Date : 05/10/2018

Dossier : INFRASTRUCTURE DE GESTION DE CLES
MINISTERE DE L'INTERIEUR

Titre :

POLITIQUES DE CERTIFICATION
AC SERVEUR

OID : 1.2.250.1.152.2.12.41.1

Référence : IGC-MI_PC_ACD_SERV_1.0

Etat :

VERSIONS SUCCESSIVES

Version	*Date*	*Objet de la modification*	*Auteur*
1.0	05/10/2017	• Création	Ministère Intérieur
		•	

TABLE DES MATIERES

1. DEFINITIONS ET ACRONYMES

1.1. ACRONYMES

Les acronymes utilisés dans la présente PC Type sont les suivants :

AA	Autorité Administrative
AC	Autorité de Certification
ACD	Autorité de Certification Déléguée
ACR	Autorité de Certification Racine
AES	Autorité d'Enregistrement Serveur
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AQSSI	Autorité Qualifiée en matière de Sécurité des Systèmes d'Information
CN	Common name ; nom commun
COSSI	Centre Opérationnel en Sécurité des Systèmes d'Information
DIMAP	Direction Interministérielle pour la Modernisation de l'Action Publique
DN	Distinguished Name ; nom distinctif
DPC	Déclaration des Pratiques de Certification
FSSI	Fonctionnaire de Sécurité des Systèmes d'Information
HFD	Haut Fonctionnaire de Défense
HFDA	Haut-Fonctionnaire de Défense Adjoint
IGC	Infrastructure de Gestion de Clés
IGC-MI	Infrastructure de Gestion de Clés du Ministère de l'Intérieur
ISO	International Organization for Standardization
LAR	Liste des certificats d'AC Révoqués
LCRs	Liste des Certificats Révoqués
MI	Ministère de l'Intérieur
OCSP	Online Certificate Status Protocol
OID	Object Identifier (Identifiant d'Objet)
PC	Politique de Certification
RCAS	Responsable du Certificat Authentification Serveur
RCC	Responsable du Certificat de Cachet
RIO	Référentiel des Identités et de l'Organisation
RSA	Rivest Shamir Adelman
SGDSN	Secrétariat Général de la Défense et de la Sécurité Nationale
SHFD	Service du Haut-Fonctionnaire de Défense
SHA-1	Secure Hash Algorithm version 1
SHA-2	Secure Hash Algorithm version 2
SP	Service de Publication

SSL	Secure Sockets Layer
TLS	Transport Layer Security
UC	Utilisateur de Certificats
URL	"Uniform Resource Locator"

1.2. DEFINITIONS

Les termes utilisés dans la présente PC sont les suivants :

Agent – Personne physique agissant pour le compte d'une autorité administrative.

Applicatif de vérification de cachet – Il s'agit de l'application mise en œuvre par l'utilisateur pour vérifier le cachet des données reçues à partir de la clé publique du serveur contenue dans le certificat correspondant.

Applicatif de vérification d'authentification – Il s'agit de l'application mise en œuvre par l'utilisateur ou le serveur pour vérifier l'authentification d'un autre serveur et établir une session sécurisée avec ce serveur, notamment générer la clé symétrique de session et la chiffrer avec la clé publique du serveur contenue dans le certificat correspondant.

Applications utilisatrices – Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur du certificat ou des besoins d'authentification ou de cachet du serveur auquel le certificat est rattaché.

Autorités administratives – Ce terme générique, défini à l'article 1 de [ORD05-1516], désigne les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.

Autorité d'enregistrement – *Cf.* chapitre 2.3.3.

Autorité d'horodatage – Autorité responsable de la gestion d'un service d'horodatage (*cf.* politique d'horodatage type du [RGS]).

Autorité de certification (AC) – Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre 2.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

Certificat électronique – Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Dans le cadre de la présente PC, le terme "certificat électronique" désigne uniquement un certificat délivré à un serveur informatique sous la responsabilité d'un RCC/RCAS et portant sur une bi-clé de cachet de données, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

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. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

Déclaration des pratiques de certification (DPC) – Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Dispositif de création de cachet – Il s'agit du dispositif matériel et/ou logiciel utilisé par le serveur pour stocker et mettre en œuvre sa clé privée pour la création de cachet.

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

Entité – Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

Fonction de génération des certificats – *Cf.* chapitre 2.3.2.

Fonction de génération des éléments secrets du porteur – *Cf.* chapitre 2.3.2.

Fonction de gestion des révocations – *Cf.* chapitre 2.3.2.

Fonction de publication – *Cf.* chapitre 2.3.2 .

Fonction de remise – *Cf.* chapitre 5.3.

Fonction d'information sur l'état des certificats – *Cf.* chapitre2.3.2.

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.

Opérateur demandeur – Cf. chapitre 1.3.4

Personne autorisée – Il s'agit d'une personne autre que le RCAS ou le RCC et qui est autorisé par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du RCC/RCAS (demande de révocation, de renouvellement…). Typiquement dans une administration il peut s'agit d'un responsable hiérarchique du RCC/RCAS ou d'un responsable RH.

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 RCC/RCAS et les utilisateurs de certificats.

Porteur – *Cf.* chapitre 2.3.5.

Prestataire de services de certification électronique (PSCE) – L'[ORD05-1516] introduit et définit les prestataires de service de confiance (PSCO). Un PSCE est un type de PSCO particulier. Un PSCE se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des RCC/RCAS et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (ACR / ACD). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

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.

Promoteur d'application – Un responsable d'un service de la sphère publique accessible par voie électronique.

Qualification d'un prestataire de services de certification électronique – Le [DécretRGS] décrit la procédure de qualification des PSCO. Un PSCE étant un PSCO particulier, la qualification d'un PSCE est un acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de certification électronique d'un PSCE (famille de certificats) à certaines exigences d'une PC pour un niveau de sécurité donné et correspondant au service visé par les certificats.

Qualification d'un produit de sécurité – Acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les fonctions de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le [RGS]. La procédure de

qualification des produits de sécurité est décrite dans le [DécretRGS]. Le [RGS] précise les trois processus de qualification : qualification de niveau élémentaire, qualification de niveau standard et qualification de niveau renforcé.

Responsable du certificat de cachet – *Cf.* chapitre 2.3.3.

Responsable du certificat authentification serveur – *Cf.* chapitre 2.3.5.

Serveur informatique – Il s'agit d'un service applicatif (disposant d'un certificat fourni par l'AC) rattaché à l'entité, (identifiée dans le certificat) détenant le nom de domaine correspondant au service ou en charge de ce service.

Système d'information – Tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.

Usager – Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques avec des autorités administratives.

Nota – Un agent d'une autorité administrative qui procède à des échanges électroniques avec une autre autorité administrative est, pour cette dernière, un usager.

Utilisateur de certificat – *Cf.* chapitre 2.3.6.

2. INTRODUCTION

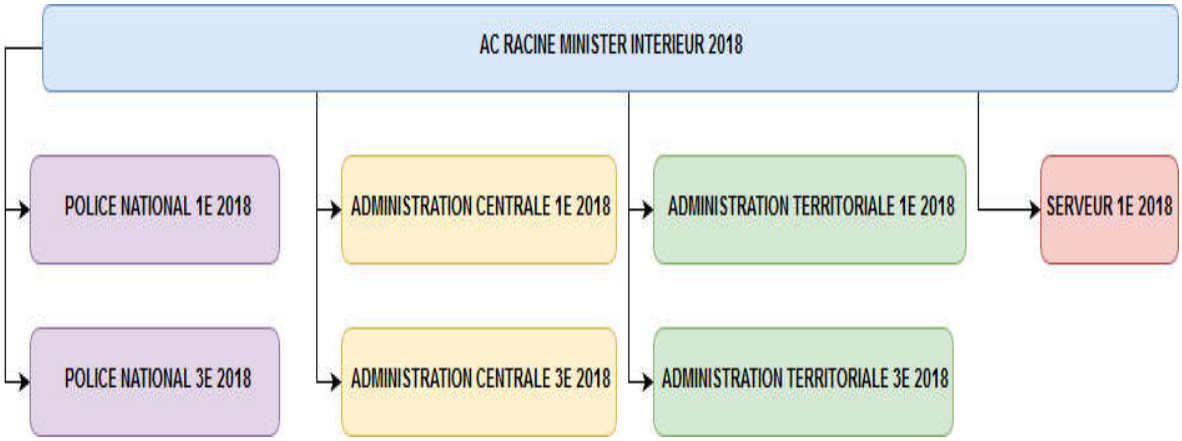
2.1. PRESENTATION GENERALE

Pour assurer la sécurité des échanges d'information au format numérique entre l'administration et les usagers, entre l'administration et ses agents, ainsi qu'entre les administrations, le Ministère de l'Intérieur a décidé de se doter d'une IGC (infrastructure de gestion de clés).

L'IGC du Ministère de l'Intérieur est constituée d'une hiérarchie de 3 niveaux de certificats :

- Certificats de l'AC RACINE MINISTERE DE L'INTERIEUR 2018 :
- Certificat AC DELEGUEES du Ministère de l'Intérieur :
- Certificats utilisateurs finaux :

L'arborescence de certification de l'IGC-MI est décrite ci-dessous :



Ce document traite de la politique de certification de l'autorité de certification déléguée du ministère relative à la délivrance de certificats serveurs de niveau de sécurité conforme au RGS *.

Cette autorité de certification délivre les certificats aux serveurs, aux clients applicatifs, aux équipements réseaux et aux serveurs d'horodatage du ministère de l'Intérieur.

L' AC SERVEUR 1E 2018 concernée par le présent document est l'AC SERVEUR 1E 2018. Elle sera utilisée pour délivrer plusieurs gammes de certificats pour répondre aux besoins du ministère de l'Intérieur.

Les gammes de certificats sont répondant aux exigences RGS 1* :

- Certificat SSL Client
- Certificat SSL Serveur
- Certificat Serveur Cachet Signature

Le présent document fait partie d'un ensemble de documents décrivant les politiques de certification définies dans le cadre du projet IGC Ministère de l'Intérieur pour l'AC **SERVEUR 1E 2018.**

Il spécifie les exigences applicables pour :

- la génération et le renouvellement de ses clés respectives,
- la certification, le renouvellement, et la révocation des clés publiques des certificats des porteurs machines,
- la génération des clés pour les certificats de type porteurs machine et la demande de certificats auprès de l'AC SERVEUR 1E 2018.

2.2. IDENTIFICATION

Ce document est identifié par l'OID **1.2.250.1.152.2.12.41.1**

Compte tenu de la très grande similarité entre les politiques des certificats de cachet *, et d'authentification serveur *, le présent document rassemble les PC correspondant à chacun de ces types de certificats le format des certificats est référencé dans le document [PC_A1_FORM_CERT].

Pour chaque type de certificats authentification, le tableau ci-dessous présente le type de certificat et l'identifiant d'objet (OID) correspondant :

2.2.1. CERTIFICATS DE TYPE AUTHENTIFICATION SSL

AC	CERTIFICATS	OID
SERVEUR 1E 2018	Certificat SSL Serveur 1* MultiSAN	1.2.250.1.152.2.12.41.1.21
	Certificat SSL Serveur 1*	1.2.250.1.152.2.12.41.1.2
	Certificat SSL Client 1*	1.2.250.1.152.2.12.41.1.3
	Certificat SSL Client 1* Multisan	1.2.250.1.152.2.12.41.1.31

2.2.2. CERTIFICATS DE TYPE CACHET SIGNATURE

Des certificats de type « cachet signature » peuvent être déclinés pour des usages spécifiques non détaillés dans le RGS et réservés dans un premier temps à l'usage interne du ministère.

AC	CERTIFICATS	OID
SERVEUR 1E 2018	Certificat Serveur Cachet 1*	1.2.250.1.152.2.12.41.1.5
	Certificat Contrôleur Domaine AD 1*	1.2.250.1.152.2.12.41.1.4
	Certificat Serveur OCSP 1*	1.2.250.1.152.2.12.41.1.6
	Certificat Signature de code 1*	1.2.250.1.152.2.12.41.1.8
	Certificat Serveur Horodatage 1*	1.2.250.1.152.2.12.41.1.11

2.2.3. CONVENTIONS TYPOGRAPHIQUES

Dans le cas où l'une des politiques se distingue des autres, les paragraphes applicables à l'une ou plusieurs d'entre elles seront marqués avec le ou les étiquettes suivantes :

Politique	Étiquette
Cachet Signature *	***[C-SIG]***
Authentification client *	***[A-CLI]***
Authentification Serveur *	***[A-SER]***
Cachet Horodatage *	***[C-HOR]***

2.3. ENTITES INTERVENANT DANS L'IGC-MI

2.3.1. AUTORITE ADMINISTRATIVE

L'AA est l'autorité administrative au sens de [ORD05-1516] – c'est-à-dire le représentant légal de l'État responsable de l'IGC-MI.

