du certificat demandé.

3.3.2 IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT APRES REVOCATION

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement doit être identique à la procédure d'enregistrement initiale ou doit être une procédure offrant un niveau de garantie équivalent.

3.4 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

La procédure de demande de révocation doit authentifier de façon sûre le demandeur qui doit être l'une des entités autorisées au chapitre 4.9.2.

Si la demande de révocation est faite via un service téléphonique ou via un service en ligne (serveur web), le demandeur doit être formellement authentifié : vérification de l'identité du demandeur et de son autorité par rapport au certificat à révoquer.

Par exemple :

- série d'au moins 3 ou 4 questions / réponses sur des informations propres au demandeur, dont au moins une réponse ne peut réellement être connue que du demandeur (question d'identification personnelle liée au demandeur et/ou dont la réponse a été choisie au moment de l'enregistrement ou lors du retrait du certificat, utilisation d'un identifiant / code confidentiel envoyé préalablement au demandeur de façon sécurisée),
- authentification en ligne à l'aide d'un certificat et d'un outil d'authentification forte,
- signature électronique de la demande à l'aide d'un certificat.

Une demande de révocation peut également être faite par courrier ou par télécopie. Elle doit alors être signée par le demandeur, et le service de gestion des révocations doit s'assurer de l'identité du demandeur (vérification de la signature manuscrite par rapport à une signature préalablement enregistrée) et de son autorité par rapport au certificat à révoquer.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 DEMANDE DE CERTIFICAT

4.1.1 ORIGINE D'UNE DEMANDE DE CERTIFICAT

Un certificat initial est toujours demandé par un responsable de l'entité ou un MC dûment mandaté pour cette entité, avec dans tous les cas consentement préalable du RCSI.

4.1.2 PROCESSUS ET RESPONSABILITES POUR L'ETABLISSEMENT D'UNE DEMANDE DE CERTIFICAT

Les informations suivantes doivent au moins faire partie de la demande de certificat (cf. chapitre 3.2 ci-dessus) :

- L'identifiant du serveur à utiliser dans le certificat ;
- Les données personnelles d'identification du RCSI ;
- Les données d'identification de l'entité (sauf si l'enregistrement est effectué par l'intermédiaire d'un MC) ;

Le dossier de demande est établi soit par le futur RCSI à partir des éléments fournis par son entité, soit par son entité et signé par le futur RCSI. Si l'entreprise n'a pas mis en place de MC, le dossier est transmis directement à l'AE. Si l'entreprise a mis en place un MC, le dossier lui est remis.

4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

4.2.1 EXECUTION DES PROCESSUS D'IDENTIFICATION ET DE VALIDATION DE LA DEMANDE

Les identités "personne physique" et "personne morale" sont vérifiées conformément aux exigences du chapitre 3.2.

L'AE, ou le MC le cas échéant, doit effectuer les opérations suivantes :

- valider l'identifiant du serveur informatique auquel le certificat doit être rattaché ;
- valider l'identité du futur RCSI ;
- vérifier la cohérence des justificatifs présentés ;
- s'assurer que le futur RCSI a pris connaissance des modalités applicables pour l'utilisation du certificat.

Dans le cas d'une demande via un MC, celui-ci retransmet le dossier à l'AE après avoir effectué les opérations ci-dessus. L'AE doit alors s'assurer que la demande correspond bien au mandat du MC.

Une fois ces opérations effectuées et après réception de la requête de certification de la clé publique, l'AE émet la demande de génération du certificat vers la fonction adéquate de l'IGC (cf. chapitre 1.3.1).

L'AE conserve ensuite une trace des justificatifs présentés :

- si le dossier est au format papier, sous la forme d'une photocopie signée à la fois par le futur RCSI et par l'AE, ou le MC le cas échéant, les signatures étant précédées de la mention "copie certifiée conforme à l'original" ;
- si le dossier est au format électronique, les différents justificatifs ayant valeur légale.

4.2.2 ACCEPTATION OU REJET DE LA DEMANDE

En cas de rejet de la demande, l'AE en informe le RCSI, ou le MC le cas échéant, en justifiant le rejet.

4.2.3 DUREE DE VIE DES CERTIFICATS

Le certificat de l'AC racine « *Secure Transactions CA Root – SHA-2 »* est établi pour une durée de 30 ans.

Les certificats de l'AC fille « *Secure Transactions CA Server – SHA-2 »* est établi pour une durée de 20 ans.

Les certificats des IGC de délégataires sont établis pour une durée de 20 ans.

Les certificats des serveurs sont établis pour une durée de 2 ans.

Les certificats des terminaux sont établis pour une durée 10 ans.

La présente PC fera l'objet de révisions périodiques afin de tenir compte de l'évolution des technologies et des recherches dans le domaine de la cryptographie.

4.3 DELIVRANCE DU CERTIFICAT

4.3.1 ACTIONS DE L'AC CONCERNANT LA DELIVRANCE DU CERTIFICAT

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de préparation des différents éléments destinés au RCSI : au minimum, le certificat. (cf. chapitre 1.3.1).

Les conditions de génération des clés et des certificats sont précisées aux chapitres 5 et 6 ci-dessous, notamment la séparation des rôles (cf. chapitre 5.2).

4.3.2 NOTIFICATION PAR L'AC DE LA DELIVRANCE DU CERTIFICAT AU RCSI

La remise du certificat doit se faire en mains propres (face-à-face). Une autre procédure peut être autorisée à condition que le face-à-face ait eu lieu au moment de l'enregistrement du RCSI et que celui-ci puisse être authentifié au moment de la remise.

4.4 ACCEPTATION DU CERTIFICAT

4.4.1 DEMARCHE D'ACCEPTATION DU CERTIFICAT

L'AC doit obtenir confirmation de l'acceptation du certificat par le RCSI de façon explicite sous la forme d'un accord signé et doit conserver une trace de cette acceptation.

4.4.2 PUBLICATION DU CERTIFICAT

Sans objet.

4.4.3 NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU CERTIFICAT

L'AC informe l'AE de la délivrance du certificat, qui se charge d'en informer le MC le cas échéant.

4.5 USAGES DE LA BICLE ET DU CERTIFICAT

Les certificats délivrés par l'AC Secure Transactions CA *Root – SHA-2* et son AC fille *Secure Transactions CA Server SHA-2* sont à destination d'entités du monde de la monétique.

L'AC *Secure Transactions CA Root - SHA-2* émet des certificats pour son AC fille *Secure Transactions CA Server - SHA-2* et pour les IGC de délégataires.

4.5.1 UTILISATION DE LA CLE PRIVEE ET DU CERTIFICAT PAR LE RCSI

Dans les paragraphes qui suivent la clé privée est celle correspondant à la clé publique pour laquelle l'AC *Secure Transactions CA Server SHA-2* ou l'AC-IGC émet le certificat.

4.5.1.1 SERVEURS

La biclé du serveur est générée par l'équipement cryptographique du serveur.

Le certificat correspondant est généré par l'AC *Secure Transactions CA Server – SHA-2*.

L'utilisation de la biclé du serveur est strictement limitée au service d'établissement d'une session sécurisée (de type SSL / TLS) : authentification du client ou du serveur[7], échange de la clé symétrique de session. Les RCSI / MC doivent s'assurer du respect strict des usages autorisés des biclés et des certificats au niveau des serveurs. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la biclé du serveur et du certificat associé doit par ailleurs être indiqué dans le certificat lui-même, via les extensions concernant les usages des clés.

4.5.1.2 IGC DE DELEGATAIRE

La biclé de l'IGC de délégataire est générée par l'équipement cryptographique de l'IGC.

Le certificat correspondant est généré par l'AC *Secure Transactions CA Root - SHA-2.*

L'utilisation de la clé privée d'une IGC de délégataire est strictement limitée au service d'émission de certificats pour des terminaux de paiement électronique, systèmes d'acceptation et éléments associés.

Les RCSI / MC doivent s'assurer du respect strict des usages autorisés des biclés et des certificats au niveau des serveurs. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la biclé de l'IGC délégataire et du certificat associé doit par ailleurs être indiqué dans le certificat lui-même, via les extensions concernant les usages des clés.

4.5.2 UTILISATION DE LA CLE PUBLIQUE ET DU CERTIFICAT PAR L'UTILISATEUR DU CERTIFICAT

Cf. chapitre précédent et chapitre 1.4.

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

4.6 RENOUVELLEMENT D'UN CERTIFICAT

Nota - Conformément au [RFC3647], la notion de "renouvellement de certificat" correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations restant identiques au certificat précédent (y compris la clé publique du RCSI).

La présente PC impose que les certificats aient la même durée de vie que les biclés, il ne peut donc pas y avoir de renouvellement de certificat sans renouvellement de la biclé.

4.7 DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BICLE

Nota - Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat au RCSI liée à la génération d'une nouvelle biclé.

[7] Le serveur d'acceptation est le client de la connexion SSL/TLS, le serveur d'acquisition est le serveur de la connexion.

4.7.1 CAUSES POSSIBLES DE CHANGEMENT D'UNE BICLE

Les biclés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les biclés des serveurs, et les certificats correspondants, seront renouvelés selon les périodicités décrites au chapitre 4.2.3.

