Date : 05/10/2018

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

Titre :

POLITIQUES DE CERTIFICATION DES AC DÉLÉGUÉES PERSONNES LOGICIELS 1E MINISTERE DE L'INTERIEUR 2018

OID :

POLICE NATIONALE 1E 2018 : 1.2.250.1.152.2.12.21.1

ADMINISTRATION CENTRALE 1E 2018 : 1.2.250.1.152.2.12.11.1

ADMINISTRATION TERRITORIALE 1E 2018 : 1.2.250.1.152.2.12.31.1

Référence : IGC-MI_PC_ACD_PERS_LOGICIEL_V1.0

SUIVI DES MODIFICATIONS

Vers.	*Date*	*Objet de la modification*	*Auteur*
1.0	05/10/2018	• Création	Ministère Intérieur
		•	

TABLE DES MATIERES

1. INTRODUCTION

1.1. 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).

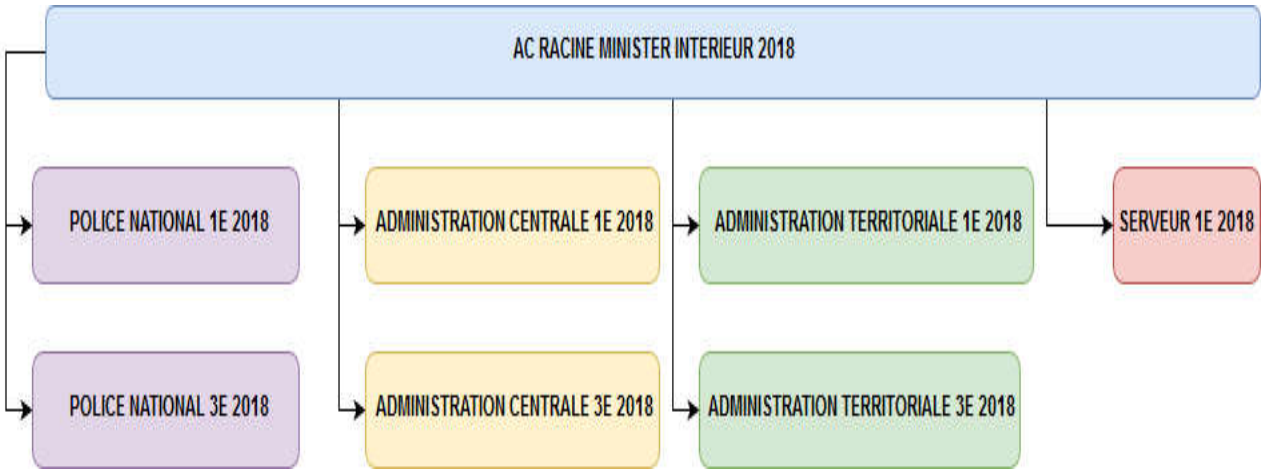
L'IGC-MI du ministère de l'Intérieur est constituée d'une hiérarchie de 3 niveaux de certificats :

- ✓ certificats d'AC RACINE MINISTERE DE L'INTERIEUR,
- ✓ certificats AC DELEGUEES ou AC Subordonnées du ministère de l'Intérieur,
- ✓ certificats utilisateurs finaux.

Le présent document porte à la connaissance des utilisateurs de certificats les informations de la politique de certification des autorités de certification déléguées du ministère, relatif aux certificats personne logiciel émis à partir des autorités de certification 2018.

Ces certificats personne logiciel sont qualifiés au niveau de sécurité RGS *.

La vue générale des ACs gérées par l'AC RACINE MINISTERE DE L'INTERIEUR est :



La liste des AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ETOILE MINISTÈRE INTÉRIEUR concernées par le présent document est la suivante :

- ✓ POLICE NATIONALE 1E 2018
- ✓ ADMINISTRATION CENTRALE 1E 2018
- ✓ ADMINISTRATION TERRITORIALE 1E 2018

Les AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ETOILE MINISTÈRE INTÉRIEUR délivrent les certificats au format PKCS12 des porteurs personnes physiques du ministère de l'Intérieur.

Les AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR sont destinées à délivrer des certificats de type « Authentification » répondant aux exigences RGS PC Type Authentification *.

Ces certificats sont des certificats logiciels. Seuls les porteurs de cartes agent avec certificats de niveau de confiance RGS 2 étoiles valides et délivrés par l'IGC-MI peuvent en bénéficier.

Le présent document fait partie d'un ensemble de documents décrivant les politiques de certification définies dans le cadre du projet IGC-MI.

Pour les AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR, il spécifie les exigences applicables :

- ✓ aux AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR, pour :

- la génération et le renouvellement de leurs clés respectives,
- la certification, le renouvellement et la révocation des clés publiques des porteurs,

✓ aux certificats des porteurs, pour :

- La génération de leurs clés ainsi que la gestion des demandes de certificats auprès des AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR.

1.2. IDENTIFICATION

La présente PC est la politique de certification des AC DELEGUEES PERSONNES LOGICIEL 1 ETOILE. Elle est identifiée par l'identifiant d'objet (OID) suivant : **1.2.250.1.152.2.12.X1.1**

Les certificats émis sont de type « authentification »

Le tableau ci-dessous présente le nom de l'AC DELEGUEE émettrice ainsi que les identifiant d'objet (OID) de l'AC :

AC DELEGUEES MINISTERE DE L'INTERIEUR	Type du certificat émis	OID
POLICE NATIONALE 1E 2018	Authentification *	**1.2.250.1.152.2.12.21.1**
ADMINISTRATION CENTRALE 1E 2018	Authentification *	**1.2.250.1.152.2.12.11.1**
ADMINISTRATION TERRITORIALE 1E 2018	Authentification *	**1.2.250.1.152.2.12.31.1**

1.3. ENTITES INTERVENANT DANS L'IGC-MI

1.3.1. Autorité administrative

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

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

Les fonctions assurées par l'AA 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 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,

✓ 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,

✓ 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 cela est nécessaire, les bi-clés des AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR et les certificats correspondants (signature de certificats, et de LCRs), puis diffuser ces certificats d'AC aux tiers utilisateurs.

1.3.2. Autorité de certification

Chaque AC DÉLÉGUÉE PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR 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'appuie pour cela sur l'IGC-MI.

Les prestations de chaque AC DÉLÉGUÉE PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR sont 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 (signature, authentification et confidentialité) à partir des informations transmises par l'Autorité d'Enregistrement, ou par l'Autorité d'Enregistrement Locale.

Fonction de publication

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

Fonction de gestion des révocations

Dans le cadre de cette fonction, chaque AC DÉLÉGUÉE PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

Fonction d'information sur l'état des certificats

Cette fonction fournit aux 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 LCR.

1.3.3. Les autorités d'enregistrement (AE)

L'AE a pour rôle de vérifier l'identité du futur porteur de certificat. Pour cela, l'AE assure les tâches suivantes :

- ✓ la prise en compte et la vérification des informations du titulaire de carte et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant lors d'une première demande, ou lors d'un renouvellement,
- ✓ l'établissement et la transmission de la demande de carte et de certificat au système de gestion des cartes de l'IGC-MI,
- ✓ la révocation des certificats,
- ✓ l'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage).