L'AA est le secrétaire général, Haut-fonctionnaire de défense, représenté par le haut-fonctionnaire de défense adjoint.

Les fonctions assurées par l'autorité administrative en tant que responsable de l'ensemble de l'IGC-MI sont les suivantes :

- rendre accessible l'ensemble des prestations déclarées dans la PC aux demandeurs de certificats, aux Autorités de Certification Déléguées, aux porteurs et aux tiers utilisateurs,
- s'assurer que les exigences de la PC et les procédures de la DPC sont adéquates et conformes aux normes en vigueur,
- s'assurer que ces exigences et procédures sont appliquées par chacun des détenteurs de rôles auprès de l'IGC-MI,
- de s'assurer de la mise en œuvre des mesures de sécurité techniques et non techniques nécessaires pour couvrir les risques identifiés et assurer la continuité de l'activité de l'IGC-MI en conformité avec les exigences de la présente PC,
- de s'assurer de la mise en œuvre des différentes fonctions identifiées dans la PC, notamment en matière de génération des certificats, de remise de certificats, 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 présente PC, notamment en termes de fiabilité, de qualité et de sécurité,
- générer, et renouveler lorsque nécessaire, les bi-clés de l'AC SERVEUR 1E 2018 et les certificats correspondants (signature de certificats, et de LCRs), puis diffuser ses certificats d'AC aux tiers utilisateurs.

2.3.2. AUTORITES DE CERTIFICATION

L'AC SERVEUR 1E 2018 a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...) et s'appuient pour cela sur l'IGC-MI.

Les prestations de l'AC SERVEUR 1E 2018 est le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats :

Fonction de génération des certificats :

Cette fonction génère les certificats (cachet serveur, authentification serveur) à partir des informations transmises par l'autorité d'enregistrement serveur.

Fonction de publication :

Cette fonction met à disposition des différentes parties concernées les différents documents établis par l'AC (Politiques et Pratiques…), les certificats d'AC et toute autre information pertinente destinée aux demandeurs, aux porteurs et aux tiers utilisateurs de certificat, hors informations d'état des certificats.

Fonction de gestion des révocations :

Dans le cadre de cette fonction, l'AC SERVEUR 1E 2018 traite les demandes de révocation (notamment identification et authentification du demandeur) et déterminent 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 tiers utilisateurs de certificats des informations sur l'état des certificats (révoqués, non révoqués). Cette fonction est mise en œuvre par publication d'informations de révocation sous forme de LCRs.

2.3.3. AUTORITE D'ENREGISTREMENT SERVEUR

L'opérateur AE Serveur a pour rôle :

- l'envoi à l'AC des demandes de certificats préalablement vérifié et validé par l'RCC/RCAS
- l'envoi à l'AC des demandes de révocation des certificats après validation du RSSI de la demande de révocation initiées par le RCC/RCAS.

2.3.4. OPERATEUR DEMANDEUR

Dans les entités du ministère susceptibles de demander des certificats serveurs, il est désigné un ou plusieurs opérateur(s) demandeur(s) chargé(s) d'initialiser la demande de certificats qui est transmise à un RCC/RCAS. Les demandes sont réalisées dans le système de gestion des cartes et des certificats après authentification forte par carte agent ministérielle.

2.3.5. RESPONSABLES DE CERTIFICATS DE CACHETS, RESPONSABLES DE CERTIFICATS D'AUTHENTIFICATION SERVEUR

RCC : le responsable du certificat de cachet est la personne physique responsable de l'utilisation du certificat de cachet du serveur identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'entité également identifiée dans ce certificat.

RCAS : le responsable de certificat d'authentification serveur est une personne physique qui est responsable de l'utilisation du certificat d'authentification du serveur identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'entité également identifiée dans ce certificat.

Le RCC, et le RCAS respectent les conditions qui leur incombent définies dans la PC de l'AC SERVEUR 1E 2018. Il est chargé localement de la fonction d'administration des opérateurs demandeurs. .

2.3.6. UTILISATEURS DE CERTIFICATS

La présente PC Type traitant de certificats de cachet (*cf.* chapitre 1.4), un utilisateur de certificats peut être notamment :

- **Un agent (personne physique) :**
  - Destinataire de données signées par un serveur informatique et qui utilise un certificat et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises par le serveur identifié dans le certificat.
  - Accédant à un serveur informatique et qui utilise le certificat du serveur et un module de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat du serveur, afin d'établir une clé de session partagée entre son poste et le serveur.
  - L'agent respecte la politique et les pratiques de sécurité édictées par le responsable de son entité.
- **Un usager :**
  - Destinataire de données provenant d'un serveur informatique d'une autorité administrative et qui utilise un certificat et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises par le serveur identifié dans le certificat.
  - Accédant à un serveur informatique d'une autorité administrative et qui utilise le certificat du serveur et un module de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat, afin d'établir une clé de session partagée entre son poste et le serveur.

- **Un serveur informatique :**
  - Destinataire de données provenant d'un autre serveur informatique et qui utilise un certificat et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises par le serveur identifié dans le certificat.
  - Accédant à un autre serveur informatique et qui utilise un certificat et un applicatif de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat, et afin d'établir une clé de session partagée entre les deux serveurs.

2.3.7. AUTRES PARTICIPANTS

*2.3.7.1. Composantes de l'**IGC-MI***

La décomposition en fonctions de l'IGC-MI est présentée au chapitre 2.3.1. Les composantes de l'IGC-MI mettant en œuvre ces fonctions sont présentées dans la DPC de l'AC.

2.3.7.1.1. SUPPORT EN LIGNE

Le support en ligne est un service téléphonique disponible aux RCC/RCAS pour assurer des fonctions de supports notamment en cas de compromission de la clé privée du serveur.
Les services du support en ligne nécessitent une authentification du RCC/RCAS.

2.3.7.1.2. SYSTEME DE GESTION DES CARTES ET DES CERTIFICATS

C'est le cœur du système de l'IGC-MI, le système de gestion des cartes est en charge de la gestion :

- des processus de gestion du cycle de vie des certificats des machines, la synchronisation des données, ainsi que la coordination de tous les traitements avec les autres composantes,
- des droits et des profils pour l'accès aux services de l'IGC-MI, notamment de l'AE serveurs,
- des interfaces d'accès aux services (génération certificat, génération de LCRs) avec l'AC SERVEUR 1E 2018,
- Des échanges avec le référentiel de gestion d'identité du ministère pour l'import des données d'enregistrement des titulaires de certificats personnes (sauf pour les certificats serveurs),
- Des traitements automatiques liés aux cycles de vie des certificats serveurs et des notifications aux autres composantes.

2.3.7.1.3. PORTAIL SELF-SERVICE

Le portail *self-service* est un composant de l'IGC-MI qui permet de fournir des services après l'émission des certificats personnes. Le portail *self-service* n'est pas utilisé pour gérer les certificats serveurs.
Le renouvellement par protocole SCEP (Simple Certificate Enrollment Protocol) sera proposé en renouvellement pour les applications compatibles sous conditions de sécurité.

2.4. USAGE DES CERTIFICATS

2.4.1. DOMAINES D'UTILISATION APPLICABLES

2.4.1.1. Bi-Clés et certificats du serveur informatique

La présente PC traite des bi-clés et des certificats utilisés par des services applicatifs déployés sur des serveurs informatiques dont la fonction est :

- de signer des données, afin que les catégories d'utilisateurs de certificats identifiées au chapitre 2.3.6 puissent en vérifier la signature (le cachet). Ces données peuvent être, par exemple, un accusé de réception suite à la transmission d'informations par un usager à un

serveur informatique, une réponse automatique d'un serveur informatique à une demande formulée par un usager ou la signature d'un jeton d'horodatage.

- de permettre que ces serveurs puissent être authentifiés dans le cadre de l'établissement de sessions sécurisées, de type SSL/TLS, avec les catégories d'utilisateurs de certificats identifiées au chapitre 2.3.6 et établir une clé symétrique de session afin que les échanges au sein de ces sessions soient chiffrés.

Ceci correspond notamment aux relations suivantes :

- apposition d'un cachet signature sur des données par un serveur informatique d'une autorité administrative et vérification de ce cachet par un usager,
- apposition d'un cachet signature sur des données par un serveur informatique et vérification de ce cachet par un agent,
- apposition d'un cachet signature sur des données par un serveur informatique et vérification de ce cachet par un autre serveur informatique.
- établissement d'une session sécurisée entre un serveur d'une autorité administrative et un usager,
- établissement d'une session sécurisée entre un serveur et un agent,
- établissement d'une session sécurisée entre deux serveurs.

2.4.1.2. Bi-Clés et certificats d'AC et de composantes

Cette PC comporte également des exigences, concernant les bi-clés et certificats de l'AC SERVEUR 1E 2018 (signature des certificats des porteurs machines, et signature des LCRs).

L'AC SERVEUR 1E 2018 génère et signe différents types d'objets : certificats finaux, LCRs, réponses OCSP.

Pour signer ces objets, l'AC SERVEUR 1E 2018 dispose d'une bi-clé, et d'un certificat dédiés, rattaché à l'ACR MINISTERE INTERIEUR 2018.

2.4.2. DOMAINES D'UTILISATION INTERDITS

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 5.5. L'AC respecte ces restrictions et impose leur respect par les RCC et les RCAS auxquels elle délivre des certificats cachet et d'authentification serveur, ainsi qu'aux utilisateurs de ces certificats serveur.

2.5. GESTION DE LA PC

2.5.1. ENTITE GERANT LA PC

L'AC SERVEUR 1E 2018 est responsables de l'établissement des présentes Politique de Certification, ainsi que de son application et de sa diffusion.

L'Autorité Administrative afférente est responsable de la validation des présentes PC.

2.5.2. POINT DE CONTACT

Toute demande d'information devra se faire auprès du :

Ministère de l'Intérieur
Secrétaire Général
Service du Haut Fonctionnaire de Défense
Place Beauvau
75800 PARIS CEDEX 08
Adresse pour le courriel : igc-mi@interieur.gouv.fr

2.5.3. ENTITE DETERMINANT LA CONFORMITE D'UNE DPC AVEC CETTE PC

L'AA détermine la conformité des DPC avec les présentes politiques de certification, soit directement soit indirectement en faisant appel à des experts indépendants spécialisés dans le domaine de la sécurité et des IGC.

2.5.4. PROCEDURES D'APPROBATION DE LA CONFORMITE DE LA DPC

La DPC est approuvée par l'AA afférente.

3. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

3.1. ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

Pour la mise à disposition des informations devant être publiées à destination des RCC /RCAS et des utilisateurs de certificats, l'AC SERVEUR 1E 2018 met en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats.

L'entité en charge de la publication de ces informations est l'autorité administrative : les PC et les certificats d'AC sont mis à disposition par le SHFD.

3.2. INFORMATIONS DEVANT ETRE PUBLIEES

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

- la PC de l'AC SERVEUR 1E 2018 en cours de validité,
- les versions antérieures de la présente Politique de Certification, tant que des certificats émis selon ces versions sont en cours de validité,
- les profils des certificats de l'AC SERVEUR 1E 2018, des certificats cachets, certificats authentification serveur, et des LCRs émises,
- les certificats de l'AC SERVEUR 1E 2018, en cours de validité et les informations permettant aux tiers utilisateurs de certificats de s'assurer de l'origine de ces certificats (empreintes),
- les LCRs en cours de validité, conforme au profil indiqué en paragraphe 7 et accessible par le protocole HTTP,
- l'adresse (URL) permettant d'obtenir des informations concernant l'AC SERVEUR 1E 2018.