Par ailleurs, une biclé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du RCSI (cf. chapitre 4.9, notamment le chapitre 4.9.1 pour les différentes causes possibles de révocation).

Nota - Dans la suite du présent chapitre, le terme utilisé est "fourniture d'un nouveau certificat".

4.7.2 ORIGINE D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

Le déclenchement de la fourniture d'un nouveau certificat serveur peut-être automatique ou bien à l'initiative du RCSI.

L'entité, via son MC le cas échéant, peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un serveur qui lui est rattaché.

4.7.3 PROCEDURE DE TRAITEMENT D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre 3.3 ci-dessus.

Pour les actions de l'AC, cf. chapitre 4.3.1.

4.7.4 NOTIFICATION AU RCSI DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT

Cf. chapitre 4.3.2.

4.7.5 DEMARCHE D'ACCEPTATION DU NOUVEAU CERTIFICAT

Cf. chapitre 4.4.1.

4.7.6 PUBLICATION DU NOUVEAU CERTIFICAT

Cf. chapitre 4.4.2.

4.7.7 NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU NOUVEAU CERTIFICAT

Cf. chapitre 4.4.3.

4.8 MODIFICATION DU CERTIFICAT

Nota - Conformément au [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique et autres que uniquement la modification des dates de validité.

La modification de certificat n'est pas autorisée dans la présente PC.

4.9 REVOCATION ET SUSPENSION DES CERTIFICATS

Nota – La suspension de certificats n'est pas mise en œuvre dans la présente PC.

4.9.1 CAUSES POSSIBLES D'UNE REVOCATION

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat serveur :

- les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple modification d'identifiant du serveur), ceci avant l'expiration normale du certificat ;
- le RCSI n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le RCSI et/ou, le cas échéant, le MC / l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- la clé privée du serveur est suspectée de compromission, est compromise, est perdue ou est volée,
- le RCSI ou une entité autorisée (représentant légal de l'entité ou MC par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du serveur et/ou de son support) ;
- l'arrêt définitif du serveur ou la cessation d'activité de l'entité du RCSI de rattachement du serveur.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.

4.9.2 ORIGINE D'UNE DEMANDE DE REVOCATION

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

- Le RCSI pour le serveur considéré ;
- Le MC ;
- un représentant légal de l'entité ;
- L'AC émettrice du certificat ou l'une de ses composantes (AE).

Nota – Le RCSI est informé des personnes / entités susceptibles d'effectuer une demande de révocation pour son certificat.

4.9.3 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE REVOCATION

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre 3.4.

L'organisation de la révocation est décrite dans la DPC.

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

- L'identifiant du serveur utilisé dans le certificat ;
- Les noms et qualité du demandeur de la révocation ;
- Toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série,...).

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée au minimum via une LCR.

Le demandeur de la révocation, ainsi que le RCSI du certificat s'il n'est pas le demandeur, doivent être informés du bon déroulement de l'opération et de la révocation effective du certificat.

L'entité, directement ou via le MC, est informée de la révocation de tout certificat serveur qui lui sont rattachés.

L'opération est enregistrée dans les journaux d'évènements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat.

Les causes de révocation définitive des certificats ne sont pas publiées.

4.9.4 DELAI ACCORDE AU RCSI POUR FORMULER LA DEMANDE DE REVOCATION

Dès que le RCSI (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation.

4.9.5 DELAI DE TRAITEMENT PAR L'AC D'UNE DEMANDE DE REVOCATION

Une fonction de gestion des révocations doit être disponible les jours ouvrés.

Toute demande de révocation d'un certificat RCSI doit être traitée dans un délai de cinq jours ouvrés, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

4.9.6 EXIGENCES DE VERIFICATION DE LA REVOCATION PAR LES UTILISATEURS DE CERTIFICATS

La vérification de l'état des certificats de l'ensemble de la chaîne de certification correspondante (via LCR) est optionnelle.

4.9.7 FREQUENCE D'ETABLISSEMENT DES LCR

La publication des LCR doit être réalisée à chaque mise à jour.

4.9.8 DELAI MAXIMUM DE PUBLICATION D'UNE LCR

Une LCR doit être publiée dans un délai d'un jour ouvré suivant sa génération.

4.9.9 DISPONIBILITE D'UN SYSTEME DE VERIFICATION EN LIGNE DE LA REVOCATION ET DE L'ETAT DES CERTIFICATS

Le service OCSP n'est pas mis en œuvre par l'IGC.

4.9.10 EXIGENCES DE VERIFICATION EN LIGNE DE LA REVOCATION DES CERTIFICATS PAR LES UTILISATEURS DE CERTIFICATS

Cf. chapitre 4.9.6 ci-dessus.

4.9.11 AUTRES MOYENS DISPONIBLES D'INFORMATION SUR LES REVOCATIONS

Sans objet.

4.9.12 EXIGENCES SPECIFIQUES EN CAS DE COMPROMISSION DE LA CLE PRIVEE

Pour les certificats serveurs, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC la révocation suite à une compromission de la clé privée doit faire l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC *Secure Transactions CA SHA-2* et éventuellement relayée par d'autres moyens.

4.10 FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS

4.10.1 CARACTERISTIQUES OPERATIONNELLES

L'AC doit fournir aux utilisateurs de certificats les moyens de vérifier et valider préalablement à son utilisation, le statut d'un certificat et de sa chaîne de certification c'est à dire vérifier également les signatures des certificats de la chaîne et les signatures garantissant l'origine et l'intégrité des LCR.

La fonction d'information sur l'état des certificats doit mettre à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR. Ces LCR sont des LCR V2.

4.10.2 DISPONIBILITE DE LA FONCTION

La fonction d'information sur l'état des certificats doit être disponible 24h/24 7j/7.

4.10.3 DISPOSITIFS OPTIONNELS

Sans objet.

4.11 FIN DE LA RELATION ENTRE LE RCSI ET L'AC

En cas de fin de relation contractuelle / hiérarchique 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 serveur pour lequel il n'y a plus de RCSI explicitement identifié.

4.12 SEQUESTRE DE CLE ET RECOUVREMENT

Sans objet.

5 MESURES DE SECURITE NON TECHNIQUES

5.1 MESURES DE SECURITE PHYSIQUE

5.1.1 SITUATION GEOGRAPHIQUE ET CONSTRUCTION DES SITES

La présente PC ne formule pas d'exigence spécifique concernant la localisation géographique.

5.1.2 ACCES PHYSIQUE

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services de l'AC, les accès aux locaux des différentes composantes de l'IGC doivent être contrôlés.

Afin d'assurer la disponibilité des systèmes, il est recommandé que l'accès aux machines soit limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.

Nota - On entend par machines l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisés pour la mise en œuvre de ces fonctions.

5.1.3 ALIMENTATION ELECTRIQUE ET CLIMATISATION

Les caractéristiques des équipements d'alimentation électrique et de climatisation doivent permettre de respecter les conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs.

Elles doivent également permettre de respecter les engagements pris par l'AC dans sa PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

L'alimentation en électricité du site hébergeant l'OC et l'AE doit être secourue et le fonctionnement général de l'électricité doit être contrôlé régulièrement. La température du site hébergeant l'OC et l'AE doit être contrôlée et maîtrisée.

5.1.4 VULNERABILITE AUX DEGATS DES EAUX

Les moyens de protection contre les dégâts des eaux doivent permettre de respecter les engagements pris par l'AC dans sa PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

Toute exposition potentielle à l'eau doit être contrôlée et détectée au plus vite afin de prévenir tout risque d'inondation ou de détérioration de matériel de l'OC ou l'AE.

5.1.5 PREVENTION ET PROTECTION INCENDIE

Les moyens de prévention et de lutte contre les incendies doivent permettre de respecter les engagements pris par l'AC dans sa PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

Toute exposition au feu doit être contrôlée et détectée au plus vite afin de prévenir tout risque d'incendie ou de détérioration de matériel de l'OC et l'AE.

5.1.6 CONSERVATION DES SUPPORTS

Les différentes informations intervenant dans les activités de l'IGC doivent être identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations doivent être traités et conservés conformément à ces besoins de sécurité.

5.1.7 MISE HORS SERVICE DES SUPPORTS

En fin de vie, les supports devront être, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes. Les procédures et moyens de destruction et de réinitialisation doivent être conformes à ce niveau de confidentialité.

5.1.8 SAUVEGARDES HORS SITE

En complément de sauvegardes sur sites, il est recommandé que les composantes de l'IGC mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes doivent être organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conforme aux engagements de l'AC dans sa PC en matière de disponibilité, en particulier pour les fonctions de gestion des révocations et d'information sur l'état des certificats.

Les informations sauvegardées hors site doivent respecter les exigences de la présente PC en matière de protection en confidentialité et en intégrité de ces informations.

Les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, au moins, doivent obligatoirement mettre en œuvre des sauvegardes hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.).

