MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ANFSI

IGC DES FORCES DE SÉCURITÉ INTÉRIEURE

Politique de certification
2024 FSI AC Machines

1.2.250.1.668.1.1.1.7.1

Direction générale de la Gendarmerie nationale
4 rue Claude Bernard
CS 60003 - 92136 Issy Les Moulineaux CEDEX
FRANCE

HISTORIQUE DES MODIFICATIONS

Version	Date	Objet de la modification	Auteur	Statut
0.1	12/2023	Création	SEALWeb	Ébauche
0.2	02/2024	Modifications	CNE MDQ	Projet
1	22/05/2024	Validation par autorité administrative	ANFSI	Validé
1.1	10/01/2025	Modifications et reformulations de plusieurs paragraphes pour préciser les pratiques. Intégration des acronymes [A-Clt], [A-Srv] et [S-Code].	ADJ HCT CEN MDQ	Projet
1.2	05/03/2025	Validation par autorité administrative	ANFSI	Validé

Table des matières

I. Introduction....8
I.1. Présentation générale....8
I.1.1. Objet du document....8
I.1.2. Architecture de l'IGC....9
I.2. Identification du document....9
I.3. Définitions et acronymes....9
I.3.1. Acronymes....9
I.3.2. Définitions....10
I.4. Entités intervenant dans l'IGC....12
I.4.1. Autorités de certification....12
I.4.2. Autorité d'enregistrement....14
I.4.3. Responsables de certificats électroniques de services applicatifs....14
I.4.4. Utilisateurs de certificats....14
I.5. Usage des certificats....15
I.5.1. Domaines d'utilisation applicables....15
I.5.1.1 Bi-clés et certificats du service applicatif....15
I.5.1.2 Bi-clés et certificats d'AC et de composantes....15
I.5.2. Domaines d'utilisation interdits....15
I.6. Gestion de la PC....16
II. Responsabilités concernant la mise à disposition des informations devant être publiées....17
III. Identification et authentification....18
III.1. Nommage....18
III.1.1. Types de noms....18
III.1.2. Nécessité d'utilisation de noms explicites....18
III.1.2.1 Nommage des Autorités de Certification....18
III.1.2.2 Nommage des services applicatifs....18
III.1.3. Pseudonymisation des services applicatifs....18
III.1.4. Règles d'interprétation des différentes formes de nom....18
III.1.5. Unicité des noms....18
III.1.6. Identification, authentification et rôle des marques déposées....19
III.2. Validation initiale de l'identité....19
III.2.1. Méthode pour prouver la possession de la clé privée....19
III.2.2. Validation de l'identité d'un organisme....19
III.2.3. Validation de l'identité d'un individu....20

III.2.3.1 Enregistrement d'un RC pour un certificat de service a*pplicatif* à émettre....20
III.2.3.2 Enregistrement d'un nouveau RC pour un certificat électronique déjà émis....20
III.2.4. Informations non vérifiées du RC et du service applicatif....20
III.2.5. Validation de l'autorité du demandeur....20
III.3. Identification et validation d'une demande de renouvellement des clés....20
III.3.1. Identification et validation pour un renouvellement courant....20
III.3.2. Identification et validation pour un renouvellement après révocation....21
III.4. Identification et validation d'une demande de révocation....21
IV. Exigences opérationnelles sur le cycle de vie des certificats....22
IV.1. Demande de certificat....22
IV.1.1. Origine d'une demande de certificat....22
IV.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat....22
IV.2. Traitement d'une demande de certificat....22
IV.2.1. Exécution des processus d'identification et de validation de la demande....22
IV.2.2. Acceptation ou rejet de la demande....22
IV.2.3. Durée d'établissement du certificat....22
IV.3. Délivrance du certificat....23
IV.3.1. Actions de l'AC concernant la délivrance du certificat....23
IV.3.2. Notification par l'AC de la délivrance du certificat au RC....23
IV.4. Acceptation du certificat....23
IV.4.1. Démarche d'acceptation du certificat....23
IV.4.2. Publication du certificat....23
IV.4.3. Notification par l'AC aux autres entités de la délivrance du certificat....23
IV.5. Usages de la bi-clé et du certificat....23
IV.5.1. Utilisation de la clé privée et du certificat par le RC....23
IV.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat....24
IV.6. Renouvellement d'un certificat....24
IV.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé....24
IV.7.1. Causes possibles de changement d'une bi-clé....24
IV.7.2. Origine d'une demande d'un nouveau certificat....24
IV.7.3. Procédure de traitement d'une demande d'un nouveau certificat....25
IV.7.4. Notification au RC de l'établissement du nouveau certificat....25
IV.7.5. Démarche d'acceptation du nouveau certificat....25
IV.7.6. Publication du nouveau certificat....25
IV.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat....25