3.3. DELAIS ET FREQUENCES DE PUBLICATION

Toute nouvelle version d'un document (PC, formats des certificats) est diffusée via le site Web du Ministère de l'Intérieur dans les 24h ouvrées suivant sa validation. Le site est accessible 24 heures / 24 et 7 jours / 7.

Les certificats d'AC sont diffusés dans le serveur web http://crl.interieur.gouv.fr du ministère préalablement à toute diffusion de certificats de porteurs et/ou de LCRs correspondants et les systèmes les publiant ont une disponibilité de 24 heures / 24 et 7 jours / 7.

3.4. CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'ensemble des informations publiées à destination des utilisateurs de certificats sont libres d'accès en lecture aux adresses suivantes

- Pour la publication des LCRs et des certificats d'AC : http://crl.interieur.gouv.fr,
- Pour les autres informations : https://www.interieur.gouv.fr/IGC.

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

L'accès en modification aux systèmes de publication des autres informations est strictement limité aux fonctions internes habilitées de l'IGC-MI.

4. IDENTIFICATION ET AUTHENTIFICATION

4.1. NOMMAGE

4.1.1. TYPES DE NOMS

Les noms utilisés dans les certificats émis par l'IGC-MI sont conformes aux spécifications de la norme X.500.

Dans chaque certificat conforme à la norme X.509, l'AC SERVEUR 1E 2018 émettrice (*issuer*) et le porteur machine (*subject*) sont identifiés par un *"Distinguished Name"* (DN) en UTF8String.

Des règles sur la construction du DN de ces champs sont précisées ci-dessous.

4.1.1.1. Certificat d'AC

Champ	SERVEUR 1E 2018
Issuer	CN=AC RACINE MINSTERE INTERIEUR 2018 OU=SERVEURS OU=0002 110014016 O=MINISTERE INTERIEUR C=FR
Subject	CN=SERVEUR 1E 2018 OU=SERVEURS OU=0002 110014016 O=MINISTERE INTERIEUR C=FR

4.1.1.2. Certificat porteur machine

Champ	Certificats de type Cachet Signature	Certificats de type authentification SSL
Issuer	CN= SERVEUR 1E 2018 OU=SERVEURS OU=0002 110014016 O=MINISTERE INTERIEUR C=FR	
Subject	CN= « Nom du serveur Cachet » OU=SERVEURS OU=0002 110014016 O=MINISTERE INTERIEUR C=FR	CN= « Nom FQDN » ou « Nom Service applicatif » OU=SERVEURS OU=0002 110014016 O=MINISTERE INTERIEUR C=FR

4.1.2. NECESSITE D'UTILISATION DE NOMS EXPLICITES

Les noms choisis pour désigner les services de création de cachet dans les certificats sont explicites.
L'identification de l'entité à laquelle ce service est rattaché est obligatoire.

4.1.3. ANONYMISATION OU PSEUDONYMISATION DES SERVICES DE CREATION DE CACHET

Sans objet.

4.1.4. REGLES D'INTERPRETATION DES DIFFERENTES FORMES DE NOM

Le document [PC-A1-FORM-CERT] fournit des règles à ce sujet.

4.1.5. UNICITE DES NOMS

Afin d'assurer l'identification unique du nom du service de création d'un cachet d'un serveur au sein du domaine de l'AC ainsi que l'entité à laquelle ce service est rattaché, notamment dans le cas du renouvellement du certificat associé, et pour éviter toute ambiguïté, le DN du champ "*subject*" de chaque certificat cachet permet d'identifier de façon unique le couple {nom du service de création d'un cachet ; entité de rattachement} au sein du domaine de l'AC.

Afin d'assurer l'identification unique du FQDN d'un serveur au sein du domaine de l'AC, notamment dans le cas du renouvellement du certificat associé, et pour éviter toute ambiguïté, le DN du champ "subject" de chaque certificat d'authentification serveur doit permettre d'identifier de façon unique le FQDN du serveur au sein du domaine de l'AC. Durant toute la durée de vie de l'AC, le FQDN d'un serveur rattaché à une entité ne peut être attribué à une autre entité.

4.1.6. IDENTIFICATION, AUTHENTIFICATION ET ROLE DES MARQUES DEPOSEES

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

4.2. VALIDATION INITIALE DE L'IDENTITE

L'enregistrement d'un serveur auquel un certificat est délivré se fait via l'enregistrement du RCC/RCAS correspondant.

[A-SER] Le RCAS devra démontrer que le nom de domaine inclus dans le FQDN du serveur appartient bien au ministère de l'Intérieur.

4.2.1. METHODE POUR PROUVER LA POSSESSION DE LA CLE PRIVEE

Les bi-clés des certificats porteurs machines ne sont pas générées par l'AC. Le demandeur fournit la requête PKCS#10 (signée par la clé privée de l'équipement, ou du serveur) qui constitue la preuve de possession de la clé privée. Le RCC/RCAS vérifie et valide la demande qui sera générée par l'opération AES.

Pour les certificats de niveau de confiance 1*, il est recommandé que les bi-clés soient générées dans un dispositif de protection qualifié au minimum au niveau standard (HSM ou dispositif équivalent). Ce type de dispositif est obligatoire pour les certificats de type « cachet », « OCSP » ou « horodatage ». Il en est de même pour le stockage et la mise en œuvre de la clé privée.

4.2.2. VALIDATION DE L'IDENTITE D'UN ORGANISME

L'entité souhaitant obtenir des certificats serveurs de niveau de confiance 1* doit effectuer une demande de référencement auprès de l'AA.

A cet effet, elle complète un formulaire indiquant les identités des personnes RCC/RCAS qu'elle désigne.

L'entité désigne aussi auprès des RCC/RCAS, les opérateurs demandeurs.

4.2.3. VALIDATION DE L'IDENTITE D'UN INDIVIDU

4.2.3.1. Enregistrement d'un opérateur demandeur

L'entité désigne un opérateur demandeur auprès d'un RCC/RCAS de son entité. L'identité du demandeur est vérifiée par le RCC/RCAS par présentation de la carte agent ministérielle du demandeur et connaissance de son numéro de RIO pour l'enregistrer dans le système de gestion des cartes et des certificats.

Un document est établi pour cet enregistrement.

4.2.3.2. Enregistrement d'un RCC/RCAS pour un certificat à émettre

L'enregistrement du futur RCC/RCAS (personne physique) représentant une entité nécessite, l'identification de cette entité et l'identification de la personne physique.

- Le dossier d'enregistrement donne un mandat au futur RCC/RCAS pour demander des certificats serveur dont le type est précisé:
- [C-SIG] RCC, pour le service de création de cachet pour lequel le certificat de cachet doit être délivré,
- [A-SER][A-CLI] RCAS pour la ou les machines sur lesquelles sera déployé le certificat d'authentification serveur devant être délivré.

Le dossier d'enregistrement est déposé auprès de l'AA pour validation. Un représentant de l'AA signe la demande d'enregistrement en cas d'acceptation.

- [C-SIG] un mandat, daté de moins de 3 mois, désignant le futur RCC comme étant habilité à être RCC pour les services de création de cachet pour lesquels les certificats de cachet doivent être délivrés. Ce mandat doit être signé par un représentant légal de l'entité et cosigné, pour acceptation, par le futur RCC,
- [A-SER] [A-CLI] un mandat, daté de moins de 3 mois, désignant le futur RCAS comme étant habilité à être le nouveau RCAS pour la ou les machines sur lesquelles seront déployés les certificats devant être délivrés. Ce mandat doit être signé par un représentant légal de l'entité et cosigné, pour acceptation, par le futur RCAS,
- Une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative,
- Un document officiel d'identité en cours de validité du futur RCC/RCAS comportant une photographie d'identité (notamment carte nationale d'identité, passeport), qui est présenté à l'AE qui en conserve une copie,
- Les conditions générales d'utilisation signées.

Nota – Le RCC/RCAS est informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. 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'AA met à jour la liste référence des RCC/RCAS et en informe l'AE.

4.2.3.3. Enregistrement d'un nouveau RCC/RCAS pour un certificat déjà émis

Les mêmes dispositions que celles du paragraphe précédent sont applicables.

4.2.4. INFORMATIONS NON VERIFIEES DU RCC/RCAS ET/OU DU SERVEUR INFORMATIQUE

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

4.2.5. VALIDATION DE L'AUTORITE DU DEMANDEUR

Elle est effectuée sur la base du référencement prévu au chapitre 4.2.2 et par tout moyen permettant le contrôle (organigramme, journal officiel, autre).

4.2.6. CERTIFICATION CROISEE D'AC

La présente PC n'autorise pas la certification croisée avec une AC SERVEUR 1 ETOILE.

4.3. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLES

La procédure d'identification et de validation de l'identité du RCC/RCAS est effectuée préalablement à toute demande de certificat et est renouvelée tous les 3 ans.

Le renouvellement de la bi-clé d'un serveur entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat serveur ne peut pas être fourni au RCC/RCAS sans renouvellement de la bi-clé correspondante (*cf.* chapitre 4.6).

4.3.1. IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT COURANT

En l'absence d'information sur un changement de statut de l'entité ou du RCC/RCAS, celui-ci peut renouveler les certificats serveurs (dans le cadre de son mandat) en respectant la même procédure que pour la demande initiale de certificat.

4.3.2. 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 est identique à la procédure de demande initiale de certificat.

4.4. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

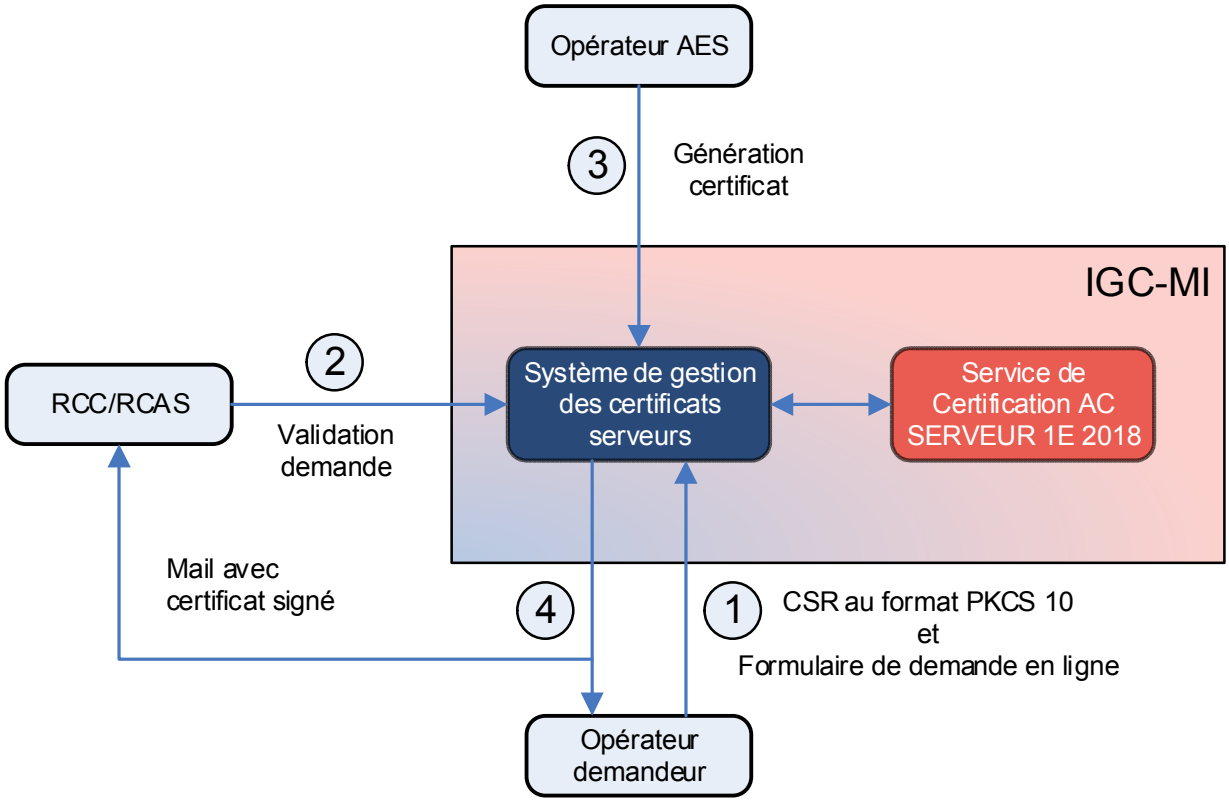
La demande de révocation doit provenir d'une entité autorisée (cf. chapitre 5.9.2).