5.2 MESURES DE SECURITE PROCEDURALES

5.2.1 ROLES DE CONFIANCE

Chaque composante de l'IGC doit distinguer au moins les cinq rôles fonctionnels[8] de confiance suivants :

- **Officier de sécurité** – L'officier de sécurité est chargé de la mise en œuvre de la politique de sécurité de l'IGC. Il gère les habilitations et les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.
- **Responsable d'application** - Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
- **Ingénieur système** - Il est chargé de l'installation, de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.
- **Opérateur** - Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.
- **Auditeur** - Personne désignée par la Direction de l'AC *Secure Transactions CA SHA-2* et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.

[8] En fonction de la taille de l'entité concernée, de la charge de travail correspondant au rôle, etc., ainsi qu'en fonction des exigences de sécurité et de continuité d'activité, un même rôle fonctionnel peut / doit être tenu par différentes personnes.

En plus de ces rôles de confiance au sein de chaque composante de l'IGC, et en fonction de l'organisation de l'IGC et des outils mis en œuvre, l'AC *Secure Transactions CA SHA-2* est amenée à distinguer également en tant que rôle de confiance, les rôles de porteurs de secrets d'IGC : cf. 6.1 et 6.2

Ces porteurs de secrets ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des secrets qui leur sont confiés.

5.2.2 NOMBRE DE PERSONNES REQUISES PAR TACHES

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Pour des raisons de sécurité, les fonctions sensibles sont réparties sur plusieurs personnes. La présente PC définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC.

La DPC de l'AC précise, en fonction des résultats de son analyse de risque, quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.).

5.2.3 IDENTIFICATION ET AUTHENTIFICATION POUR CHAQUE ROLE

Chaque entité opérant une composante de l'IGC doit faire vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

- que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.

Ces contrôles sont décrits dans la DPC et doivent être conformes à la politique de sécurité de la composante.

Chaque attribution d'un rôle à un membre du personnel de l'IGC doit être notifiée par écrit.

5.2.4 ROLES EXIGEANT UNE SEPARATION DES ATTRIBUTIONS

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non-cumul doivent être respectées.

Les attributions associées à chaque rôle doivent être décrites dans la DPC de l'AC et être conformes à la politique de sécurité de l'AC *Secure Transactions CA SHA-2* concernant les règles de sécurité sur la gestion des clés.

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- auditeur et tout autre rôle ;
- officier de sécurité et ingénieur système / opérateur ;

- ingénieur système et opérateur.

5.3 MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

5.3.1 QUALIFICATIONS, COMPETENCES ET HABILITATIONS REQUISES

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont soumis à une clause de confidentialité vis-à-vis de l'AC *Secure Transactions CA SHA-2*.

Chaque entité opérant une composante de l'IGC doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.

L'AC doit informer toute personne intervenant dans des rôles de confiance de l'IGC :

- de ses responsabilités relatives aux services de l'IGC ;
- des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2 PROCEDURES DE VERIFICATION DES ANTECEDENTS

Chaque entité opérant une composante de l'IGC doit mettre en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante, ceci en conformité avec les règles du droit du travail et les procédures de gestion des ressources humaines appliquées au sein de l'AC *Secure Transactions CA SHA-2* .

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

5.3.3 EXIGENCES EN MATIERE DE FORMATION INITIALE

Le personnel doit être préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à son rôle dans la composante au sein de laquelle il opère.

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

5.3.4 EXIGENCES ET FREQUENCE EN MATIERE DE FORMATION CONTINUE

Le personnel concerné doit recevoir une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

5.3.5 FREQUENCE ET SEQUENCE DE ROTATION ENTRE DIFFERENTES ATTRIBUTIONS

Un personnel ayant détenu une partie d'un secret dans le cadre de son rôle dans une composante de l'AC, ne doit pas pouvoir accéder à un poste qui lui donnerait accès à une autre partie de ce secret.

5.3.6 SANCTIONS EN CAS D'ACTIONS NON AUTORISEES

Les éventuelles sanctions sont décrites dans la DPC.

5.3.7 EXIGENCES VIS-A-VIS DU PERSONNEL DES PRESTATAIRES EXTERNES

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC doit également respecter les exigences du présent chapitre 5.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

En aucun cas, des personnels temporaires (contractuels, stagiaires, etc.) ne peuvent être possesseurs de secrets relatifs à l'activité de l'AC.

5.3.8 DOCUMENTATION FOURNIE AU PERSONNEL

Chaque personnel doit disposer au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille.

5.4 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

La journalisation d'évènements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 TYPE D'EVENEMENTS A ENREGISTRER

Chaque entité opérant une composante de l'IGC doit au minimum journaliser les évènements suivants, automatiquement dès le démarrage d'un système et sous forme électronique, concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre de l'IGC :

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres évènements doivent aussi être recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les accès physiques ;
- les actions de maintenance et de changements de la configuration des systèmes ;
- les changements apportés au personnel ;
- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les RCSI,...).

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'IGC doivent également être journalisés, notamment :

- réception d'une demande de certificat (initiale et renouvellement) ;
- validation / rejet d'une demande de certificat ;

- évènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...) ;
- la génération des éléments secrets du serveur (biclé, codes d'activation,…) ;
- génération des certificats des serveurs ;
- transmission des certificats aux RCSI et, selon les cas, acceptations / rejets explicites par les RCSI ;
- publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
- réception d'une demande de révocation ;
- validation / rejet d'une demande de révocation ;
- génération puis publication des LCR ;

Chaque enregistrement d'un évènement dans un journal doit contenir au minimum les champs suivants :

- type de l'évènement ;
- nom de l'exécutant ou référence du système déclenchant l'évènement ;
- date et heure de l'évènement ;
- résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'évènements.

De plus, en fonction du type de l'évènement, chaque enregistrement devra également contenir les champs suivants :

- destinataire de l'opération ;
- nom du demandeur de l'opération ou référence du système effectuant la demande ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- cause de l'évènement.

Les opérations de journalisation doivent être effectuées au cours du processus.

En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'évènement.

5.4.2 FREQUENCE DE TRAITEMENT DES JOURNAUX D'EVENEMENTS

Cf. chapitre 5.4.8 ci-dessous.

5.4.3 PERIODE DE CONSERVATION DES JOURNAUX D'EVENEMENTS

Les journaux d'évènements doivent être conservés sur site pendant au moins 1 mois. Ils doivent être archivés le plus rapidement possible après leur génération et au plus tard 1 mois (recouvrement possible entre la période de conservation sur site et la période d'archivage).

5.4.4 PROTECTION DES JOURNAUX D'EVENEMENTS

La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements doivent être protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non)

Le système de datation des évènements doit respecter les exigences du chapitre 5.5.5.

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

5.4.5 PROCEDURE DE SAUVEGARDE DES JOURNAUX D'EVENEMENTS

Chaque entité opérant une composante de l'IGC doit mettre en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC et en fonction des résultats de l'analyse de risque de l'AC.

5.4.6 SYSTEME DE COLLECTE DES JOURNAUX D'EVENEMENTS

La présente PC ne formule pas d'exigence spécifique sur le sujet.

5.4.7 NOTIFICATION DE L'ENREGISTREMENT D'UN EVENEMENT AU RESPONSABLE DE L'EVENEMENT

La présente PC ne formule pas d'exigence spécifique sur le sujet.

5.4.8 EVALUATION DES VULNERABILITES

Chaque entité opérant une composante de l'IGC doit être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements doivent être contrôlés une fois par 24h dans les périodes où l'AC est en fonction, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux doivent être analysés dans leur totalité au moins une fois par semaine et dès la détection d'une anomalie. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) doit être une fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

5.5 ARCHIVAGE DES DONNEES

5.5.1 TYPES DE DONNEES A ARCHIVER

Des dispositions en matière d'archivage doivent également être prises par l'AC. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

Il doit également permettre la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC ;
- les DPC ;
- les accords contractuels avec d'autres AC ;
- les certificats et LCR tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les justificatifs d'identité des RCSI et, le cas échéant, de leur entité de rattachement ;
- les journaux d'évènements des différentes entités de l'IGC.

5.5.2 PERIODE DE CONSERVATION DES ARCHIVES

Dossiers de demande de certificat

Tout dossier de demande de certificat accepté doit être archivé pendant au moins cinq ans, comptés au maximum à partir de l'acceptation du certificat par le RCSI.

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées.

Ce dossier, complété par les mentions consignées par l'AE, doit permettre de retrouver l'identité réelle du RCSI responsable, à un instant « *T* » du serveur désigné dans le certificat émis par l'AC.

Certificats et LCR émis par l'AC

Les certificats de serveurs et d'AC, ainsi que les LCR produites, doivent être archivés pendant au moins cinq ans après l'expiration de ces certificats.

Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 seront archivés pendant cinq ans après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage devront offrir le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements devra être assurée tout au long de leur cycle de vie.

Autres journaux

Pour l'archivage des journaux autres que les journaux d'évènements traités au chapitre 5.4, aucune exigence n'est stipulée. La DPC précise les moyens mis en œuvre pour archiver ces journaux.

5.5.3 PROTECTION DES ARCHIVES

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, doivent :

- être protégées en intégrité ;
- être accessibles aux personnes autorisées ;
- pouvoir être relues et exploitées.

