Ministère de l'Intérieur

Date : 01/08/2014

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

POLITIQUE DE CERTIFICATION AC RACINE IGC-MINISTERE INTERIEUR

Titre :

OID : ***1.2.250.1.152.2.1***

Référence : AA100008/PC0014 version 2.0

État : **APPROUVE**

SUIVI DES MODIFICATIONS

Version	*Date*	*Objet de la modification*	*Auteur*	*Statut*
1.0	08/08/2011	• Création	Ministère Intérieur	Approuvé
2.0	01/08/2014	• Renouvellement des ACD	Ministère Intérieur	Approuvé

RÉFÉRENCES DOCUMENTAIRES

Référence	Version et date	Titre
[ORD05-1516]	JO du 9/12/2005	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]	JO du 4/02/2010	Décret no 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
[IGC/A-PC]	Version 2.1 du 18/08/2011	IGC/A – Politique de Certification concernant les Autorités de certification racines gouvernementales OID : 1.2.250.1.223.1.1.2.
[RGS]	Version 1.0 du 6/05/2010	Référentiel Général de Sécurité
[RGS-PC]	Version 2.3 du 11/02/2010	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-profils]	Version 2.3 du 11/02/2010	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

TABLE DES MATIERES

SUIVI DES MODIFICATIONS **2**

RÉFÉRENCES DOCUMENTAIRES **3**

1. INTRODUCTION **8**
1.1. PRÉSENTATION GÉNÉRALE 8
1.1.1. Présentation du projet AC Racine Ministère Intérieur 8
1.1.2. Présentation de la politique de certification AC Racine Ministère Intérieur 8
1.2. IDENTIFICATION DU DOCUMENT 9
1.3. RELATION AVEC LA PC DE L'IGC/A ET LE RGS 9
1.4. DOMAINES D'UTILISATION APPLICABLES 9
1.5. DÉFINITIONS, ABRÉVIATIONS ET SIGLES 9
1.5.1. Définitions 9
1.5.2. Sigles 11
1.6. ORGANISATION HIÉRARCHIQUE DE L'IGC-MI 12
1.7. ENTITÉS INTERVENANT DANS L'IGC-MI 14
1.7.1. Autorité administrative de l'AC Racine 14
1.7.2. Autorité de certification racine 14
1.7.3. Autorité d'enregistrement auprès de l'AC Racine 15
1.7.4. Autorité de certification déléguée 15
1.7.5. Tiers utilisateurs de certificats 16
1.7.6. Composantes internes 16
1.8. GESTION DE LA PC 16
1.8.1. Entité gérant la PC 16
1.8.2. Point de contact 16
1.8.3. Déclaration des pratiques de certification (DPC) 17
1.8.4. Procédure d'approbation de la DPC 17

2. RESPONSABILITÉS CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS PUBLIÉES **18**
2.1. ENTITÉS CHARGÉES DE LA MISE À DISPOSITION DES INFORMATIONS 18
2.2. INFORMATIONS PUBLIÉES 18
2.2.1. Délais de publication et disponibilité de l'information 18
2.2.2. Contrôle d'accès aux informations publiées 19
2.3. FONCTION D'INFORMATION SUR L'ÉTAT DES CERTIFICATS 19
2.3.1. Caractéristiques opérationnelles 19
2.3.2. Délais de publication et disponibilité de l'information 20

3. AC RACINE : EXIGENCES RELATIVES AU CYCLE DE VIE DES CERTIFICATS **21**
3.1. DISPOSITIONS GÉNÉRALES 21
3.1.1. Mode de fonctionnement 21
3.1.2. Garantie de fonctionnement 21
3.2. EXIGENCES RELATIVES AU CYCLE DE VIE DES CERTIFICATS DE L'AC RACINE 21
3.2.1. Nommage 21
3.2.2. Génération d'une biclé et d'un certificat de l'ACR 21
3.2.3. Renouvellement d'une biclé et d'un certificat de l'ACR 22
3.2.4. Révocation d'un certificat de l'ACR 22
3.2.5. Certification croisée 23
3.3. EXIGENCES RELATIVES AU CYCLE DE VIE DES CERTIFICATS D'AC DÉLÉGUÉES 23

3.3.1. Nommage 23
3.3.2. Procédure de demande pour une AC Déléguée 23
3.3.3. Génération d'un certificat pour une AC Déléguée 23
3.3.4. Renouvellement du certificat d'une AC Déléguée 24
3.3.5. Révocation d'un certificat d'une ACD 25
3.3.6. Certification croisée 25

4. MESURES DE SÉCURITÉ NON TECHNIQUES 26
4.1. MESURES DE SÉCURITÉ PHYSIQUE 26
4.1.1. Situation géographique et construction des sites 26
4.1.2. Accès physique 26
4.1.3. Alimentation éléctrique et climatisation 26
4.1.4. Vulnérabilité aux dégâts des eaux 26
4.1.5. Prévention de protection incendie 26
4.1.6. Conservation des supports 26
4.1.7. Mise hors service des supports 27
4.1.8. Sauvegardes hors site 27
4.2. MESURES DE SÉCURITÉ PROCÉDURALES 27
4.2.1. Rôles de confiance relatifs aux cérémonies des clés 27
4.2.2. Rôles de confiance auprès de l'ACR 27
4.2.3. Rôles de confiance mutualisés 27
4.2.4. Nombre de personnes requises par tâches 28
4.2.5. Identification et authentification pour chaque rôle 28
4.2.6. Rôles exigeant une séparation des attributions 29
4.3. MESURES DE SÉCURITÉ VIS-À-VIS DU PERSONNEL 29
4.3.1. Qualifications, compétences et habilitations requises 29
4.3.2. Procédures de vérification des antécédents 29
4.3.3. Formation initiale 29
4.3.4. Formation continue 29
4.3.5. Fréquence et séquence de rotation entre différentes attributions 30
4.3.6. Sanctions en cas d'actions non autorisées 30
4.3.7. Exigences vis-à-vis du personnel des prestataires externes 30
4.3.8. Documentation fournie au personnel 30
4.4. PROCÉDURES DE CONSTITUTION DES DONNÉES D'AUDIT 30
4.4.1. Types d'évènements enregistrés 30
4.4.2. Fréquence de traitement des journaux d'évènements et dossiers d'enregistrement 32
4.4.3. Période de conservation des journaux d'évènements et dossiers d'enregistrement sur site 32
4.4.4. Protection des journaux d'évènements et dossiers d'enregistrement 32
4.4.5. Procédure de sauvegarde des journaux d'évènements 33
4.4.6. Système de collecte des journaux d'évènements 33
4.4.7. Notification de l'enregistement d'un évènement au responsable de l'évènement 33
4.4.8. Évaluation des vulnérabilités 33
4.5. ARCHIVAGE DES DONNÉES 34
4.5.1. Types de données archivées 34
4.5.2. Période de conservation des archives 34
4.5.3. Protection des archives 35
4.5.4. Procédure de sauvegarde des archives 35
4.5.5. Datation des données 35
4.5.6. Système de collecte des archives 36
4.5.7. Procédures de récupération et de vérification des archives 36
4.6. CHANGEMENT DE CLÉ D'ACR 36
4.7. REPRISE SUITE À COMPROMISSION ET SINISTRE 36
4.7.1. Procédures de remontée et de traitement des incidents et des compromissions 36
4.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels ou données) 37

4.7.3. Procédures de reprise en cas de compromission de la clé privée de l'ACR ou de l'une de ses composantes 37
4.7.4. Capacités de continuité d'activité suite à un sinistre 37
4.8. FIN DE VIE DE L'ACR 37

5. MESURES DE SÉCURITÉ TECHNIQUES 38
5.1. GÉNÉRATION DES BICLÉS 38
5.1.1. Génération des biclés des autorités de l'AC Racine 38
5.1.2. Transmission de la clé publique d'une ACD à l'ACR 38
5.1.3. Transmission des clés publiques des ACD et de l'ACR aux utilisateurs de certificat 38
5.1.4. Tailles des clés 38
5.1.5. Vérification de la génération des paramètres des biclés et de leur qualité 38
5.1.6. Objectifs d'usage des clés 38
5.2. MESURES DE SÉCURITÉ POUR LA PROTECTION DES CLÉS PRIVÉES ET POUR LES MODULES CRYPTOGRAPHIQUES 39
5.2.1. Modules cryptographiques de l'ACR 39
5.3. AUTRES ASPECTS DE LA GESTION DES BICLÉS 39
5.3.1. Archivage des clés publiques 39
5.3.2. Durées de vie des biclés et des certificats 39
5.4. DONNÉES D'ACTIVATION DES CLÉS D'AC 39
5.4.1. Génération et installation des données d'activation 39
5.4.2. Protection des données d'activation 39
5.5. MESURES DE SÉCURITÉ DES SYSTÈMES INFORMATIQUES 39
5.6. MESURES DE SÉCURITÉ DES SYSTÈMES DURANT LEUR CYCLE DE VIE 40
5.6.1. Mesures de la sécurité liées au développement des systèmes 40
5.6.2. Mesures liées à la gestion de la sécurité 40
5.7. MESURES DE SÉCURITÉ RÉSEAU 40
5.8. SYSTÈME DE DATATION 40
5.9. EXIGENCES SUR LES ÉCHANGES DE DONNÉES ENTRE COMPOSANTES 40
5.9.1. Protection des données échangées entre composantes 40
5.9.2. Dispositions applicables aux certificats de composantes 41
5.9.3. Protection des données échangées avec la base de données 41
5.9.4. Protection des données échangées entre sites 41

6. PROFILS DES CERTIFICATS ÉMIS PAR L'AC RACINE 42
6.1. AC RACINE 42
6.2. CERTIFICAT AC DÉLÉGUÉE 44
6.3. FORMAT LAR 45

7. AC RACINE : AUDITS INTERNES ET DE CONFORMITÉ 46
7.1. AUDITS INTERNES 46
7.1.1. Fréquence et / ou circonstances des évaluations 46
7.1.2. Identités / qualification des évaluateurs 46
7.1.3. Relations entre évaluateurs et entités évaluées 46
7.1.4. Sujets couverts par les évaluations 46
7.1.5. Actions prises suite aux conclusions des évaluations 46
7.1.6. Communication des résultats 47
7.2. AUDITS DE CONFORMITÉ 47
7.2.1. Fréquence des contrôles de conformité 47
7.2.2. Identification et qualification du contrôleur 47
7.2.3. Sujets couverts par le contrôle de conformité 47
7.2.4. Mesures à prendre en cas de non-conformité 47
7.2.5. Communication des résultats 47

8. AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES 48
8.1. CONFIDENTIALITÉ DES DONNÉES PERSONNELLES 48

8.1.1. Périmètre des informations confidentielles 48
8.1.2. Responsabilités en terme de protection des informations confidentielles 48
8.2. PROTECTION DES DONNÉES PERSONNELLES 48
8.2.1. Politique de protection des données personnelles 48
8.2.2. Informations à caractère personnel 48
8.2.3. Informations à caractère non personnel 48
8.2.4. Responsabilité en terme de protection des données personnelles 48
8.2.5. Notification et consentement d'utilisation des données personnelles....49
8.2.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou adminsitratives 49
8.2.7. Autres circonstances de divulgation d'informations personnelles 49
8.3. DROITS SUR LA PROPRIÉTÉ INTELLECTUELLE ET INDUSTRIELLE 49
8.4. LIMITE DE RESPONSABILITÉ....49
8.5. INDEMNITÉS 49
8.5.1. Durée de validIté et fin de validité de la présente PC 49
8.5.2. Effets de la fin de validité et clauses restant applicables....49
8.6. AMENDEMENTS À LA PC....50
8.6.1. Procédures d'amendements 50
8.6.2. Mécanisme et période d'information sur les amendements 50
8.6.3. Circonstances selon lesquelles l'OID doit être changé....50
8.7. DISPOSITIONS CONCERNANT LA RÉSOLUTION DE CONFLITS 50
8.8. JURIDICTIONS COMPÉTENTES....50
8.9. CONFORMITÉ AUX LÉGISLATIONS ET RÉGLEMENTATIONS....50

9. OBLIGATIONS RESPECTIVES 51
9.1. OBLIGATIONS APPLICABLES À L'AA DE L'AC RACINE....51
9.2. OBLIGATIONS APPLICABLES À L'AC RACINE....51
9.3. OBLIGATIONS DES ADMINISTRATEURS CENTRAUX DE L'AC RACINE 52
9.4. OBLIGATIONS APPLICABLES À L'AC RACINE SUITE AU RATTACHEMENT À L'IGC/A....52
9.5. OBLIGATIONS APPLICABLES AUX AC DÉLÉGUÉES....52
9.6. OBLIGATIONS APPLICABLES AUX DEMANDEURS DE CERTIFICATS D'ACD 53
9.7. OBLIGATIONS APPLICABLES AUX PORTEURS DE CERTIFICATS....53
9.8. OBLIGATIONS APPLICABLES AUX TIERS UTILISATEURS 53

1. INTRODUCTION

1.1. PRÉSENTATION GÉNÉRALE

1.1.1. PRESENTATION DU PROJET AC RACINE MINISTERE INTERIEUR

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 MI a décidé de se doter d'une IGC (Infrastructure de Gestion de Clés).

L'AC RACINE MINISTÈRE INTÉRIEUR est destinée à certifier plusieurs Autorités de Certification (ACD), en particulier les premières ACD rattachées seront :

- ✓ des AC délivrant des certificats d'authentification, de signature et de confidentialité au niveau RGS ** pour des personnes et des services applicatifs,
- ✓ des AC délivrant des certificats d'authentification, de signature et de confidentialité au niveau RGS * pour des personnes et des services applicatifs.

D'autre part, l'AC RACINE MINISTÈRE INTÉRIEUR est rattachée au domaine de confiance interministériel défini par l'IGC/A.

Les certificats émis par l'IGC/A permettent d'identifier officiellement les Autorités de Certification des administrations de l'État français. Ils attestent également de la qualité des pratiques de gestion des clefs publiques mises en œuvre par ces autorités. Ils sont délivrés au terme d'un audit et peuvent être révoqués en cas de défaillance.

Cette démarche de rattachement de l'AC RACINE MINISTÈRE INTÉRIEUR au domaine de confiance de l'IGC/A s'inscrit dans le cadre de l'article 10 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.