IV.8. Modification du certificat....25
IV.9. Révocation et suspension des certificats....25
IV.9.1. Causes possibles d'une révocation....25
IV.9.1.1 Certificats de *services applicatifs*....25
IV.9.1.2 Certificats d'une composante de l'IGC....26
IV.9.2. Origine d'une demande de révocation....26
IV.9.2.1 Certificats de services applicatifs....26
IV.9.2.2 Certificats d'une composante de l'IGC....26
IV.9.3. Procédure de traitement d'une demande de révocation....26
IV.9.3.1 Révocation d'un certificat électronique....26
IV.9.3.1.1 Révocation par le RC....26
IV.9.3.1.2 Révocation par l'AE....26
IV.9.3.1.3 Révocation par l'AC émettrice du certificat....27
IV.9.3.1.4 Traitement de la demande de révocation....27
IV.9.3.2 Révocation d'un certificat d'une composante de l'IGC....27
IV.9.4. Délai accordé au RC pour formuler la demande de révocation....27
IV.9.5. Délai de traitement par l'AC d'une demande de révocation....27
IV.9.5.1 Révocation d'un certificat de service applicatif....27
IV.9.5.2 Disponibilité du système de traitement des demandes de révocation.27
IV.9.5.3 Révocation d'un certificat d'une composante de l'IGC....27
IV.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats....28
IV.9.7. Fréquence d'établissement et durée de validité des LCR....28
IV.9.8. Délai maximum de publication d'une LCR....28
IV.9.9. Exigences sur la vérification en ligne de la révocation et de l'état des certificats....28
IV.9.10. Autres moyens disponibles d'information sur les révocations....28
IV.9.11. Exigences spécifiques en cas de compromission de la clé privée....28
IV.9.12. Causes possibles d'une suspension....28
IV.9.13. Origine d'une demande de suspension....28
IV.9.14. Procédure de traitement d'une demande de suspension....29
IV.9.15. Limites de la période de suspension d'un certificat....29
IV.10. Fonction d'information sur l'état des certificats....29
IV.10.1. Caractéristiques opérationnelles....29
IV.10.2. Disponibilité de la fonction d'information sur l'état des certificats....29
IV.10.3. Dispositifs optionnels....29
IV.11. Fin de la relation entre le RC et l'AC....29
IV.12. Séquestre de clé et recouvrement....29

IV.12.1. Politique et pratiques de recouvrement par séquestre des clés....29
IV.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session....29
V. Mesures de sécurité non techniques....30
VI. Mesures de sécurité techniques....31
VI.1. Génération et installation de bi-clés....31
VI.1.1. Génération des bi-clés....31
VI.1.1.1 Clés du service applicatif générées par l'AE technique....31
VI.1.1.2 Clés du service applicatif générées au niveau du service applicatif....31
VI.1.2. Transmission de la clé privée à son propriétaire....31
VI.1.3. Transmission de la clé publique à l'AC....31
VI.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats....31
VI.1.5. Tailles des clés....32
VI.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité....32
VI.1.7. Objectifs d'usage de la clé....32
VI.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques....32
VI.2.1. Standards et mesures de sécurité pour les modules cryptographiques....32
VI.2.1.1 Modules cryptographiques de l'AC....32
VI.2.1.2 Dispositifs de protection des éléments secrets du service applicatif....32
VI.2.2. Contrôle de la clé privée par plusieurs personnes....32
VI.2.3. Séquestre de la clé privée....32
VI.2.4. Copie de secours de la clé privée....33
VI.2.5. Archivage de la clé privée....33
VI.2.6. Transfert de la clé privée vers / depuis le module cryptographique....33
VI.2.7. Stockage de la clé privée dans un module cryptographique....33
VI.2.8. Méthode d'activation de la clé privée....33
VI.2.8.1 Clés privées d'AC....33
VI.2.8.2 Clés privées des services applicatifs....33
VI.2.9. Méthode de désactivation de la clé privée....33
VI.2.9.1 Clés privées des d'AC....33
VI.2.9.2 Clés privées des services applicatifs....33
VI.2.10. Méthode de destruction des clés privées....34
VI.2.10.1 Clés privées des d'AC....34
VI.2.10.2 Clés privées des services applicatifs....34
VI.2.11. Niveau de qualification du module cryptographique et des dispositifs de protection des éléments secrets....34