5.5.4 PROCEDURE DE SAUVEGARDE DES ARCHIVES

La DPC précise les moyens mis en œuvre pour archiver les pièces en toute sécurité. Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives.

5.5.5 EXIGENCES D'HORODATAGE DES DONNEES

Cf. chapitre 5.4.4 pour la datation des journaux d'évènements.

Les certificats doivent également être datés au moment de leur génération et cette information doit être archivée avec le certificat correspondant.

Le chapitre 6.8 précise les exigences en matière de datation / horodatage.

5.5.6 SYSTEME DE COLLECTE DES ARCHIVES

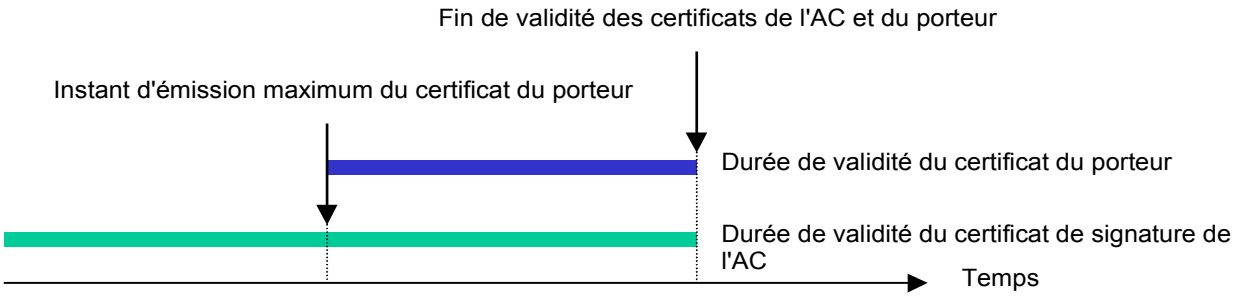
La présente PC ne formule pas d'exigence spécifique sur le sujet, si ce n'est que le système de collecte des archives, qu'il soit interne ou externe, doit respecter les exigences de protection des archives concernées.

5.5.7 PROCEDURES DE RECUPERATION ET DE VERIFICATION DES ARCHIVES

Les archives (papier et électroniques) doivent pouvoir être récupérées dans un délai inférieur à deux jours ouvrés, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

5.6 CHANGEMENT DE CLE D'AC

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



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

Dès qu'une nouvelle biclé d'AC est générée, seule la nouvelle clé privée doit être utilisée pour signer des certificats.

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

5.7 REPRISE SUITE A COMPROMISSION ET SINISTRE

5.7.1 PROCEDURES DE REMONTEE ET DE TRAITEMENT DES INCIDENTS ET DES COMPROMISSIONS

Chaque entité opérant une composante de l'IGC doit mettre 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.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. Le cas de l'incident majeur doit être impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible.

L'AC préviendra sans délai la Direction de l'AC *Secure Transactions CA SHA-2* pour déclenchement d'un sinistre majeur et convocation d'une cellule de crise interne à l'AC *Secure Transactions CA SHA-2*.

5.7.2 PROCEDURES DE REPRISE EN CAS DE CORRUPTION DES RESSOURCES INFORMATIQUES (MATERIELS, LOGICIELS ET / OU DONNEES)

Chaque composante de l'IGC doit disposer d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant des engagements de l'AC et des résultats de l'analyse de risque de l'IGC, notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

Ce plan doit être testé au minimum une fois tous les deux ans.

5.7.3 PROCEDURES DE REPRISE EN CAS DE COMPROMISSION DE LA CLE PRIVEE D'UNE COMPOSANTE

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante doit être traité dans le plan de continuité de la composante (cf. chapitre ci-dessus).

Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué : cf. chapitre 4.9.

5.7.4 CAPACITES DE CONTINUITE D'ACTIVITE SUITE A UN SINISTRE

Les différentes composantes de l'IGC doivent disposer des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC.

5.8 FIN DE VIE DE L'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

Transfert d'activité ou cessation d'activité[9] affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC doit entre autres obligations :

- Mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des RCSI et des informations relatives aux certificats).
- Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC.
- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des RCSI ou des utilisateurs de certificats, l'AC doit les en aviser aussitôt que nécessaire et, au moins, sous un mois.

[9] Cessation d'activité d'une composante autre que l'AC

Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux 1), 2), et 3) ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'un règlement ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans cette PC.

Lors de l'arrêt du service, l'AC doit :

- s'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- révoquer son certificat ;
- révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- informer tous les MC et/ou RCSI des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.

6 MESURES DE SECURITE TECHNIQUES

6.1 GENERATION ET INSTALLATION DE BICLES

6.1.1 GENERATION DES BICLES

6.1.1.1 CLES DE L'AC *SECURE TRANSACTIONS CA SHA-2* ET DES AC FILLES

La génération et la mise en œuvre des clés de signature de l'AC *Secure Transactions CA SHA-2* doit être effectuée dans un environnement sécurisé (cf. chapitre 5) dans un module cryptographique conforme aux exigences de l'annexe 10.2.

La génération des clés de signature de l'AC *Secure Transactions CA SHA-2* doit être effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre 5.2.1), dans le cadre de "cérémonies de clés". Ces cérémonies doivent se dérouler suivant des scripts préalablement définis.

L'initialisation de l'IGC et/ou la génération des clés de signature d'AC peut s'accompagner de la génération de parts de secrets d'IGC. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC.

Par exemple, ces parts de secrets peuvent être des parties de la (ou des) clé(s) privée(s) d'AC, décomposée(s) suivant un schéma à seuil de Shamir (n parties parmi m sont nécessaires et suffisantes pour reconstituer la clé privée), ou encore, il peut s'agir de données permettant de déclencher le chargement sécurisé, dans un nouveau module cryptographique, de la (ou des) clé(s) privée(s) d'AC sauvegardée(s) lors de la cérémonie de clés.

Suite à leur génération, les parts de secrets doivent être remises à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets doit être mise en œuvre par son porteur.

Les cérémonies de clés doivent se dérouler sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins un est externe à l'AC et est impartial. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

6.1.1.2 CLES SERVEURS ET IGC DE DELEGATAIRE GENEREES PAR LEURS EQUIPEMENTS

Cette génération doit être effectuée dans un dispositif aux exigences de l'annexe 10.2. L'AC doit s'en assurer auprès du RCSI, au minimum au travers d'un engagement contractuel clair.

6.1.2 TRANSMISSION DE LA CLE PUBLIQUE A L'AC

La transmission de la clé publique du serveur vers l'AC *Secure Transactions CA Server – SHA-2* devra être protégée en intégrité et son origine devra en être authentifiée.

La transmission de la clé publique de l'IGC de délégataire vers l'AC-IGC devra être protégée en intégrité et son origine devra en être authentifiée.

6.1.3 TRANSMISSION DE LA CHAINE DE CONFIANCE DE L'AC *SECURE TRANSACTIONS CA SHA-2* AUX UTILISATEURS DE CERTIFICATS

La chaîne de confiance composée des certificats d'AC jusqu'à la racine de l'AC *Secure Transactions CA SHA-2* est diffusée auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et qui en authentifie l'origine.

La clé publique de l'AC *Secure Transactions CA SHA-2* est contenue dans un certificat autosigné.

Un certificat racine autosigné ne permet pas de garantir par lui-même que la clé publique correspondante appartient bien à l'AC considérée. Sa diffusion doit s'accompagner de la diffusion, via des sources de confiance, de l'empreinte numérique du certificat, et éventuellement de la clé publique, ainsi que d'une déclaration qu'il s'agit bien d'une clé publique de l'AC.

La clé publique des AC de l'IGC *Secure Transactions CA SHA-2*, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) doivent pouvoir être récupérées aisément par les utilisateurs de certificats.

6.1.4 TAILLES ET PARAMETRES DES CLES

Les clés de l'AC *Secure Transactions CA* root - *SHA-2* sont des clés RSA de 4096 bits.

Les clés de l'AC *Secure Transactions CA server - SHA-2* et de l'AC-IGC sont des clés RSA de 2048 bits.

Les clés des serveurs sont des clés RSA de 2048 bits.

Les clés des IGC de délégataire sont des clés RSA de 2048 bits.

Les clés des terminaux sont des clés RSA de 1024 bits au minimum.

Les exposants publics sont $2^{16} + 1$.

La présente PC fera l'objet de révisions périodiques afin de tenir compte de l'évolution des technologies et des recherches dans le domaine de la cryptographie.

6.1.5 VERIFICATION DE LA GENERATION DES PARAMETRES DES BICLES ET DE LEUR QUALITE

L'équipement de génération de biclés doit utiliser des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la biclé.

6.1.6 OBJECTIFS D'USAGE DES BICLES

L'utilisation d'une clé privée d'IGC et du certificat associé est strictement limitée à la signature de certificats, de LCR (cf. chapitre 1.4.1).

L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service d'établissement d'une session sécurisée SSL / TLS (cf. chapitres 1.4.1).