1.1.2. PRESENTATION DE LA POLITIQUE DE CERTIFICATION AC RACINE MINISTERE INTERIEUR

Le présent document fait partie d'un ensemble de documents décrivant les politiques de certification définies dans le cadre du projet de l'AC RACINE MINISTÈRE INTÉRIEUR.

Il spécifie les exigences applicables :

- ✓ à l'ACR, pour :

1) la génération et le renouvellement de ses clés,
2) la certification des clés publiques des ACD demandant leur rattachement, et la révocation des certificats des ACD émis par l'ACR,

- ✓ aux ACD, pour :

3) la génération et le renouvellement de leurs clés ainsi que pour la gestion des demandes de certificats auprès de l'Autorité Racine,

- ✓ à l'application IGC, pour :

4) la garantie de l'intégrité des codes mobiles utilisés par l'application IGC.

La politique est définie indépendamment des détails de l'environnement utilisé pour la mise en œuvre de l'IGC.

Ces exigences sont établies de façon à être conformes à celles de l'IGC/A pour la certification de l'AC RACINE MINISTÈRE INTÉRIEUR.

Les détenteurs de rôle de confiance de l'IGC-MI et les tiers utilisateurs des certificats objets de cette politique respectent les obligations spécifiques définies dans cette politique de certification et qui leur sont applicables. La liste de ces rôles est détaillée section 4.2.

1.2. IDENTIFICATION DU DOCUMENT

La présente PC est dénommée « POLITIQUE DE CERTIFICATION AC RACINE MINISTERE INTERIEUR ».

L'OID de la présente PC « POLITIQUE DE CERTIFICATION AC RACINE MINISTERE INTERIEUR » est **1.2.250.1.152.2.1.**

La version 2 de la présente PC modifie la version 1 dans les paragraphes suivants :

- ✓ Paragraphe 1.6 sur l'organisation hiérarchique de l'IGC-MI ;
- ✓ En-tête du paragraphe 6 pour prise en compte de la nouvelle version de l'annexe 1 politique de certification format des certificats ;
- ✓ Paragraphe 6.2 avec l'insertion des OID des nouvelles ACD générées en 2014.

1.3. RELATION AVEC LA PC DE L'IGC/A ET LE RGS

Cette Politique de Certification, qui est celle d'une ACR gouvernementale, se veut cohérente avec les exigences stipulées par [IGC/A-PC], et reste conforme aux documents [RGS-PC] et [RGS-profils] quant aux tailles de clés et algorithmes utilisés.

1.4. DOMAINES D'UTILISATION APPLICABLES

L'ACR et les ACD limitent la délivrance de leurs certificats :

- ✓ à des ACD sous la responsabilité d'une ou plusieurs autorités administratives du MI,
- ✓ à des personnes physiques, en lien ou sous la responsabilité du MI,
- ✓ à des services applicatifs (cachet, authentification de serveur) sous la responsabilité du MI.

Toute délivrance de certificat à une administration autre que celle du MI sera soumise à l'autorisation préalable de l'IGC/A (voir chapitre 3).

1.5. DÉFINITIONS, ABRÉVIATIONS ET SIGLES

1.5.1. DEFINITIONS

Pour les besoins du présent document, les termes et définitions suivants s'appliquent :

Administrateur :

Personne autorisée par l'AC à gérer les droits d'accès logiciels à l'Autorité, avec la granularité suivante : gestion de la liste d'administrateurs, gestion des droits d'accès aux différentes composantes de l'Autorité pour chacun des administrateurs. De ce fait, détenteur lui-même de droits d'accès précis aux différentes composantes de l'autorité, l'administrateur est autorisé à utiliser et configurer les fonctionnalités correspondantes des composantes de l'autorité.

Administrateur central :

Administrateur autorisé par l'AC à avoir accès à toutes les composantes de l'autorité auxquelles un administrateur peut prétendre avoir accès.

Autorité Administrative de l'AC :

Personne responsable de l'AC sur le plan réglementaire et juridique.

Autorité de Certification (AC) :

Dans le cadre du présent document, ce terme désigne, selon les cas :

- ✓ la personne ou l'Autorité chargée de l'application de la présente politique de certification,
- ✓ l'infrastructure technique réalisant les fonctions dévolues à l'AC. À cet effet, elle utilise notamment les clés de signature de l'AC.

Autorité de Certification Déléguée (ACD) :

Autorité de Certification dont la biclé est certifiée par l'ACR.

Autorité de Certification Racine (ACR) :

Autorité de certification point de confiance de l'IGC-MI, et certifiant les ACD.

Autorité d'Enregistrement (AE) :

Autorité désignée par l'autorité administrative qui a pour rôle d'organiser l'enregistrement du porteur et la gestion des clés.

Certificat électronique :

Certificat délivré à une personne physique ou à une composante technique et portant sur une biclé détenue par celle-ci. L'usage de ce certificat est indiqué au sein de celui-ci (authentification client ou serveur, signature, signature de certificat ou de LCR…).

Code d'activation : (ou code PIN)

Code d'activation de la carte d'authentification administrateur, choisi par l'administrateur et permettant l'usage des clés privées associées aux certificats stockés.

Composante de l'AC :

Module applicatif jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'AC.

Déclaration des Pratiques de Certification (DPC) :

Énoncé des pratiques de certification effectivement mises en œuvre par l'AC pour l'émission, la gestion, la révocation, le renouvellement des certificats en conformité avec la PC qu'elle s'est engagée à respecter.

Identifiant d'objet (OID) :

Série d'entiers globalement unique permettant d'identifier un objet.

Infrastructure de Gestion de Clés (IGC) :

Ensemble de composantes, fonctions et procédures dédiées à la génération et à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance.

Infrastructure de Gestion de clés de l'Administration (IGC/A) :

Ensemble de services de certification électronique, participant à la validation par l'État français des certificats électroniques utilisés dans les échanges entre les usagers et les autorités administratives et entre les autorités administratives.

Liste des Certificats Révoqués (LCR) :

Liste signée par l'AC et indiquant un ensemble de certificats qui ne sont plus considérés comme valides par l'AC.

Ministère (MI):

Ministère de l'Intérieur

Politique de Certification (PC) :

Ensemble de règles, comportant un identifiant (OID) et 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.

Porteur :

Autorité identifiée dans le certificat et détentrice de la clé privée correspondant à la clé publique présente dans ce certificat.

Dans le cas où l'Autorité Racine certifie la clé publique de l'Autorité Déléguée, le porteur est une Autorité.

Il fournit la preuve qu'il possède la clé privée de l'ACD via une demande de certification au format PKCS #10.

Rôle de confiance :

Rôle dévolu à un acteur, personne physique nommément identifiée, intervenant dans la mise en œuvre ou l'exploitation de l'AC afin d'assurer, ou maintenir en opération, une ou plusieurs de ses fonctions.

Tiers utilisateur :

Utilisateur ou système faisant confiance à un certificat.

Format X.509 v3 :

Format standard de certificat électronique.

1.5.2. SIGLES

Pour les besoins du présent document, les sigles suivants s'appliquent :

AA	Autorité Administrative
AC	Autorité de Certification
ACD	Autorité de Certification Déléguée
ACR	Autorité de Certification Racine
AE	Autorité d'Enregistrement
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
CSR	Certificate Signing Request (demande de signature de certificat)
DN	Distinguished Name ; nom distinctif
DPC	Déclaration des Pratiques de Certification
FSSI	Fonctionnaire de Sécurité des Systèmes d'Information
HFD	Haut Fonctionnaire de Défense
HFDA	Haut Fonctionnaire de Défense Adjoint
IGC	Infrastructure de Gestion de Clés
IGC/A	Infrastructure de Gestion de Clés de l'Administration
IGC-MI	Infrastructure de Gestion de Clés du MI

ISO	International Organization for Standardization
LAR	Liste des Autorités Révoquées (liste des certificats d'AC révoqués)
LCR	Liste des Certificats Révoqués
MI	Ministère de l'Intérieur
OCSP	Online Certificate Status Protocol
OID	Object Identifier : Identifiant d'Objet
PC	Politique de Certification
PIN	Personal Identification Number ; nombre d'identification personnel
RSA	Rivest Shamir Adelman
SGDSN	Secrétariat Général de la Défense et de la Sécurité Nationale
SHA-1	Secure Hash Algorithm version 1
SHA-2	Secure Hash Algorithm version 2
SHFD	Service du Haut Fonctionnaire de Défense
SP	Service de Publication
UC	Utilisateur de Certificats
URL	Uniform Resource Locator ; localisateur uniforme de ressource
UTC	Universal Time Coordinated ; temps universel coordonné

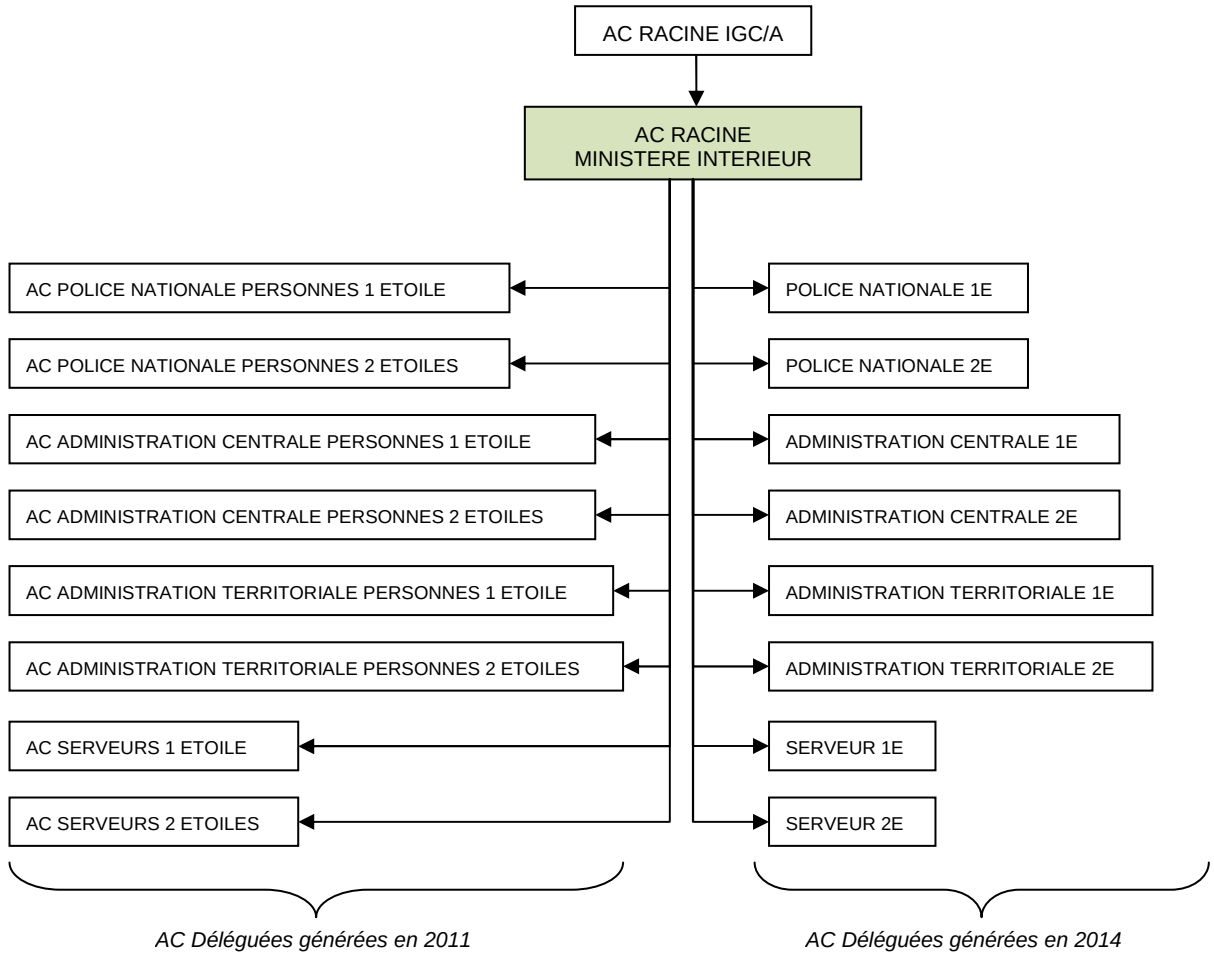
1.6. ORGANISATION HIÉRARCHIQUE DE L'IGC-MI

L'AC RACINE MINISTÈRE INTÉRIEUR assure principalement les fonctions suivantes :

- ✓ la génération de ses clés de signature et la certification de ses certificats,
- ✓ la certification des ACD préalablement autorisées placées sous l'autorité du ministère.

L'AC RACINE MINISTÈRE INTÉRIEUR est rattachée à l'IGC/A.

L'organigramme suivant illustre le schéma de certification :



1.7. ENTITÉS INTERVENANT DANS L'IGC-MI

1.7.1. AUTORITE ADMINISTRATIVE DE L'AC RACINE

L'AA est l'autorité administrative au sens de [ORD05-1516] - c'est-à-dire le représentant légal de l'État responsable de l'IGC 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'Autorité Administrative en tant que responsable de l'ensemble de l'IGC-MI sont les suivantes :

- ✓ rendre accessible l'ensemble des prestations déclarées dans la PC aux demandeurs de certificats, aux Autorités de Certification Déléguées, aux porteurs et aux tiers utilisateurs,
- ✓ s'assurer que les exigences de la PC et les procédures de la DPC sont adéquates et conformes aux normes en vigueur,
- ✓ s'assurer que ces exigences et procédures sont appliquées par chacun des détenteurs de rôles auprès de l'IGC-MI,
- ✓ 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 des certificats, de gestion des révocations et d'information sur l'état des certificats,
- ✓ mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans la présente PC, notamment en termes de fiabilité, de qualité et de sécurité,
- ✓ générer, et renouveler lorsque nécessaire, la biclé de l'ACR et le certificat correspondant (signature de certificats et de LAR), puis diffuser son certificat d'AC aux tiers utilisateurs,
- ✓ autoriser, après avis, l'initialisation de nouvelles ACD.

1.7.2. AUTORITE DE CERTIFICATION RACINE

L'ACR du ministère est représentée par le sous-directeur de la protection du ministère au sein du SHFD.

L'ACR a en charge la fourniture des prestations de gestion des certificats des ACD et de ses administrateurs tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...) et s'appuie pour cela sur une infrastructure gestion de clés technique.