VI.3. Autres aspects de la gestion des bi-clés....34
VI.3.1. Archivage des clés publiques....34
VI.3.2. Durées de vie des bi-clés et des certificats....34
VI.4. Données d'activation....34
VI.4.1. Génération et installation des données d'activation....34
VI.4.1.1 Génération et installation des données d'activation correspondant à la clé privée de l'AC....34
VI.4.1.2 Génération et installation des données d'activation correspondant à la clé privée du service applicatif....34
VI.4.2. Protection des données d'activation....34
VI.4.2.1 Protection des données d'activation correspondant aux clés privées de l'AC....34
VI.4.2.2 Protection des données d'activation correspondant aux clés privées des services applicatifs....35
VI.4.3. Autres aspects liés aux données d'activation....35
VI.5. Mesures de sécurité des systèmes informatiques....35
VI.6. Mesures de sécurité des systèmes durant leur cycle de vie....35
VI.7. Mesures de sécurité réseau....35
VI.8. Horodatage / Système de datation....35
VII. Profils des certificats et des LCR....36
VII.1. Format du certificat de 2024 FSI AC Machines....36
VII.2. Format des certificats des services applicatifs....37
VII.3. Format des listes de révocation (LCR) émises par l'2024 FSI AC Machines....40
VIII. Audit de conformité et autres évaluations....42
IX. Autres problématiques métiers et légales....42
Annexe 1 : Documents cités en référence....43
I.1. Documents techniques....43

I. Introduction

I.1. Présentation générale

I.1.1. Objet du document

L'Agence du Numérique des Forces de Sécurité Intérieure (ANFSI) a mis en place et exploite une infrastructure de gestion des clés (IGC), disposant d'une autorité de certification (AC) racine et d'AC subordonnées. L'IGC de l'ANFSI sera notée « IGC/FSI » dans ce document.

Le présent document constitue la politique de certification (PC) de l'AC subordonnée « 2024 FSI AC Machines ».

Dans le cadre de cette politique de certification, cette AC émet des certificats d'authentification pour les machines de l'ANFSI.

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

Le présent document est accompagné du document [MESURES_IGC], qui fait partie intégrale de la PC et de la DPC. Ce document décrit les mesures communes aux différentes AC de l'IGC de l'ANFSI.

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

La gestion d'un certificat comprend toutes les phases du cycle de vie d'un certificat, de la demande d'attribution à la fin de vie de ce certificat. Le but de la présente PC est de fournir aux opérateurs et aux utilisateurs de certificats les informations relatives aux garanties offertes sur les certificats émis par l'IGC de l'Agence du Numérique des Forces de Sécurité Intérieure, ainsi que les conditions d'utilisation de ces certificats.

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

Cette PC vise la conformité aux exigences du [RGS] v2 * (une étoile), et a été élaborée à partir de la PC Type du [RGS].