6.2 MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES

6.2.1 STANDARDS ET MESURES DE SECURITE POUR LES MODULES CRYPTOGRAPHIQUES

6.2.1.1 MODULES CRYPTOGRAPHIQUES DE L'AC *SECURE TRANSACTIONS CA SHA-2* ET DES AC FILLES

Les modules cryptographiques, utilisés par l'AC *Secure Transactions CA SHA-2*, pour la génération et la mise en œuvre de ses clés de signature, ainsi que le cas échéant pour la génération des clés des serveurs, doivent être des modules cryptographiques répondant aux exigences de l'annexe 10.2.

6.2.1.2 DISPOSITIFS DE PROTECTION DE CLES PRIVEES DES SERVEURS ET DES IGC

Les dispositifs de protection de clés privées des serveurs et des IGC, pour la mise en œuvre de leurs clés privées, doivent respecter les exigences de l'annexe 10.2.

La protection des clés privées des serveurs et des IGC est de la responsabilité de l'entité qui les génère par l'intermédiaire de son RCSI.

6.2.2 CONTROLE DE LA CLE PRIVEE DE L'AC PAR PLUSIEURS PERSONNES

Ce chapitre porte sur le contrôle de la clé privée de l'AC *Secure Transactions CA SHA-2*, pour l'exportation / l'importation hors / dans un module cryptographique. La génération de la biclé est traitée au chapitre 6.1.1.1, l'activation de la clé privée au chapitre 6.2.7 et sa destruction au chapitre 6.2.9.

Le contrôle des clés privées de signature de l'AC doit être assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets (systèmes où n exploitants parmi m doivent s'authentifier, avec n au moins égal à 2).

6.2.3 SEQUESTRE DE LA CLE PRIVEE

Ni les clés privées d'AC, ni les clés privées des serveurs ne doivent en aucun cas être séquestrées.

6.2.4 COPIE DE SECOURS DE LA CLE PRIVEE

Les clés privées des serveurs ne doivent faire l'objet d'aucune copie de secours par l'AC.

Les clés privées de l'AC *Secure Transactions CA SHA-2* peuvent faire l'objet de copies de secours, soit dans un module cryptographique conforme aux exigences de l'annexe 10.2, soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuyer sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les opérations de chiffrement et de déchiffrement doivent être effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique.

La longueur des clés symétriques de chiffrement utilisées sera de préférence au moins égale à 128 bits (ex : AES) et en aucun cas inférieur à 100 bits (ex : triple DES).

La taille des blocs utilisés devra être au minimum de 64 bits, et de préférence de 128 bits (triple DES, AES-128 bits). Par ailleurs, le mode opératoire utilisé doit apporter une "bonne sécurité" et permettre de protéger la clé privée de l'AC en confidentialité mais aussi en intégrité. Pour ce faire, le mode opératoire CBC-MAC pourrait être utilisé.

Pour toute information complémentaire sur les algorithmes, il est recommandé de se référer au document sur les règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard de l'agence gouvernementale chargée de la sécurité des systèmes d'information du pays de résidence de l'AC *Secure Transactions CA SHA-2*.

Le contrôle des opérations de chiffrement / déchiffrement doit être conforme aux exigences du chapitre 6.2.2.

6.2.5 ARCHIVAGE DE LA CLE PRIVEE

Les clés privées de l'AC ne doivent en aucun cas être archivée.

Les clés privées des serveurs ne doivent en aucun cas être archivées ni par l'AC ni par aucune des composantes de l'IGC.

6.2.6 STOCKAGE DE LA CLE PRIVEE DANS UN MODULE CRYPTOGRAPHIQUE

Il est recommandé de stocker les clés privées d'AC dans un module cryptographique répondant au minimum aux exigences de l'annexe 10.2.

Cependant, le stockage peut être effectué en dehors d'un module cryptographique moyennant le respect des exigences du chapitre 6.2.4.

6.2.7 METHODE D'ACTIVATION DE LA CLE PRIVEE

6.2.7.1 CLES PRIVEES DE L'AC *SECURE TRANSACTIONS CA SHA-2* ET DES AC FILLES

L'activation des clés privées de l'AC dans un module cryptographique doit être contrôlée via des données d'activation (cf. chapitre 6.4) et doit faire intervenir au moins deux personnes dans des rôles de confiance (par exemple, officier de sécurité et opérateur).

6.2.7.2 CLES PRIVEES DES SERVEURS

La méthode d'activation de la clé privée du serveur dépend du dispositif utilisé par l'entité utilisatrice. L'activation de la clé privée du serveur doit au minimum être contrôlée via des données d'activation (cf. chapitre 6.4).

6.2.8 METHODE DE DESACTIVATION DE LA CLE PRIVEE

6.2.8.1 CLES PRIVEES DE L'AC

La désactivation des clés privées d'AC dans un module cryptographique doit être automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc. Une clé privée d'AC peut également être désactivée après une certaine période d'inactivité.

6.2.8.2 CLES PRIVEES DES SERVEURS ET DES IGC

Les conditions de désactivation de la clé privée d'un serveur et d'une IGC sont de la responsabilité (par l'intermédiaire de son RCSI) de l'entité qui les utilise. Ces conditions doivent garantir un équilibre entre le niveau de sécurité et les besoins d'exploitation basé sur une analyse des risques.

6.2.9 METHODE DE DESTRUCTION DES CLES PRIVEES

6.2.9.1 CLES PRIVEES DE L'AC

La méthode de destruction des clés privées d'AC doit permettre de répondre aux exigences de l'annexe 10.2.

En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), cette clé doit être systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.9.2 CLES PRIVEES DES SERVEURS

En fin de vie de la clé privée d'un serveur, la méthode de destruction de cette clé privée doit permettre de répondre aux exigences de l'annexe 10.2.

6.2.10 NIVEAU D'EVALUATION SECURITE DU MODULE CRYPTOGRAPHIQUE

Les modules cryptographiques de l'AC doivent être évalués au niveau correspondant à l'usage visé, tel que précisé à l'annexe 10.2.

Les dispositifs de protection de clés privées des serveurs doivent être évalués au niveau correspondant à l'usage visé, tel qu'à l'annexe 10.2.

6.3 AUTRES ASPECTS DE LA GESTION DES BICLES

6.3.1 ARCHIVAGE DES CLES PUBLIQUES

Les clés publiques de l'AC, des serveurs et des IGC sont archivées dans le cadre de l'archivage des certificats correspondants.

6.3.2 DUREES DE VIE DES BICLES ET DES CERTIFICATS

Voir chapitre 4.2.3.

6.4 DONNEES D'ACTIVATION

6.4.1 GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION

6.4.1.1 GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION CORRESPONDANT A LA CLE PRIVEE DE L'AC *SECURE TRANSACTIONS CA SHA-2* ET DES AC FILLES

La génération et l'installation des données d'activation d'un module cryptographique de l'AC doivent se faire lors de la phase d'initialisation et de personnalisation de ce module. Si les données d'activation ne sont pas choisies et saisies par les responsables de ces données eux-mêmes, elles doivent leur être transmises de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne doivent être connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. chapitre 5.2.1).

6.4.2 PROTECTION DES DONNEES D'ACTIVATION

6.4.2.1 PROTECTION DES DONNEES D'ACTIVATION CORRESPONDANT A LA CLE PRIVEE DE L'AC

Les données d'activation qui sont générées par l'AC pour les modules cryptographiques de l'AC doivent être protégées en intégrité et en confidentialité jusqu'à la remise à leur porteur. Celui-ci a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

6.4.3 AUTRES ASPECTS LIES AUX DONNEES D'ACTIVATION

Sans objet.

6.5 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

Les mesures de sécurité relatives aux systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque que l'AC doit mener (cf. chapitre 1.3.1).

6.5.1 EXIGENCES DE SECURITE TECHNIQUE SPECIFIQUES AUX SYSTEMES INFORMATIQUES

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'AC est défini dans la DPC de l'AC. Il répond aux objectifs de sécurité suivants :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique) ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- Protection du réseau contre toute intrusion d'une personne non autorisée ;
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- Fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- Eventuellement, gestion des reprises sur erreur.

Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires.

Des dispositifs de surveillance et des procédures d'audit des paramétrages du système doivent être mis en place.

6.5.2 NIVEAU D'EVALUATION SECURITE DES SYSTEMES INFORMATIQUES

La présente PC ne formule pas d'exigence spécifique sur le sujet.

6.6 MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque menée par l'AC.

6.6.1 MESURES DE SECURITE LIEES AU DEVELOPPEMENT DES SYSTEMES

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC doit être documentée. La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau doivent être documentées et contrôlées.

6.6.2 MESURES LIEES A LA GESTION DE LA SECURITE

Toute évolution significative d'un système d'une composante de l'IGC doit être signalée à l'AC pour validation. Elle doit être documentée et doit apparaître dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

6.6.3 NIVEAU D'EVALUATION SECURITE DU CYCLE DE VIE DES SYSTEMES

La présente PC ne formule pas d'exigence spécifique sur le sujet.

6.7 MESURES DE SECURITE RESEAU

L'interconnexion vers des réseaux publics doit être protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.