Les prestations de l'ACR sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des biclés et des certificats :

Fonction de génération des certificats :

Cette fonction génère les certificats à partir des informations transmises par l'Autorité d'Enregistrement.

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 certificats, hors informations d'état des certificats.

Fonction de gestion des révocations :

Dans le cadre de cette fonction, l'ACR 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 LAR.

L'ACR assure également les fonctions suivantes :

- ✓ mettre en œuvre les 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,
- ✓ mettre en œuvre les 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.

1.7.3. AUTORITE D'ENREGISTREMENT AUPRES DE L'AC RACINE

L'autorité d'enregistrement (AE) est le chef de la section des réseaux sécurisés du SHFD. Il s'appuie sur plusieurs agents pour l'exécution de ses missions.

Elle recueille les demandes d'initialisation des ACD, recueille les avis de l'ACR de l'IGC/A, du FSSI du ministère, instruit le dossier et propose à l'autorité administrative l'acceptation ou le refus de la demande.

L'AE de l'ACR permet l'enregistrement des ACD et de ses administrateurs centraux, la remise des certificats et la prise en compte des demandes de révocation pour les certificats émis. Pour cela, elle assure les fonctions suivantes :

Fonction d'enregistrement des demandes de certificats :

Cette fonction assure la vérification des informations d'identification des demandeurs d'un certificat, la vérification des données à inclure dans le certificat, la constitution du dossier d'enregistrement correspondant, et la transmission de cette demande de certificat à l'ACR.

Fonction de remise du certificat aux demandeurs :

Cette fonction remet le certificat à son ou à ses demandeurs une fois qu'il a été généré par l'ACR.

Fonction de gestion des révocations :

Dans le cadre de cette fonction, l'AE prend en compte les demandes de révocation pour transmission et traitement par l'ACR.

1.7.4. AUTORITE DE CERTIFICATION DELEGUEE

Chaque ACD procède à la génération de sa biclé et la fait certifier par l'ACR. Elle doit aussi demander la révocation de son certificat en cas de compromission réelle ou suspectée de sa clé privée, de changement de nom de l'AC ou de cessation d'activité.

Les responsabilités incombant à chaque ACD et relatives à la délivrance et à la gestion des certificats qu'elle émet sont décrites dans les politiques de certification de cette AC.

Ce document complète ces politiques en décrivant les fonctions nécessaires à la création, au renouvellement et à la révocation des certificats de chaque ACD.

Les fonctions assurées par les ACD sont :

Fonction de création d'une demande de certificat d'une ACD :

Cette fonction assure la génération initiale d'une biclé et la création d'un fichier de demande de certificat pour une nouvelle Autorité Déléguée au format PKCS #10.

Fonction de demande de renouvellement du certificat d'une ACD :

Cette fonction assure la génération d'une nouvelle biclé et la création d'un fichier de demande de certificat pour une Autorité Déléguée existante au format PKCS #10.

Fonction de demande de révocation du certificat d'une ACD :

Cette fonction assure la demande de révocation d'un certificat d'ACD.

1.7.5. TIERS UTILISATEURS DE CERTIFICATS

Les tiers utilisateurs concernent les utilisateurs des certificats émis selon la présente politique de certification :

- ✓ certificat de l'AC RACINE MINISTÈRE INTÉRIEUR,
- ✓ certificats des ACD émis par l'AC RACINE MINISTÈRE INTÉRIEUR.

Les tiers utilisateurs sont les systèmes et les applications informatiques utilisant des certificats porteurs ou serveurs émis par l'une des ACD rattachées à l'AC RACINE MINISTÈRE INTÉRIEUR, et à ce titre nécessitant les certificats du chemin de certification.

Les utilisateurs internes sont les utilisateurs qui accèdent aux services de l'IGC-MI.

1.7.6. COMPOSANTES INTERNES

L'infrastructure technique de l'IGC-MI est composée de deux plates-formes indépendantes, l'une nominale et l'autre de secours, aux architectures et composantes internes strictement identiques.

L'AC RACINE MINISTÈRE INTÉRIEUR comporte les composantes internes suivantes :

- ✓ des composantes assurant les services d'AE. Elles permettent d'effectuer des demandes de création de certificat, de renouvellement de certificat ou de révocation de certificat,
- ✓ une composante assurant les services de certification et de signature de LAR,
- ✓ une composante de publication des certificats émis,
- ✓ une composante d'administration (gestion des droits auprès des composantes de l'Autorité concernée),
- ✓ une composante permettant l'accès à la journalisation d'événements de l'Autorité concernée,
- ✓ une composante assurant les fonctions de gestion des cartes d'authentification administrateur.

L'ensemble de ces composantes est disponible par service HTTPS et après authentification par certificat émis par l'Autorité à laquelle est liée la composante.

1.8. GESTION DE LA PC

1.8.1. ENTITE GERANT LA PC

L'ACR est responsable de l'établissement de la présente PC, ainsi que de son application, sa diffusion et sa révision.

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

1.8.2. POINT DE CONTACT

Toute demande d'information devra se faire auprès du :

Ministère de l'Intérieur

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

1.8.3. DECLARATION DES PRATIQUES DE CERTIFICATION (DPC)

L'ACR s'engage à rédiger une DPC décrivant les procédures et mesures mises en œuvre pour le respect des dispositions de la présente PC. Ce document n'est pas public.

1.8.4. PROCEDURE D'APPROBATION DE LA DPC

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

2. RESPONSABILITÉS CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS PUBLIÉES

2.1. ENTITÉS CHARGÉES DE LA MISE À DISPOSITION DES INFORMATIONS

Pour la mise à disposition des informations devant être publiées à destination des tiers utilisateurs de certificats, l'ACR met en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats.

2.2. INFORMATIONS PUBLIÉES

L'AC RACINE MINISTÈRE INTÉRIEUR publie les informations suivantes à destination des tiers utilisateurs de certificats :

- ✓ la politique de certification de l'ACR en cours de validité (le présent document),
- ✓ les versions antérieures de la présente PC, tant que des certificats émis selon ces versions sont en cours de validité,
- ✓ les profils des certificats de l'ACR, des ACD, et des LAR émises par l'ACR,
- ✓ les certificats de l'ACR, en cours de validité et les informations permettant aux tiers utilisateurs de certificats de s'assurer de l'origine de ces certificats (empreintes),
- ✓ la LAR en cours de validité, conforme au profil indiqué au chapitre 6 et accessible par le protocole HTTP,
- ✓ l'adresse (URL) permettant d'obtenir des informations concernant l'AC RACINE MINISTÈRE INTÉRIEUR,
- ✓ les certificats de l'ACR émis par l'IGC/A,
- ✓ une copie de LAR publiée sur le site de publication des LAR de l'IGC/A,
- ✓ l'adresse (URL) permettant d'obtenir des informations concernant l'IGC/A, et notamment les certificats auto-signés de l'IGC/A.

2.2.1. DELAIS DE PUBLICATION ET DISPONIBILITE DE L'INFORMATION

Les délais de publication et la disponibilité de l'information dépendent des informations concernées :

Informations liées à l'IGC (nouvelle version de la PC, etc.) :	
Délais de publication :	L'information est publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.
Disponibilité de l'information :	L'infrastructure assurant cette fonction est disponible les jours ouvrés, avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 8 heures (jours ouvrés) et une durée totale maximale d'indisponibilité par mois de 32 heures (jours ouvrés), ceci hors cas de force majeure.
Certificats de l'ACR et des ACD	
Délais de publication :	Ceux-ci sont diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LAR correspondants sous un délai de 24 heures.

Disponibilité de l'information :	L'infrastructure assurant cette fonction a une disponibilité de 24h/24 7j/7, avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2 heures et une durée totale maximale d'indisponibilité par mois de 8 heures, ceci hors cas de force majeure.
Informations d'état des certificats (LAR)	
Délais de publication :	Les exigences portant sur la fonction de publication de ces informations sont définies au chapitre 2.3.
Disponibilité de l'information :	

2.2.2. CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'information publiée est accessible avec accès en lecture seulement sur le site Internet du ministère, aux adresses suivantes :

- ✓ Pour la publication des LAR des AC : http://crl.interieur.gouv.fr
- ✓ Pour les autres informations : http://www.igc.interieur.gouv.fr

L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) est strictement limité aux rôles de confiance de l'IGC-MI adéquats et identifiés, 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 rôles de confiance de l'IGC-MI adéquats et identifiés, au travers d'un contrôle d'accès restreint et contrôlé.

2.3. FONCTION D'INFORMATION SUR L'ÉTAT DES CERTIFICATS

2.3.1. CARACTERISTIQUES OPERATIONNELLES

L'ACR fournit aux tiers utilisateurs de certificats émis par l'AC RACINE MINISTÈRE INTÉRIEUR les informations leur permettant de vérifier et de valider via la consultation libre de la LCR et préalablement à son utilisation, le statut d'un certificat, c'est-à-dire :

- ✓ de vérifier la signature d'un certificat par l'ACR,
- ✓ de vérifier la présence ou non d'un certificat d'un porteur (Service de validation ou Autorité) dans la LAR émise par l'ACR,
- ✓ de vérifier la signature de cette LAR par l'ACR.

L'ACR publie, au point de distribution de la liste de révocation indiqué dans le certificat qui lui a été délivré par l'IGC/A, une copie de la LAR publiée sur le site de publication des LAR de l'IGC/A. L'ACR vérifie, avant publication de cette copie, que celle-ci est intègre, notamment en vérifiant la signature apposée par l'IGC/A.

2.3.2. DELAIS DE PUBLICATION ET DISPONIBILITE DE L'INFORMATION

Les délais de publication et la disponibilité de l'information dépendent des informations concernées :

Information sur l'état des certificats via les LAR	
Délais de publication :	La fréquence de publication des LAR est mensuelle. En cas de décision de révocation (cf. 3.3.5), une nouvelle LAR sera publiée indépendamment de cette périodicité, la publication des LAR dans ce cas est faite dans les 72 h. Les LAR ont une durée maximale de validité de 36 jours. Une LAR urgente est publiée dans un délai maximum de 30 minutes suivant sa génération. L'ACR a un délai maximum de 5 jours pour publier une copie de la LAR signée par l'ACR de l'IGC/A.
Disponibilité de l'information :	La fonction d'information sur l'état des certificats est disponible 7j/7, avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4 heures (jours ouvrés) et une durée totale maximale d'indisponibilité par mois de 16 heures, ceci hors cas de force majeure.

3. AC RACINE : EXIGENCES RELATIVES AU CYCLE DE VIE DES CERTIFICATS

3.1. DISPOSITIONS GÉNÉRALES

3.1.1. MODE DE FONCTIONNEMENT

L'AC RACINE MINISTÈRE INTÉRIEUR n'est pas accessible depuis un environnement considéré comme non sûr ou hors contrôle de l'AC.

3.1.2. GARANTIE DE FONCTIONNEMENT

L'ACR garantit son fonctionnement même en cas de sinistre majeur. Le délai de remise en service de l'ACR en cas de besoin est inférieur à 24 heures.

3.2. EXIGENCES RELATIVES AU CYCLE DE VIE DES CERTIFICATS DE L'AC RACINE

3.2.1. NOMMAGE

Dans chaque certificat X.509v3 d'ACR, les champs émetteur (« *issuer* ») et sujet (« *subject* ») sont identiques et contiennent un nom distinctif (DN : « *Distinguished Name* ») de type X.501.

Le nom distinctif de l'AC RACINE MINISTÈRE INTÉRIEUR est construit à partir des composants suivants :

- ✓ CN=AC RACINE MINISTERE INTERIEUR,
- ✓ OU=0002 110014016,
- ✓ O=MINISTERE INTERIEUR,
- ✓ C=FR.

Remarque :

OU= 0002 110014016 : Code SIREN du MI, précédé des quatre chiffres 0002 séparés par un espace.

3.2.2. GENERATION D'UNE BICLE ET D'UN CERTIFICAT DE L'ACR

La génération de la biclé de l'ACR est réalisée dans le cadre d'une cérémonie des clés.

Le but de cette cérémonie est de générer la clé de signature de l'ACR ainsi qu'un certificat racine auto-signé qui a été soumis pour signature à l'IGC/A. La création du certificat par l'IGC/A, ainsi que sa publication n'entrent pas dans le périmètre de la cérémonie des clés.

La génération de la clé de signature de l'ACR est réalisée au sein d'un module cryptographique, conforme aux exigences du chapitre 6.2.1 du document [IGC/A-PC].

La cérémonie implique la présence d'au moins les personnes tenant les rôles de confiance suivants, outre le maître de cérémonie :

- ✓ témoins de l'Autorité Administrative, garants du déroulement conforme au scénario de la cérémonie établi,

- ✓ opérateurs de l'IGC-MI et des modules cryptographiques, garants du fait que les systèmes (matériels, logiciels et modules cryptographiques) sont correctement configurés et opérationnels conformément au document de cérémonie des clés,
- ✓ responsable sécurité pour la cérémonie, garant du bon déroulement de la cérémonie sur le plan de la sécurité,
- ✓ détenteurs de secret et de supports sensibles.

L'ACR s'engage à établir le scénario complet de la cérémonie. Ce document n'est pas public.

L'ACR s'engage à émettre des procès-verbaux pour chaque étape importante de la cérémonie, marquant notamment la conformité de la cérémonie déroulée, et l'engagement des détenteurs de secret à respecter les règles de conservation des secrets remis. Ces documents ne sont pas publics.

La publication du certificat de l'Autorité Racine par l'AC marque l'acceptation de ce certificat par celle-ci.

3.2.3. RENOUVELLEMENT D'UNE BICLE ET D'UN CERTIFICAT DE L'ACR

Les exigences concernant cette cérémonie sont similaires à la cérémonie décrite ci-dessus.

3.2.4. REVOCATION D'UN CERTIFICAT DE L'ACR

Différentes circonstances peuvent être à l'origine de la révocation des certificats de l'ACR:

- ✓ l'ACR cesse son activité,
- ✓ un module cryptographique de l'ACR a été utilisé frauduleusement,
- ✓ décision suite à une non-conformité révélée lors d'un contrôle de conformité,
- ✓ le certificat n'est plus utilisé par l'ACR,
- ✓ fin anticipée de l'usage de la biclé,
- ✓ non-respect de la PC de l'IGC/A par l'ACR (cette cause n'entraîne pas obligatoirement la révocation du certificat),
- ✓ obsolescence d'informations d'identification contenues dans le certificat de l'ACR, dès lors que ces informations, si elles ne sont pas modifiées, empêchent l'identification de l'ACR.