I.1.2. Architecture de l'IGC

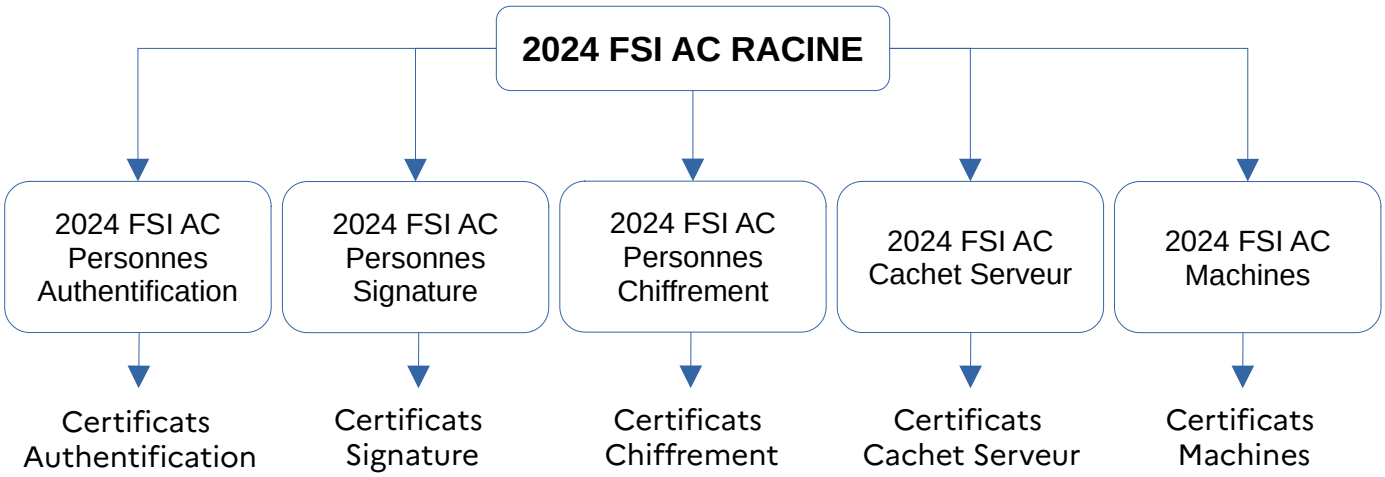

Illustration : Hiérarchie des AC de l'IGC des Forces de Sécurité Intérieure

I.2. Identification du document

Ce document constitue la PC pour l'AC subordonnée « 2024 FSI AC Machines », identifiée par l'OID 1.2.250.1.668.1.1.1.7.1.

La construction de l'OID est réalisée ainsi :

```
iso(1) member-body(2) fr(250) type-org(1) anfsi(668) igc(1) documentation(1) PC(1)
Machines(7) Version(1)
```

I.3. Définitions et acronymes

I.3.1. Acronymes

AA	Autorité Administrative
AC	Autorité de Certification
AE	Autorité d'Enregistrement
ANFSI	Agence du Numérique des Forces de Sécurité Intérieure
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CGU	Conditions Générales d'Utilisation
DGGN (le)	Directeur Général de la Gendarmerie Nationale
DGGN (la)	Direction Générale de la Gendarmerie Nationale
DN	*Distinguished Name*
DPC	Déclaration des Pratiques de Certification
DSA	Direction de la Sécurité et de l'Architecture
D2S	Département des Services Socles
ETSI	*European Telecommunications Standards Institute*
IGC	Infrastructure de Gestion de Clés
LAR	Liste des certificats d'AC Révoqués

LCR	Liste des Certificats Révoqués
OCSP	*Online Certificate Status Protocol*
OID	Object Identifier
PC	Politique de Certification
PSCE	Prestataire de Services de Certification Électronique
RC	Responsable du Certificat de service applicatif
RSA	Rivest Shamir Adleman
SGI	Section de la Gestion des Identités
SIC	Systèmes d'Information et de Communication
SSI	Sécurité des Systèmes d'Information
STIG	Service de Traitement de l'Information Gendarmerie
URL	*Uniform Resource Locator*

I.3.2. Définitions

Applications utilisatrices – Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification du service applicatif auquel le certificat est rattaché.

A-Clt – Désigne une règle spécifique aux certificats électroniques d'usage « authentification client » ; cf. chapitre I.5.1.1.

A-Srv – Désigne une règle spécifique aux certificats électroniques d'usage « authentification serveur » ; cf. chapitre I.5.1.1.

Autorité responsable d'application (ARA) – Une ARA est l'autorité responsable d'une IGC, tant pour la technologie mise en œuvre que pour le cadre réglementaire et contractuel. Elle confie l'élaboration de la PC à une autorité administrative et sa mise en œuvre à des autorités de certification.
L'ARA de l'IGC/FSI est le directeur de l'ANFSI, par délégation du DGGN.

Autorité administrative – L'AA est l'autorité qui élabore la/ou les PC d'une IGC et les DPC afférentes, et qui est garante de leur application.

L'AA de l'IGC/FSI est le chef de la DSA de l'ANFSI.

Autorité de certification racine (ACR) – L'ACR est l'autorité qui dispose d'une IGC lui permettant d'enregistrer, de générer, d'émettre et de révoquer des certificats, principalement des certificats d'AC subordonnées, conformément à la PC et à la DPC définies par son AA. L'ACR de l'ANFSI est auto-signée. L'ACR est opérée par le D2S. Les différentes opérations sont menées sur convocation des représentants des différents services.

L'ACR de l'IGC/FSI est représentée par le chef du DSS DSA ANFSI.

Sont administrateurs de l'ACR les personnels nominativement désignés à cette fin : cf. [GESTION_ROLES].

Autorité de certification subordonnée (AC subordonnée) – L'AC subordonnée est l'autorité qui dispose d'une IGC (qui peut être le même que l'ACR de l'IGC) lui permettant d'enregistrer, de générer, d'émettre et de révoquer des certificats finaux (personnes ou machines), conformément à ses propres PC et DPC. Le certificat de cette AC subordonnée est signé par

l'ACR de l'IGC/FSI. L'AC subordonnée est représentée par le chef du D2S. Sont administrateurs de l'AC subordonnée les personnels nominativement désignés à cette fin : cf. [GESTION_ROLES].