Deux catégories d'autorités d'enregistrement sont utilisées pour les AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR :

- ✓ Autorité d'Enregistrement Nationale (AEN) : elle détient des droits d'enregistrement pour l'ensemble des titulaires de certificats du ministère de l'Intérieur. Elle est compétente pour l'ensemble des entités administratives (services) de l'organisation du MI, et possède une visibilité sur tous les porteurs du système, y compris ceux gérés par les autorités d'enregistrement locales.
- ✓ Autorité d'Enregistrement Locale (AEL) : elle détient des droits d'enregistrement des titulaires rattachés à un ou plusieurs services du MI et dispose d'une visibilité restreinte aux seuls titulaires rattachés aux services dont elle a la charge.

1.3.4. Porteurs de certificats (Titulaires de certificats)

Dans le cadre de la présente PC, un porteur (titulaire) de certificats ne peut être qu'une personne physique.

Les porteurs sont les agents publics, les contractuels, les prestataires, les intérimaires, enfin toute personne ayant besoin de se connecter au système d'information et de communication (SIC) dans le cadre de sa mission au MI.

1.3.5. Utilisateurs de certificats

Un utilisateur de certificats peut être notamment :

- ✓ Un service de l'administration accessible par voie électronique aux usagers (application, serveur Internet, base de données, etc.), sous la responsabilité d'une personne physique ou morale, qui utilise :
  - un certificat et un service de vérification d'authentification :

    Pour authentifier le titulaire afin de l'autoriser à utiliser le poste de travail ou accéder aux services électroniques en ligne ou pour authentifier l'origine d'un message ou de données transmises par le porteur du certificat. L'application met en œuvre la politique et les pratiques de sécurité édictées par le responsable d'application.
- ✓ Un agent (personne physique) émetteur ou destinataire d'un message ou de données et qui utilise :
  - un certificat et un service de vérification d'authentification :

    Pour en authentifier l'origine. L'agent respecte la politique et les pratiques de sécurité édictées par le responsable de son entité.
- ✓ Un usager, porteur de certificat, destinataire d'un message ou de données provenant d'un agent et qui utilise:
  - un certificat et un service de vérification d'authentification :

    Pour en authentifier l'origine.

Les utilisateurs de certificats doivent prendre toutes autres précautions prescrites dans les éventuels accords ou tout autre document, notamment ceux précisés aux chapitres 9.6.3 et 9.6.4. En particulier, l'AC respecte ses engagements envers les utilisateurs qui ont « raisonnablement » confiance dans un certificat.

1.3.6. Autres participants

1.3.6.1. Référentiel des identités et de l'organisation

Le Référentiel des Identités et de l'Organisation (RIO) est le référentiel consolidant en un point unique les données d'identité et d'organisation issues des systèmes RH du ministère.

1.3.6.2. Autres Composantes de l'IGC-MI

La décomposition en fonctions de l'IGC-MI est présentée au chapitre 1.3. Les composantes de l'IGC-MI mettant en œuvre ces fonctions seront présentées dans la DPC de l'ACD.

1.3.6.2.1. Support

Le support aux porteurs est assuré par les opérateurs AEL locaux qui sont chargés de faire les demandes de certificats logiciels. Ils sont en mesure d'apporter un soutien aux porteurs et de révoquer les certificats en cas compromission.

Le portail self-service (https://portail-agent-cartes.minint.fr/)

La demande de certificat faite le porteur reçoit un fichier PKCS#12 du certificat d'authentification qualifié 1 étoile. Afin d'obtenir le mot de passe à usage unique, l'opérateur doit se connecter au portail self-service à l'aide de sa carte agent.

1.3.6.2.2. Système de gestion des cartes

C'est le cœur du système de l'IGC-MI qui est en charge des :

- ✓ cycles de vie des certificats logiciels des titulaires, de la synchronisation des données, ainsi que de la coordination de tous les traitements avec les autres composantes,
- ✓ droits et profils pour l'accès aux services de l'IGC-MI, notamment des opérateurs AE/AEL, des opérateurs AD/ADR,

- ✓ interfaces d'accès aux services (génération certificat, génération de LCRs) des AC déléguées,
- ✓ échanges avec le centre de pré-personnalisation des cartes,
- ✓ échanges avec le RIO du ministère pour l'import et la synchronisation des données d'enregistrement des titulaires,
- ✓ traitements automatiques liés aux cycles de vie des cartes et des certificats des porteurs, et aux notifications aux autres composantes.

1.3.6.2.3. Système de gestion des clés

Le système de gestion de clés est une composante de l'IGC-MI en charge de la gestion des clés cryptographiques, cela inclut :

- ✓ la gestion sécurisée des clés maîtres des cartes à puce et de séquestre / recouvrement des clés de confidentialité,
- ✓ la génération, le séquestre et le recouvrement sécurisé des bi-clés de confidentialité des porteurs,
- ✓ la gestion des clés cryptographiques intervenant dans l'autorisation d'accès à certaines opérations sur les cartes des titulaires, notamment :
  - le déblocage des cartes par *challenge / response,*
  - la génération des bi-clés dans les cartes,
  - l'écriture des codes d'activation des cartes des porteurs,
  - l'écriture et la modification des données, des clés, des certificats des cartes des porteurs,
- ✓ la gestion des clés de protection de données incluses dans les fichiers de production par lot des cartes (fichiers échangés avec le centre de pré-personnalisation des cartes).

Le système de gestion des clés s'appuie sur plusieurs HSM cryptographiques pour la protection des clés.

1.4. USAGE DES CERTIFICATS

1.4.1. Domaines d'utilisation applicables

1.4.1.1. Bi-clés et certificats des porteurs

Les présentes PC traitent des bi-clés et des certificats correspondant à la catégorie de certificat : authentification**,** à destination des porteurs identifiés au chapitre 1.3.4, afin que ces porteurs puissent s'authentifier sur les services mis à disposition des agents dans le cadre de leur travail.

Les certificats porteurs émis en vertu des présentes politiques sont appropriés pour établir le lien entre l'identité d'un porteur et une clé publique pour les applications suivantes dans un cadre strictement limité aux activités professionnelles du porteur pour ses attributions :

- ✓ AUTHENTIFICATION

L'entité responsable d'une application souhaitant utiliser un des certificats doit préalablement en demander l'autorisation au SHFD qui tient donc à jour la liste des applications autorisées à employer un des certificats.

Dans tous les cas, les AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR limitent la délivrance de certificats à des personnes physiques, en lien ou sous sa responsabilité.

1.4.1.2. Bi-clés et certificats d'AC

Les présentes PC couvrent également des exigences concernant les bi-clés et certificats des AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR (signature des certificats des porteurs, et signature des LCR).

Les AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR génèrent et signent différents types d'objets : certificats et LCR.

Pour signer ces objets, les AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR disposent chacune d'une bi-clé et d'un certificat dédiés, rattachés à l'AC RACINE MINISTERE INTERIEUR 2018.

1.4.2. Domaines d'utilisation interdits

Toute utilisation d'un certificat porteur autre que celles prévues dans le cadre des présentes PC est interdite. En cas de non respect de cette interdiction, la responsabilité des AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR ne saurait être engagée.

1.5. GESTION DE LA PC

1.5.1. Entité gérant la PC

Les AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR sont responsables de l'établissement des présentes PC, ainsi que de leurs applications et de leurs diffusions.
L'AA afférente est responsable de la validation des présentes PC.

1.5.2. Point de contact

Toute demande d'information devra se faire auprès du ministère de l'Intérieur à l'adresse suivante :

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

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

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

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

La DPC est approuvé par l'AA. La procédure d'approbation de la DPC est décrite dans la DPC.