Lorsque la demande de révocation est faite via le service téléphonique du support en ligne, l'identité du demandeur est formellement authentifiée.

5. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

5.1. DEMANDE DE CERTIFICAT

L'IGC-MI s'appuie sur plusieurs composantes pour assurer sa mission d'émission des certificats serveur. La figure ci-dessous permet d'illustrer le fonctionnement de l'IGC-MI et les interactions entre les composantes :



1- L'opérateur demandeur du certificat serveur se connecte au système de gestion des cartes et des certificats en utilisant un certificat d'authentification RGS qualifié au niveau de sécurité RGS 2 étoiles puis remplit le formulaire de demande de certificat avec les informations demandées, joint une CSR au format PKSC10 préalablement généré en respect avec la PC, choisit le type de certificat et valide sa demande, qui est transmise au RCC/RCAS.
2- Le RCC/RCAS se connecte au système de gestion des cartes et des certificats en utilisant un certificat d'authentification RGS qualifié au niveau de sécurité RGS 2 étoiles. Il vérifie la demande puis rejette la demande en cas de non conformité ou la valide. La demande de certificat est transmise à l'autorité d'enregistrement serveur.
3- L'AES autorise la génération du certificat par l'Autorité AC SERVEUR 1E 2018 qui signe la CSR du demandeur.
4- Le système de gestion des cartes transmet le certificat signé au RCC/RCAS et à l'opérateur demandeur par courrier électronique.

5.1.1. ORIGINE D'UNE DEMANDE DE CERTIFICAT

Un certificat est demandé au sein d'une entité par un opérateur demandeur, validé par un RCC/RCAS ayant obtenu un droit d'accès au système de gestion des cartes et des certificats en utilisant un certificat d'authentification RGS qualifié au niveau de sécurité RGS 2 étoiles.

5.1.2. 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 4.2 ci-dessus) :

- [C-SIG] [C-HOR] le nom du service de création de cachet à utiliser dans le certificat,
- [A-SER] le FQDN du serveur à utiliser dans le certificat,
- [A-CLI] le nom du serveur à utiliser dans le certificat,
- La requête au format PKCS#10.

La demande est établie directement par l'opérateur demandeur en se connectant sur le système de gestion des cartes et des certificats avec sa carte agent ministérielle). Cette demande doit être validée par le RCC/RCAS en se connectant au même système avec sa carte agent ministérielle. Les exceptions de rejet de demandes sont listées au chapitre 5.2.2.

Finalement l'AES par le même processus de connexion au système génère le certificat signé par l'AC SERVEUR 1E 2018 qui sera transmis par mail au demandeur et au RCC/RCAS sous format PEM.

5.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

5.2.1. 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 4.2.

Le RCC/RCAS effectue les opérations suivantes :

- vérifier les informations du demandeur.
- vérifier que la demande est conforme à l'accréditation (type de certificats demandés, noms de domaines) et la possession de la clé privée lié à la CSR
- vérifier l'intégrité et l'origine du code à signer par les certificats de signature de code,
- vérifier l'utilisation d'un module cryptographique qualifié pour la génération et le stockage dés clé s'il s'agit d'une demande de certificat initial serveur de niveau pour les types « cachet », « OCSP » ou « horodatage » conforme à l'accord de l'AA.

5.2.2. ACCEPTATION OU REJET DE LA DEMANDE

Pour toute demande de certificat initial serveur de niveau de confiance 1 étoile de type « cachet », « OCSP » ou « horodatage », un avis favorable de l'AA est impératif avant la génération du certificat par l'AE. Des justificatifs complémentaires peuvent être demandés.

Le rejet de la demande est systématique si :

- l'utilisation du nom de domaine n'est pas autorisée,
- le type de certificat demandé n'a pas été autorisé pour le RCC/RCAS.

L'acceptation ou le rejet d'une demande est ensuite soumise à l'approbation de l'AE. En cas de rejet de la demande, l'AES ou l'AA (selon le cas) en informe le RCC/RCAS, en justifiant le rejet.

5.2.3. DUREE D'ETABLISSEMENT DU CERTIFICAT

La durée d'établissement du certificat est d'au plus une semaine après acceptation de la demande.

5.3. DELIVRANCE DU CERTIFICAT

5.3.1. 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 du RCC/RCAS, l'AC déclenche les processus de génération et de préparation du certificat.

Les conditions de génération des certificats et les mesures de sécurité à respecter sont précisées aux chapitres 6 et 7, notamment la séparation des rôles de confiance (*cf.* chapitre 6.2).

5.3.2. NOTIFICATION PAR L'AC DE LA DELIVRANCE DU CERTIFICAT AU RCC/RCAS

La remise du certificat ne se fait pas en mains propres. Le certificat complet et conforme à la demande est transmis par le système au RCC/RCAS et à l'opérateur demandeur par *e-mail* : l'adresse *e-mail* utilisée est celle fournie par le RCC/RCAS au cours de l'enregistrement de la demande.

5.4. ACCEPTATION DU CERTIFICAT

5.4.1. DEMARCHE D'ACCEPTATION DU CERTIFICAT

L'acceptation du certificat par le RCC/RCAS est implicite. À partir de la date d'envoi de l'*e-mail* contenant le certificat, le RCC/RCAS peut signaler son refus du certificat auprès de l'AC pour révocation.

L'installation du certificat sur un serveur par le RCC/RCAS vaut acceptation du certificat. Il appartient donc au RCC/RCAS de vérifier le contenu du certificat avant toute installation sur un serveur.

5.4.2. PUBLICATION DU CERTIFICAT

L'AC ne publie pas les certificats serveur, le certificat est simplement fourni au RCC/RCAS qui le met en œuvre s'il l'accepte et selon ses propres procédures.

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

Sans objet dans cette PC.

5.5. USAGES DE LA BI-CLE ET DU CERTIFICAT

5.5.1. UTILISATION DE LA CLE PRIVEE ET DU CERTIFICAT PAR LE RCC/RCAS

[C-SIG] L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service de cachet de données émises par le serveur (*cf.* chapitre 2.4.1.1).

Pour les certificats de type signature de code 1*, le RCC s'assure que le certificat de signature de code sera utilisé pour signer des codes développés par des personnels du ministère ou par des prestataires extérieurs dans le cadre d'un marché passé par une entité du ministère de l'intérieur. Ce code devra être exempt de faille de sécurité et son utilisation réservée aux applications interne au ministère de l'Intérieur.

[A-CLI][A-SER] L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service d'authentification et d'établissement d'une session sécurisée : authentification du serveur, échange de la clé symétrique de session (cf. chapitre 2.4.1.1).

Les RCC/RCAS doivent s'assurer du respect strict des usages autorisés des bi-clés et des certificats au niveau des serveurs. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé du serveur et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des clés (*cf.* [RGS_A_14]). Faisant partie du dossier d'enregistrement, les conditions générales d'utilisation sont portées à la connaissance du RCC/RCAS par l'AC avant d'entrer en relation contractuelle.

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

Cf. chapitre précédent et chapitre 2.4.

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

5.6. RENOUVELLEMENT D'UN CERTIFICAT

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 sont identiques au certificat précédent (y compris la clé publique du serveur).

Dans la cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. L'AC s'en assure, auprès du RCC/RCAS, au travers d'un engagement contractuel clair et explicite.

5.6.1. CAUSES POSSIBLES DE RENOUVELLEMENT D'UN CERTIFICAT

Sans objet dans cette PC.

5.6.2. ORIGINE D'UNE DEMANDE DE RENOUVELLEMENT

Sans objet dans cette PC.

5.6.3. PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE RENOUVELLEMENT

Sans objet dans cette PC.

5.6.4. NOTIFICATION AU RCC DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT

Sans objet dans cette PC.

5.6.5. DEMARCHE D'ACCEPTATION DU NOUVEAU CERTIFICAT

Sans objet dans cette PC.

5.6.6. PUBLICATION DU NOUVEAU CERTIFICAT

Sans objet dans cette PC.

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

Sans objet dans cette PC.

5.7. DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE

Ce chapitre traite de la délivrance d'un nouveau certificat lié à la génération d'une nouvelle bi-clé.

5.7.1. CAUSES POSSIBLES DE CHANGEMENT D'UNE BI-CLE

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des serveurs et les certificats correspondants seront renouvelés au minimum tous les 3 ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du serveur (*cf.* chapitre 5.9, notamment le chapitre 5.9.1 pour les différentes causes possibles de révocation).

5.7.2. ORIGINE D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

Le déclenchement de la fourniture d'un nouveau certificat serveur est à l'initiative du RCC/RCAS.

5.7.3. PROCEDURE DE TRAITEMENT D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

Le traitement d'une demande d'un nouveau certificat est identique au traitement d'une demande initiale (cf. §5.2).

5.7.4. NOTIFICATION AU RCC/RCAS DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT

Cf. chapitre 5.3.2.

5.7.5. DEMARCHE D'ACCEPTATION DU NOUVEAU CERTIFICAT

Cf. chapitre 5.4.1.

5.7.6. PUBLICATION DU NOUVEAU CERTIFICAT

Cf. chapitre 5.4.2.

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

Sans objet dans cette PC.

5.8. MODIFICATION DU CERTIFICAT

Conformément au [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique (*cf.* chapitre 5.7) et autres qu'uniquement la modification des dates de validité (*cf.* chapitre 5.6).

La modification de certificat n'est pas autorisée par la présence PC.

5.8.1. CAUSES POSSIBLES DE MODIFICATION D'UN CERTIFICAT

Sans objet dans cette PC.

5.8.2. ORIGINE D'UNE DEMANDE DE MODIFICATION D'UN CERTIFICAT

Sans objet dans cette PC.

5.8.3. PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE MODIFICATION D'UN CERTIFICAT

Sans objet dans cette PC.

5.8.4. NOTIFICATION AU RCC DE L'ETABLISSEMENT DU CERTIFICAT MODIFIE

Sans objet dans cette PC.

5.8.5. DEMARCHE D'ACCEPTATION DU CERTIFICAT MODIFIE

Sans objet dans cette PC.

5.8.6. PUBLICATION DU CERTIFICAT MODIFIE

Sans objet dans cette PC.

5.8.7. NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU CERTIFICAT MODIFIE

Sans objet dans cette PC.

5.9. REVOCATION ET SUSPENSION DES CERTIFICATS

5.9.1. CAUSES POSSIBLES D'UNE REVOCATION

5.9.1.1. Certificats cachet et certificats serveur

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

- 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 du nom du serveur), ceci avant l'expiration normale du certificat,
- le RCC/RCAS n'a pas respecté les modalités applicables d'utilisation du certificat,
- le RCC/RCAS ou l'entité n'a pas respecté son obligation découlant de la présente PC,
- 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, (éventuellement les données d'activation associées),
- le RCC/RCAS, ou une entité autorisée (représentant légal de l'entité, 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 RCC/RCAS de rattachement du serveur,
- un certificat de cachet qui n'a plus de de RCC/RCAS explicitement identifié est révoqué

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 est révoqué.

5.9.1.2. Certificats d'une composante de l'IGC-MI

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC-MI (y compris un certificat d'AC pour la génération de certificats, de LCRs et/ou de réponses OCSP) :

- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante,
- décision de changement de composante de l'IGC-MI suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif),
- cessation d'activité de l'entité opérant la composante.

5.9.2. ORIGINE D'UNE DEMANDE DE REVOCATION

5.9.2.1. Certificats cachet et certificats serveur

Les personnes et entités qui peuvent demander la révocation d'un certificat de cachet ou d'authentification sont les suivantes :

- le RCC/RCAS pour le serveur considéré,
- un représentant légal de l'entité,
- l'AC émettrice du certificat.

5.9.2.2. Certificats d'une composante de l'IGC-MI

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.

La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

5.9.3. PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE REVOCATION

5.9.3.1. Révocation d'un certificat cachet et d'un certificat serveur

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 4.4.

Les demandes de révocation sont faites par le RCC/RCAS ou un représentant légal de l'entité en utilisant l'imprimé disponible sur le site http://ssi.minint.fr/index.php/services/certificats-serveurs-de-ligc-mi .