De plus, les échanges entre composantes au sein de l'IGC peuvent nécessiter la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

Une analyse de risque relative à l'interconnexion devra avoir été menée afin d'établir les objectifs et les solutions de sécurité adaptées.

6.8 HORODATAGE / SYSTEME DE DATATION

Plusieurs exigences de la présente PC nécessitent la datation par les différentes composantes de l'IGC d'évènements liés aux activités de l'IGC.

Pour dater ces évènements, les différentes composantes de l'IGC utilisent 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, cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système doit toutefois pouvoir ordonner les évènements avec une précision suffisante.

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 PROFIL DES CERTIFICATS

7.1.1 CERTIFICATS DE L'AC *SECURE TRANSACTIONS CA ROOT - SHA2*

Ce chapitre porte sur le certificat de clé de l'AC *Secure Transactions CA Root - SHA2* lié à la signature de certificats de serveurs et à la signature de LCR.

7.1.1.1 CHAMPS DE BASE

Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3. Un certificat d'AC doit respecter, de base, les exigences correspondantes du [RFC3280], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Les algorithmes utilisés sont référencés dans le document [RFC3279] et [RFC4055].

Champ	Commentaires
Version	Version 3 : la valeur de ce champ doit être "2"
Serial number	Pas d'exigence supplémentaire par rapport au [RFC3280] (entier positif unique inférieur ou égal à 20 octets)
Signature	Sha2RSA = sha256WithRSAEncryption L'algorithme de signature utilisé est le RSA. La longueur de la clé d'AC Secure Transactions CA Root - SHA2 est 4096 bits. L'algorithme d'empreinte numérique est le SHA-256
Issuer	DN = {C=FR, O= Secure Transactions Certification Authority, CN = Secure Transactions CA Root - SHA2}
Validity	Pas d'exigence supplémentaire par rapport au [RFC3280]
Subject	DN = {C=FR, O= Secure Transactions Certification Authority, CN = Secure Transactions CA Root - SHA2}
Subject Public Key Info	Sha2RSA = sha256WithRSAEncryption L'algorithme de signature utilisé est le RSA. La longueur de la clé de l'AC Secure Transactions CA Root - SHA2 est 4096 bits. L'algorithme d'empreinte numérique est le SHA-256
Extensions	*Cf. chapitre suivant.*

7.1.1.2 EXTENSIONS

Le tableau ci-dessous présente les exigences requises par la présente PC en complément des exigences définies dans [RFC3280], en précisant le caractère obligatoire de chaque extension (colonne "O", O(ui)/N(on)) et sa criticité (colonne "C", O(ui)/N(on)).

Les extensions qui apparaissent dans ce tableau doivent respecter l'ensemble des exigences correspondantes du [RFC3280], moyennant les compléments et/ou modifications d'exigences définis ici.

Les autres extensions traitées dans le [RFC3280] et qui n'apparaissent pas dans ce tableau doivent respecter strictement les exigences du [RFC3280]. Notamment, les extensions obligatoires pour les certificats d'AC (Basic Constraints, Authority / Subject Key Identifiers,...) doivent être intégrées.

L'intégration de ces autres extensions (obligatoires et non obligatoires) doit respecter les exigences de criticité imposées par le [RFC3280]. Lorsque le [RFC3280] n'impose pas d'exigence de criticité, l'extension doit être systématiquement marquée "non critique". De même, l'AC peut intégrer des

extensions non traitées ni dans le [RFC3280] ni dans le présent document, y compris des extensions propriétaires, mais ces extensions doivent obligatoirement être marquées "non critiques".

Champ	O	C	Commentaires
Key Usage	O	O	Signature du certificat, Signature de la liste de révocation de certificats
Basic Constraints	O	O	Type d'objet= Autorité de certification Contrainte de longueur de chemin d'accès=Aucune

7.1.2 CERTIFICATS DE L'AC FILLE *SECURE TRANSACTIONS CA SERVER - SHA2*

Ce chapitre porte sur le certificat de clé de l'AC fille « Secure Transactions CA Server - SHA2 ».

7.1.2.1 CHAMPS DE BASE

Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3. Un certificat d'AC doit respecter, de base, les exigences correspondantes du [RFC3280], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Commentaires
Version	Version 3 : la valeur de ce champ doit être "2"
Serial number	Pas d'exigence supplémentaire par rapport au [RFC3280] (entier positif unique inférieur ou égal à 20 octets)
Signature	Sha2RSA = sha256WithRSAEncryption L'algorithme de signature utilisé est le RSA. La longueur de la clé de l'AC *Secure Transactions CA SHA-2* est 4096 bits. L'algorithme d'empreinte numérique est le SHA-256
Issuer	DN = {C=FR, O= Secure Transactions Certification Authority, CN = Secure Transactions CA Root - SHA2}
Validity	Pas d'exigence supplémentaire par rapport au [RFC3280]
Subject	DN = {C=FR, O= Secure Transactions Certification Authority, CN = Secure Transactions CA Server - SHA2}
Subject Public Key Info	Sha2RSA = sha256WithRSAEncryption L'algorithme de signature utilisé est le RSA. La longueur de la clé de l'AC fille serveur est 2048 bits. L'algorithme d'empreinte numérique est le Sha-256
Extensions	*Cf. chapitre suivant.*

7.1.2.2 EXTENSIONS

Le tableau ci-dessous présente les exigences requises par la présente PC en complément des exigences définies dans [RFC3280], en précisant le caractère obligatoire de chaque extension (colonne "O", O(ui)/N(on)) et sa criticité (colonne "C", O(ui)/N(on)).

Les extensions qui apparaissent dans ce tableau doivent respecter l'ensemble des exigences correspondantes du [RFC3280], moyennant les compléments et/ou modifications d'exigences définis ici.

Les autres extensions traitées dans le [RFC3280] et qui n'apparaissent pas dans ce tableau doivent respecter strictement les exigences du [RFC3280]. Notamment, les extensions obligatoires pour les certificats d'AC (Basic Constraints, Authority / Subject Key Identifiers,...) doivent être intégrées.

L'intégration de ces autres extensions (obligatoires et non obligatoires) doit respecter les exigences de criticité imposées par le [RFC3280]. Lorsque le [RFC3280] n'impose pas d'exigence de criticité, l'extension doit être systématiquement marquée "non critique".

Champ	O	C	Commentaires
Authority Key Identifier	O	N	Valeur du champ "Subject Key Identifier" du certificat de l'AC Secure Transactions CA Root - SHA2
Key Usage	O	O	Signature du certificat, Signature de la liste de révocation de certificats
Basic Constraints	O	O	Type d'objet= Autorité de certification Contrainte de longueur de chemin d'accès=Aucune

7.1.3 CERTIFICATS DES SERVEURS

Ce chapitre porte sur les certificats de clé des serveurs.

7.1.3.1 CHAMPS DE BASE

Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3.

Champ	Commentaires
Version	Version 3 : la valeur de ce champ doit être "2"
Serial number	Pas d'exigence supplémentaire par rapport au [RFC3280] (entier positif unique inférieur ou égal à 20 octets)
Signature	Sha256RSA = sha256WithRSAEncryption L'algorithme de signature utilisé est le RSA. La longueur de la clé de l'AC Serveur est 2048 bits. L'algorithme d'empreinte numérique est le SHA-256
Issuer	DN = {C=FR, O= Secure Transactions Certification Authority, CN = Secure Transactions CA Server - SHA2}
Validity	Pas d'exigence supplémentaire par rapport au [RFC3280]
Subject	DN du serveur
Subject Public Key Info	Sha256RSA = sha256WithRSAEncryption L'algorithme de signature utilisé est le RSA. La longueur de la clé d'un serveur est 2048 bits. L'algorithme d'empreinte numérique est le SHA-256
Extensions	*Cf. chapitre suivant.*

7.1.3.2 EXTENSIONS

Le tableau ci-dessous présente les exigences requises par la présente PC en complément des exigences définies dans [RFC3280], en précisant le caractère obligatoire de chaque extension (colonne "O", O(ui)/N(on)) et sa criticité (colonne "C", O(ui)/N(on)).

Les extensions qui apparaissent dans ce tableau doivent respecter l'ensemble des exigences correspondantes du [RFC3280], moyennant les compléments et/ou modifications d'exigences définis ici.

Les autres extensions traitées dans le [RFC3280] et qui n'apparaissent pas dans ce tableau doivent respecter strictement les exigences du [RFC3280].

L'intégration de ces autres extensions (obligatoires et non obligatoires) doit respecter les exigences de criticité imposées par le [RFC3280]. Lorsque le [RFC3280] n'impose pas d'exigence de criticité, l'extension doit être systématiquement marquée "non critique".