1.7. DEFINITIONS ET ACRONYMES

1.7.1. Abréviations

Les acronymes utilisés dans la présente PC sont les suivants :

AA	Autorité Administrative
AC	Autorité de Certification
ACD	Autorité de Certification Déléguée
ACR	Autorité de Certification Racine
AD	Autorité de Délivrance
ADR	Autorité de Délivrance de Rattachement
AE	Autorité d'Enregistrement
AEL	Autorité d'Enregistrement Locale
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
DN	*Distinguished Name* ; nom distinctif

DPC	Déclaration des Pratiques de Certification
DIMAP	Direction Interministérielle pour la modernisation de l'action publique
FSSI	Fonctionnaire de Sécurité des Systèmes d'Information
HFD	Haut Fonctionnaire de Défense
HFDA	Haut-Fonctionnaire de Défense adjoint
IGC-MI	Infrastructure de Gestion de Clés du ministère de l'Intérieur
ISO	International Organization for Standardization
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de certification
MI	Ministère de l'Intérieur
OCSP	Online Certificate Status Protocol
OID	Object Identifier (Identifiant d'Objet)
PC	Politique de Certification
PCA	Plan de Continuité d'Activité
PSCE	Prestataire de service de certification électronique
RIO	Référentiel des Identités et de l'Organisation
RSA	Rivest Shamir Adelman
SHA-1	Secure Hash Algorithm version 1
SHA-2	Secure Hash Algorithm version 2
SP	Service de Publication
UC	Utilisateur de Certificats
URL	"Uniform Resource Locator" ; localisateur uniforme de ressource
UTC	Universal Time Coordinated ; temps universel coordonné

1.7.2. Définitions

Les termes utilisés dans la présente PC sont les suivants :

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

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'AC pour des besoins d'authentification, de confidentialité 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 l' [ORD05-1516], désigne les administrations de l'État, 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 1.3.3.

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

Autorité de certification - 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 1.3.2 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la PC, 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 à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une AC. 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 une personne physique et portant sur une bi-clé d'authentification, de signature ou de chiffrement, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, etc.).

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-MI. 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 - 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 PC qu'elle s'est engagée à respecter.

Dispositif d'authentification - Il s'agit du dispositif matériel et/ou logiciel utilisé par le porteur pour mettre en œuvre et stocker sa clé privée d'authentification.

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

Dispositif de création de signature - Il s'agit du dispositif matériel et/ou logiciel utilisé par le porteur pour mettre en œuvre et stocker sa clé privée de signature.

Entité - Désigne une AA 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 1.3.2.

Fonction de génération des éléments secrets du porteur - Cf. chapitre 1.3.2

Fonction de gestion des révocations - Cf. chapitre 1.3.2.

Fonction de publication - Cf. chapitre 1.3.2..

Fonction d'information sur l'état des certificats - Cf. chapitre 1.3.2.

Infrastructure de gestion de clés - 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 AC, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, d'une entité d'archivage, d'une entité de publication, etc.

Personne autorisée - Il s'agit d'une personne autre que le porteur qui est autorisée par la PC de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, etc.). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du porteur ou d'un responsable des ressources humaines.

Politique de certification - Ensembles de règles, identifiés chacun 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 porteurs et les utilisateurs de certificats.

Porteur - Cf. chapitre 1.3.4

Prestataire de services de certification électronique – 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 porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en

fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

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 [DEC2010-112] 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 [DEC2010-112]. Le [RGS] précise les trois processus de qualification : qualification de niveau élémentaire, qualification de niveau standard et qualification de niveau renforcé.

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 1.3.5

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

2.1. ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

Pour la mise à disposition des informations devant être publiées à destination des tiers utilisateurs de certificats, les AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR mettent en œuvre au sein de l'IGC-MI 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'AA : les PC et les certificats d'AC sont mis à disposition par le SHFD.

2.2. INFORMATIONS DEVANT ETRE PUBLIEES

Les AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR publient les informations suivantes à destination des tiers utilisateurs de certificats :

- ✓ les PC des AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR en cours de validité (le présent document),
- ✓ les versions antérieures des présentes PC, tant que des certificats émis selon ces versions sont en cours de validité,
- ✓ les profils des certificats des AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR, des porteurs, et des LCR émises,
- ✓ les certificats des AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR, 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, conformes au profil indiqué au chapitre 7, accessibles par le protocole HTTP,
- ✓ l'adresse (URL) permettant d'obtenir des informations concernant les AC DÉLÉGUÉES PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR

2.3. DELAIS ET FREQUENCES DE PUBLICATION

Toute nouvelle version d'un document (PC, formats des certificats) est diffusée via le site Web du MI dans les 24 heures 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 du ministère préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondants, et les systèmes les publiant ont une disponibilité de 24 heures / 24 et 7 jours / 7.

Dans l'annuaire interne du ministère, également accessible 24 heures / 24 et 7 jours / 7 :

- ✓ les certificats des porteurs sont diffusés dans les 24 heures ouvrées suivant leur génération ;
- ✓ les LCRs sont diffusées toutes les 24 heures (week-ends et jours fériés compris).

2.4. 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 des AC: http://crl.interieur.gouv.fr,
- ✓ pour la publication des certificats d'AC : https://www.interieur.gouv.fr/fr/IGC/Certificat,
- ✓ 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.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1. NOMMAGE

3.1.1. Types de noms

Les noms utilisés dans les certificats émis par l'IGC-MI sont conformes aux spécifications de la norme X.509.

Dans chaque certificat conforme à la norme X.509, l'AC DÉLÉGUÉE PERSONNES LOGICIEL 1 ÉTOILE MINISTÈRE INTÉRIEUR émettrice (*issuer*) et le porteur (*subject*) sont identifiés par un *"Distinguished Name"* (DN) en UTF8String.

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

3.1.1.1. Certificat d'AC

Pour les certificats des AC Déléguées Personnes logiciels 1 étoile :

Nom	Police Nationale 1E 2018	Administration Centrale 1E 2018	Administration Territoriale 1E 2018
Emetteur	CN=AC RACINE MINISTERE INTERIEUR 2018 OU=SERVEURS OU=0002 110014016 O=MINISTERE INTERIEUR C=FR		
Sujet	CN=POLICE NATIONALE 1E 2018 OU=SERVEURS OU=0002 110014016 O=MINISTERE INTERIEUR C=FR	CN=ADMINISTRATION CENTRALE 1E 2018 OU=SERVEURS OU=0002 110014016 O=MINISTERE INTERIEUR C=FR	CN=ADMNISTRATION TERRITORIALE 1E 2018 OU=SERVEURS OU=0002 110014016 O=MINISTERE INTERIEUR C=FR

3.1.1.2. Certificat porteur (titulaire)

Champ	Certificat d'authentification	Certificat d'authentification	Certificat d'authentification
Emetteur	CN=POLICE NATIONALE 1E 2018 OU=SERVEURS OU=0002 110014016 O=MINISTERE INTERIEUR C=FR	CN=ADMINISTRATION CENTRALE 1E 2018 OU=SERVEURS OU=0002 110014016 O=MINISTERE INTERIEUR C=FR	CN=ADMNISTRATION TERRITORIALE 1E 2018 OU=SERVEURS OU=0002 110014016 O=MINISTERE INTERIEUR C=FR
Sujet	CN= « Prénom Nom N° RIO» SN = « Nom » GN = « Prénom » UID= «n°RIO» OU=PERSONNES OU=0002 110014016 O=MINISTERE INTERIEUR C=FR		

N° RIO : numéro d'identification unique du porteur dans le Référentiel des Identités et de l'Organisation.