Lorsqu'une des circonstances ci-dessus se réalise et qu'un détenteur de rôle de confiance auprès de l'ACR en a connaissance, l'évènement est déclaré auprès d'un administrateur de l'ACR sous 24 heures. Dans ces conditions, l'ACR :

- ✓ informe de l'événement, dans les plus brefs délais, l'AC de l'IGC/A,
- ✓ demande la révocation de son certificat auprès de l'IGC/A,
- ✓ révoque tous les certificats qu'elle a signés avec cette clé privée et qui seraient encore en cours de validité,
- ✓ prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante,
- ✓ publie largement cette information (en ayant pour cible les Autorités Déléguées rattachées, les porteurs et tiers utilisateurs des certificats émis en utilisant la clé compromise), dans un délai de trois jours. En particulier, l'information est publiée sur les sites web http://crl.interieur.gouv.fr (pour les CRL des AC) et http://www.igc.interieur.gouv.fr (pour les autres informations).

Dans le cas d'une fin d'activité de l'ACR, la fin de vie effective de l'ACR prend effet 3 mois minimum après l'annonce de la fin de vie de l'activité.

Les procédures exactes seront déterminées lorsque les circonstances ci-dessus se réalisent.

3.2.5. CERTIFICATION CROISEE

L'ACR de l'IGC/A est informée des accords de reconnaissance avec d'autres AC que l'ACR souhaite passer.

3.3. EXIGENCES RELATIVES AU CYCLE DE VIE DES CERTIFICATS D'AC DÉLÉGUÉES

3.3.1. NOMMAGE

Afin d'assurer une continuité d'une identification unique du porteur au sein du domaine de l'ACR dans ses certificats successifs (renouvellement) et pour éviter toute ambiguïté, le DN du champ « *subject* » de chaque certificat de porteur permet d'identifier de façon unique le porteur (ou de l'entité responsable) correspondant au sein du domaine de l'ACR.

Ce DN respecte par conséquent les exigences suivantes :

- ✓ CN =« Nom de l'autorité de certification déléguée »,
- ✓ OU=0002 Numéro de SIRET/SIREN,
- ✓ O=MINISTERE INTERIEUR,
- ✓ C=FR.

Durant toute la durée de vie de l'AC RACINE MINISTÈRE INTÉRIEUR, un DN attribué à une ACD ne peut être attribué à une autre ACD. L'ACR vérifie l'unicité du DN demandé avant de valider la demande de certificat de l'ACD.

3.3.2. PROCEDURE DE DEMANDE POUR UNE AC DELEGUEE

Les demandes de création d'ACD sont adressées à l'AE de l'ACR. Le responsable de l'ACD doit :

- ✓ remplir le formulaire de demande disponible auprès du SHFD,
- ✓ s'engager sur la conformité de son AC à la présente PC,
- ✓ s'engager sur la conformité aux règles fixées par l'annexe A du [RGS],
- ✓ s'engager à être qualifiée selon la procédure décrite dans le décret [DEC2010-112],
- ✓ Fournir une requête de signature de certificat (CSR) pour son ACD (PKCS#10).

L'AE étudie la recevabilité du dossier et, s'il est complet, instruit la demande et consulte notamment l'IGC/A et le FSSI du ministère. L'autorité administrative décide de l'acceptation ou du refus de la demande. Dans tous les cas, le demandeur est tenu informé de la décision.

3.3.2.1. DELAI DE TRAITEMENT DES DEMANDES DE CERTIFICAT

L'AE traite les demandes recevables dans un délai maximum de six mois.

3.3.2.2. DELAI D'ETABLISSEMENT DES CERTIFICATS

Une fois la demande acceptée, l'ACR émet le certificat d'ACD dans un délai maximum de trois mois.

3.3.3. GENERATION D'UN CERTIFICAT POUR UNE AC DELEGUEE

L'ACD doit s'assurer auprès de l'AA de l'ACR que le nom qu'elle propose d'utiliser pour s'identifier n'est pas déjà réservé pour une autre ACD : l'ACD propose donc ce nom puis l'AA, grâce aux informations

dont elle dispose, signale à l'ACD que ce nom est déjà utilisé si c'est le cas. Dans ce cas, la demande de certification n'est pas transmise à l'Autorité de Certification.

La demande de certification de la clé publique d'une ACD doit se faire lors d'un face-à-face, en la présence du responsable sécurité de l'ACD et d'au moins un témoin de l'Autorité Administrative de l'ACD et signataire du procès verbal de la cérémonie de génération de la clé de l'ACD et qui atteste par sa présence l'accord de l'AA de l'ACD.

Les opérations suivantes s'inscrivent dans le cadre d'une cérémonie des clés d'ACD :

- ✓ génération des biclés d'une ACD et émission de la demande de certificat correspondante,
- ✓ installation du certificat suite à sa génération par l'AC RACINE MINISTÈRE INTÉRIEUR.

Le but de cette cérémonie est de générer une biclé ainsi qu'un fichier de demande de certificat, et de créer un procès-verbal de demande de certificat.

Le résultat de la première opération sert à constituer le dossier d'enregistrement présenté à l'administrateur central de l'ACR. Il est constitué :

- ✓ d'un procès verbal signé de la cérémonie de génération de la clé de l'ACD et incluant l'empreinte de la CSR dont la certification est demandée à l'AC RACINE MINISTÈRE INTÉRIEUR,
- ✓ d'un fichier PKCS #10 signé, afin de prouver la possession de la clé privée.

Le résultat de la seconde opération donne lieu à l'établissement d'un procès-verbal signé.

La cérémonie implique la présence d'au moins les personnes tenant les rôles suivants :

- ✓ témoins de l'Autorité Administrative, garants du déroulement conforme de la cérémonie,
- ✓ opérateurs de l'IGC-MI et des modules cryptographiques, garants du fait que les systèmes (matériels, logiciels et modules cryptographiques) sont correctement configurés et opérationnels,
- ✓ responsable sécurité pour la cérémonie, garant du bon déroulement de la cérémonie sur le plan de la sécurité,
- ✓ détenteurs de secret et de supports sensibles.

L'ACD s'engage à établir un descriptif complet de chaque cérémonie. Ce document n'est pas public.

L'ACD s'engage à émettre des procès-verbaux pour chaque étape importante du processus. Ces documents ne sont pas publics.

L'opérateur de l'ACR remet au responsable sécurité de la cérémonie de l'ACD le certificat une fois qu'il a été généré.

L'utilisation du certificat généré pour l'ACD par le responsable sécurité de l'ACD marque l'acceptation de celui-ci.

L'AE conserve les dossiers d'enregistrement papier.

3.3.4. RENOUVELLEMENT DU CERTIFICAT D'UNE AC DELEGUEE

La demande de renouvellement du certificat de la clé publique d'une ACD est soumise aux mêmes exigences que la demande de certification initiale d'une ACD.

À cette occasion, la biclé de l'ACD est renouvelée. L'ACD s'engage à procéder à la destruction de la biclé précédente.

La valeur du champ qui identifie l'ACD, le champ DN, au sein du certificat issu du renouvellement est identique à la valeur du champ DN utilisée dans le certificat précédent.

Le numéro de série du certificat issu du renouvellement est incrémenté, comparativement au numéro de série du certificat précédent.

3.3.5. REVOCATION D'UN CERTIFICAT D'UNE ACD

En cas de compromission réelle ou suspectée d'une clé d'ACD ou tout autre évènement motivant la révocation d'un certificat d'ACD, l'événement est déclaré par l'ACD auprès de l'AA sous 24 heures, laquelle décide ou non, sur la base d'un rapport écrit, de procéder à la révocation de l'ACD. Alors, dans un délai de 3 jours ouvrés, un administrateur de l'ACR procède à la révocation du certificat de l'ACD (et l'information est publiée).

Suite à la révocation du certificat d'une ACD, l'ACR en informe aussi l'entité responsable de l'ACD.

La révocation d'un certificat d'ACD peut également être demandée par l'AA de l'ACR, dans le cas où cette ACD ne respecte pas les exigences prévues par la présente PC.

3.3.6. CERTIFICATION CROISEE

L'ACR de l'IGC-MI et l'ACR de l'IGC/A sont informées des accords de reconnaissance avec d'autres AC que l'ACD souhaite passer.

4. MESURES DE SÉCURITÉ NON TECHNIQUES

4.1. MESURES DE SÉCURITÉ PHYSIQUE

4.1.1. SITUATION GEOGRAPHIQUE ET CONSTRUCTION DES SITES

L'infrastructure de l'IGC-MI est hébergée sur le site nominal dans un local sécurisé vis-à-vis des risques naturels.

Les sites d'hébergement des composantes de l'ACR se trouvent sur le territoire national.

4.1.2. ACCES PHYSIQUE

Les zones hébergeant les systèmes informatiques de l'ACR sont physiquement protégées. 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, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant un tel accès.

4.1.3. ALIMENTATION ELECTRIQUE ET CLIMATISATION

Les locaux hébergeant l'ACR sont climatisés.

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

4.1.4. VULNERABILITE AUX DEGATS DES EAUX

La plate-forme hébergeant l'ACR de l'IGC-MI est stockée dans un local qui n'est pas sujet aux inondations. Le risque dégât des eaux ne pouvant être écarté, le site de secours et le plan de reprise d'activité couvrent cette éventualité.

4.1.5. PREVENTION DE PROTECTION INCENDIE

Les locaux hébergeant l'ACR bénéficient des moyens de prévention et de lutte contre les incendies par des dispositifs de détection d'incendie et d'extinction.

4.1.6. CONSERVATION DES SUPPORTS

Les sauvegardes des données et de l'application opérant l'ACR sont conservées dans une enceinte sécurisée, accessible aux seules personnes habilitées, autorisées et désignées à ces fins.

Les supports papier de l'ACR sont également conservés par le SHFD avec des mesures de sécurité compatibles avec leur niveau de sensibilité.

La DPC identifie les différentes informations et données intervenant dans les activités de l'ACR, ainsi que les mesures de sécurité qui leur sont appliquées, afin d'en garantir la confidentialité, l'intégrité et la disponibilité.

4.1.7. MISE HORS SERVICE DES SUPPORTS

Les supports papier et électroniques de l'ACR en fin de vie sont systématiquement détruits par des moyens appropriés, permettant d'éviter toute perte de confidentialité.

Les matériels et supports informatiques de l'ACR ne sont pas utilisés à d'autres fins avant destruction complète des informations liées à l'ACR qu'ils sont susceptibles de contenir.

4.1.8. SAUVEGARDES HORS SITE

La procédure de sauvegarde des données et logiciels appliquée permet de garantir la continuité d'activité de l'ACR, y compris en cas de destruction des sauvegardes situées sur le site nominal, dans un délai inférieur à 3 jours ouvrés.

4.2. MESURES DE SÉCURITÉ PROCÉDURALES

4.2.1. ROLES DE CONFIANCE RELATIFS AUX CEREMONIES DES CLES

Les rôles de confiance spécifiques aux cérémonies des clés sont décrits dans le document de cérémonie des clés. Ce document n'est pas public.

4.2.2. ROLES DE CONFIANCE AUPRES DE L'ACR

Les rôles de confiance définis au niveau de l'ACR sont :

Responsable d'application :

Personne chargée de la configuration applicative et du maintien en conditions opérationnelles de l'application IGC-MI, de l'habilitation des administrateurs centraux, ainsi que de l'analyse régulière des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission.

Auditeur :

Personne désignée par l'Autorité Administrative dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par l'AC RACINE MINISTÈRE INTÉRIEUR par rapport à la PC et à la DPC de l'AC RACINE MINISTÈRE INTÉRIEUR.

Responsable fonctionnel :

Personne ayant reçu délégation par l'ACR de la mise en œuvre de la PC et de la DPC de l'ACR, au niveau de l'application IGC-MI. Sa responsabilité couvre l'ensemble des fonctions rendues par l'application IGC-MI et des performances correspondantes.

Responsable du référentiel documentaire :

Personne chargée du maintien ou du suivi des documents de gestion de l'ACR. Ceux-ci comportent notamment la PC et la DPC de l'ACR, mais aussi les documents référencés par la DPC.

4.2.3. ROLES DE CONFIANCE MUTUALISES

Ci-dessous sont décrites les fonctions assurées par ces rôles dans le cadre de l'IGC-MI ou ayant une incidence sur les processus de l'IGC-MI :

Administrateur sécurité :

Personne chargée d'assurer la gestion de la sécurité au niveau des systèmes.

Exploitant :

Personne chargée d'assurer l'exploitation, la surveillance et la maintenance des systèmes et des réseaux. Cette personne est également chargée d'assurer l'administration des systèmes, la mise en route et la configuration des équipements composant l'infrastructure. Elle réalise notamment le contrôle des fichiers d'audit du système, ainsi que de l'analyse courante des journaux d'évènements système afin de détecter tout incident, anomalie, tentative de compromission, etc.

Fonctionnaire de Sécurité des Systèmes d'Informations (FSSI) :

Personne chargée de la Politique de Sécurité du SI du Ministère.

Responsable de salle :

Personne chargée de la gestion des accès physiques aux salles informatiques hébergeant l'infrastructure et aux équipements.

4.2.4. NOMBRE DE PERSONNES REQUISES PAR TACHES

Les rôles liés à la gestion des systèmes sont distincts des rôles de gestion de l'application IGC-MI, ainsi que des rôles intervenants sur les données enregistrées au niveau de l'application.

Ces différents rôles sont assurés par des personnes distinctes.

Par ailleurs, toute opération relative au cycle de vie d'un certificat autorité nécessite l'intervention d'au moins deux personnes.

La DPC précise les opérations nécessitant l'intervention de plusieurs personnes ainsi que les contraintes que ces personnes doivent respecter.

4.2.5. IDENTIFICATION ET AUTHENTIFICATION POUR CHAQUE ROLE

Tout accès à l'application IGC-MI est soumis à authentification forte, les droits d'accès étant définis en fonction des rôles. Notamment, toute personne susceptible d'intervenir auprès de l'application IGC-MI, et ainsi de modifier des données ou des informations de configuration, est préalablement enregistrée dans l'application IGC-MI et dispose d'un certificat d'authentification[1].