Autorité d'enregistrement (AE) – L'AE est l'autorité qui a pour rôle de vérifier la validité d'une demande de certificat et en suit l'instruction.

L'**AE technique** est réalisée par l'application **Certilibre**. Au sein du processus de demande de certificat dans Certilibre, l'autorité d'enregistrement est assurée par un valideur tel que défini ci-dessous. Sont administrateurs de l'AE technique les personnels nominativement désignés à cette fin : cf. [GESTION_ROLES].

Certificat électronique – Fichier sous forme électronique attestant du lien entre une clé publique et l'identité de son propriétaire. Cette attestation prend la forme d'une signature électronique réalisée par un PSCE. Il est délivré par une AC. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Les usages des certificats électroniques régis par le présent document sont définis au chapitre I.5.1.1.

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

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

Dispositif de protection des éléments secrets – Un dispositif de protection des éléments secrets désigne un dispositif de stockage des éléments secrets remis au RC.

Entité – Désigne une administration ou une entreprise au sens large.

Infrastructure de gestion de clés (IGC) – Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

Politique de certification (PC) – Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les RC et les utilisateurs de certificats.

Porteur de certificat – Le porteur de certificat est normalement la personne physique identifiée dans le certificat comme porteur de la clé privée liée à la clé publique figurant dans le certificat. Dans le contexte de cette PC consacrée à une AC délivrant des certificats à des machines, il faut interpréter le terme porteur comme le Responsable du certificat.

Public Key Cryptographic Standards (PKCS) – Standards de cryptographie à clé publique, soit l'ensemble des normes régissant les objets cryptographiques utilisés dans une IGC. Plus spécifiquement, le *PKCS#10* est le standard d'une requête de signature de certificat.

Responsable du certificat – Personne en charge et responsable du certificat électronique de service applicatif.

S-Code – Désigne une règle spécifique aux certificats électroniques d'usage « signature de code » ; cf. chapitre I.5.1.1.

Usager – Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques avec des autorités administratives. Selon le contexte, un usager peut être un porteur ou un utilisateur de certificats.

Utilisateur de certificat – Entité ou personne physique qui utilise un certificat et qui s'y fie pour vérifier une signature électronique ou une authentification provenant d'un service applicatif ou d'une personne physique disposant d'un certificat dédié à cet usage.

N.B. : un agent d'une administration qui procède à des échanges électroniques avec une autre administration est, pour cette dernière, un usager.

Valideur – Personne physique qui valide une demande de certificat effectuée sur l'AE technique. Au sein du processus de demande de certificat dans Certilibre, les demandes sont validées par l'une de personnes suivantes qui assurent alors les fonctions de valideur dans la demande de certificat machine :

- le chef ou un des adjoints de l'unité du demandeur ;
- le chef ou un des adjoints de l'unité hiérarchiquement supérieure à l'unité du demandeur, quand ce dernier est le chef de son unité ;
- à titre exceptionnel, un administrateur de l'AE technique.

Dans tous les cas, le demandeur ne peut valider sa propre demande.

I.4. Entités intervenant dans l'IGC

I.4.1. Autorités de certification

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

Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats.

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI dans le domaine (cf. [ETSI_NQCP], la décomposition *fonctionnelle* de l'IGC qui est retenue dans la présente PC est la suivante :

- **Fonction de génération des éléments secrets** – Cette fonction génère des éléments secrets (clés privées) à partir des informations transmises par l'AE technique.
- **Fonction de génération des certificats** – Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'AE et de la clé publique du service provenant soit du RC, soit de la fonction de génération des éléments secrets du service, si c'est cette dernière qui génère la bi-clé du service applicatif.
- **Fonction de remise au RC –** Cette fonction remet au RC le certificat du service applicatif ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif de protection des éléments secrets, clé privée du service applicatif, codes d'activation,...).

- **Fonction de publication** – Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux RC et aux utilisateurs de certificats, hors informations d'état des certificats.
- **Fonction de gestion des révocations** – Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.
- **Fonction d'information sur l'état des certificats** – Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction est mise en œuvre par une publication à intervalles réguliers de LCR.

D'autres fonctions de l'IGC (contrôles d'identité, remise, révocation…) sont détaillées au chapitre ci-dessous.

D'autres entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment (voir les définitions au chapitre I.3.2 et les descriptions des fonctions dans les paragraphes suivants) :

- responsable du certificat
- utilisateur de certificat.