3.1.2. Nécessité d'utilisation de noms explicites

Dans tous les cas, l'identité du porteur est construite à partir des nom et prénom de son état-civil tels que portés sur un document officiel d'identité.

3.1.3. Pseudonymisation des porteurs

L'utilisation des pseudonymes n'est pas autorisée par les présentes PC.

3.1.4. Règles d'interprétation des différentes formes de nom

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

3.1.5. Unicité des noms

Le DN du champ « *subject* » de chaque certificat de porteur contient un identifiant unique d'utilisateur dont la valeur est le numéro RIO, et qui permet d'identifier de façon unique chaque porteur correspondant au sein du domaine de l'IGC-MI.

3.1.6. Identification, authentification et rôle des marques déposées

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

3.2. VALIDATION INITIALE DE L'IDENTITE

3.2.1. Méthode pour prouver la possession de la clé privée

Les bi-clés d'authentification sont générées dans le système de gestion de clés de l'IGC-MI, et le certificat

et la clé privée du porteur sont envoyés au porteur sous forme d'un jeton cryptographique logiciel PKCS#12.

3.2.2. Validation de l'identité d'un organisme

La validité de l'identité de l'organisme de rattachement d'un demandeur est considérée comme acquise par le fait de la présence de celui-ci dans le RIO.

3.2.3. Validation de l'identité d'un individu

3.2.3.1. Enregistrement d'un porteur [ADMINISTRATION]

L'enregistrement d'un porteur s'appuie sur :

- ✓ Les informations du RIO détenues dans l'application cartes précédemment utilisées pour la demande de carte embarquant les certificats qualifiés RGS 2 étoiles et pour la demande de certificats personne logiciel 1 étoile. Pour cet enregistrement, une adresse de messagerie professionnelle personnelle est exigée,
- ✓ Une demande officielle motivée validée par son entité d'emploi.

3.2.3.2. Enregistrement d'un Mandataire de Certification

Sans objet. La présente PC n'utilise pas de mandataire de certification.

3.2.3.3. Enregistrement d'un porteur [ADMINISTRATION] via un MC

Sans objet.

3.2.4. Informations non vérifiées du porteur

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

3.2.5. Validation de l'autorité du demandeur

Sans objet.

3.2.6. Certification croisée d'AC

Les présentes PC n'autorisent pas la certification croisée par les AC déléguées.

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

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

3.3.1. Identification et validation pour un renouvellement courant

Lors d'un renouvellement, l'AE/AEL du porteur vérifie que les informations du porteur sont à jour par import des données du référentiel d'identité du MI (aucune modification des informations contenues dans le certificat du porteur) et procède à la validation de la demande de renouvellement.

3.3.2. Identification et validation pour un renouvellement après révocation

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 d'enregistrement initial.

3.4. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE FOURNITURE DE NOUVEAUX CERTIFICATS

Suite à la modification des informations contenues dans le certificat du porteur, ou changement d'affectation, la procédure d'identification et de validation est identique à la procédure d'enregistrement initial.

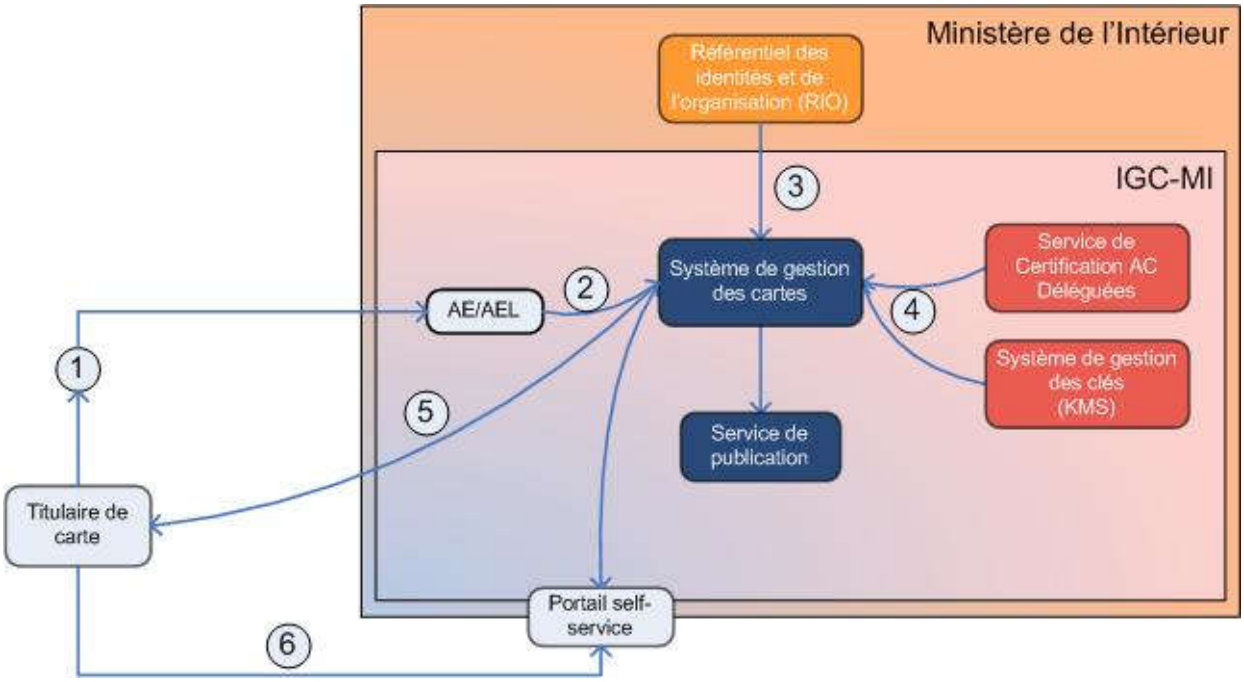
3.5. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

La demande de révocation doit provenir d'une entité autorisée (chapitre 4.8.2).

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1. DEMANDE DE CERTIFICAT

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



1. Le titulaire s'adresse à son autorité d'enregistrement pour faire une demande de certificat validée par une autorité de son service.
2. L'autorité d'enregistrement recherche le profil du titulaire, valide les informations inscrites et effectue une demande de certificat pour le titulaire.
3. Si nécessaire, un import ou mise à jour du profil du titulaire est lancé par interrogation du RIO du ministère de l'intérieur.
4. Le système de gestion des cartes lance la génération d'une bi-clé, et d'un certificat pour l'utilisateur sous forme d'un jeton logiciel PKCS#12, protégé par un mot de passe.
5. Le système de gestion de carte envoie le jeton contenant certificat et clé privée au titulaire par courrier électronique.
6. Le titulaire reçoit son jeton par courrier électronique et s'authentifie sur le portail *self service* avec sa carte à puce pour la récupération du mot de passe du jeton.

4.1.1. Origine d'une demande de certificat

Les demandes de certificats sont effectuées par tout agent disposant d'un certificat AC PERSONNES qualifié 2 étoiles et d'une adresse de messagerie professionnelle personnelle.