Pour les autres rôles en relation avec l'IGC-MI, l'AA fait vérifier l'identité et les autorisations du personnel concerné avant :

- ✓ que son nom soit ajouté aux listes de contrôle d'accès aux locaux hébergeant la plate-forme de l'IGC-MI,
- ✓ 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 ces systèmes.

Ces contrôles sont décrits dans la DPC associée à cette PC, et chaque attribution de rôle dans l'IGC-MI est portée à la connaissance de la personne désignée.

[1] Ces certificats d'authentification sont délivrés par une IGC technique.

4.2.6. ROLES EXIGEANT UNE SEPARATION DES ATTRIBUTIONS

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Les attributions associées à chaque rôle sont décrites dans la DPC de l'ACR.

Les règles de non-cumul des rôles de confiance sont décrites au sein de la DPC.

4.3. MESURES DE SÉCURITÉ VIS-À-VIS DU PERSONNEL

Au sein de la présente section, le terme « personnel » désigne les détenteurs de rôles de confiance.

4.3.1. QUALIFICATIONS, COMPETENCES ET HABILITATIONS REQUISES

Tous les personnels intervenant sur l'IGC-MI sont soumis à un devoir de réserve.

Le responsable de l'application IGC-MI s'assure que les attributions des personnels détenteurs de rôle de confiance correspondent à leurs compétences professionnelles et tient à jour la liste des personnels intervenants sur l'IGC-MI.

Le personnel d'encadrement possède l'expertise appropriée à son rôle et est familier des procédures de sécurité en vigueur au sein de l'AC RACINE MINISTÈRE INTÉRIEUR.

L'AA de l'AC RACINE MINISTÈRE INTÉRIEUR informe toute personne intervenant dans des rôles de confiance de l'AC :

- ✓ de ses responsabilités relatives aux services de l'AC RACINE MINISTÈRE INTÉRIEUR,
- ✓ des procédures liées à la sécurité du système et au contrôle du personnel.

4.3.2. PROCEDURES DE VERIFICATION DES ANTECEDENTS

Le personnel amené à assurer un rôle de confiance vis-à-vis de l'AC RACINE MINISTÈRE INTÉRIEUR ne doit pas avoir de condamnation incompatible avec ses attributions.

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

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

4.3.3. FORMATION INITIALE

En préalable à leur entrée en fonction, les administrateurs centraux sont formés aux concepts et objectifs de l'AC RACINE MINISTÈRE INTÉRIEUR, ainsi qu'aux procédures à mettre en œuvre.

Les exploitants et administrateurs système sont formés aux concepts et objectifs de l'AC RACINE MINISTÈRE INTÉRIEUR, ainsi qu'aux logiciels, matériels et procédures d'exploitation applicables.

Les administrateurs centraux sont formés aux concepts et objectifs de l'AC RACINE MINISTÈRE INTÉRIEUR, aux diverses procédures à mettre en œuvre au niveau de l'application IGC-MI.

4.3.4. FORMATION CONTINUE

Avant toute évolution majeure de l'infrastructure de l'AC RACINE MINISTÈRE INTÉRIEUR ou des procédures, une étude d'impact est réalisée par l'AC, avec élaboration d'un plan de formation le cas échéant.

4.3.5. FREQUENCE ET SEQUENCE DE ROTATION ENTRE DIFFERENTES ATTRIBUTIONS

Aucune rotation programmée des attributions n'est prévue.

4.3.6. SANCTIONS EN CAS D'ACTIONS NON AUTORISEES

En cas d'actions non autorisées par le personnel, sont applicables les actions disciplinaires s'il y a lieu.

4.3.7. EXIGENCES VIS-A-VIS DU PERSONNEL DES PRESTATAIRES EXTERNES

Le personnel des prestataires externes intervenant dans les locaux et/ou sur la plate-forme hébergeant l'AC RACINE MINISTÈRE INTÉRIEUR respecte également les exigences du chapitre 4.3. Ceci est traduit en clauses adéquates dans les contrats avec ces prestataires.

4.3.8. DOCUMENTATION FOURNIE AU PERSONNEL

Le personnel dispose de la documentation relative aux procédures opérationnelles ou organisationnelles et aux outils spécifiques qu'il met en œuvre.

4.4. PROCÉDURES DE CONSTITUTION DES DONNÉES D'AUDIT

Cette section s'applique exclusivement aux événements liés aux certificats objets de la présente PC.

4.4.1. TYPES D'EVENEMENTS ENREGISTRES

4.4.1.1. ENREGISTREMENTS SUR PAPIER OU BUREAUTIQUE

Sont enregistrés sur papier :

- ✓ les opérations et événements survenant à l'occasion des cérémonies des clés. Ces enregistrements sont décrits dans le document de cérémonie des clés. Ce document n'est pas public.

Sont enregistrés sur outil bureautique :

- ✓ les actions de maintenance et de changements de configuration des systèmes de l'infrastructure ; suivant les procédures d'exploitation,
- ✓ les changements apportés au personnel détenteur de rôle de confiance,
- ✓ les mises à jour de la présente PC, au sein du présent document.

4.4.1.2. ENREGISTREMENTS ÉLECTRONIQUES PAR L'APPLICATION IGC-MI

Toute action sur un dossier lié à un certificat émis par l'AC RACINE MINISTÈRE INTÉRIEUR est enregistrée, et un historique complet du dossier est conservé dans la base de données de l'AC RACINE MINISTÈRE INTÉRIEUR.

De plus, les événements suivants font l'objet d'un enregistrement électronique de type *log* par l'application IGC-MI :

- ✓ acceptation ou refus de connexion à l'application IGC-MI,
- ✓ demande de certificat,
- ✓ demande de renouvellement de certificat,

- ✓ génération des certificats,
- ✓ demande de révocation,
- ✓ révocation de certificat,
- ✓ génération des LAR,
- ✓ modification des droits des personnels autorisés à intervenir auprès de l'application IGC-MI,
- ✓ modification des paramètres de configuration de l'application IGC-MI.

4.4.1.3. AUTRES ENREGISTREMENTS ÉLECTRONIQUES

Les accès physiques aux locaux hébergeant l'infrastructure matérielle font l'objet d'un enregistrement électronique automatique.

Les événements suivants font l'objet d'un enregistrement électronique au niveau des systèmes d'exploitation de la plate-forme hébergeant l'AC RACINE MINISTÈRE INTÉRIEUR, dès le démarrage de ceux-ci :

- ✓ 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 détenteurs des rôles de confiance, et les tentatives non réussies correspondantes.

Les évènements suivants font également l'objet d'un enregistrement électronique :

- ✓ publication des LAR.

4.4.1.4. CARACTÉRISTIQUES COMMUNES

Pour tous les types d'enregistrements présentés ci-dessus : chaque enregistrement d'événement contient au minimum les informations suivantes :

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

La personne, le service ou le système ayant exécuté l'événement est responsable de sa journalisation.

Les opérations de journalisation électronique sont effectuées au cours du processus ou à la fin de celui-ci.

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

4.4.2. FREQUENCE DE TRAITEMENT DES JOURNAUX D'EVENEMENTS ET DOSSIERS D'ENREGISTREMENT

4.4.2.1. ENREGISTREMENTS SUR PAPIER OU BUREAUTIQUE

Les enregistrements sous forme papier ou bureautique peuvent éventuellement être revus lors des différents audits.

4.4.2.2. ENREGISTREMENTS ÉLECTRONIQUES PAR L'APPLICATION IGC-MI

Les journaux d'événement sont extraits et revus tous les mois.

Le contenu du journal électronique d'événements applicatifs de l'application IGC-MI peut être éventuellement contrôlé avant toute utilisation de la plate-forme afin de vérifier l'absence d'utilisation non autorisée de l'AC RACINE MINISTÈRE INTÉRIEUR.

4.4.2.3. AUTRES ENREGISTREMENTS ÉLECTRONIQUES

Les autres journaux d'enregistrement sous forme électronique peuvent éventuellement être revus lors des opérations de corrélation avec les journaux de l'application IGC-MI.

4.4.3. PERIODE DE CONSERVATION DES JOURNAUX D'EVENEMENTS ET DOSSIERS D'ENREGISTREMENT SUR SITE

4.4.3.1. ENREGISTREMENTS SUR PAPIER OU BUREAUTIQUE

Les enregistrements papier sont conservés sur site et par leur dépositaire comme suit :

- ✓ compte-rendu de cérémonie de clés : à conserver durant 5 ans après la fin de vie des biclés ou des certificats concernés par cette cérémonie.

4.4.3.2. ENREGISTREMENTS ÉLECTRONIQUES PAR L'APPLICATION IGC-MI

Les enregistrements des journaux sont conservés au sein de l'application IGC-MI sans limitation de durée.

4.4.3.3. AUTRES ENREGISTREMENTS ÉLECTRONIQUES

Les autres journaux d'enregistrement sous forme électronique sont sauvegardés puis purgés suivant une fréquence prévue par les procédures internes du MI, hormis ceux situés sur la plate-forme de l'ACR, non purgés.

4.4.4. PROTECTION DES JOURNAUX D'EVENEMENTS ET DOSSIERS D'ENREGISTREMENT

4.4.4.1. ENREGISTREMENTS SUR PAPIER OU BUREAUTIQUE

Les journaux sous forme papier sont conservés en lieu sûr par leur dépositaire.

Les journaux sous forme de document bureautique sont soumis à contrôle d'accès en écriture. Ces contrôles d'accès sont gérés par le rédacteur du document.

4.4.4.2. ENREGISTREMENTS ÉLECTRONIQUES PAR L'APPLICATION IGC-MI

Les journaux d'événements conservés par l'application IGC-MI sont protégés en intégrité.

Ils ne sont accessibles qu'en lecture et exclusivement pour les administrateurs centraux.

4.4.4.3. AUTRES ENREGISTREMENTS ÉLECTRONIQUES

Les droits en modification/suppression/écriture des journaux d'événements des systèmes d'exploitation sont réservés aux utilisateurs avec droits avancés (« compte administrateur » du système d'exploitation).

4.4.5. PROCEDURE DE SAUVEGARDE DES JOURNAUX D'EVENEMENTS

4.4.5.1. ENREGISTREMENTS SUR PAPIER OU BUREAUTIQUE

Les enregistrements papier font l'objet d'une archive, ce qui est précisé au chapitre 4.5.

Les enregistrements sous forme de documents bureautiques sont sauvegardés selon les procédures applicables à ce type de documents.

4.4.5.2. ENREGISTREMENTS ÉLECTRONIQUES PAR L'APPLICATION IGC-MI

Les journaux d'événements de l'application IGC-MI sont sauvegardés selon la procédure de sauvegarde des données de l'application IGC-MI. Les journaux sauvegardés sont protégés en intégrité par le même mécanisme qu'au sein de l'application IGC-MI.

4.4.5.3. AUTRES ENREGISTREMENTS ÉLECTRONIQUES

Les autres journaux sous forme électroniques sont sauvegardés par un système centralisé de sauvegardes, hormis ceux hébergés sur la plate-forme de l'ACR, non sauvegardés.

4.4.6. SYSTEME DE COLLECTE DES JOURNAUX D'EVENEMENTS

Dans tous les cas, il n'est pas prévu de système de collecte des journaux d'événements.

4.4.7. NOTIFICATION DE L'ENREGISTEMENT D'UN EVENEMENT AU RESPONSABLE DE L'EVENEMENT

Dans tous les cas, il n'est pas prévu de notifier l'enregistrement d'un événement à son responsable.

4.4.8. ÉVALUATION DES VULNERABILITES

L'ACR est une AC hors-ligne, hébergée sur un site sécurisé du MI.

4.5. ARCHIVAGE DES DONNÉES

4.5.1. TYPES DE DONNEES ARCHIVEES

4.5.1.1. DONNÉES SOUS FORME PAPIER OU BUREAUTIQUE :

Les données conservées sous forme papier et archivées par leur dépositaire sont :

- ✓ les journaux d'événements tels qu'identifiés au chapitre 4.4.1.1.

Les données conservées sous forme de document bureautique et archivées sont :

- ✓ les journaux d'événements tels qu'identifiés dans la section ci-dessus, archivés selon la procédure d'archivage applicable à ce type de document. L'archivage est sous la responsabilité de leurs rédacteurs,
- ✓ l'ensemble des documents référencés applicables à l'AC RACINE MINISTÈRE INTÉRIEUR : L'archivage est sous la responsabilité du responsable de l'application IGC-MI.

4.5.1.2. DONNÉES DE L'APPLICATION IGC-MI (SOUS FORME ÉLECTRONIQUE)

L'ensemble des données créées ou utilisées par l'application IGC-MI est archivé, y compris les LAR.

4.5.1.3. AUTRES DONNÉES SOUS FORME ÉLECTRONIQUE :

Les logiciels et fichiers de configuration sont sauvegardés périodiquement mais non archivés.

Les journaux d'événements autres que ceux de l'application IGC-MI et tels que définis au chapitre 4.4.1.3 ne sont pas archivés.

4.5.2. PERIODE DE CONSERVATION DES ARCHIVES

4.5.2.1. DOSSIERS D'ENREGISTREMENT, CERTIFICATS ET CLÉS PRIVÉES

Certificats d'Autorités Déléguées de l'ACR émis par l'ACR :

Les certificats d'ACD de l'ACR du ministère émis par l'ACR sont archivés pendant au moins 5 années après leur expiration.

Les dossiers électroniques, les dossiers papier d'enregistrement et les certificats attachés sont conservés par l'application IGC-MI pendant toute la vie de l'AC RACINE MINISTÈRE INTÉRIEUR sans être purgés.

Les dossiers d'enregistrement et les certificats attachés peuvent être présentés par l'ACR lors de toute sollicitation par les autorités habilitées.

Ces dossiers permettent de retrouver :

- ✓ l'identité des personnes physiques désignées dans le certificat émis, dans le cas de certificat de personne,
- ✓ la dénomination de l'ACD pour laquelle le certificat a été émis, dans le cas de certificat d'ACD.

Certificat auto-signé de l'ACR :

Le certificat auto-signé de l'ACR est émis sitôt la génération de la clé de l'Autorité Racine. Il n'est donc pas constitué de dossier d'enregistrement relatif à ce certificat (hormis le P.-V. de cérémonie de clés).