L'autorité de certification est le tiers de confiance de référence reconnu par l'ensemble de ses utilisateurs. À ce titre, l'AC engage sa responsabilité sur le respect des exigences décrites dans la présente PC, et s'engage à ce que les composantes de l'IGC, internes et externes à l'AC, respectent aussi les exigences qui les concernent.

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle sous-traite à des entités externes, l'AC s'engage, en tant que responsable de l'ensemble de l'IGC, au respect des exigences suivantes :

- Être une entité légale au sens de la loi française.
- Être en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats de services applicatifs de cette entité. L'AC peut aussi, le cas échéant, être en relation contractuelle / hiérarchique / réglementaire avec le ou les mandataires de certification choisis par l'entité.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux RC, aux utilisateurs de certificats, ceux qui mettent en œuvre ses certificats.
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, notamment en matière de génération des certificats, de remise au RC, de gestion des révocations et d'information sur l'état des certificats.
- Élaborer, mettre en œuvre, contrôler et maintenir de façon itérative les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, et correspondant au minimum aux exigences de la présente PC, notamment en termes de fiabilité, de qualité et de sécurité. À ce titre, elle doit posséder un ou des systèmes de gestion de la qualité et de la sécurité de l'information adaptés aux services de certification qu'elle assure.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats et de LCR), ou faire renouveler ses certificats si l'AC est

rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux RC et utilisateurs de certificats.
- Suivre les demandes en capacité et réaliser des projections concernant les futurs besoins en capacité afin de garantir la disponibilité du service, notamment en matière de capacité de traitement et de stockage.

I.4.2. Autorité d'enregistrement

L'AE technique a pour rôle de vérifier l'identité du futur RC et les informations liées au service applicatif. Pour cela, l'AE assure les tâches suivantes :

- La prise en compte et la vérification des informations du futur RC et du service applicatif, ainsi que de leur unité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- L'établissement et la transmission de la demande de certificat à la fonction de génération de l'IGC ;
- L'archivage du formulaire de demande de certificat ;
- La protection en confidentialité et en intégrité des données personnelles d'authentification du RC, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles). L'ensemble des flux sont chiffrés, y compris avec les autres fonctions de l'IGC.

L'AE de l'IGC/FSI est l'autorité qui vérifie les données propres aux utilisateurs souhaitant faire certifier leurs bi-clés par l'IGC/FSI. L'AE technique de l'IGC/FSI met à disposition un formulaire électronique de demande de certification et un formulaire papier de demande de révocation pour l'IGC/FSI.

I.4.3. Responsables de certificats électroniques de services applicatifs

Un RC est une personne physique qui est responsable de l'utilisation du certificat électronique identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'unité de rattachement du certificat.

Le RC respecte les conditions qui lui incombent définies dans cette PC.

Tout personnel de l'ANFSI ainsi que tout personnel de la chaîne SIC de la Gendarmerie nationale possède implicitement, du fait de ses fonctions et de son affectation, la qualité potentielle de RC. Cette qualité s'actualisera, pour un certificat donné, quand il exercera effectivement les fonctions qui lui sont associées concernant ledit certificat : demande de génération, de renouvellement, de révocation.

Le certificat est attaché, non au RC, mais à l'unité d'affectation du RC à l'origine de la première demande de certificat pour un service applicatif donné. Ce RC peut être amené à changer en cours de validité du certificat : départ du RC de l'entité, changement d'affectation et de responsabilité au sein de l'entité, etc. C'est la raison pour laquelle la génération et le renouvellement d'un certificat font l'objet d'une validation par un valideur *ad hoc*.

I.4.4. Utilisateurs de certificats

Un utilisateur de certificat électronique peut être notamment :

- Un serveur ou une personne qui exécute une application signée et qui souhaite l'authentifier avant de l'autoriser à accéder à des ressources sensibles.

- Une personne accédant à un serveur et qui utilise le certificat du serveur et un module de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat du serveur, afin d'établir une clé de session partagée entre son poste et le serveur.
- Un service applicatif accédant à un serveur informatique et qui utilise un certificat et un applicatif de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat, et afin d'établir une clé de session partagée entre les deux serveurs.
- Un service applicatif, A, auquel accède un autre service applicatif, B : A met en œuvre un applicatif de vérification d'authentification afin d'authentifier B, qui est identifié dans le certificat qu'il présente lors de sa connexion à A.