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

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

- ✓ le nom du porteur à utiliser dans le certificat,
- ✓ les données personnelles d'identification du porteur,
- ✓ l'adresse de messagerie professionnelle personnelle du porteur.

La demande est établie sur la base des informations relatives au porteur, telles que contenues dans le RIO et la base de gestion des cartes.

4.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

Les identités sont vérifiées conformément aux exigences du chapitre 3.2.

L'AE/AEL doit effectuer les opérations suivantes :

- ✓ valider l'identité du futur porteur et la conformité de la carte agent, avec certificat AC PERSONNES qualifié 2 étoiles, présentée,
- ✓ vérifier la cohérence des justificatifs présentés, notamment vis-à-vis des informations contenues dans le RIO,
- ✓ s'assurer de la validité de l'adresse de messagerie présente dans l'application Cartes,
- ✓ s'assurer que le futur porteur a pris connaissance des modalités applicables pour l'utilisation du certificat (voir les conditions générales d'utilisation).

Une fois ces opérations effectuées, l'AE/AEL émet la demande de production du jeton.

La conservation de la demande est effectuée dans le système d'information.

4.2.2. Acceptation ou rejet de la demande

L'acceptation ou le rejet d'une demande est à la discrétion de l'AE/AEL. Le demandeur est informé, le cas échéant, du rejet de sa demande.

4.2.3. Durée d'établissement du certificat

La délivrance du certificat est immédiate.

4.3. DELIVRANCE DU CERTIFICAT

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

Voir schéma ci-dessus.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitre 5 et 6, notamment la séparation des rôles de confiance (*cf.* chapitre 5.2).

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

Le certificat est envoyé par e-mail au porteur, à l'adresse issue du RIO et référencée dans sa demande. Voir schéma ci-dessus.

4.4. ACCEPTATION DU CERTIFICAT

4.4.1. Démarche d'acceptation du certificat

L'acceptation du certificat est tacite dès le retrait du mot de passe par le porteur via le portail. Le porteur doit vérifier son certificat dès la récupération de son mot de passe. En cas d'incident ou d'erreur constatée dans le certificat, le porteur doit en aviser immédiatement l'AE/AEL ayant fait la demande afin notamment de révoquer le certificat.

4.4.2. Publication du certificat

Les certificats d'authentification 1 étoile des porteurs ne sont pas publiés par l'AC.

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

L'AE (ou AEL) effectuant la demande est informée via l'interface de gestion des cartes.

4.5. USAGES DE LA BI-CLE ET DU CERTIFICAT

4.5.1. Utilisation de la clé privée et du certificat par le porteur

L'utilisation des clés privées du porteur et des certificats associés est strictement limitée aux services d'authentification (*cf.* chapitre 1.4.1.1). Les porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de chaque bi-clé du porteur et de son certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des clés.

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

Cf. chapitre 4.5.1 et chapitre 1.4.

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

4.6. RENOUVELLEMENT D'UN CERTIFICAT

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 porteur).

Dans le cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante.

4.6.1. Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2. Origine d'une demande de renouvellement

Sans objet.

4.6.3. Procédure de traitement d'une demande de renouvellement

Sans objet.

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

Sans objet.

4.6.5. Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6. Publication du nouveau certificat

Sans objet.

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

Sans objet.

La procédure de délivrance d'un nouveau certificat suite à un changement de bi-clé est la même que la demande initiale.

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

Les bi-clés sont périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi, les bi-clés des porteurs, et les certificats correspondants, sont renouvelés au minimum à une fréquence de : 3 ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du porteur (*cf.* chapitre 4.8, notamment le chapitre 4.8.1.1 pour les différentes causes possibles de révocation).

Nota - Dans la suite du présent chapitre, le terme utilisé est "fourniture d'un nouveau certificat". Ce terme recouvre également, dans le cas où elle est générée par l'AC, la fourniture de la nouvelle bi-clé du porteur.

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

Le déclenchement de la fourniture d'un nouveau certificat est à l'initiative du porteur.

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

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

Pour les actions de l'AC, se reporter au chapitre 4.3.1.

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

Cf. chapitre 4.3.2.

4.6.12. Démarche d'acceptation du nouveau certificat

Cf. chapitre 4.4.1.

4.6.13. Publication du nouveau certificat

Cf. chapitre 4.4.2.

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

Cf. chapitre 4.4.3

4.7. 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 4.1) et autres qu'uniquement la modification des dates de validité (*cf.* chapitre 4.6).

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

4.7.1. Causes possibles de modification d'un certificat

Sans objet.

4.7.2. Origine d'une demande de modification d'un certificat

Sans objet.

4.7.2.1. Procédure de traitement d'une demande de modification d'un certificat

Sans objet.

4.7.3. Notification au porteur de l'établissement du certificat modifié

Sans objet.

4.7.4. Démarche d'acceptation du certificat modifié

Sans objet.

4.7.5. Publication du certificat modifié

Sans objet.

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

Sans objet.

4.8. REVOCATION ET SUSPENSION DES CERTIFICATS

4.8.1. Causes possibles d'une révocation

4.8.1.1. Certificats de porteurs

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

- ✓ les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple le changement d'entité du porteur d'un certificat), ceci avant l'expiration normale du certificat,
- ✓ le porteur n'a pas respecté les modalités applicables d'utilisation du certificat,
- ✓ le porteur ou l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC,
- ✓ une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur,
- ✓ la clé privée du porteur est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées),
- ✓ le porteur 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 porteur et/ou de son support),
- ✓ le décès ou la cessation d'activité du porteur,
- ✓ la cessation d'activité de l'entité du porteur.

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.

4.8.1.2. 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 LCR) :

- ✓ 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 énoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif),
- ✓ cessation d'activité de l'entité opérant la composante.

4.8.2. Origine d'une demande de révocation

4.8.2.1. Certificats de porteurs

Les entités qui peuvent demander la révocation d'un certificat de porteur sont les suivantes :

- ✓ le porteur au nom duquel le certificat a été émis,
- ✓ un représentant légal de l'entité,
- ✓ l'AC émettrice du certificat ou l'une de ses composantes (AEL).

Nota : Le porteur est informé des personnes / entités susceptibles d'effectuer une demande de révocation de son certificat.

4.8.2.2. 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, par l'AC RACINE MINISTERE INTERIEUR 2018 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.

4.8.3. Procédure de traitement d'une demande de révocation

4.8.3.1. Révocation d'un certificat de porteur

Les demandes de révocation sont effectuées auprès de l'AE ou des AEL.

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

- ✓ l'identité du porteur du certificat utilisée dans le certificat (nom, prénom),
- ✓ le nom du demandeur de la révocation,
- ✓ toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (numéro de série, etc.),
- ✓ éventuellement, la cause de révocation.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée au minimum via une LCR signée par une entité désignée par l'AC. D'autres moyens de diffusion complémentaires peuvent également être utilisés par l'AC.

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

L'entité est informée de la révocation de tout certificat des porteurs qui lui sont rattachés.

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

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

Les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC-MI sont précisées dans la DPC.

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 porteurs concernés que leurs certificats ne sont plus valides. Pour cela, l'IGC-MI pourra par exemple envoyer des récépissés aux AEL. Ces derniers devront informer les porteurs de certificats 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.

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

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

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

4.8.5.1. Révocation d'un certificat de porteur

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.

4.8.5.2. 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 évènement décrit dans le paragraphe des 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.

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCRs) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

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

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

4.8.7. Fréquence d'établissement des LCRs

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

4.8.8. Délai maximum de publication d'une LCRs

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

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

Sans objet.