Les certificats de l'ACR sont archivés par le SHFD pendant au moins 5 années après leur expiration.

Certificats de l'ACR signés par l'IGC/A :

Ces certificats sont archivés pendant au moins 5 années après leur expiration par le SHFD.

4.5.2.2. LAR ÉMISES PAR L'AC

Les LAR successives produites sont archivées pour une durée d'au minimum 5 ans après leur expiration par l'application IGC-MI.

4.5.2.3. JOURNAUX D'ÉVÉNEMENTS

Les journaux d'événements de l'application IGC-MI sont conservés par celle-ci sans limitation de durée. Leur intégrité est garantie par les mécanismes mis en œuvre lors de leur constitution.

4.5.2.4. DONNÉES SOUS FORME PAPIER ET BUREAUTIQUE

Les données sont archivées durant au moins 5 ans après leur expiration, hormis l'ensemble des documents référencés applicables à l'ACR, qui sont archivés sans limitation de durée.

4.5.3. PROTECTION DES ARCHIVES

Pendant tout le temps de leur conservation, les archives :

- ✓ sont protégées en intégrité selon les mécanismes mis en œuvre lors de la constitution des données qu'elles contiennent,
- ✓ sont accessibles uniquement aux personnes autorisées,
- ✓ peuvent être relues et exploitées.

Les moyens mis en œuvre pour archiver les pièces en toute sécurité sont indiqués dans la DPC.

4.5.4. PROCEDURE DE SAUVEGARDE DES ARCHIVES

4.5.4.1. DONNÉES SOUS FORME PAPIER OU BUREAUTIQUE

Les archives des données sous forme papier ou bureautique ne sont pas sauvegardées.

4.5.4.2. DONNÉES DE L'APPLICATION IGC-MI (SOUS FORME ÉLECTRONIQUE)

Les données de l'application IGC-MI sont archivées par l'application IGC-MI elle-même et font donc l'objet de sauvegardes régulières selon les modalités définies au chapitre 4.4.5.

4.5.5. DATATION DES DONNEES

4.5.5.1. DONNÉES SOUS FORME PAPIER OU BUREAUTIQUE

La datation des données enregistrées est réalisée à partir d'une source de temps d'utilisation courante supposée correcte avec une précision inférieure à 30 minutes.

4.5.5.2. DONNÉES DE L'APPLICATION IGC-MI (SOUS FORME ÉLECTRONIQUE)

La datation des données est réalisée selon les modalités définies au chapitre 5.8.

4.5.6. SYSTEME DE COLLECTE DES ARCHIVES

4.5.6.1. DONNÉES SOUS FORME PAPIER OU BUREAUTIQUE

Les archives des données sous forme papier ou bureautique ne sont pas collectées mais conservées par leur rédacteur ou dépositaire.

4.5.6.2. DONNÉES DE L'APPLICATION IGC-MI (SOUS FORME ÉLECTRONIQUE)

Les données électroniques sont collectées et conservées en ligne dans la base de données de l'ACR.

4.5.7. PROCEDURES DE RECUPERATION ET DE VERIFICATION DES ARCHIVES

4.5.7.1. DONNÉES SOUS FORME PAPIER OU BUREAUTIQUE

Les archives sous format papier et bureautique peuvent être récupérées dans un délai inférieur à deux jours ouvrés.

4.5.7.2. DONNÉES DE L'APPLICATION IGC-MI (SOUS FORME ÉLECTRONIQUE)

Les archives électroniques sont disponibles en ligne via l'application IGC-MI pour les personnes autorisées à y accéder.

4.6. CHANGEMENT DE CLÉ D'ACR

Le renouvellement du certificat d'ACR et de sa biclé privée est planifié de façon à pouvoir émettre des certificats sans discontinuité.

Le renouvellement du certificat d'ACR est réalisé tous les 6 ans, à partir de la date de génération du certificat auto-signé de l'ACR.

La nouvelle biclé générée est utilisée pour signer les nouveaux certificats émis ainsi que les LAR relatives aux certificats émis par l'ACR, qu'ils soient signés par la nouvelle ou l'ancienne biclé.

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

4.7. REPRISE SUITE À COMPROMISSION ET SINISTRE

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

Les responsables de l'AC RACINE MINISTÈRE INTÉRIEUR mettent en œuvre des procédures et des moyens de remontée et de traitement des compromissions, notamment au travers de l'analyse des différents journaux d'évènements, par exemple avant utilisation de l'AC RACINE MINISTÈRE INTÉRIEUR.

Les procédures de traitement des incidents et des compromissions font l'objet du Plan de Reprise d'Activité de l'IGC-MI. Ce document n'est pas public.

En cas d'incident impactant durablement ses services, l'ACR s'engage à prévenir dans les meilleurs délais les porteurs et tiers utilisateurs de certificat en utilisant tout moyen à sa convenance (messagerie, appel téléphonique, affichage, site Web, etc.).

Les incidents ou compromissions détectés par l'ACR font l'objet d'une information à l'ACR de l'IGC/A, qui en saisit au besoin la commission d'homologation de l'IGC/A.

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

L'AC RACINE MINISTÈRE INTÉRIEUR est dupliquée sur un autre site sécurisé du ministère. Ce second site est mis à jour en fonction des opérations effectuées sur le site principal (au minimum, deux fois par an).

Les sites secondaires et principaux sont utilisés en alternance au moins une fois tous les trois ans de manière à assurer la continuité d'activité de l'ACR.

4.7.3. PROCEDURES DE REPRISE EN CAS DE COMPROMISSION DE LA CLE PRIVEE DE L'ACR OU DE L'UNE DE SES COMPOSANTES

Dans le cas de la compromission de sa clé privée, l'AC RACINE MINISTÈRE INTÉRIEUR procède à sa cessation d'activité, et en informe selon tout moyen à sa disposition, les ACD rattachées, les porteurs et tiers utilisateurs des certificats émis par l'AC RACINE MINISTÈRE INTÉRIEUR.

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

En cas d'incident impactant l'infrastructure de l'AC RACINE MINISTÈRE INTÉRIEUR, les services de l'AC RACINE MINISTÈRE INTÉRIEUR sont restaurés sur une infrastructure semblable dans un délai inférieur à 8 heures en période ouvrée, permettant le respect des exigences de la présente PC en matière de disponibilité des fonctions de l'application IGC-MI, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

4.8. FIN DE VIE DE L'ACR

Dans l'hypothèse d'une cessation d'activité totale, l'ACR s'engage à assurer la continuité des fonctions de révocation des certificats et la publication des LAR, dans la limite de ses propres possibilités.

En particulier, lors de l'arrêt du service, l'ACR :

- ✓ demande la révocation de son certificat auprès de l'IGC/A,
- ✓ révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité,
- ✓ prend toutes les mesures nécessaires pour détruire ses clés privées de signature,
- ✓ publie cette information sur les sites web http://crl.interieur.gouv.fr (dédié aux CRL des AC) et http://www.igc.interieur.gouv.fr (dédié aux autres informations).

L'ACR s'engage de plus à :

- ✓ communiquer à l'ACR de l'IGC/A son intention de cessation d'activité, au plus tard 3 mois avant celle-ci,
- ✓ indiquer à l'ACR de l'IGC/A le moyen permettant d'accéder à ses archives, et la date de leur destruction programmée.

5. MESURES DE SÉCURITÉ TECHNIQUES

5.1. GÉNÉRATION DES BICLÉS

5.1.1. GENERATION DES BICLES DES AUTORITES DE L'AC RACINE

La génération des clés de signature des autorités est effectuée dans un environnement sécurisé utilisant un module cryptographique matériel qualifié au niveau EAL4+.

Les clés de signature d'ACR sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre 6.2.1 du document [IGC/A-PC].

La génération de la clé de signature de l'ACR est effectuée dans des circonstances contrôlées, par des personnels dans des rôles de confiance, dans le cadre de cérémonies de clés. Ces cérémonies se déroulent suivant des scripts préalablement définis. Ces documents ne sont pas publics.

L'initialisation de l'IGC-MI s'accompagne de la génération de jetons matériels N parmi M ; ces jetons sont des données permettant d'initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signature d'ACR.

5.1.2. TRANSMISSION DE LA CLE PUBLIQUE D'UNE ACD A L'ACR

La clé publique de l'ACD peut être transmise pour certification à l'ACR via une CSR générée par l'ACD.

Lors de la transmission de la clé publique d'une ACD vers l'ACR en vue de sa certification, son origine est authentifiée.

5.1.3. TRANSMISSION DES CLES PUBLIQUES DES ACD ET DE L'ACR AUX UTILISATEURS DE CERTIFICAT

La clé publique de l'ACR est contenue dans un certificat signé par l'IGC/A et diffusée dans un certificat signé par l'IGC/A.

La clé publique d'une ACD est diffusée dans un certificat signé par l'AC RACINE MINISTÈRE INTÉRIEUR.

5.1.4. TAILLES DES CLES

Les clés des certificats suivants respectent les exigences de caractéristiques (tailles, algorithmes, etc.) du RGS et sont de type :

- ✓ pour le certificat de l'AC RACINE MINISTÈRE INTÉRIEUR : RSA de 4096 bits,
- ✓ pour les certificats des ACD : RSA de 4096 bits.

5.1.5. VERIFICATION DE LA GENERATION DES PARAMETRES DES BICLES ET DE LEUR QUALITE

Les équipements de génération des biclés utilisent des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la biclé.

5.1.6. OBJECTIFS D'USAGE DES CLES

L'utilisation des clés privées des différentes autorités et des certificats associés est strictement limitée à la signature de certificats et de LCR/LAR.

5.2. MESURES DE SÉCURITÉ POUR LA PROTECTION DES CLÉS PRIVÉES ET POUR LES MODULES CRYPTOGRAPHIQUES

5.2.1. MODULES CRYPTOGRAPHIQUES DE L'ACR

Les modules cryptographiques, utilisés par l'ACR pour la génération et la mise en œuvre de ses clés de signature, répondent au minimum aux exigences du chapitre 6.2.1 du document [IGC/A-PC]. Les cartes cryptographiques utilisées ont été évaluées selon les *Critères Communs* au niveau EAL4+.

Les clés privées d'AC ne sont ni séquestrées, ni archivées.

5.3. AUTRES ASPECTS DE LA GESTION DES BICLÉS

5.3.1. ARCHIVAGE DES CLES PUBLIQUES

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

5.3.2. DUREES DE VIE DES BICLES ET DES CERTIFICATS

La période de validité du certificat de l'ACR est de **douze (12) ans**.

La durée de validité des certificats d'ACD est de **six (6) ans**.

5.4. DONNÉES D'ACTIVATION DES CLÉS D'AC

5.4.1. GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION

La génération et l'installation des données d'activation des modules cryptographiques de l'IGC-MI, au sein desquels sont mises en œuvre les clés de signature de l'ACR, se font lors de la phase d'initialisation et de personnalisation de ce module, pendant la cérémonie des clés. Les données d'activation sont choisies et saisies par les porteurs de secret responsables de ces données.

5.4.2. PROTECTION DES DONNEES D'ACTIVATION

Les données d'activation ne sont connues que par les porteurs de secret nommément identifiés dans le cadre des rôles qui leurs sont attribués.

Elles sont scellées et conservées en coffre-fort par les responsables de ces données eux-mêmes, de manière à les protéger en intégrité et en confidentialité.

5.5. MESURES DE SÉCURITÉ DES SYSTÈMES INFORMATIQUES

Les mesures de sécurité mises en place au niveau des systèmes informatiques couvrent les objectifs de sécurité suivants :

- ✓ identification et authentification forte des détenteurs de rôles de confiance pour l'accès à la plate-forme de l'AC RACINE MINISTÈRE INTÉRIEUR,
- ✓ identification et authentification forte des administrateurs centraux pour l'accès à l'application IGC-MI,
- ✓ gestion des comptes des administrateurs centraux au niveau de l'application IGC-MI,

- ✓ gestion des comptes des détenteurs de rôles de confiance au niveau des systèmes de la plate-forme de l'AC RACINE MINISTÈRE INTÉRIEUR,
- ✓ fonctions d'audits (imputabilité des actions effectuées),
- ✓ gestion des incidents,
- ✓ protection en confidentialité, en intégrité et en disponibilité des clés nécessaires au fonctionnement de l'AC RACINE MINISTÈRE INTÉRIEUR.

L'ACR est installée sur un serveur hors-ligne.

5.6. MESURES DE SÉCURITÉ DES SYSTÈMES DURANT LEUR CYCLE DE VIE

5.6.1. MESURES DE LA SECURITE LIEES AU DEVELOPPEMENT DES SYSTEMES

La configuration des systèmes de la plate-forme de l'AC RACINE MINISTÈRE INTÉRIEUR (systèmes d'exploitation, application IGC…), ainsi que toute modification et mise à niveau, sont documentées et contrôlées.

5.6.2. MESURES LIEES A LA GESTION DE LA SECURITE

Le FSSI est tenu informé de toute évolution majeure sur les systèmes de la plate-forme de l'AC RACINE MINISTÈRE INTÉRIEUR.

Celle-ci est documentée et apparaît dans les procédures d'exploitation de l'ACR (document non public).

5.7. MESURES DE SÉCURITÉ RÉSEAU

La plate-forme hébergeant l'AC RACINE MINISTÈRE INTÉRIEUR est déconnectée de tout réseau.

5.8. SYSTÈME DE DATATION

La datation des évènements enregistrés par les différentes fonctions de l'ACR dans les journaux est basée sur l'heure système de la plate-forme hébergeant l'ACR et vérifiée avant toute utilisation avec une précision inférieure à 5 minutes. Il n'est pas mis en œuvre de mécanisme de synchronisation.

5.9. EXIGENCES SUR LES ÉCHANGES DE DONNÉES ENTRE COMPOSANTES

Les échanges de données entre composantes au sein de l'AC RACINE MINISTÈRE INTÉRIEUR répondent aux exigences présentées ci-après. Des précisions sont apportées dans la DPC.

5.9.1. PROTECTION DES DONNEES ECHANGEES ENTRE COMPOSANTES

Les échanges entre les différentes composantes de chaque AC sont protégés :

- ✓ en intégrité,
- ✓ en confidentialité,
- ✓ avec garantie de l'origine.

De même, les échanges entre les utilisateurs « humains » d'une composante (administrateurs centraux) et cette composante sont protégés selon les mêmes dispositions.