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

- le nom du serveur utilisé dans le certificat,
- [A-SER] le FQDN du serveur utilisé dans le certificat,
- le nom du demandeur de la révocation,
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série,),
- éventuellement, la cause de révocation.

La demande est envoyée par courriel au pôle SSI à l'adresse suivante **dsic-polessi@interieur.gouv.fr**

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 CRL signée par l'AC.

Le demandeur de la révocation, RCC/RCAS et l'opérateur demandeur, sont informés par mail du bon déroulement de l'opération et de la révocation effective du certificat.

L'opération est enregistrée dans les journaux d'événements de l'IGC-MI.

5.9.3.2. Révocation d'un certificat d'une composante de l'IGC-MI

La DPC de l'AC décrit les procédures appliquées dans le cas d'une révocation d'un certificat de composante de l'AC.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des RCC/RCAS concernés que leurs certificats correspondants ne sont plus valides. Pour cela, l'IGC-MI pourra par exemple envoyer des

récépissés aux AE. Ces derniers devront informer les RCC/RCAS en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Le point de contact identifié sur le site http://references.modernisation.gouv.fr et l'ANSSI sont immédiatement informés en cas de révocation d'un des certificats de la chaîne de certification. La DIMAP et l'ANSSI se réservent le droit de diffuser l'information par tout moyen auprès des promoteurs d'applications au sein des autorités administratives et auprès des usagers.

5.9.4. DELAI ACCORDE AU RCC/RCAS POUR FORMULER LA DEMANDE DE REVOCATION

Dès que le RCC/RCAS (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation d'un certificat de son ressort, est effective. il doit formuler sa demande de révocation sans délai.

5.9.5. DELAI DE TRAITEMENT PAR L'AC D'UNE DEMANDE DE REVOCATION

5.9.5.1. Révocation d'un certificat cachet et d'un certificat serveur

Par nature, une demande de révocation est traitée en urgence.

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

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) inférieure à 2 heures (jours ouvrés) et une durée maximale totale d'indisponibilité par mois inférieure à 16 heures (jours ouvrés).

Toute demande de révocation d'un certificat porteur qualifié 1 étoile est traitée dans un délai inférieur à 24 heures, 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.

5.9.5.2. Révocation d'un certificat d'une composante de l'IGC-MI

La révocation d'un certificat d'une composante de l'IGC-MI est effectuée dès la détection d'un événement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat, et que cette liste est accessible au téléchargement.

5.9.6. EXIGENCES DE VERIFICATION DE LA REVOCATION PAR LES UTILISATEURS DE CERTIFICATS

L'utilisateur d'un certificat est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à son application.

5.9.7. FREQUENCE D'ETABLISSEMENT DES LCRS

La fréquence de publication des LCRs est inférieure à 24 heures.

5.9.8. DELAI MAXIMUM DE PUBLICATION D'UNE LCRS

Une LCR est publiée dans un délai de maximum 30 minutes suivant sa génération.

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

Sans objet dans cette PC.

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

Cf. chapitre 5.9.6.

5.9.11. AUTRES MOYENS DISPONIBLES D'INFORMATION SUR LES REVOCATIONS

Sans objet dans cette PC.

5.9.12. EXIGENCES SPECIFIQUES EN CAS DE COMPROMISSION DE LA CLE PRIVEE

Pour les certificats serveur 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, outre les exigences du chapitre 5.9.3.2, la révocation suite à une compromission de la clé privée fait l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

5.9.13. CAUSES POSSIBLES D'UNE SUSPENSION

La suspension de certificats n'est pas autorisée dans la présente PC.

5.9.14. ORIGINE D'UNE DEMANDE DE SUSPENSION

Sans objet dans cette PC.

5.9.15. PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE SUSPENSION

Sans objet dans cette PC.

5.9.16. LIMITES DE LA PERIODE DE SUSPENSION D'UN CERTIFICAT

Sans objet dans cette PC.

5.10. FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS

5.10.1. CARACTERISTIQUES OPERATIONNELLES

L'AC fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'ACR), c'est-à-dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR / LAR et l'état du certificat de l'ACR.

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR sur le site web http://crl.interieur.gouv.fr.

5.10.2. DISPONIBILITE DE LA FONCTION

La fonction d'information sur l'état des certificats est disponible : 24 heures sur 24 et 7 jours sur 7.

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) inférieure à 2 heures (jours ouvrés) et une durée maximale totale d'indisponibilité par mois inférieure à 16 heures (jours ouvrés).

5.10.3. DISPOSITIFS OPTIONNELS

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

5.11. FIN DE LA RELATION ENTRE LE RCC/RCAS ET L'AC

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et l'entité de rattachement du serveur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier est révoqué.

De plus, l'AC révoquera tout certificat serveur pour lequel il n'y a plus de RCC/RCAS explicitement identifié.

5.12. SEQUESTRE DE CLE ET RECOUVREMENT

Le séquestre des clés privées des serveurs est interdit par la présente PC.

Les clés privées d'AC ne doivent pas non plus être séquestrées.

5.12.1. POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR SEQUESTRE DES CLES

Sans objet dans cette PC.

5.12.2. POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR ENCAPSULATION DES CLES DE SESSION

Sans objet dans cette PC.

6. MESURES DE SECURITE NON TECHNIQUES

6.1. MESURES DE SECURITE PHYSIQUE

6.1.1. SITUATION GEOGRAPHIQUE ET CONSTRUCTION DES SITES

La construction des sites respecte les règlements et normes en vigueur ainsi qu'éventuellement des exigences spécifiques face à des risques de type tremblement de terre ou explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques,…)

6.1.2. ACCES PHYSIQUE

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

En outre, toute personne ne bénéficiant pas d'une autorisation permanente d'accès qui entre dans ces zones physiquement sécurisées ne doit pas être laissée, pendant une période de temps significative, sans la surveillance d'une personne autorisée.

Pour les fonctions de génération des certificats et de gestion des révocations :

L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

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.

6.1.3. ALIMENTATION ELECTRIQUE ET CLIMATISATION

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

Elles permettent de respecter les exigences de la présente PC en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

6.1.4. VULNERABILITE AUX DEGATS DES EAUX

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences de la présente PC en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

6.1.5. PREVENTION ET PROTECTION INCENDIE

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences de la présente PC en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

6.1.6. CONSERVATION DES SUPPORTS

Les différentes informations intervenant dans les activités de l'IGC-MI sont identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité). L'AC maintient un inventaire de ces informations. L'AC met en place des mesures pour éviter la compromission et le vol de ces informations.

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations sont gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils sont manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.

Des procédures de gestion protègent ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

6.1.7. 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 sont conformes à ce niveau de confidentialité (voir notamment le guide [972-1]).

6.1.8. SAUVEGARDES HORS SITE

En complément de sauvegardes sur sites, les composantes de l'IGC-MI mettent en œuvre des sauvegardes hors site de leurs applications et de leurs informations. Ces sauvegardes sont organisées de façon à assurer une reprise des fonctions de l'IGC-MI après incident le plus rapidement possible, et conforme aux exigences de la présente PC en matière de disponibilité, en particulier pour les fonctions de gestion des révocations et d'information sur l'état des certificats (*cf.* chapitres 5.9.5.1 et 5.10.2).

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

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

Les fonctions de sauvegarde et de restauration sont effectuées par les rôles de confiance appropriés et conformément aux mesures de sécurité procédurales.

6.2. MESURES DE SECURITE PROCEDURALES

6.2.1. ROLES DE CONFIANCE

Chaque composante de l'IGC-MI distingue au moins les cinq rôles fonctionnels de confiance suivants :

- Responsable de sécurité - il est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère 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. Il est responsable des opérations de génération et de révocation des certificats.
- Responsable d'application - il 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-MI 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 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 – il réalise au sein d'une composante de l'IGC-MI, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.
- Contrôleur - personne désignée par une autorité compétente 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-MI et aux politiques de sécurité de la composante.

En plus de ces rôles de confiance au sein de chaque composante de l'IGC-MI, et en fonction de l'organisation de l'IGC-MI et des outils mis en œuvre, l'AC distingue également en tant que rôle de confiance, les rôles de porteur de parts de secrets d'IGC : *cf.* chapitres 7.1 et 7.2.

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

De manière générale, des procédures sont établies et appliquées pour tous les rôles administratifs et les rôles de confiance ayant trait à la fourniture de services de certification.

Ces rôles sont décrits et définis dans la description des missions relatives à chaque entité opérant une des composantes de l'IGC-MI sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles doivent déterminer la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilisation des employés.

Lorsqu'appropriées, ces descriptions différencient les fonctions générales des fonctions spécifiques à l'AC. L'AC implémente techniquement ce principe de moindre privilège via les mécanismes de contrôle d'accès qu'elle met en œuvre.

De plus, les opérations de sécurité de l'AC sont séparées des opérations normales. Les responsabilités des opérations de sécurité incluent :

- les procédures et responsabilités opérationnelles,
- la planification et la validation des systèmes sécurisés,
- la protection contre les logiciels malicieux,
- l'entretien,
- la gestion de réseaux,
- la surveillance active des journaux d'audit, l'analyse des évènements et les suites,
- la manipulation et la sécurité des supports,
- l'échange de données et de logiciels.

Ces responsabilités sont gérées par les opérations de sécurité de l'AC, mais peuvent être réalisées par du personnel opérationnel non spécialiste (en étant supervisé), tel que défini dans la politique de sécurité appropriée et les documents relatifs aux rôles et responsabilités.

6.2.2. 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-MI (*cf.* chapitre 7).

La DPC de l'AC précise 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.).

6.2.3. IDENTIFICATION ET AUTHENTIFICATION POUR CHAQUE ROLE

Chaque entité opérant une composante de l'IGC-MI fait 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-MI.

Ces contrôles sont décrits dans la DPC de l'AC et sont conformes à la politique de sécurité de la composante.

Chaque attribution d'un rôle à un membre du personnel de l'IGC-MI est notifiée par écrit et chaque attribution de rôle dans l'IGC-MI est portée à la connaissance de la personne désignée.

6.2.4. 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 sont respectées.

Les attributions associées à chaque rôle sont décrites dans la DPC de l'AC et doivent être conformes à la politique de sécurité de la composante concernée.

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

- (pendant une cérémonie) responsable de sécurité et tout autre rôle
- (de façon générale) opérateurs et ingénieurs
- Les porteurs de secret ne doivent jamais détenir deux parts différentes d'un même secret.
- L'administrateur sécurité ne peut pas être exploitant ou responsable fonctionnel
- La fonction d'auditeur ne peut être cumulée avec aucun autre rôle

6.3. MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

6.3.1. QUALIFICATIONS, COMPETENCES ET HABILITATIONS REQUISES

Tous les personnels amenés à travailler au sein de composantes de l'IGC-MI sont soumis à une clause de confidentialité vis-à-vis de leur employeur. Dans le cas des agents, ceux-ci sont soumis à leur devoir de réserve.

Chaque responsable d'entité opérant une composante de l'IGC-MI s'assure que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

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

L'AC informe toute personne intervenant dans des rôles de confiance de l'IGC-MI :

- de ses responsabilités relatives aux services de l'IGC-MI,
- des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.

En particulier, les personnes intervenant dans des rôles de confiance y sont formellement affectées par l'encadrement supérieur chargé de la sécurité.

6.3.2. PROCEDURES DE VERIFICATION DES ANTECEDENTS

Chaque entité opérant une composante de l'IGC-MI met 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. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions. Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

6.3.3. EXIGENCES EN MATIERE DE FORMATION INITIALE

Le personnel est 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 la composante au sein de laquelle il opère.

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

6.3.4. EXIGENCES ET FREQUENCE EN MATIERE DE FORMATION CONTINUE

Le personnel concerné reçoit 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.

6.3.5. FREQUENCE ET SEQUENCE DE ROTATION ENTRE DIFFERENTES ATTRIBUTIONS

Se référer à la DPC de l'AC.

6.3.6. SANCTIONS EN CAS D'ACTIONS NON AUTORISES

Se référer à la DPC de l'AC.