- **Pour l'authentification Serveur (cas des serveurs d'acquisition) :**

Champ	O	C	Commentaires
Authority Key Identifier	O	N	Valeur du champ "Subject Key Identifier" du certificat de l'AC Serveur
Key Usage	O	O	Les bits "keyEncipherment" et "digitalSignature" sont à "1" les autres bits sont à "0"
Certificate Policies	O	N	1.2.250.1.201.1.1.1
Subject Alternative Name	N	N	Adresse IP du serveur DNS Name = Full DNS name of the server
CRL Distribution Points	O	N	http://www.secure-transactions-CA.eu/LCR
Extended Key Usage	O	N	Contient la valeur "id-kp-serverAuth"

- **Pour l'authentification Client (cas des serveurs d'acceptation) :**

Champ	O	C	Commentaires
Authority Key Identifier	O	N	Valeur du champ "Subject Key Identifier" du certificat de l'AC Serveur
Key Usage	O	O	Les bits "keyEncipherment" et "digitalSignature" sont à "1" les autres bits sont à "0"
Certificate Policies	O	N	1.2.250.1.201.1.1.1
Subject Alternative Name	N	N	Adresse IP du serveur DNS Name = Full DNS name of the server
CRL Distribution Points	O	N	http://www.secure-transactions-CA.eu/LCR
Extended Key Usage	O	N	Contient la valeur "id-kp-clientAuth"

7.1.4 CERTIFICATS DES AC DE DELEGATAIRES

Ce chapitre porte sur les certificats de clé des AC de délégataires émis par l'AC-*Secure Transactions CA SHA-2.*

7.1.4.1 CHAMPS DE BASE

Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3. Un certificat d'AC doit respecter, de base, les exigences correspondantes du [RFC3280], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Commentaires
Version	Version 3 : la valeur de ce champ doit être "2"
Serial number	Pas d'exigence supplémentaire par rapport au [RFC3280] (entier positif unique inférieur ou égal à 20 octets)
Signature	Sha2RSA = sha256WithRSAEncryption L'algorithme de signature utilisé est le RSA. La longueur de la clé de l'AC *Secure Transactions CA SHA-2* est 4096 bits. L'algorithme d'empreinte numérique est le Sha-1
Issuer	DN = {C=FR, O= Secure Transactions Certification Authority, CN = Secure Transactions CA Root - SHA2 }
Validity	Pas d'exigence supplémentaire par rapport au [RFC3280]
Subject	DN de l'IGC délégataire
Subject Public Key Info	Sha2RSA = sha256WithRSAEncryption L'algorithme de signature utilisé est le RSA. La longueur de la clé des AC filles est 2048 bits. L'algorithme d'empreinte numérique est le SHA-256
Extensions	*Cf. chapitre suivant.*

7.1.4.2 EXTENSIONS

Le tableau ci-dessous présente les exigences requises par la présente PC en complément des exigences définies dans [RFC3280], en précisant le caractère obligatoire de chaque extension (colonne "O", O(ui)/N(on)) et sa criticité (colonne "C", O(ui)/N(on)).

Les extensions qui apparaissent dans ce tableau doivent respecter l'ensemble des exigences correspondantes du [RFC3280], moyennant les compléments et/ou modifications d'exigences définis ici.

Les autres extensions traitées dans le [RFC3280] et qui n'apparaissent pas dans ce tableau doivent respecter strictement les exigences du [RFC3280]. Notamment, les extensions obligatoires pour les certificats d'AC (Basic Constraints, Authority / Subject Key Identifiers,...) doivent être intégrées.

L'intégration de ces autres extensions (obligatoires et non obligatoires) doit respecter les exigences de criticité imposées par le [RFC3280]. Lorsque le [RFC3280] n'impose pas d'exigence de criticité, l'extension doit être systématiquement marquée "non critique".

Champ	O	C	Commentaires
Authority Key Identifier	O	N	Valeur du champ "Subject Key Identifier" du certificat de l'AC Secure Transactions CA Root - SHA2
Key Usage	O	O	Signature du certificat, Signature de la liste de révocation de certificats
Certificate Policies	O	N	1.2.250.1.201.1.1.1
Basic Constraints	O	O	Type d'objet= Autorité de certification Contrainte de longueur de chemin d'accès=Aucune
CRL Distribution Points	O	N	http://www.secure-transactions-CA.eu/LCR

7.2 LISTE DE CERTIFICATS REVOQUES

7.2.1 CHAMPS DE BASE

Le tableau ci-dessous reprend l'ensemble des champs de base d'une LCR X.509v2. Une LCR doit respecter, de base, les exigences correspondantes du [RFC3280], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Commentaires
Version	Version 2 : la valeur de ce champ doit être "1"
Signature	Sha2RSA = sha256WithRSAEncryption L'algorithme de signature utilisé est le RSA. La longueur de la clé de l'AC Secure Transactions CA Server - SHA2 est 2048 bits. L'algorithme d'empreinte numérique est le SHA-256
Issuer	DN = {C=FR, O= Secure Transactions Certification Authority, CN = Secure Transactions CA Server - SHA2 }
This Update	Pas d'exigence supplémentaire par rapport au [RFC3280]
Next Update	Pas d'exigence supplémentaire par rapport au [RFC3280]
Revoked Certificates	userCertificate : pas d'exigence supplémentaire par rapport au [RFC3280] revocationDate : pas d'exigence supplémentaire par rapport au [RFC3280] crlEntryExtensions : voir chapitre 7.2.2
Extensions de LCR	Cf. chapitre suivant.

7.2.2 EXTENSIONS DE LCR

Champ	O	C	Commentaires
Authority Key Identifier	O	N	Même valeur que le champ "Subject Key Identifier" du certificat de l'AC émettrice.
CRL Number	O	N	Cette extension doit obligatoirement être présente, être marquée "non critique" et être conforme aux exigences du [RFC3280].

7.3 EXTENSIONS D'ENTREE DE LCR

Sans objet.

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

La suite du présent chapitre ne concerne que les audits et évaluation de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC.

8.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC doit procéder à un contrôle de conformité de cette composante.

L'AC doit également procéder une fois tous les deux ans à un contrôle de conformité de l'ensemble de son IGC.

8.2 IDENTITES / QUALIFICATIONS DES EVALUATEURS

Le contrôle d'une composante est réalisé par une équipe d'auditeurs mandatés par la Direction de l'AC *Secure Transactions CA SHA-2*. Les auditeurs doivent être compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

8.3 RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES

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

8.4 SUJETS COUVERTS PAR LES EVALUATIONS

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 vise à vérifier le respect des engagements et pratiques définies dans la présente PC et dans la DPC qui y correspond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

Les audits doivent être réalisés sur la base des référentiels conformes à l'état de l'art. Au minimum toutes les exigences mentionnées dans la PC doivent être audités.

8.5 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

A l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : "réussite", "échec", "à confirmer". Les mesures à prendre doivent suivre les procédures définies et utilisées par la Direction de l'AC *Secure Transactions CA SHA-2*.

8.6 COMMUNICATION DES RESULTATS

Les résultats des audits de conformité seront conservés par la Direction de l'AC *Secure Transactions CA SHA-2*.

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 TARIFS

9.1.1 TARIFS POUR LA FOURNITURE OU LE RENOUVELLEMENT DE CERTIFICATS

Les informations relatives à ce chapitre sont détaillées dans le contrat de souscription attaché aux conditions générales de services.

9.1.2 TARIFS POUR ACCEDER AUX CERTIFICATS

Les informations relatives à ce chapitre sont détaillées dans le contrat de souscription attaché aux conditions générales de services.

9.1.3 TARIFS POUR ACCEDER AUX INFORMATIONS D'ETAT ET DE REVOCATION DES CERTIFICATS

L'accès aux LCR est en accès libre en lecture.

9.1.4 TARIFS POUR D'AUTRES SERVICES

Les informations relatives à ce chapitre sont détaillées dans le contrat de souscription attaché aux conditions générales de services.

9.1.5 POLITIQUE DE REMBOURSEMENT

Les informations relatives à ce chapitre sont détaillées dans le contrat de souscription attaché aux conditions générales de services.

9.2 RESPONSABILITE FINANCIERE

9.2.1 COUVERTURE PAR LES ASSURANCES

L'activité de l'IGC entre dans le cadre de l'activité professionnelle de l'AC *Secure Transactions CA SHA-2* et est couverte par son assurance professionnelle.

9.2.2 AUTRES RESSOURCES

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.2.3 COUVERTURE ET GARANTIE CONCERNANT LES ENTITES UTILISATRICES

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

9.3.1 PERIMETRE DES INFORMATIONS CONFIDENTIELLES

Les informations considérées comme confidentielles sont au moins les suivantes :

- 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[10] ;
- Tous les secrets de l'IGC ;
- Les journaux d'évènements des composantes de l'IGC ;
- Le dossier d'enregistrement du RCSI ;
- Les causes de révocations, sauf accord explicite de publication ;

9.3.2 INFORMATIONS HORS DU PERIMETRE DES INFORMATIONS CONFIDENTIELLES

Sans objet.

9.3.3 RESPONSABILITES EN TERME DE PROTECTION DES INFORMATIONS CONFIDENTIELLES

L'AC est tenue de respecter la législation et la réglementation en vigueur sur son territoire.

9.4 PROTECTION DES DONNEES PERSONNELLES

9.4.1 POLITIQUE DE PROTECTION DES DONNEES PERSONNELLES

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire où elle opère ses services, en particulier de la loi sur la protection des données nominatives.