Les certificats d'authentification et de chiffrement SSL des composantes de chaque AC sont émis par l'autorité concernée.

Les certificats d'authentification et de chiffrement SSL des serveurs Web internes à l'application d'IGC-MI sont émis par l'AC RACINE MINISTÈRE INTÉRIEUR pour les serveurs Web utilisés par l'AC RACINE MINISTÈRE INTÉRIEUR, selon la présente PC.

5.9.2. DISPOSITIONS APPLICABLES AUX CERTIFICATS DE COMPOSANTES

Ces dispositions s'appliquent à chaque autorité pour ses propres composantes :

- ✓ génération : lors de l'installation, les certificats d'authentification SSL des composantes sont générés lors de l'installation de l'autorité concernée et sont signés par la clé privée de cette autorité,
- ✓ renouvellement : le renouvellement de l'ensemble de ces certificats d'authentification est effectué simultanément à chaque changement de clé de l'autorité concernée,
- ✓ révocation : la suspicion de compromission d'un certificat de composante entraîne la mise en œuvre des procédures détaillées dans le Plan de Reprise d'Activité de l'AC concernée (ACR ou ACD). Ce document n'est pas public.

5.9.3. PROTECTION DES DONNEES ECHANGEES AVEC LA BASE DE DONNEES

Les communications entre les composantes et la base de données sont protégées en intégrité et en confidentialité.

5.9.4. PROTECTION DES DONNEES ECHANGEES ENTRE SITES

Les informations de la base de données de l'AC RACINE MINISTÈRE INTÉRIEUR sont répliquées après chaque utilisation du site principal, du site principal vers le site de secours. Les informations échangées sont protégées en intégrité et en confidentialité.

6. PROFILS DES CERTIFICATS ÉMIS PAR L'AC RACINE

Les profils :

- ✓ du certificat de l'ACR,
- ✓ des certificats des ACD émis par l'ACR,
- ✓ des LAR émises par l'ACR,

sont décrits dans les annexes ANNEXE 1 POLITIQUE DE CERTIFICATION FORMAT DES CERTIFICATS Ref : AA100008/PCA0012 V1.0 et V2.0

6.1. AC RACINE

Champs de base

CHAMP	VALEUR
Version	2 (version 3)
CertificateSerialNumber	11:21:ae:cb:78:04:39:d8:82:a0:fc:c5:a7:b1:80:36:79:b1
Signature Algorithm	SHA-256WithRSAEncryption
Issuer	CN = IGC/A AC racine Etat francais OU = 0002 130007669 O = ANSSI C = FR
Validity	Not Before: Dec 22 09:00:00 2011 GMT Not After : Aug 8 08:00:00 2023 GMT
Subject	CN=AC RACINE MINISTERE INTERIEUR OU=0002 110014016 O=MINISTERE INTERIEUR C=FR
Public Key Algorithm	rsaEncryption
SubjectPublicKey	Clé RSA (4096bits)

CHAMP	VALEUR
SignatureValue	a4:aa:11:3f:9a:c9:ce:1d:14:d4:80:c6:a9:c0:0d:27:c8:e8: e9:b7:1f:f5:20:2e:2a:75:a7:95:2a:ff:71:04:00:19:79:55: b2:9c:3e:62:1c:5d:bc:22:21:c0:8b:1f:9f:c1:e0:98:23:b2: 71:9d:e7:94:f4:83:7f:c8:98:52:13:73:85:38:83:15:56:af: 9e:70:1d:2d:69:6e:ee:53:27:29:a0:bf:46:a8:19:8c:e4:4b: bb:e6:60:e9:dc:89:3d:35:72:08:35:01:01:d7:f6:a7:28:42: a3:9c:a9:80:8e:f9:53:09:13:dc:08:60:d1:8b:2f:27:e0:e8: df:0e:b9:28:74:2d:a1:de:1b:b7:3e:9d:0b:5a:c6:38:e4:56: b4:0b:7a:61:af:a8:22:80:04:40:ff:b9:c2:be:7e:4e:c0:d3: c6:53:9f:e9:bd:73:aa:fe:a7:f2:ab:37:a9:22:06:71:15:05: 0c:d9:dc:dc:9c:33:7b:f9:8e:c8:fb:c0:79:3f:6c:21:24:68: 67:e9:94:7b:a6:6b:ef:ad:b1:44:6e:a1:d2:40:f4:3a:38:a5: 55:b3:d9:c4:46:5e:2f:7b:90:a5:76:6b:e7:db:33:04:f1:e1: 5f:87:9f:53:d7:f2:af:cb:46:3b:0d:cc:d2:82:06:d1:31:24: 1a:40:6c:7c:2f:68:1a:f6:72:56:e2:77:40:c0:83:b0:8b:c1: 9e:31:c0:82:62:da:13:e0:14:93:02:d7:a2:9f:27:07:a2:87: 7d:7d:da:31:42:98:2e:92:f7:ba:87:e7:04:ed:38:70:f3:ae: 7f:1b:b0:5b:e9:39:f5:f0:a0:37:59:3c:58:09:5b:bc:2f:05: 22:44:c7:3c:0d:06:7f:43:bd:85:b4:c1:53:d5:2d:52:59:19: 8d:98:da:37:18:69:18:17:aa:29:25:b6:c9:06:95:96:7d:4c: b4:f3:8d:9c:a3:ae:96:72:e0:ff:dd:af:5e:43:6f:82:d3:75: 8e:0b:62:f1:14:59:63:ec:d1:fb:95:1a:07:78:7a:a9:7e:ff: 74:34:75:6a:1f:8f:4a:29:72:47:17:03:0c:c5:d8:de:66:2f: ae:c9:4c:74:20:86:3e:30:13:f2:60:e3:25:0e:3e:a5:d5:e1: 91:3d:55:04:cf:16:8b:55:40:55:9a:8c:4b:f3:0a:3d:fe:42: 75:cd:be:06:7d:13:19:ac:c1:5f:96:2d:fd:4d:24:ca:cd:67: df:70:0f:dd:7f:ac:e6:7c:27:8f:8a:09:00:88:d4:8a:e6:c4: af:a8:83:3c:17:de:7a:74:b0:2a:6e:ae:4b:ff:77:0b:0d:79: d1:61:25:27:98:90:ce:e1

Extensions

CHAMP	CRITICITE	VALEUR	REMARQUES
Key Usage	Critique	Certificate Sign, CRL Sign	
Subject Key identifier	Non Critique	D2:B6:9F:DE:5F:F3:49:56:EC:46:C9:13:8D:42:C1:B6:D0:31:94:1E	
Authority Key Identifier	Non Critique	keyid:9F:AA:D3:29:96:DF:00:E5:43:E0:F1:63:AC:DE:12:8E:C2:27:78:FA	
BasicConstraint	Critique	CA = true	
CertificatePolicies	Non Critique	1.2.250.1.223.1.1.2	IGC/A

CHAMP	CRITICITE	VALEUR	REMARQUES
CRL Distribution Points	Non-critique	URI: http://crl.interieur.gouv.fr/igca4096.crl	

6.2. CERTIFICAT AC DÉLÉGUÉE

Champs de base

CHAMP		VALEUR	REMARQUES
Version		2 (version 3)	
CertificateSerialNumber		alloué automatiquement	
Signature Algorithm		SHA-256WithRSAEncryption	
Issuer		CN=AC RACINE MINISTERE INTERIEUR OU=0002 110014016 O=MINISTERE INTERIEUR C=FR	
Validity		Not before : << Date d'émission >> NotAfter: << Date d'émission + 6 years >>	
Subject		CN= « Nom de l'AC DELEGUE» OU=0002 110014016 O=MINISTERE INTERIEUR C=FR	
Public Key Algorithm		rsaEncryption	
SubjectPublicKey		Clé RSA (4096bits)	
SignatureValue		Valeur de la signature	

Extensions

CHAMP	CRITICITE	VALEUR	REMARQUES
Key Usage	Critique	KeyCertSign CrlSign,	
Authority Key identifier	Non Critique	hash of IssuerPublicKey	
Subject Key identifier	Non Critique	hash of SubjectPublicKey	
BasicConstraint	Critique	CA = true	
CertificatePolicies	Non Critique	OID = 1.2.250.1.152.2.1.[1, 2, 3, 4, 12, 22, 32 ou 42] CPSuri = http://www.igc.interieur.gouv.fr	so(1) member-body(2) fr(250) type-org(1) ministère-intérieur(152) igc(2) politique-certification(1)
CRLDistributionPoint	Non Critique	Uri	
AuthorityInformation Access	Non critique	accessMethod : id-ad-caIssuers accessLocation : URI de l'AC émettrice	URI de l'AC émettrice (certificat ACR du MI ou certificat AC émis par l'IGC/A

6.3. FORMAT LAR

Champs de base

champ		VALEUR	REMARQUES
Version		V2	
Signature Algorithm		SHA-256WithRSAEncryption	
Issuer		CN= AC RACINE MINISTERE INTERIEUR OU=0002 110014016 O=MINISTERE INTERIEUR C=FR	
thisUpdate		« Date d'émission»	
nextUpdate		« Date de la prochaine publication »	36 jours après la date d'émission pour une LAR normale de l'ACR.
RevokedCertificates			
userCertificate		n° de série du certificat	
revocationDate		date de révocation du certificat	
signatureAlgorithm		sha256WithRSAEncryption	
signatureValue		Valeur de la signature numérique	

Extensions

CHAMP	CRITICITE	VALEUR	REMARQUES
Authority Key Identifier	Non Critique	hash of IssuerPublicKey	
CRLnumber	Non Critique	Numéro de série de la CRL	

7. AC RACINE : AUDITS INTERNES ET DE CONFORMITÉ

L'Autorité Administrative de l'AC RACINE MINISTÈRE INTÉRIEUR fait contrôler la conformité de son ACR avec les exigences de la présente PC. Les audits internes ont notamment pour but de vérifier que l'ACR respecte ce qui est écrit dans la présente PC et dans la DPC associée.

Dans le cadre du rattachement à l'IGC/A, l'AC RACINE MINISTÈRE INTÉRIEUR est soumise à des audits de conformité, mandatés par l'AA de l'IGC/A. Les modalités de cet audit initial ainsi que des audits au cours du cycle de vie de l'AC RACINE MINISTÈRE INTÉRIEUR sont définies par l'AA de l'IGC/A. L'audit de conformité initial se situe après la cérémonie des clés de l'ACR et avant la certification initiale de l'ACR par l'IGC/A.

Par ailleurs, il est rappelé que, dans le cadre du rattachement à l'IGC/A, l'AC RACINE MINISTÈRE INTÉRIEUR réalise un audit de conformité selon le rythme [F_CONFORM] de la PC IGC/A.

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

7.1. AUDITS INTERNES

Le présent chapitre ne concerne que les audits et évaluation internes de la responsabilité de l'AC RACINE MINISTÈRE INTÉRIEUR afin de s'assurer du bon fonctionnement de son AC.

7.1.1. FREQUENCE ET / OU CIRCONSTANCES DES EVALUATIONS

Suite à la première mise en service de l'application IGC-MI ou suite à toute modification significative de celle-ci ou des procédures fonctionnelles applicables, l'AA de l'ACR fait procéder à un audit interne global ou limité au périmètre de l'impact de la modification.

L'AA de l'AC RACINE MINISTÈRE INTÉRIEUR fait aussi procéder régulièrement à un audit interne de l'ensemble de son AC, une fois tous les deux ans.

7.1.2. IDENTITES / QUALIFICATION DES EVALUATEURS

Le contrôle d'un périmètre particulier de l'IGC-MI (procédure, application, fonction, rôle) est assigné par l'AA de l'AC RACINE MINISTÈRE INTÉRIEUR à une équipe d'auditeurs, compétents en sécurité des systèmes d'information et dans le domaine couvert par le périmètre à auditer.

7.1.3. RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES

L'auditeur ne doit pas posséder de rôle de confiance auprès de l'AC RACINE MINISTÈRE INTÉRIEUR autre que le présent rôle et est dûment autorisé à pratiquer les contrôles visés.

7.1.4. SUJETS COUVERTS PAR LES EVALUATIONS

Les audits internes portent sur un rôle, une procédure, une fonction de l'AC RACINE MINISTÈRE INTÉRIEUR, sur l'application 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 présente PC et dans la DPC associée, ainsi que des éléments qui en découlent (procédures opérationnelles, ressources déployées, etc.).

7.1.5. ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

A l'issue d'un contrôle, l'auditeur rend à l'AA 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'auditeur émet des recommandations à l'AA de l'AC RACINE MINISTÈRE INTÉRIEUR pouvant être la cessation (temporaire ou définitive) d'activité, la suppression du rôle de confiance, la modification de la procédure, 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'AA de l'AC RACINE MINISTÈRE INTÉRIEUR et respecte ses politiques de sécurité internes,
- ✓ en cas de résultat « À confirmer », l'auditeur remet à l'AA de l'ACR un avis précisant sous quel délai les non-conformités sont réparées. Puis, un contrôle de « confirmation » permet de vérifier que tous les points critiques ont bien été résolus,
- ✓ en cas de réussite, l'auditeur confirme à l'AA de l'AC RACINE MINISTÈRE INTÉRIEUR la conformité aux exigences de la présente PC et la DPC associée.

En cas d'échec ou de résultat « à confirmer », l'AA informe, selon un moyen à sa convenance, les tiers utilisateurs de ce résultat.

7.1.6. COMMUNICATION DES RESULTATS

Les résultats des audits internes ne sont communiqués qu'à la discrétion de l'AA de l'ACR.

7.2. AUDITS DE CONFORMITÉ

Le présent chapitre ne concerne que les audits de conformité effectués suite au rattachement de l'AC RACINE MINISTÈRE INTÉRIEUR à l'IGC/A.

L'AC RACINE MINISTÈRE INTÉRIEUR autorise l'IGC/A à contrôler ou faire contrôler la conformité de ses pratiques à la présente PC.

7.2.1. FREQUENCE DES CONTROLES DE CONFORMITE

Les contrôles de conformité s'effectuent tous les 3 ans ou à la demande de l'IGC/A.

7.2.2. IDENTIFICATION ET QUALIFICATION DU CONTROLEUR

L'identification et les qualifications des contrôleurs sont précisées dans la convention liant l'IGC/A et l'AC RACINE MINISTÈRE INTÉRIEUR.