6.3.7. EXIGENCES VIS-AVIS DU PERSONNEL DES PRESTATAIRES EXTERNES

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC-MI doit également respecter les exigences du présent chapitre 6.3. Ceci est traduit en clauses adéquates dans les contrats avec ces prestataires.

6.3.8. DOCUMENTATION FOURNIE AU PERSONNEL

Chaque personnel disposera 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. En particulier, il doit lui être remis la ou les politique(s) de sécurité l'impactant.

6.4. PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

La journalisation d'évènements consiste à les enregistrer de façon manuelle ou automatique. Les fichiers résultant, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

6.4.1. TYPE D'EVENEMENTS A ENREGISTRER

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre de l'IGC-MI, chaque entité opérant une composante de l'IGC-MI journalise les évènements décrits ci-après, sous forme électronique. La journalisation est automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

- 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 RCC/RCAS.).

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC-MI, des évènements spécifiques aux différentes fonctions de l'IGC-MI 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, etc.) ;
- génération des certificats demandés par les RCC/RCAS ;
- transmission des certificats aux RCC/RCAS et, selon les cas, acceptations / rejets explicites par ceux-ci ;
- le cas échéant, remise du dispositif de protection de clés privées du serveur au RCAS ou remise du dispositif de création de cachet du serveur au RCC;
- 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 contient 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 (l'heure exacte des évènements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat sont enregistrées) ;
- 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 figure 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 ;
- toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

Les opérations de journalisation sont effectuées au cours du processus.

En cas de saisie manuelle, l'écriture a lieu, sauf exception, le même jour ouvré que l'évènement.

6.4.2. FREQUENCE DE TRAITEMENT DES JOURNAUX D'EVENEMENTS

Cf. chapitre 6.4.8.

6.4.3. PERIODE DE CONSERVATION DES JOURNAUX D'EVENEMENTS

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

6.4.4. PROTECTION DES JOURNAUX D'EVENEMENTS

La journalisation est 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 permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

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

Le système de datation des évènements respecte les exigences du chapitre 6.5.5.

Les journaux d'événements de l'IGC-MI sont signés et chaînés (protection en intégrité). Les journaux enregistrés en base sont protégés via les mécanismes de protection de celle-ci. Les journaux du système de gestion des cartes sont protégés par chiffrement.

6.4.5. PROCEDURE DE SAUVEGARDE DES JOURNAUX D'EVENEMENTS

Chaque entité opérant une composante de l'IGC-MI met 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.

6.4.6. SYSTEME DE COLLECTE DES JOURNAUX D'EVENEMENTS

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

6.4.7. NOTIFICATION DE L'ENREGISTREMENT D'UN EVENEMENT AU RESPONSABLE DE L'EVENEMENT

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

6.4.8. ÉVALUATION DES VULNERABILITES

Chaque entité opérant une composante de l'IGC-MI est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements sont contrôlés une fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité au moins une fois par jour ouvré 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 fait 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.) est effectué au moins une fois par semaine, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

6.5. ARCHIVAGE DES DONNEES

6.5.1. TYPES DE DONNEES A ARCHIVER

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

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

Les données archivées sont 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 RCC/RCAS et de leur entité de rattachement ;
- les journaux d'évènements des différentes entités de l'IGC-MI.

6.5.2. PERIODE DE CONSERVATION DES ARCHIVES

6.5.2.1. Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable.

Les facteurs à prendre en compte dans la détermination de la "loi applicable" sont la loi du pays dans lequel l'AC est établie.

La durée de conservation des dossiers d'enregistrement est portée à la connaissance du RCC/RCAS.

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

6.5.2.2. Certificats et LCR émis par l'AC.

Les certificats de clés de serveur et d'AC, ainsi que les LCR / LAR produites, sont archivés pendant au moins 8 ans années après leur expiration.

6.5.2.3. Journaux d'évènements

Les journaux d'évènements traités au chapitre 6.4 seront archivés pendant 8 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.

6.5.2.4. Autres journaux

Pour l'archivage des journaux autres que les journaux d'évènements traités au chapitre 6.4, aucune exigence n'est stipulée. La DPC précise les moyens mis en œuvre pour archiver ces journaux.

6.5.3. 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.

La DPC précise les moyens mis en œuvre pour archiver les pièces en toute sécurité.

6.5.4. PROCEDURE DE SAUVEGARDE DES ARCHIVES

La DPC décrit la procédure de sauvegarde des archives. Le niveau de protection des sauvegardes est au moins équivalent au niveau de protection des archives.

6.5.5. EXIGENCES D'HORODATAGE DES DONNEES

Cf. chapitre 6.4.4 pour la datation des journaux d'évènements.

Le chapitre 7.8 précise les exigences en matière de datation / horodatage.

6.5.6. 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.

6.5.7. 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-MI qui ne peut récupérer et consulter que les archives de la composante considérée).

6.6. 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 du certificat correspondant de l'AC. La période de validité de ce certificat de l'AC est donc 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 bi-clé d'AC est générée, seule la nouvelle clé privée est utilisée pour signer des certificats.

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

6.7. REPRISE SUITE A COMPROMISSION ET SINISTRE

6.7.1. PROCEDURES DE REMONTEE ET DE TRAITEMENT DES INCIDENTS ET DES COMPROMISSIONS

Chaque entité opérant une composante de l'IGC-MI met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements. Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.

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 est impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, est faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé …). L'AC prévient directement et sans délai le point de contact identifié sur le site : http://references.modernisation.gouv.fr et l'ANSSI.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses serveurs devient insuffisant pour son utilisation prévue restante, alors l'AC :

- informe tous les RCC/RCAS et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou à d'autres formes de relations établies. En complément, cette information est mise à disposition des autres utilisateurs de certificats ;
- révoque tout certificat concerné.

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

Chaque composante de l'IGC-MI dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC-MI découlant de la présente PC, notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

Ce plan est testé au minimum suivant la fréquence une fois par an.

6.7.3. 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 est traité dans le plan de continuité de la composante (*cf.* chapitre 6.7.2) en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat correspondant est immédiatement révoqué : *cf.* chapitre 5.9.

En outre, l'AC s'engage à :

- Informer les entités suivantes de la compromission : tous les RCC/RCAS et les autres entités avec lesquelles l'AC a passé des accords ou à d'autres formes de relations établies, parmi lesquelles des tiers utilisateurs et d'autres AC. En complément, cette information est mise à disposition des autres tiers utilisateurs ;
- Indiquer que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

6.7.4. CAPACITES DE CONTINUITE D'ACTIVITE SUITE A UN SINISTRE

Les différentes composantes de l'IGC-MI doivent disposer des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC (*cf.* chapitre 6.7.2).

6.8. FIN DE VIE DE ACD SERVEUR DE L'IGC-MI.

Une ou plusieurs composantes de l'IGC-MI peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'AC prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC-MI 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-MI comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

Dans le cas d'une cessation d'activité, l'ACD met en place un groupe de travail chargé de planifier et suivre la réalisation des actions suivantes :

- L'ensemble des certificats non-expirés émis par l'ACD seront révoqués
- Demande la révocation de son certificat auprès de l'AC RACINE MINISTÈRE INTÉRIEUR.
- Révoque tous les certificats qu'elle a signés et en cours de validité (dernière CRL).
- Une dernière LCR qui comporte l'extension « ExpiredCertsOnCRL » sera publiée ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s « 99991231235959Z »
- Prend toutes les mesures nécessaires pour détruire ses clés privées de signature ;
- Signale l'arrêt effectif du service sur les sites web http://crl.interieur.gouv.fr (dédié aux CRL des AC) et https://www.interieur.gouv.fr/IGC (dédié aux autres informations).
- Archive sa dernière CRL, les P.-V. de destruction des clés.

6.8.1. TRANSFERT D'ACTIVITE OU CESSATION D'ACTIVITE AFFECTANT UNE COMPOSANTE DE L'IGC-MI

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

1. Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des serveurs et des informations relatives aux certificats).
2. Assure 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.
3. Communique au point de contact identifié sur le site : http://references.modernisation.gouv.fr et à l'ANSSI les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC communiquera à l'ANSSI, selon les différentes

composantes de l'IGC-MI concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les RCC/RCAS et les utilisateurs de certificats.

4. Tient informée l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des RCC/RCAS ou des utilisateurs de certificats, l'AC les en avise aussitôt que nécessaire et, au moins, sous le délai d'un mois.

6.8.2. CESSATION D'ACTIVITE 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'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LCRs conformément aux engagements pris dans sa PC.

L'AC stipule dans ses pratiques les dispositions prises en cas de cessation de service. Elles incluent :

- ✓ La notification des entités affectées,
- ✓ Le transfert de ses obligations à d'autres parties,
- ✓ La gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

7. MESURES DE SECURITE TECHNIQUES

7.1. GENERATION ET INSTALLATION DE BI-CLES

7.1.1. GENERATION DES BI-CLES

7.1.1.1. Clés d'AC

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé (*cf.* chapitre 6).

Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre 11.

La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (*cf.* chapitre 6.2.1), dans le cadre de "cérémonies de clés". Ces cérémonies se déroulent suivant des scripts préalablement définis.

Selon le cas, l'initialisation de l'IGC-MI 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 (3 parties parmi 5 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 sont confiées à des entités différentes du ministère qui décident de les confier 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. L'entité prend toute disposition pour que ce secret soit disponible à tout moment par un porteur dûment habilité pour répondre à toute sollicitation ordonnée par l'autorité administrative.

Les cérémonies de clés se déroulent 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.

7.1.1.2. Clés serveurs générées par l'AC

7.1.1.3. Clés serveurs générées au niveau du serveur

Le RCC/RCAS s'engage contractuellement à ce que cette génération soit effectuée dans un dispositif répondant aux exigences du chapitre 12.

7.1.2. TRANSMISSION DE LA CLE PRIVEE AU SERVEUR

Sans objet dans cette PC.

7.1.3. TRANSMISSION DE LA CLE PUBLIQUE A L'AC

La clé publique du serveur est transmise à l'AC dans une requête PKCS#10. La vérification de la signature de la requête permet d'attester de l'intégrité de la clé publique. La requête PKCS#10 est transmise à l'AC dans une requête signée par le système de gestion de cartes, ce qui permet de garantir l'origine de la clé par l'AC.

7.1.4. TRANSMISSION DE LA CLE PUBLIQUE DE L'AC AUX UTILISATEURS DE CERTIFICATS

La clé publique de l'AC, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) sont mises à la disposition des utilisateurs de certificats sur le site mentionnés au chapitre 3.4.

7.1.5. TAILLES DES CLES

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé (*cf.* [RGS_A_14]).

Les certificats d'AC sont signés par une clé RSA 4096 bits.

Les bi-clés des certificats porteurs sont en RSA 2048 bits.

7.1.6. VERIFICATION DE LA GENERATION DES PARAMETRES DES BI-CLES ET DE LEUR QUALITE

Voir 7.1.5.

7.1.7. OBJECTIFS D'USAGE DE LA CLE

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR et/ou de réponses OCSP (*cf.* chapitre 2.4.1.2).

[C-SIG][C-HOR] L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service de cachet des données émises par ce serveur (*cf.* chapitres 2.4.1.1, 5.5).

[A-CLI][A-SER] L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service d'authentification et d'établissement d'une session sécurisée (*cf.* chapitres 2.4.1.1, 5.5).

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

7.2.1. STANDARDS ET MESURES DE SECURITE POUR LES MODULES CRYPTOGRAPHIQUES

7.2.1.1. Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, 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, sont des modules cryptographiques répondant au minimum aux exigences du chapitre 11.

7.2.1.2. Dispositifs de création de cachet des serveurs et dispositifs de protection de Clés privées des serveurs

Les RCC/RCAS s'engagent contractuellement à ce que les dispositifs de création de cachet, d'authentification et de protection de clés privées des serveurs, pour la mise en œuvre de leurs clés privées, respectent les exigences du chapitre 12.

7.2.2. CONTROLE DE LA CLE PRIVEE PAR PLUSIEURS PERSONNES

Ce chapitre porte sur le contrôle de la clé privée de l'AC pour l'exportation / l'importation hors / dans un module cryptographique. La génération de la bi-clé est traitée au chapitre 7.1.1.1, l'activation de la clé privée, au chapitre 7.2.8, et sa destruction, au chapitre 7.2.10.