I.5. Usage des certificats

I.5.1. Domaines d'utilisation applicables

I.5.1.1 Bi-clés et certificats du service applicatif

Lorsque le certificat électronique délivré par le PSCE est un certificat d'**authentification d'un service applicatif serveur**, la fonction du certificat est l'authentification du service applicatif comme serveur auprès d'autres serveurs ou auprès de personnes, dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS ou IPsec visant à établir une clé symétrique de session afin que les échanges au sein de ces sessions soient chiffrés. L'établissement de la clé de session peut se faire par un mécanisme cryptographique asymétrique, de type RSA (génération de la clé symétrique par le client et chiffrement de cette clé symétrique par la clé publique du serveur) ou de type Diffie-Hellman (obtention de la clé symétrique via un algorithme combinant la clé privée du client et la clé publique du serveur, et inversement). De tels certificats sont désignés par [A-Srv] *infra*.

Lorsque le certificat électronique délivré par le PSCE est un certificat d'**authentification d'un service applicatif client**, la fonction du certificat est l'authentification du service applicatif comme client d'autres serveurs. De tels certificats sont désignés par [A-Clt] *infra*.

Lorsque le certificat électronique délivré par le PSCE est un certificat de **signature de code**, son usage est la signature électronique d'un code applicatif. De tels certificats sont désignés par [S-Code] *infra*.

I.5.1.2 Bi-clés et certificats d'AC et de composantes

Cette PC comporte également des exigences concernant les bi-clés et certificats de l'AC (signature des certificats des services applicatifs et des LCR) ainsi que des clés, bi-clés et certificats des composantes de l'IGC (sécurisation des échanges entre composantes, authentification des opérateurs, etc.).

L'AC génère et signe différents types d'objets : certificats et LCR. Pour signer ces objets, l'AC dispose d'une seule et même bi-clé, dont le certificat est émis par l'ACR. Cette bi-clé et ce certificat ne sont utilisés qu'à cette fin.

I.5.2. Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au IV.5 ci-dessous. L'AC doit respecter ces restrictions et imposer leur respect par les RC et ses utilisateurs de certificats.

À cette fin, elle doit communiquer à tous les RC et utilisateurs potentiels les termes et conditions relatives à l'utilisation du certificat.

I.6. Gestion de la PC

La gestion de la PC et de la DPC est décrite dans le chapitre B de [MESURES_IGC].

II. Responsabilités concernant la mise à disposition des informations devant être publiées

Voir chapitre C de [MESURES_IGC].

III. Identification et authentification

III.1. Nommage

III.1.1. Types de noms

Les noms utilisés sont conformes aux spécifications du [RGS].

Dans chaque certificat, l'AC émettrice (issuer) et le service applicatif (subject) sont identifiés par un « Distinguished Name » (DN).

III.1.2. Nécessité d'utilisation de noms explicites

III.1.2.1 Nommage des Autorités de Certification

Le DN de l'autorité de certification 2024 FSI AC Machines est construit comme suit :

Attribut	Valeur	Commentaires
C	FR	Pays
O	ANFSI	Organisation
OU	0002 130031404	Numéro SIREN de l'Agence du Numérique des Forces de Sécurité Intérieure, obligatoire pour le respect du [RGS]
CN	2024 FSI AC Machines	Identification de l'AC parmi celles de l'IGC/FSI

III.1.2.2 Nommage des services applicatifs

Les noms choisis pour désigner les services applicatifs dans les certificats sont explicites.

L'identification de l'entité à laquelle le service applicatif est rattaché est obligatoire.

Le DN des services applicatifs est défini dans le paragraphe VII.2. Par exemple, le DN peut être : C = FR, O = ANFSI, OU = 0002 130031404, OU = Machines, CN = igc.gendarmerie.fr

III.1.3. Pseudonymisation des services applicatifs

S'agissant de certificats délivrés à des services applicatifs, les notions d'anonymisation ou de pseudonymisation sont sans objet.

III.1.4. Règles d'interprétation des différentes formes de nom

Sans objet.

III.1.5. Unicité des noms

Afin d'assurer l'identification unique du service applicatif au sein du domaine de l'AC ainsi que l'entité à laquelle ce service est rattaché, notamment dans le cas du renouvellement du certificat associé et pour éviter toute ambiguïté, le DN du champ « *subject* » de chaque certificat électronique doit permettre d'identifier de façon unique ce service : cf. la construction du DN décrite au chapitre III.1.2.2.