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

Cf. chapitre 4.8.6.

4.8.11. Autres moyens disponibles d'information sur les révocations

Ces autres moyens d'information sur les révocations peuvent être mis en place à condition qu'ils respectent les exigences d'intégrité, de disponibilité et de délai de publication décrite dans la présente PC.

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

Pour les certificats de porteur, 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 4.8.3.2, 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.).

4.8.13. Causes possibles d'une suspension

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

4.8.14. Origine d'une demande de suspension

Sans objet.

4.8.15. Procédure de traitement d'une demande de suspension

Sans objet.

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

Sans objet.

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

4.9.1. Caractéristiques opérationnelles

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'AC Racine), c'est-à-dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCRs / LARs et l'état du certificat de l'AC Racine.

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR / LAR.

4.9.2. Disponibilité 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 4 heures (jours ouvrés) et une durée maximale totale d'indisponibilité par mois inférieure à 32 heures (jours ouvrés).

4.9.3. Dispositifs optionnels

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

4.10. FIN DE LA RELATION ENTRE LE PORTEUR ET L'AC

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

4.11. SEQUESTRE DE CLE ET RECOUVREMENT

Ni les clés privées d'AC, ni les clés privées d'authentification des porteurs ne sont séquestrées.

4.11.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

4.11.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

5. MESURES DE SECURITE NON TECHNIQUES

5.1. MESURES DE SECURITE PHYSIQUE

5.1.1. Situation géographique 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,…).

5.1.2. Accès 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 significatif, 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.

5.1.3. Alimentation électrique 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.

5.1.4. Vulnérabilité aux dégâts 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.

5.1.5. Prévention 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.

5.1.6. 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.

5.1.7. Mise hors service des supports

En fin de vie, les supports devront être, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.

Les procédures et moyens de destruction et de réinitialisation des disques durs de l'infrastructure IGC-MI sont conformes à ce niveau de confidentialité (voir notamment le guide [972-1]).

5.1.8. Sauvegarde 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 4.8.5.1 et 4.9.2).

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.

5.2. MESURES DE SECURITE PROCEDURALES

5.2.1. Rôles 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-MI : *cf.* chapitres 6.1 et 6.2.

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 différentient 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.

5.2.2. Nombre de personnes requises par tâches

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 6).

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.).

5.2.3. Identification et authentification pour chaque rôle

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 portée à la connaissance de la personne désignée.

5.2.4. Rôles exigeant une séparation 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.

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

5.3.1. Qualifications, compétences 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.

5.3.2. Procédures de vérification des antécédents

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).

5.3.3. Exigences en matière 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.

5.3.4. Exigence et fréquence en matière 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.

5.3.5. Fréquence et séquence de rotation entre différentes attributions

Se référer à la DPC de l'AC

5.3.6. Sanctions en cas d'actions non-autorisées

Se référer à la DPC de l'AC

5.3.7. Exigences vis-à-vis 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 5.3. Ceci est traduit en clauses adéquates dans les contrats avec ces prestataires.

5.3.8. 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.

5.4. PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

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

5.4.1. Type d'évènements à 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 porteurs).

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),
- ✓ le cas échéant, génération des éléments secrets du porteur (bi-clé, codes d'activation),
- ✓ génération des certificats des porteurs,
- ✓ transmission des certificats aux porteurs et, selon les cas, acceptations / rejets explicites par les porteurs,
- ✓ le cas échéant, remise de son dispositif de création de signature au porteur,
- ✓ 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 est enregistrée),
- ✓ 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.

5.4.2. Fréquence de traitement des journaux d'évènements

Cf. chapitre **Erreur ! Source du renvoi introuvable.**.

5.4.3. Période de conservation des journaux d'évènements

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

5.4.4. Protection des journaux d'évènements

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 6.8.

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.

5.4.5. Procédure de sauvegarde des journaux d'évènements

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

5.4.6. Système de collecte des journaux d'événements

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

5.4.7. Notification de l'enregistrement d'un évènement au responsable de l'évènement

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

5.4.8. Evaluation des vulnérabilités

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 1 fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité au moins 1 fois par semaine et dès la détection d'une anomalie. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé 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 1 fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

5.5. ARCHIVAGE DES DONNEES

5.5.1. Types de données 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 LCRs tels qu'émis ou publiés,
- ✓ les récépissés ou notifications (à titre informatif),
- ✓ les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement,
- ✓ les journaux d'évènements des différentes entités de l'IGC-MI.

5.5.2. Période de conservation des archives

5.5.2.1. 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.

Lorsque les porteurs sont enregistrés par une autorité d'enregistrement dans un autre pays que celui ou l'AC est établie, alors il convient que cette AE applique également la réglementation de son propre pays.

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

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.

Ce dossier, complété par les mentions consignées par l'AE, permet de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.

5.5.2.2. Certificats et LCRs émis par l'AC

Les certificats de clés de porteurs et d'AC, ainsi que les LCRs / LARs produites, sont archivés pendant au moins 8 ans après leur expiration.

5.5.2.3. Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 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.

5.5.2.4. Autres journaux

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

5.5.3. Protection des archives

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

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

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

5.5.4. Procédure 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.

5.5.5. Exigences d'horodatage des données

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

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

5.5.6. Système de collecte des archives

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

5.5.7. Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) doivent pouvoir être récupérées dans un délai inférieur à 2 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).

5.6. CHANGEMENT DE CLE D'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration 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 aient expiré.

5.7. REPRISE SUITE A COMPROMISSION ET SINISTRE

5.7.1. Procédures de remontée 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 porteurs devient insuffisant pour son utilisation prévue restante, alors l'AC :

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

5.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

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 1 fois tous les 2 ans.

5.7.3. Procédures de reprise en cas de compromission de la clé privée 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 5.7.2) en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat correspondant est immédiatement révoqué : *cf.* chapitre 4.8.

En outre, l'AC s'engage à :

- ✓ informer les entités suivantes de la compromission : tous les porteurs et les autres entités avec lesquelles l'AC a passé des accords ou a 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.

5.7.4. Capacités de continuité d'activité suite à 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 5.7.2).

5.8. FIN DE VIE D'UNE 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
- Une dernière LCR qui comporte l'extension « ExpiredCertsOnCRL » sera publiée ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s « 99991231235959Z ».

Au plus tôt, et dès la prise de décision de cesser l'activité, l'ACD informe les utilisateurs et les porteurs de la décision par le biais des sites web http://crl.interieur.gouv.fr (dédié aux CRL des AC) et https://www.interieur.gouv.fr/IGC (dédié aux autres informations).

À la date de l'arrêt du service, l'ACD :

- ✓ Demande la révocation de son certificat auprès de l'AC RACINE MINISTÈRE INTÉRIEUR 2018 ;
- ✓ Révoque tous les certificats qu'elle a signés et en cours de validité (dernière CRL) ;
- ✓ 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 CRLs des AC) et https://www.interieur.gouv.fr/IGC (dédié aux autres informations)
- ✓ Archive sa dernière CRL, les P.-V. de destruction des clés.

5.8.1. Transfert d'activité ou cessation d'activité 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 porteurs et des informations relatives aux certificats).
2. Assure la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCRs), 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 porteurs 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 porteurs ou des utilisateurs de certificats, l'AC les en avise aussitôt que nécessaire et, au moins, sous le délai suivant : 1 mois.