Le contrôle des clés privées de signature de l'AC est 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).

7.2.3. SEQUESTRE DE LA CLE PRIVEE

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

7.2.4. COPIE DE SECOURS DE LA CLE PRIVEE

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

Les clés privées d'AC font l'objet de copies de secours, soit dans un module cryptographique conforme aux exigences du chapitre 11, 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 règles à respecter sont définies dans le document [RGS_B_1].

Le contrôle des opérations de chiffrement / déchiffrement est conforme aux exigences du chapitre 7.2.2.

7.2.5. ARCHIVAGE DE LA CLE PRIVEE

Les clés privées de l'AC ne sont en aucun cas archivées.

Les clés privées des serveurs ne sont en aucun cas archivées, ni par l'AC, ni par aucune des composantes de l'IGC-MI.

7.2.6. TRANSFERT DE LA CLE PRIVEE VERS / DEPUIS LE MODULE CRYPTOGRAPHIQUE

Pour les clés privées d'AC, tout transfert se fait sous forme chiffrée, conformément aux exigences du chapitre 7.2.4.

7.2.7. STOCKAGE DE LA CLE PRIVEE DANS UN MODULE CRYPTOGRAPHIQUE

L'AC garantit que les clés privées d'AC ne sont pas compromises pendant leur stockage ou leur transport.

7.2.8. METHODE D'ACTIVATION DE LA CLE PRIVEE

7.2.8.1. Clés privées d'AC

La méthode d'activation des clés privées d'AC dans un module cryptographique permet de répondre aux exigences définies dans le chapitre 11.

L'activation des clés privées d'AC dans un module cryptographique est contrôlée via des données d'activation (*cf.* chapitre 6.4) et fait intervenir au moins deux personnes dans des rôles de confiance (par exemple, responsable sécurité et opérateur).

7.2.8.2. Clés privées des serveurs

La méthode d'activation de la clé privée du serveur dépend du dispositif utilisé. L'activation de la clé privée du serveur est contrôlée via des données d'activation (*cf.* chapitre 7.4) et permet de répondre aux exigences définies dans le chapitre 13.

7.2.9. METHODE DE DESACTIVATION DE LA CLE PRIVEE

7.2.9.1. Clés privées d'AC

La désactivation des clés privées d'AC dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc. Les conditions de désactivation permettent de répondre aux exigences définies dans le chapitre 12.

7.2.9.2. Clés privées des serveurs

Les conditions de désactivation de la clé privée d'un serveur doivent permettre de répondre aux exigences définies dans le chapitre 13.

7.2.10. METHODE DE DESTRUCTION DES CLES PRIVEES

7.2.10.1. Clés privées d'AC

La méthode de destruction des clés privées d'AC est conforme aux exigences définies dans le chapitre 12.

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

7.2.10.2. Clés privées des serveurs

En fin de vie de la clé privée d'un serveur, la méthode de destruction de cette clé privée permet de répondre aux exigences définies dans le chapitre 13.

7.2.11. NIVEAU DE QUALIFICATION DU MODULE CRYPTOGRAPHIQUE ET DES DISPOSITIFS DE CREATION DE CACHET ET AUTHENTIFICATION SERVEUR

L'exigence de qualification du module cryptographique est précisée au chapitre 11.

Le dispositif de création de cachet et d'authentification des serveurs n'est pas fourni par le PSCE. Il doit cependant être conforme aux exigences du chapitre 12 en ce qui concerne la protection et l'usage de la clé privée.

7.3. AUTRES ASPECTS DE LA GESTION DES BI-CLES

7.3.1. ARCHIVAGE DES CLES PUBLIQUES

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

7.3.2. DUREES DE VIE DES BI-CLES ET DES CERTIFICATS

Les bi-clés et les certificats des serveurs couverts par la présente PC doivent avoir une durée de vie d'au plus 3 ans.

La fin de validité d'un certificat d'AC est postérieure à la fin de vie des certificats cachet et d'authentification serveurs qu'elle émet. La durée de vie des clés de signature d'AC et des certificats correspondants est de 6 ans. Cette durée de vie est cohérente avec les caractéristiques de l'algorithme et la longueur de clé utilisés (*cf.* [RGS_A_14]) et est au maximum égale à 10 ans.

7.4. DONNEES D'ACTIVATION

7.4.1. GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION

7.4.1.1. Génération et installation des données d'activation correspondant à la clé privée de l'AC

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC-MI sont faites lors de la phase d'initialisation et de personnalisation de ce module. 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 6.2).

7.4.1.2. Génération et installation des données d'activation correspondant à la clé privée du serveur

Les RCC/RCAS sont responsables de la génération et de l'installation des données d'activation de la clé privée du serveur, conformément aux exigences de sécurité du chapitre 13.

7.4.2. PROTECTION DES DONNEES D'ACTIVATION

7.4.2.1. Protection des données d'activation correspondant à la clé privée de l'AC

Les données d'activation qui sont générées par l'AC pour les modules cryptographiques de l'IGC-MI sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

7.4.2.2. Protection des données d'activation correspondant aux clés privées des serveurs

Les RCC/RCAS sont responsables de la protection des données d'activation.

7.4.3. AUTRES ASPECTS LIES AUX DONNEES D'ACTIVATION

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

7.5. MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

Les mesures de sécurité relatives aux systèmes informatiques s'appuient sur la politique de sécurité du S.I. du ministère.

7.5.1. EXIGENCES DE SECURITE TECHNIQUE SPECIFIQUES AUX SYSTEMES INFORMATIQUES

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC-MI est défini dans la DPC de l'AC. Il répond en particulier 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 des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles),
- 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),
- éventuellement, gestion des reprises sur erreur.

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

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle (*cf.* chapitre 2.4.1.2) fait l'objet de mesures particulières.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) sont mis en place.

7.5.2. NIVEAU DE QUALIFICATION DES SYSTEMES INFORMATIQUES

Les systèmes informatiques de l'IGC-MI mettent en œuvre des modules cryptographiques qualifiés conformément au niveau standard défini par le [RGS] et en respectant les exigences du [CWA 14167-1].

7.6. MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE

7.6.1. MESURES DE SECURITE LIEES AU DEVELOPPEMENT DES SYSTEMES

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

L'AC garantit que les objectifs de sécurité sont définis lors des phases de spécification et de conception.

L'AC utilise des systèmes et des produits fiables qui sont protégés contre toute modification.

7.6.2. MESURES LIEES A LA GESTION DE LA SECURITE

Toute évolution significative d'un système d'une composante de l'IGC-MI est signalée à l'AC pour validation. Elle est 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.

7.6.3. NIVEAU D'EVALUATION SECURITE DU CYCLE DE VIE DES SYSTEMES

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

7.7. MESURES DE SECURITE RESEAU

L'interconnexion vers des réseaux publics est protégée par des passerelles sécurisées et configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC-MI.

L'IGC-MI est mise en œuvre dans une architecture sécurisée dédiée.

L'AC garantit que les composants du réseau local d'interface avec l'IGC-MI (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'AC.

De plus, les échanges entre composantes au sein de l'IGC-MI font l'objet 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.).

7.8. HORODATAGE / SYSTEME DE DATATION

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

Un dispositif de synchronisation par rapport au temps UTC est mis en œuvre sur les composantes de l'IGC-MI.

8. PROFILS DES CERTIFICATS, OCSP ET DES LCR

Voir document [PC-A1-FORM-CERT].

9. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits et les évaluations concernent, d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification au sens de l'[ORD05-1516] (schéma de qualification des prestataires de services de confiance conformément au [DécretRGS]) et, d'autre part, ceux que doit réaliser, ou faire réaliser, l'AC afin de s'assurer que l'ensemble de son IGC, est bien conforme à ses engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC.

La démarche et les exigences liées aux audits de qualification de PSCO de type PSCE sont définies dans [PROG_ACCRED] et ne sont pas reprises dans ce chapitre.

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

9.1. 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 procède à un contrôle de conformité de cette composante.

L'AC procède régulièrement à un contrôle de conformité de l'ensemble de son IGC suivant la fréquence : une fois tous les 2 ans.

9.2. IDENTITES / QUALIFICATIONS DES EVALUATEURS

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

9.3. RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES

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

9.4. SUJETS COUVERTS PAR LES EVALUATIONS

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

9.5. ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : "réussite", "échec", "à confirmer".

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.
- En cas de résultat "à confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités sont levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, L'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

9.6. COMMUNICATION DES RESULTATS

Les documents décrivant les résultats des audits sont de niveau « Diffusion Restreinte »

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

10. AUTRES PROBLEMATIQUES METIERS ET LEGALES

10.1. TARIFS

10.1.1. TARIFS POUR LA FOURNITURE OU LE RENOUVELLEMENT DE CERTIFICATS

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

10.1.2. TARIFS POUR ACCEDER AUX CERTIFICATS

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

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

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

10.1.4. TARIFS POUR D'AUTRES SERVICES

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

10.1.5. POLITIQUE DE REMBOURSEMENT

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

10.2. RESPONSABILITE FINANCIERE

Conformément à ses obligations, l'AC prend les dispositions nécessaires pour couvrir, éventuellement financièrement, ses responsabilités liées à ses opérations et/ou activités.

10.2.1. COUVERTURE PAR LES ASSURANCES

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

10.2.2. AUTRES RESSOURCES

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

10.2.3. COUVERTURE ET GARANTIE CONCERNANT LES ENTITES UTILISATRICES

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

10.3. CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

10.3.1. 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,
- tous les secrets de l'IGC-MI,
- les journaux d'événements des composantes de l'IGC-MI,
- les dossiers d'enregistrement des serveurs et des RCC/RCAS,

10.3.2. INFORMATIONS HORS DU PERIMETRE DES INFORMATIONS CONFIDENTIELLES

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

10.3.3. RESPONSABILITES EN TERMES DE PROTECTION DES INFORMATIONS CONFIDENTIELLES

L'AC est tenue d'appliquer des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre 10.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

De plus, lorsque ces données sont échangées, l'AC en garantit l'intégrité.

L'AC respecte la législation et la réglementation en vigueur sur le territoire français. En particulier, elle met à disposition les dossiers d'enregistrement des certificats cachet et des certificats d'authentification serveur à des tiers dans le cadre de procédures légales. Elle donne l'accès à ces informations au RCC/RCAS.

10.4. PROTECTION DES DONNEES PERSONNELLES

10.4.1. 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 français, en particulier de la loi [CNIL].

10.4.2. 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 RCC/RCAS),
- les dossiers d'enregistrement des RCC/RCAS.

10.4.3. INFORMATIONS A CARACTERE NON PERSONNEL

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

10.4.4. RESPONSABILITE EN TERMES DE PROTECTION DES DONNEES PERSONNELLES

Cf. législation et réglementation en vigueur sur le territoire français. Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les porteurs à l'AC ne doivent ni être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

Cf. législation et réglementation en vigueur sur le territoire français.

10.4.6. AUTRES CIRCONSTANCES DE DIVULGATION D'INFORMATIONS PERSONNELLES

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

10.5. DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

Application de la législation et de la réglementation en vigueur sur le territoire français.

10.6. INTERPRETATIONS CONTRACTUELLES ET GARANTIES

Les obligations communes aux composantes de l'IGC-MI 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 et les documents qui en découlent,
- respecter et appliquer la partie de la DPC leur incombant (cette partie est communiquée à la composante correspondante),
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre 8) et l'organisme de qualification,
- respecter les accords ou contrats qui les lient entre elles ou aux RCC/RCAS,
- 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.