9.4.2 INFORMATIONS A CARACTERE PERSONNEL

Les informations considérées comme personnelles sont au moins les suivantes :

- Les causes de révocation des certificats des serveurs (qui sont considérées comme confidentielles sauf accord explicite du RCSI) ;
- Le dossier d'enregistrement du RCSI ;
- Le dossier d'enregistrement du MC.

9.4.3 INFORMATIONS A CARACTERE NON PERSONNEL

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.4.4 RESPONSABILITE EN TERMES DE PROTECTION DES DONNEES PERSONNELLES

L'AC *Secure Transactions CA SHA-2* est soumis à la législation et réglementation en vigueur sur le territoire français.

9.4.5 NOTIFICATION ET CONSENTEMENT D'UTILISATION DES DONNEES PERSONNELLES

L'AC *Secure Transactions CA SHA-2* est soumis à la législation et réglementation en vigueur sur le territoire français.

[10] La confidentialité des données d'activation des clés privées des RCSI doit être garantie par l'AC tant qu'elles les détient.

9.4.6 CONDITIONS DE DIVULGATION D'INFORMATIONS PERSONNELLES AUX AUTORITES JUDICIAIRES OU ADMINISTRATIVES

L'AC *Secure Transactions CA SHA-2* est soumis à la législation et réglementation en vigueur sur le territoire français.

9.4.7 AUTRES CIRCONSTANCES DE DIVULGATION D'INFORMATIONS PERSONNELLES

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

La présente PC ne formule pas d'exigence spécifique sur le sujet. Application de la législation et de la réglementation en vigueur sur le territoire français.

9.6 INTERPRETATIONS CONTRACTUELLES ET GARANTIES

Les obligations communes aux composantes de l'IGC sont les suivantes :

- Protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ;
- N'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC *Secure Transactions CA SHA-2* pour les environnements de terminaux de paiement en mode IP et les documents qui en découlent ;
- Respecter et appliquer la partie de la DPC leur incombant ;
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre 8) ;
- Respecter les accords ou contrats qui lient l'AC aux RCSI ;
- Documenter leurs procédures internes de fonctionnement ;
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1 AUTORITES DE CERTIFICATION

L'AC est responsable de la bonne fin de son activité dans le cadre de ses missions au sein de l'AC *Secure Transactions CA SHA-2*.

L'AC a pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un serveur donné et que le RCSI correspondant a accepté le certificat, conformément aux exigences du chapitre 4.4 ci-dessus ;
- Garantir et maintenir la cohérence de sa DPC avec sa PC ;
- Prendre toutes les mesures raisonnables pour s'assurer que ses RCSI sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre un RCSI et l'AC est formalisée par un lien contractuel / hiérarchique précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

9.6.2 AUTORITE D'ENREGISTREMENT

L'AE est responsable de la bonne fin de son activité dans le cadre de ses missions au sein de l'AC *Secure Transactions CA SHA-2*.

Les obligations de l'AE sont inhérentes à sa fonction :

- Vérifier les données d'enregistrement d'un RCSI ;
- Enregistrer un RCSI ;
- Authentifier les demandes de révocation des certificats et transmission à l'AC ;
- Conserver et protéger en confidentialité et en intégrité des données personnelles des RCSI transmises pour l'enregistrement ;
- Respecter et appliquer les procédures de l'AC *Secure Transactions CA SHA-2* ;
- Se soumettre aux audits internes et externes, en respecter les conclusions et remédier aux non-conformités éventuelles ;
- Documenter ses procédures internes de fonctionnement ;
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles l'AE s'engage par le présent document.

9.6.3 RCSI

Le RCSI a le devoir de :

- Prendre connaissance de la présente PC et se conformer aux obligations qui s'appliquent à lui ;
- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- Protéger sa clé privée par des moyens appropriés à son environnement ;
- Protéger ses données d'activation et, le cas échéant, les mettre en place ;
- Protéger l'accès à sa base de certificats ;
- Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- Informer l'AE de toute modification concernant les informations contenues dans son certificat ;
- Faire, sans délai, une demande de révocation de son certificat auprès de l'AE en cas de l'AE, du MC de son entité ou de l'AC en cas de compromission ou de suspicion de compromission de sa clé privée.

La relation entre le RCSI et l'AC ou ses composantes est formalisée par un engagement du RCSI visant à certifier l'exactitude des renseignements et des documents fournis.

9.6.4 UTILISATEURS DE CERTIFICATS

Les applications utilisatrices utilisant les certificats émis par l'AC *Secure Transactions CA SHA-2* doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Vérifier la signature numérique de l'AC émettrice du certificat en parcourant la chaîne de certification jusqu'à l'AC racine de celle-ci ;
- Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC ;
- Contrôler la validité des certificats (dates de validité, statut de révocation).

9.6.5 AUTRES PARTICIPANTS

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.7 LIMITE DE GARANTIE

Sans objet.

9.8 LIMITE DE RESPONSABILITE

L'AC *Secure Transactions CA SHA-2* ne peut être mise en cause en cas de dommages usuellement qualifiés « *d'indirects* » tels que les pertes d'exploitation et autres préjudices commerciaux ou moraux (y compris le dommage à la réputation ou à l'image).

L'AC ne peut être mise en cause pour quelque raison que ce soit dans le cas :

- De mise en œuvre de dispositions afin de protéger l'intégrité de son infrastructure ;
- De dommages résultant d'un cas de force majeure tel que prévu par la jurisprudence française.

9.9 INDEMNITES

Sans objet.

9.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

9.10.1 DUREE DE VALIDITE

La présente PC doit rester en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 FIN ANTICIPEE DE VALIDITE

La publication d'une nouvelle version de la présente PC peut être nécessaire en fonction des évolutions apportées à l'IGC. La mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

9.10.3 EFFETS DE LA FIN DE VALIDITE ET CLAUSES RESTANT APPLICABLES

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.11 NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC devra 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'AC et de ses différentes composantes.

9.12 AMENDEMENTS A LA PC

9.12.1 PROCEDURES D'AMENDEMENTS

En cas de changement important il est recommandé à l'AC de se coordonner avec les responsables d'applications utilisant ses certificats pour en contrôler l'impact.

9.12.2 MECANISME ET PERIODE D'INFORMATION SUR LES AMENDEMENTS

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.12.3 CIRCONSTANCES SELON LESQUELLES L'OID DOIT ETRE CHANGE

L'OID de la PC de l'AC *Secure Transactions CA SHA-2* étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des RCSI, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

9.13 CLAUSE COMPROMISSOIRE

Tout différent relatif au présent document sera résolu définitivement par voie d'arbitrage, conformément aux règles de la Chambre de Commerce Internationale. Les arbitres se réuniront à Paris et statueront selon le droit français.

9.14 JURIDICTIONS COMPETENTES

Sans objet.

9.15 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

L'AC est tenue de respecter la législation et la réglementation en vigueur sur le territoire français.

9.16 DISPOSITIONS DIVERSES

Sans objet.

10 ANNEXES

10.1 RÉFÉRENCES

[9594-8] ISO/IEC 9594-8 (1995) - « Information Technology – Open Systems Interconnection : The Directory : Authentication Framework » (Egalement Recommandation ITU-T X.509 (1997)).

NF ISO/CEI 9594-8 (1996) – « Technologies de l'information – Interconnexions de systèmes ouverts (OSI) – L'annuaire : Cadre d'authentification ».

[CNIL] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Art. 323-1 à 323-3 du Code pénal).

[ETSI_CERT] ETSI - TS 102 280 V1.1.1 - X.509 V3 Certificate Profile for Certificates Issued to Natural Persons, 03/2004

[RFC3279] IETF - Internet X.509 Public Key Infrastructure, Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[RFC3280] IETF - Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, RFC 3280 04/2002

[RFC3647] IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - 11/2003

[RFC3739] IETF - Internet X.509 Public Key Infrastructure, Qualified Certificates Profile, RFC 3726 03/2004

[RFC4055] IETF - Internet X.509 Public Key Infrastructure, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

10.2 EXIGENCES DE SECURITE SUR LES MODULES CRYPTOGRAPHIQUES

10.2.1 EXIGENCES SUR LES OBJECTIFS DE SECURITE

Le dispositif de protection de clés privées, utilisé par le serveur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa biclé, doit répondre aux exigences de sécurité suivantes :

- si la biclé du serveur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la biclé générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer une authentification qui ne peut être falsifiée sans la connaissance de la clé privée ;
- assurer pour le serveur légitime uniquement, d'une part, la fonction d'authentification et, d'autre part, la fonction de déchiffrement de clés symétriques de session, et protéger la clé privée contre toute utilisation par des tiers ;

- permettre de garantir l'authenticité et l'intégrité de la clé symétrique de session, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

Le module cryptographique de l'AC doit détecter les tentatives d'altérations physiques et entrer dans un état sûr quand une tentative d'altération est détectée.

10.2.2 EXIGENCES SUR LA CERTIFICATION

Le module cryptographique utilisé par l'AC doit permettre de démontrer une assurance moyenne que le module cryptographique répond bien aux exigences ci-dessus (équivalent à un niveau EAL2+ des critères communs avec une résistance élevée des mécanismes).

A défaut d'évaluation selon les critères communs, le module cryptographique doit être certifié FIPS 140-2 level 3.