5.8.2. Cessation d'activité affectant l'AC

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

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'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 LCR 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.

6. MESURES DE SECURITE TECHNIQUES

6.1. GENERATION ET INSTALLATION DE BI-CLES

6.1.1. Génération des bi-clés

6.1.1.1. Clés d'AC

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé (*cf.* chapitre 6.5).

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 5.2.1), 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-MI. 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.

6.1.1.2. Clés porteurs générées par l'AC

La génération des clés des porteurs est effectuée dans un environnement sécurisé (*cf.* chapitre 6.5). Les bi-clés des porteurs sont générées dans un module cryptographique conforme aux exigences du chapitre 11, puis transférées de manière sécurisée dans le dispositif de protection de clés privées, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée.

6.1.1.3. Clés porteurs générées par le porteur

Aucune clé n'est générée par le porteur.

6.1.2. Transmission de la clé privée à son propriétaire

La clé privée est transmise au porteur par envoi mail au format PKSC12 protégé par mot de passe accessible via une connexion par certificat d'authentification personnes qualifié 2 étoiles.

6.1.3. Transmission de la clé publique à l'AC

Sans objet.

6.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats

Les clés publiques de vérification de signature de l'AC sont diffusées auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et qui en authentifie l'origine.

La clé publique de l'AC, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) sont librement récupérables par les utilisateurs de certificats sur les sites mentionnés en 2.4.

6.1.5. Tailles des clés

Les clés d'AC et de porteurs respectent les exigences de caractéristiques (tailles, algorithmes, etc.) du document [RGS_A_14].

6.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité

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 sont signés par une clé RSA 4096 bits.

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

6.1.7. Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR (*cf.* chapitre 1.4.1.2 et document [RGS_A_14]).

L'utilisation des clés privées du porteur et des certificats associés est strictement limitée aux services mentionnés aux chapitres 1.4.1.1 et 4.5 du présent document.

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

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1. 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 porteurs, sont des modules cryptographiques répondant au minimum aux exigences du chapitre 11.

6.2.2. Contrôle de la clé privée 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 6.1.1.1, l'activation de la clé privée au chapitre 6.2.8 et sa destruction au chapitre 6.2.10.

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

6.2.3. Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées de signature et d'authentification des porteurs ne sont en aucun cas séquestrées.

Concernant les clés d'authentification des porteurs, voir chapitre 4.11.

6.2.4. Copie de secours de la clé privée

Les clés privées des porteurs 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 offre un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuyé sur un algorithme d'une longueur de clé et avec 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].

Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique.

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

6.2.5. Archivage de la clé privée

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

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

6.2.6. Transfert de la clé privée vers / depuis le module cryptographique

Si l'AC génère les clés privées des porteurs en dehors du dispositif du porteur, le transfert est effectué conformément aux exigences du chapitre 6.1.1.2.

Pour les clés privées d'AC, tout transfert est effectué sous forme chiffrée, conformément aux exigences du chapitre 6.2.4.

6.2.7. Stockage de la clé privée dans un module cryptographique

Les clés privées d'AC sont stockées dans un module cryptographique répondant au minimum aux exigences du chapitre 11.

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

6.2.8. Méthode d'activation de la clé privée

6.2.8.1. Clés privées d'AC

La méthode d'activation des clés privées d'AC dans un module cryptographique est conforme 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).

6.2.8.2. Clés privées des porteurs

L'activation de la clé privée du porteur est contrôlée via des données d'activation (code porteur de la carte) (*cf.* chapitre 6.4) et permet de répondre aux exigences définies dans le chapitre 12.

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. 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. Ces conditions de désactivation permettent de répondre aux exigences définies dans le chapitre 11.

6.2.9.2. Clés privées des porteurs

Les conditions de désactivation de la clé privée d'un porteur permettent de répondre aux exigences définies dans le chapitre 12.

6.2.10. Méthode de destruction des clés privées

6.2.10.1. Clés privées d'AC

La méthode de destruction des clés privées d'AC est conforme aux exigences définies dans le chapitre 11.

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.

6.2.10.2. Clés privées des porteurs

En fin de vie de la clé privée d'un porteur, la méthode de destruction de cette clé privée permet de répondre aux exigences définies dans le chapitre 12.

6.2.11. Niveau de qualification du module cryptographique et des dispositifs de création de signature

Ces exigences sont précisées aux chapitres 11 et 12.

6.3. AUTRES ASPECTS DE LA GESTION DES BI-CLES

6.3.1. Archivage des clés publiques

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

6.3.2. Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des porteurs couverts par la présente PC ont une durée de vie d'au moins 3 ans.

La fin de validité d'un certificat d'AC est postérieure à la fin de vie des certificats porteurs qu'elle émet. La duré de vie des clés de signature d'AC et des certificats correspondants est de 6 ans.

Note : Cette durée de vie est cohérente avec les caractéristiques de l'algorithme, la longueur de clés utilisées (*cf.* [RGS_A_14]) et ne dépassent pas 10 ans.

6.4. DONNEES D'ACTIVATION

6.4.1. Génération et installation des données d'activation

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

6.4.1.2. Génération et installation des données d'activation correspondant à la clé privée du porteur

Les clés privées du porteur sont générées sur sa carte au moment de la remise, à l'exception des clés de confidentialité. Les clés de confidentialité sont installées sur la carte lors de la remise à travers un canal sécurisé (voir processus de délivrance ci-dessus).

Le code d'activation est transmis par courrier directement au porteur.

6.4.2. Protection des données d'activation

6.4.2.1. 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.

6.4.2.2. Protection des données d'activation correspondant aux clés privées des porteurs

Si les données d'activation des dispositifs de création de signature des porteurs sont générées par l'AC, elles sont protégées en intégrité et en confidentialité jusqu'à la remise aux porteurs.

Les données d'activation ne sont pas sauvegardées par l'AC

6.4.3. Autres aspects liés aux données d'activation

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

6.5. 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.

6.5.1. Exigences de sécurité technique spécifiques aux systèmes 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 aux objectifs de sécurité suivants :

- ✓ identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs),
- ✓ 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 1.4.1.2) 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.

6.5.2. Niveau de qualification des systèmes 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].

6.6. 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 et respecte dans la mesure du possible des normes de modélisation et d'implémentation. 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,
- ✓ utilise des systèmes et des produits fiables qui sont protégés contre toute modification.

6.6.1. Mesures liées à la gestion de la sécurité

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

6.6.2. Niveau d'évaluation sécurité du cycle de vie des systèmes

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

6.7. 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.).

6.8. HORODATAGE / SYSTEME DE DATATION

Plusieurs exigences de la présente PC nécessitent la datation par les différentes composantes de l'IGC-MI d'évènements liés aux activités de l'IGC-MI (*cf.* chapitre 5.4).

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

7. PROFILS DES CERTIFICATS ET DES LCR

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

8. 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 [DEC2010-112]) et, d'autre part, ceux que doit réaliser, ou faire réaliser, l'AC afin de s'assurer que l'ensemble de l'IGC-MI, 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 l'IGC-MI.

8.1. FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

Avant la première mise en service d'une composante de l'IGC-MI 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 l'IGC-MI suivant la fréquence : 1 fois tous les 2 ans.

8.2. 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.

8.3. RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES

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

8.4. SUJETS COUVERTS PAR LES EVALUATIONS

Les contrôles de conformité portent sur une composante de l'IGC-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.).