10.6.1. AUTORITES DE CERTIFICATION

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 RCC/RCAS correspondant a accepté le certificat, conformément aux exigences du chapitre 5.4.,
- garantir et maintenir la cohérence de sa DPC avec sa PC,
- protéger ses clés privées et leurs moyens d'activation, en intégrité et en confidentialité,
- utiliser ses clés publiques et privées, et ses certificats, aux seules fins pour lesquelles ils ont été émis et avec les outils spécifiés, conformément à la présente PC,
- contrôler les accès physiques aux locaux hébergeant les composantes de l'AC SERVEUR 1E 2018 et les limiter aux personnels autorisés,
- enregistrer et archiver les informations pertinentes,
- demander la révocation de son certificat en cas de compromission, suspicion de compromission, vol, perte des moyens de reconstitution de sa clé privée (perte du secret principal, perte du code d'activation et perte de plus de deux secrets partagés),
- prendre toutes les mesures raisonnables pour s'assurer que les détenteurs de rôle de confiance auprès de l'AC ont connaissance de leurs droits et obligations conférés de par l'attribution de ce rôle,
- être conformes aux règles fixées les annexes A du [RGS],
- être qualifiée selon la procédure décrite dans le décret [DEC2010-112],
- Informer l'ACR de tout sinistre, compromission ou suspicion de compromission relatif à son certificat,
- Prendre toutes les mesures raisonnables pour s'assurer que ses RCC/RCAS 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-MI. La relation entre un RCC /RCAS et l'AC est formalisée par un lien hiérarchique et réglementaire précisant les droits et obligations des parties et, notamment, les garanties apportées par l'AC.

L'AC est responsable de la conformité de sa *Politique de Certification* avec les exigences émises dans les documents [RGS_A_09], [RGS_A_10] et [RGS_A_12]. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC par elle-même ou l'une de ses composantes. Elle prend les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et

posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente politique.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des RCC/RCAS à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni est approuvée par les instances de haut niveau de l'AC.

10.6.2. SERVICE D'ENREGISTREMENT

Cf. les obligations pertinentes de la section 9.6.1.

10.6.3. RCC/RCAS

Le RCC/RCAS a le devoir de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat,
- protéger la clé privée du serveur dont il a la responsabilité par des moyens appropriés à son environnement,
- protéger les données d'activation de cette clé privée et, le cas échéant, les mettre en œuvre,
- protéger l'accès à la base de certificats du serveur,
- respecter les conditions d'utilisation de la clé privée du serveur et du certificat correspondant,
- faire, sans délai, une demande de révocation du certificat de cachet dont il est responsable auprès de l'AE ou de l'AC en cas de compromission ou de suspicion de compromission de la clé privée correspondante (ou de ses données d'activations),
- informer l'AA et l'AE Serveur de tout événement relatif à ses fonctions de RCC/RCAS (cessation, transfert,...),
- informer l'AA et l'AE Serveur de l'arrêt définitif ou de changement de contexte d'emploi du service applicatif pour lequel le certificat a été délivré.

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

10.6.4. UTILISATEURS DE CERTIFICATS

Les utilisateurs de la sphère publique utilisant les certificats doivent :

- vérifier et respecter l'usage pour lequel un certificat a été émis,
- contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application,
- pour chaque certificat de la chaîne de certification, du certificat du serveur jusqu'à l'ACR, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation),
- vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.

10.6.5. AUTRES PARTICIPANTS

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

10.7. LIMITE DE GARANTIE

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

10.8. LIMITE DE RESPONSABILITE

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

10.9. INDEMNITES

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

10.10. DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

10.10.1. DUREE DE VALIDITE

La PC de l'AC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

10.10.2. FIN ANTICIPEE DE VALIDITE

La publication d'une nouvelle version des documents [RGS_A_09], [RGS_A_10] et [RGS_A_12] peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC. Le délai de mise en conformité est arrêté conformément aux modalités prévues par la réglementation en vigueur.

De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

10.10.3. EFFETS DE LA FIN DE VALIDITE ET CLAUSES RESTANT APPLICABLES

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

10.11. NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

En cas de changement de toute nature intervenant dans la composition de l'IGC-MI, 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,
- au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

10.12. AMENDEMENTS A LA PC

10.12.1. PROCEDURES D'AMENDEMENTS

L'AC devra contrôler que tout projet de modification de sa PC reste conforme aux exigences de [RGS_A_09], [RGS_A_10] et [RGS_A_12], et des éventuels documents complémentaires du [RGS].

10.12.2. MECANISME ET PERIODE D'INFORMATION SUR LES AMENDEMENTS

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

10.12.3. CIRCONSTANCES SELON LESQUELLES L'OID DOIT ETRE CHANGE

L'OID de la présente PC 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 porteurs, 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.

En particulier, l'OID de la présente PC doit évoluer dès lors qu'un changement majeur (et qui sera signalé comme tel, notamment par une évolution de l'OID de la présente PC) intervient dans les exigences de la PC applicable à la famille de certificats considérée.

10.13. DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

À défaut d'une résolution à l'amiable, les conflits seront résolus par les tribunaux compétents.

10.14. JURIDICTIONS COMPETENTES

La nature et l'origine du conflit entre un utilisateur final et l'IGC-MI déterminent la juridiction compétente pour la résolution du litige.

10.15. CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre 11.

PES IGC-MI apporte la justification du respect de la propriété des droits intellectuels afférents à réalisation de la composante.

10.16. DISPOSITIONS DIVERSES

10.16.1. ACCORD GLOBAL

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

10.16.2. TRANSFERT D'ACTIVITES

Cf. chapitre 6.8.1.

10.16.3. CONSEQUENCES D'UNE CLAUSE NON VALIDE

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

10.16.4. APPLICATION ET RENONCIATION

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

10.16.5. FORCE MAJEURE

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un événement irrésistible, insurmontable et imprévisible.

10.17. AUTRES DISPOSITIONS

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

Le Préfet,
Haut fonctionnaire de défense adjoint

11. ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

11.1. REGLEMENTATION

Renvoi	Document
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
[DIRSIG]	Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.
[LCEN]	Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
[ORD05-1516]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
[DécretRGS]	Décret pris pour l'application des artiClés 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005
[DEC2010-112]	Décret n° 2010-112 du 2 février 2010 pris pour l'application des artiClés 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
[SIG]	Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.

11.2. DOCUMENTS TECHNIQUES

Renvoi	Document
[RGS]	Référentiel Général de Sécurité – Version 1.0
[RGS_A_1]	RGS_A_1_fonction_de_securite_ »Confidentialite »_V2-3 OID : 1.2.250.1.137.2.2.1.2.1.7
[RGS_A_2]	RGS_A_2_fonction_de_securite_ « Authentification »_V2-3 OID : 1.2.250.1.137.2.2.1.2.1.5
[RGS_A_3]	RGS - Fonction de sécurité « Signature électronique » - Version 2.3 OID : 1.2.250.1.137.2.2.1.2.1.6
[RGS_A_4]	RGS_A_4_fonction_de_securite_Authentification_Serveur_V2-3 OID1.2.250.1.137.2.2.1.2.1.10
[RGS_A_5]	RGS_A_5_fonction_de_securite_Cachet_V2-3 OID : 1.2.250.1.137.2.2.1.2.1.9
[RGS_A_6]	RGS_A_6_PC-Type_Confidentialite_V2-3 OID : 1.2.250.1.137.2.2.1.2.2.3
[RGS_A_7]	RGS_A_7_PC-Type_Authentification_V2-3 OID : 1.2.250.1.137.2.2.1.2.2.1

Renvoi	Document
[RGS_A_8]	RGS_A_8_PC-Type_Signature_V2-3 OID : 1.2.250.1.137.2.2.1.2.2.2
[RGS_A_9]	RGS_A_9_PC-Type_Authentification_Serveur_V2-3 OID : 1.2.250.1.137.2.2.1.2.2.5
[RGS_A_10]	RGS_A_10_PC-Type_Cachet_V2.3 OID : 1.2.250.1.137.2.2.1.2.2.6
[RGS_A_11]	RGS_A_11_PC-Type_Authentification_et_Signature_V2.3 OID : 1.2.250.1.137.2.2.1.2.2.7
[RGS_A_12]	RGS_A_12_PC-Type_Horodatage_v2.3 OID : 1.2.250.1.137.2.2.1.2.2.4
[RGS_A_13]	RGS - Politiques de Certification Types - Variables de Temps - V 2.3 OID : 1.2.250.1.137.2.2.1.2.1.3
[RGS_A_14]	RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – V 2.3 OID : 1.2.250.1.137.2.2.1.2.1.4
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques - Version 1.20
[CWA14167-1]	CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1
[CWA14167-2]	CWA 14167-2 (2003-10) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP). Ce PP a été certifié EAL4+.
[CWA14167-3]	CWA 14167-3 (2003-10) Cryptographic Module for CSP Key Génération Services - Protection Profile (CMCKG-PP)
[CWA14167-4]	CWA 14167-4 (2003-10) Cryptographic Module for CSP Signing Operations – Protection Profile (CMCSO-PP). Ce PP a été certifié EAL4+.
[CWA14169]	CWA 14169 (2002-04) Secure Signature Création Devices (SSCD). Ce PP a été certifié EAL4+.
[ETSI_QCP]	ETSI TS 101 456 V1.4.3 (mai 2007) Policy Requirements for Certification Authorities issuing qualified certificates
[ETSI_SigPol]	ETSI TR 102 272 - ASN.1 format for signature policies V1.1.1 (décembre 2003) ETSI TR 102 038 - XML format for signature policies V1.1.1 (avril 2002)
[IGC-MI/PC-ACR]	IGC-MI - Politique de Certification concernant l'Autorité de certification racine du Ministère de l'Intérieur - AA100008/PC0014 version 1
[PC_A1_FORM_CERT]	Annexe 1 Politique de certification Format des certificats - AA100008/PCA012 V1
[ExigencesSitesPerso]	Exigences de sécurité des sites de personnalisation, V1.0 (août 2007) http://www.references.modernisation.gouv.fr/sites/default/files/Exigences_sites_de_perso_V1_0.pdf

Renvoi	Document
[PROG_ACCRED]	COFRAC. - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – version publiée cf www.cofrac.fr
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version mars 2000 (complétée par les correctifs techniques n° 1 d'octobre 2001, n° 2 d'avril 2002 et n° 3 d'avril 2004)
[972-1]	DCSSI - Guide Technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter – N° 972-1/SGDN/DCSSI du 17/07/2003

12. ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC

12.1. EXIGENCES SUR LES OBJECTIFS DE SECURITE

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCRs et, éventuellement, des réponses OCSP), ainsi que, le cas échéant, générer les bi-clés des serveurs, doit répondre aux exigences de sécurité suivantes :

- si les bi-clés des serveurs sont générées par ce module, garantir que ces générations sont réalisées exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées,
- si les bi-clés des serveurs sont générées par ce module, assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques des serveurs lorsqu'elles sont sous la responsabilité de l'AC et pendant leur transfert vers le dispositif de protection des clés privées du serveur et assurer leur destruction sûre après ce transfert,
- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie,
- être capable d'identifier et d'authentifier ses utilisateurs,
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné,
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur,
- permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées,
- créer des enregistrements d'audit pour chaque modification concernant la sécurité,
- si une fonction de sauvegarde et de restauration des clés privées de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration,
- Il est recommandé que le module cryptographique de l'AC détecte les tentatives d'altérations physiques et entre dans un état sûr quand une tentative d'altération est détectée.

12.2. EXIGENCES SUR LA QUALIFICATION

Le module cryptographique utilisé par l'AC doit être qualifié au niveau renforcé (sous réserve qu'il existe au moins une telle référence au catalogue des produits qualifiés par l'A.N.S.S.I. Dans le cas contraire, le P.S.C.E. souhaitant faire qualifier son offre de certificats d'authentification de serveur doit obtenir une dérogation de l'A.N.S.S.I.), selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre 12.1 ci-dessus.

13. ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF DE CREATION DE CACHET OU D'AUTHENTIFICATION

13.1. EXIGENCES SUR LES OBJECTIFS DE SECURITE

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

- si la bi-clé 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 bi-clé 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 régénération 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,
- [C-SIG][C-HOR] générer un cachet qui ne peut être falsifié sans la connaissance de la clé privée,
- [C-SIG][C-HOR] assurer, pour le serveur légitime uniquement, la fonction de génération des cachets électroniques et protéger la clé privée contre toute utilisation par des tiers,
- [A-CLI][A-SER] générer une authentification qui ne puisse être falsifiée sans la connaissance de la clé privée,
- [A-CLI][A-SER] 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,
- [A-CLI][A-SER] 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.

13.2. EXIGENCES SUR LA QUALIFICATION

Le PSCE ne fournit pas le dispositif de création de cachet ou d'authentification au RCC/RCAS. Il est du ressort du RCC/RCAS de s'assurer que son dispositif technique respecte les éventuelles exigences de qualification du RGS pour le service applicatif qu'il propose.