7.2.3. SUJETS COUVERTS PAR LE CONTROLE DE CONFORMITE

Les éléments relatifs au contrôle de conformité (audit initial pour la certification, ou visite de contrôle) de l'AC RACINE MINISTÈRE INTÉRIEUR sont décrits dans le référentiel d'audit de l'IGC/A.

7.2.4. MESURES A PRENDRE EN CAS DE NON-CONFORMITE

Les mesures à prendre en cas de non-conformité sont décidées conformément aux exigences de l'IGC/A sur ce point.

7.2.5. COMMUNICATION DES RESULTATS

Les résultats des contrôles de conformité sont communiqués à l'AA de l'AC RACINE MINISTÈRE INTÉRIEUR par l'autorité d'audit.

8. AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

8.1. CONFIDENTIALITÉ DES DONNÉES PERSONNELLES

8.1.1. PERIMETRE DES INFORMATIONS CONFIDENTIELLES

Les informations et données à caractère confidentiel sont listées et classées au sein de la DPC. La DPC détaille les mesures de sécurité applicables à chaque niveau de sécurité identifié.

8.1.2. RESPONSABILITES EN TERME DE PROTECTION DES INFORMATIONS CONFIDENTIELLES

La présente PC ne formule pas d'exigence supplémentaire au regard de la législation et de la réglementation en vigueur sur le territoire français relatives à la protection des informations confidentielles.

8.2. PROTECTION DES DONNÉES PERSONNELLES

8.2.1. POLITIQUE DE PROTECTION DES DONNEES PERSONNELLES

Toute collecte et tout usage de données à caractère personnel par l'AC et les rôles de confiance de l'AC sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier la *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.

L'IGC-MI en tant qu'infrastructure de stockage et de gestion de données nominatives contenues dans les certificats électroniques, est déclarée auprès de la CNIL selon les termes de la Loi *n° 78-17 du 6 janvier 1978 « Informatique et Libertés »*.

8.2.2. INFORMATIONS A CARACTERE PERSONNEL

Les informations considérées comme personnelles sont les suivantes :

- ✓ le dossier d'enregistrement d'une ACD,
- ✓ les P.V. de cérémonie des clés.

8.2.3. INFORMATIONS A CARACTERE NON PERSONNEL

Sont considérées comme non personnelles l'ensemble des informations n'étant pas identifiées comme personnelles.

8.2.4. RESPONSABILITE EN TERME DE PROTECTION DES DONNEES PERSONNELLES

La présente PC ne formule pas d'exigence supplémentaire au regard de la législation et de la réglementation en vigueur sur le territoire français relatives à la protection des données personnelles.

8.2.5. NOTIFICATION ET CONSENTEMENT D'UTILISATION DES DONNEES PERSONNELLES

La présente PC ne formule pas d'exigence particulière sur ce point.

8.2.6. CONDITIONS DE DIVULGATION D'INFORMATIONS PERSONNELLES AUX AUTORITES JUDICIAIRES OU ADMINSITRATIVES

La communication aux autorités judiciaires des données personnelles sera effectuée en cas de demande de leur part.

8.2.7. AUTRES CIRCONSTANCES DE DIVULGATION D'INFORMATIONS PERSONNELLES

La présente PC ne formule pas d'exigence particulière sur ce point.

8.3. DROITS SUR LA PROPRIÉTÉ INTELLECTUELLE ET INDUSTRIELLE

La présente PC ne formule pas d'exigence supplémentaire au regard de la législation et la réglementation en vigueur sur le territoire français.

8.4. LIMITE DE RESPONSABILITÉ

L'objectif de l'AC RACINE MINISTÈRE INTÉRIEUR est d'émettre des certificats à destination des ACD composant l'IGC-MI.

La responsabilité de l'AA ne peut être engagée qu'en cas d'un manquement à l'une de ses obligations ou à celles des AA, AC, et AE de l'IGC-MI.

L'AA ne pourra pas être tenue pour responsable d'un fait dommageable qui relève de sa compétence en cas de 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.

L'ACR décline toute responsabilité à l'égard de l'usage des certificats émis par elle ou des bi-clés publiques/privées associées dans des conditions et à des fins autres que celles prévues dans la présente PC.

8.5. INDEMNITÉS

Sans objet.

8.5.1. DUREE DE VALIDITE ET FIN DE VALIDITE DE LA PRESENTE PC

La présente PC de l'ACR cesse d'être valide :

- ✓ soit six mois après qu'il n'y a plus aucun certificat valide émis conformément à la présente PC,
- ✓ soit, de manière anticipée, sur information publique de la part de l'AA, de l'invalidité de la présente PC. Dans ce cas, les certificats publiés selon la présente PC seront également révoqués.

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

Les traces d'audit enregistrées avant la fin de validité de la PC restent valables.

8.6. AMENDEMENTS À LA PC.

8.6.1. PROCEDURES D'AMENDEMENTS

La procédure d'amendement à la PC est initiée par l'AA ou l'AC de l'AC RACINE MINISTÈRE INTÉRIEUR, ou encore l'AA de l'IGC/A.

En cas de changement important, l'ACR s'engage à faire appel à un auditeur pour en contrôler l'impact.

8.6.2. MECANISME ET PERIODE D'INFORMATION SUR LES AMENDEMENTS

Les tiers utilisateurs de certificats peuvent prendre connaissance des amendements au moyen du site web http://www.igc.interieur.gouv.fr. L'IGC/A sera également informée de ces amendements.

8.6.3. CIRCONSTANCES SELON LESQUELLES L'OID DOIT ETRE CHANGE

L'OID de la présente PC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) ou du document décrivant les profils associés se traduit par une évolution de l'OID. En particulier, des modifications de forme n'entraînent pas une modification de l'OID.

Le nouvel OID, si nouvel OID il y a, apparaît dans tout nouveau certificat émis par l'ACR. Ainsi, les tiers utilisateurs de certificat peuvent clairement distinguer quels certificats correspondent à quelles exigences.

8.7. DISPOSITIONS CONCERNANT LA RÉSOLUTION DE CONFLITS

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

8.8. JURIDICTIONS COMPÉTENTES

En cas de litiges, ces derniers seront soumis à l'appréciation des tribunaux compétents.

8.9. CONFORMITÉ AUX LÉGISLATIONS ET RÉGLEMENTATIONS

L'ACR s'engage à respecter les textes de lois et décrets d'application relatifs aux moyens de cryptologie, selon l'article 28 de la loi n°90-1170 du 29 décembre 1990 (Loi de Réforme des Télécommunications).

9. OBLIGATIONS RESPECTIVES

9.1. OBLIGATIONS APPLICABLES À L'AA DE L'AC RACINE

Les obligations de l'AA de l'AC RACINE MINISTÈRE INTÉRIEUR consistent à :

- ✓ approuver la PC de l'ACR et des composantes de l'AC RACINE MINISTÈRE INTÉRIEUR (le présent document),
- ✓ approuver la DPC de l'ACR et des composantes de l'AC RACINE MINISTÈRE INTÉRIEUR,
- ✓ définir les exigences minimales applicables aux ACD souhaitant obtenir un certificat de l'AC RACINE MINISTÈRE INTÉRIEUR,
- ✓ décider du rattachement de l'AC RACINE MINISTÈRE INTÉRIEUR à l'IGC/A,
- ✓ décider des mesures à appliquer lorsqu'un détenteur de rôle de confiance auprès de l'AC RACINE MINISTÈRE INTÉRIEUR abuse de ses droits ou effectue une opération non conforme à ses attributions,
- ✓ prononcer si nécessaire la décision de révocation de l'ACR ou/et de ses composantes,
- ✓ déclarer si nécessaire la cessation d'activité de l'ACR.

9.2. OBLIGATIONS APPLICABLES À L'AC RACINE

L'AC RACINE MINISTÈRE INTÉRIEUR s'oblige à :

- ✓ élaborer et respecter les exigences définies dans la présente PC et la DPC afférente,
- ✓ élaborer la DPC relative à la présente PC, et garantir et maintenir la cohérence entre cette DPC et la présente PC,
- ✓ demander l'autorisation à l'AA pour toute évolution de son système,
- ✓ autoriser l'ACR de l'IGC/A à contrôler ou faire contrôler la conformité de ses pratiques à la présente PC,
- ✓ réaliser régulièrement un audit de la sécurité de son IGC,
- ✓ soumettre à approbation de l'IGC/A toute création d'ACD,
- ✓ 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,
- ✓ assurer la disponibilité de son certificat,
- ✓ mettre à la disposition d'un utilisateur de certificat la présente PC afin de lui permettre d'apprécier la confiance à accorder à un certificat,
- ✓ procéder à un changement de certificat en cas de compromission, suspicion de compromission, vol, perte des moyens de reconstitution de la clé privée de l'ACR (perte du secret principal, perte du code d'activation et perte de plus de deux secrets partagés),
- ✓ documenter les schémas de certification qu'elle entretient avec les ACD,
- ✓ vérifier la complémentarité des clés publique et privée d'une ACD souhaitant être certifiée par l'AC RACINE MINISTÈRE INTÉRIEUR,
- ✓ générer le certificat d'une ACD dès lors que les conditions de certification posées dans la PC sont remplies par l'ACD,

- ✓ renouveler le certificat d'une ACD dès lors que les conditions de renouvellement du certificat posées dans la PC sont remplies par l'ACD,
- ✓ obtenir confirmation de l'acceptation du certificat par l'ACD sous la forme d'un accord signé,
- ✓ révoquer le certificat d'une ACD selon les conditions posées et dans le respect des procédures déterminées dans la présente PC,
- ✓ enregistrer et archiver les informations pertinentes,
- ✓ respecter les impératifs des contrôles,
- ✓ respecter les conditions de disponibilité définies dans la présente PC et la DPC afférente,
- ✓ publier des informations authentiques et intègres.

9.3. OBLIGATIONS DES ADMINISTRATEURS CENTRAUX DE L'AC RACINE

Les administrateurs centraux de l'AC RACINE MINISTÈRE INTÉRIEUR, dans le cadre de leur rôle d'AE, ont pour obligation :

- ✓ d'assurer leur rôle dans le respect de la présente PC, et notamment d'assurer les fonctions dévolues à l'AE telles que précisées dans la présente PC,
- ✓ de vérifier l'identité du demandeur de demande de génération de certificat,
- ✓ de vérifier l'identité du demandeur de demande de révocation de certificat,
- ✓ d'assister les demandeurs de certificats dans l'utilisation et la gestion des certificats,
- ✓ de respecter les exigences décrites dans les documents de cérémonies des clés,
- ✓ de conserver et protéger en confidentialité et en intégrité les données d'identification transmises pour l'enregistrement,
- ✓ d'enregistrer et d'archiver ces informations conformément à la présente PC, et notamment les demandes de certificats d'ACD.

Note : les administrateurs centraux de l'AC RACINE MINISTÈRE INTÉRIEUR, dans leur rôle d'AE, assurent l'enregistrement des ACD et des nouveaux administrateurs centraux de l'AC RACINE MINISTÈRE INTÉRIEUR.

9.4. OBLIGATIONS APPLICABLES À L'AC RACINE SUITE AU RATTACHEMENT À L'IGC/A

L'AC RACINE MINISTÈRE INTÉRIEUR doit se conformer à la PC de l'IGC/A en vigueur, et actuellement référencée par l'OID : 1.2.250.1.223.1.1.2. À ce titre, elle est une « ACR gouvernementale ».

9.5. OBLIGATIONS APPLICABLES AUX AC DÉLÉGUÉES

La présente section définit les obligations applicables à chaque ACD dans le cadre de la présente PC, et donc relatives à :

- ✓ sa qualité d'autorité subordonnée à l'ACR du MI,
- ✓ la gestion de ses certificats de composantes.

Chaque ACD s'oblige donc, dans le cadre de la présente PC, à :

- ✓ respecter les exigences définies dans la présente PC et la DPC afférente,
- ✓ 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'ACD 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 la clé privée de l'ACD (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'ACD ont connaissance de leurs droits et obligations conférés de par l'attribution de ce rôle,
- ✓ être conforme 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.

Les obligations applicables à chaque ACD relatives à son propre rôle d'autorité sont définies au sein des PC émises par l'ACD elle-même.

9.6. OBLIGATIONS APPLICABLES AUX DEMANDEURS DE CERTIFICATS D'ACD

Les demandeurs de certificats d'ACD ont le devoir de respecter les exigences décrites dans les documents de cérémonies des clés des ACD. Ces documents ne sont pas publics.

9.7. OBLIGATIONS APPLICABLES AUX PORTEURS DE CERTIFICATS

Les porteurs de certificats sont les administrateurs centraux de l'AC RACINE MINISTÈRE INTÉRIEUR.

En tant que porteurs de certificats d'authentification émis par l'AC RACINE MINISTÈRE INTÉRIEUR, ils ont le devoir de respecter les obligations suivantes :

- ✓ garder personnelle et incessible leur carte d'authentification administrateur,
- ✓ conserver de façon sûre leur carte d'authentification administrateur et son code d'activation. En particulier, celui-ci n'est pas communiqué,
- ✓ remettre au responsable de l'application d'IGC-MI leur carte d'authentification administrateur en cas de départ ou de changement de fonction au sein du ministère,
- ✓ signaler sans délai toute suspicion de vol ou tentative de compromission de leur carte d'authentification administrateur, ainsi que leur perte,
- ✓ suivre les procédures et directives du responsable de l'application IGC-MI, notamment pour le renouvellement du certificat d'authentification ou de la carte d'authentification administrateur.

9.8. OBLIGATIONS APPLICABLES AUX TIERS UTILISATEURS

Les tiers utilisateurs tels que définis dans la présente PC doivent :

- ✓ vérifier et respecter les usages pour lesquels un certificat a été émis,
- ✓ contrôler la validité du certificat utilisé :
  - par contrôle de la signature par l'AC émettrice,
  - par contrôle des dates de validité du certificat,

- par contrôle de l'absence de révocation, d'après la dernière LCR en cours de validité émise par l'AC émettrice.

✓ contrôler de la même façon chaque certificat de la chaîne de certification, jusqu'au certificat racine.

La fréquence des interrogations de la LCR (liée à la durée de validité des informations éventuellement gardées dans un cache) est à l'appréciation des tiers utilisateurs de certificats selon les contraintes liées à leur application.

Le Préfet,
Haut fonctionnaire de défense adjoint

Philippe Riffaut