8.5. 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

8.6. 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.

9. AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1. TARIFS

9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

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

9.1.2. Tarifs pour accéder aux certificats

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

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

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

9.1.4. Tarifs pour d'autres services

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

9.1.5. Politique de remboursement

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

9.2. RESPONSABILITE FINANCIERE

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

9.2.1. Couverture par les assurances

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

9.2.2. Autres ressources

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

9.2.3. Couverture et garantie concernant les entités utilisatrices

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

9.3. CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

9.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

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

9.3.2. Informations hors du périmètre des informations confidentielles

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

9.3.3. Responsabilités 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 9.3.1, 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 notamment la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des porteurs à des tiers dans le cadre de procédures légales. Elle donne l'accès à ces informations au porteur.

9.4. PROTECTION DES DONNEES PERSONNELLES

9.4.1. Politique de protection des données 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].

9.4.2. Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- ✓ les causes de révocation des certificats des porteurs (qui sont considérées comme confidentielles sauf accord explicite du porteur),
- ✓ le dossier d'enregistrement du porteur.

9.4.3. Informations à caractère non personnel

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

9.4.4. Responsabilité en termes de protection des données personnelles

Cf. législation et réglementation en vigueur sur le territoire français (notamment *cf.* chapitre 10).

9.4.5. Notification et consentement d'utilisation des données personnelles

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.

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

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

9.4.7. Autres circonstances de divulgation d'informations personnelles

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

9.5. DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

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

9.6. INTERPRETATIONS CONTRACTUELLES ET GARANTIES

Les obligations communes aux composantes de l'IGC-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 doit être 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 porteurs,
- ✓ documenter leurs procédures internes de fonctionnement,
- ✓ mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1. Autorités de Certification

L'AC a pour obligation de :

- ✓ pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, conformément aux exigences du chapitre 4.4.,
- ✓ 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 DÉLÉGUÉES PERSONNES 2 ÉTOILES MINISTÈRE INTÉRIEUR 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 par 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 porteurs 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 porteur et l'AC est formalisée par un lien contractuel / hiérarchique / 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 *PC Type RGS Authentification **, Signature* ** et confidentialité **. 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 activités et possède 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 porteurs 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.

En cas de non-respect ponctuel des obligations décrites dans la présente PC, l'Administration se réserve le droit de refuser temporairement ou définitivement les certificats de l'AC conformément à la réglementation en vigueur.

9.6.2. Service d'enregistrement

Cf. les obligations pertinentes du chapitre 9.6.1.

9.6.3. Porteurs de certificats

Le porteur a le devoir de :

- ✓ communiquer des informations d'état-civil exactes à l'administration et signaler sans délai toute modification de celles-ci,
- ✓ protéger sa clé privée par des moyens appropriés à son environnement,
- ✓ protéger ses données d'activation et, le cas échéant, les mettre en œuvre,
- ✓ protéger l'accès à sa base de certificats,
- ✓ respecter les conditions d'utilisation de sa clé privée et du certificat correspondant,
- ✓ informer l'AC de toute modification concernant les informations contenues dans son certificat,
- ✓ faire, sans délai, une demande de révocation de son certificat auprès de l'AE ou de l'AC en cas de compromission ou de suspicion de compromission de sa clé privée (ou de ses données d'activation).

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

9.6.4. 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,
- ✓ pour chaque certificat de la chaîne de certification, du certificat du porteur jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation).

9.6.5. Autres participants

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

9.7. LIMITE DE GARANTIE

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

9.8. LIMITE DE RESPONSABILITE

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

9.9. INDEMNITES

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

9.10. DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

9.10.1. Durée de validité

La présente PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de celle-ci.

9.10.2. Fin anticipée de validité

La publication d'une nouvelle version des PC type du [RGS] peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer la présente PC.

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

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

9.11. NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

En cas de changement de toute nature intervenant dans la composition de l'IGC-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.

9.12. AMENDEMENTS A LA PC

9.12.1. Procédures d'amendements

L'AC devra contrôler que tout projet de modification de sa PC reste conforme aux exigences des PC Type et des éventuels documents complémentaires du [RGS]. En cas de changement important, il est recommandé à l'AC de faire appel à une expertise technique pour en contrôler l'impact.

9.12.2. Mécanisme et période d'information sur les amendements

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

9.12.3. Circonstances selon lesquelles l'OID doit être changé

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.

9.13. DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

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

9.14. 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.

9.15. CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre 10.

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

9.16. DISPOSITIONS DIVERSES

9.16.1. Accord global

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

9.16.2. Transfert d'activités

Cf. chapitre 5.8.

9.16.3. Conséquences d'une clause non valide

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

9.16.4. Application et renonciation

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

9.16.5. Force majeure

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

9.17. AUTRES DISPOSITIONS

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

Le Préfet,
Haut fonctionnaire de défense adjoint

10. ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1. 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
[DEC2010-112]	Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 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.

10.2. DOCUMENTS TECHNIQUES

Renvoi	Document
[RGS]	Référentiel Général de Sécurité – Version 1.0
[RGS-PC_A]	Référentiel Général de Sécurité version 1. Annexe A7 Politique de Certification Type « Authentification » OID : 1.2.250.1.137.2.2.1.2.2.1
[RGS-PC_S]	Référentiel Général de Sécurité version 1. Annexe A8 Politique de Certification Type « Signature » OID : 1.2.250.1.137.2.2.1.2.2.2
[RGS-PC_C]	Référentiel Général de Sécurité version 1. Annexe A6 Politique de Certification Type « confidentialité » OID : 1.2.250.1.137.2.2.1.2.2.3
[RGS-profils]	Référentiel Général de Sécurité version 1.0 Annexe A14 Profils de Certificats / LCR / OCSP et Algorithmes Cryptographiques OID : 1.2.250.1.137.2.2.1.2.1.4
[RGS_A_3]	RGS - Fonction de sécurité « Signature électronique » - Version 2.3
[RGS_A_13]	RGS - Politiques de Certification Types - Variables de Temps - Version 2.3
[RGS_A_14]	RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.3

Renvoi	Document
[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 Generation 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 Creation 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://references.modernisation.gouv.fr/sites/default/files/Exigences_sites_de_perso_V1_0.pdf
[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

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

11.1. 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 L.C.R.), 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,
- ✓ garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

11.2. EXIGENCES SUR LA QUALIFICATION

Le module cryptographique utilisé par l'AC est qualifié au niveau renforcé.

12. ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF CRYPTOGRAPHIQUE DU PORTEUR

12.1. EXIGENCES SUR LES OBJECTIFS DE SECURITE

Le dispositif de protection de clés privées utilisé par le porteur pour stocker et mettre en œuvre ses clés privées d'authentification doit répondre aux exigences de sécurité suivantes :

- ✓ si la bi-clé 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,
- ✓ générer une authentification et une signature qui ne puissent être falsifiées sans la connaissance de la clé privée,
- ✓ assurer pour le porteur légitime uniquement, d'une part, les fonctions de signature et d'authentification et, d'autre part, la fonction de déchiffrement de clés symétriques de session, et protéger la clé privée contre toute utilisation par des tiers,
- ✓ permettre de garantir l'authenticité et l'intégrité de la clé symétrique de session, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données,
- ✓ permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

12.2. EXIGENCES SUR LA QUALIFICATION

Le dispositif cryptographique fourni est qualifié au minimum au niveau standard.