L'AE technique n'autorise l'émission d'un nouveau certificat avec un DN déjà utilisé que si l'unité de rattachement du certificat est identique. Dans le cas contraire, la demande est enregistrée mais non transmise immédiatement à l'AC : les administrateurs de l'AE technique sont saisis. Ils se chargent de vérifier la conformité et l'opportunité de la demande : tel serait,

par exemple, le cas pour un service applicatif qui ne serait plus pris en charge par la même unité au sein de l'ANFSI.

III.1.6. Identification, authentification et rôle des marques déposées

L'AC est responsable de l'unicité des noms des services applicatifs utilisés dans ses certificats et de la résolution des litiges portant sur la revendication d'utilisation d'un nom.

III.2. Validation initiale de l'identité

L'enregistrement d'un service applicatif pour lequel un certificat doit être délivré se fait par la demande du RC correspondant effectuée auprès de l'AE technique. La connexion du RC à celle-ci est authentifiée grâce au certificat électronique d'authentification conforme aux exigences du niveau [RGS] ** contenu dans sa carte professionnelle, garantissant ainsi la validation initiale de son identité.

Le formulaire de demande de certificat sur l'AE technique est signé électroniquement par le RC, à l'aide d'un procédé de signature électronique conforme aux exigences du niveau [RGS] **. Le valideur vérifie et, s'il le juge opportun, valide la demande, également à l'aide d'un procédé de signature électronique conforme aux exigences du niveau [RGS] **. La vérification et la validation des signatures sont effectuées par l'AE technique.

[A-Clt][A-Srv] L'AE technique vérifie que le nom de domaine totalement qualifié sollicité dans la demande est conforme à la politique des noms de domaine de l'ANFSI.

III.2.1. Méthode pour prouver la possession de la clé privée

Lorsque la demande de certificat est réalisée avec une requête de certificat, le RC fournit à l'AC, via l'AE technique, une preuve de possession de la clé privée correspondant à la clé publique contenue dans la demande de certificat électronique, sous forme de requête de certificat au format *PKCS#10*, signée par la clé privée.

Pour les serveurs hébergés dans les centres de données pour lesquels le RC ne possède pas de droits d'accès en administration, la génération de la bi-clé et la signature du certificat sont réalisées respectivement par l'AE technique et par l'AC, dans les deux cas directement dans le boîtier cryptographique. Ces éléments font l'objet d'un double chiffrement avant transmission aux personnels chargés de leur déchiffrement :

- au moyen du certificat de chiffrement de la carte professionnelle des seuls personnels autorisés à les déchiffrer ;
- au moyen d'une clé publique dont la partie privée n'est présente que sur le poste déconnecté de tout réseau auquel lesdits personnels autorisés se connectent pour les déchiffrer.

Une fois déchiffré, ils sont remis aux groupes exploitants, chargés de leur déploiement sur les machines concernées, au moment de supports chiffrés. Ces opérations sont tracées sur l'outil de gestion de tickets.

III.2.2. Validation de l'identité d'un organisme

Sans objet.

III.2.3. Validation de l'identité d'un individu

III.2.3.1 Enregistrement d'un RC pour un certificat de service applicatif à émettre

Depuis l'AE technique, le futur RC renseigne un formulaire électronique de demande de certificat. Un document PDF est automatiquement généré. Il comprend :

- l'identité du demandeur : nom, prénom, grade ;
- l'unité d'appartenance du demandeur ;
- le nom du service applicatif pour lequel la demande est réalisée ;
- [A-Srv] les éventuels autres noms alternatifs sollicités ;
- le lien de téléchargement des conditions générales d'utilisation du certificat, ainsi que son condensé.

Ce document PDF est signé par le RC et contre-signé par le valideur, dans les deux cas à l'aide d'un procédé de signature électronique conforme aux exigences du niveau [RGS] **.

III.2.3.2 Enregistrement d'un nouveau RC pour un certificat électronique déjà émis

Le certificat étant attaché à une unité SIC de la Gendarmerie nationale ou de l'ANFSI et non au RC, ce dernier peut être amené à changer en cours de validité du certificat. C'est la raison pour laquelle chaque opération du cycle de vie (génération, révocation) peut être réalisée par le demandeur ou un personnel de l'unité de rattachement, *i.e.* l'unité dans laquelle le demandeur se trouvait quand il a effectué la demande initiale.

Tout personnel de l'unité de rattachement du certificat peut demander, après validation du valideur *ad hoc*, le renouvellement du certificat afin d'assurer la continuité d'activité.

III.2.4. Informations non vérifiées du RC et du service applicatif

Sans objet.

III.2.5. Validation de l'autorité du demandeur

Cette validation est faite par l'AE lors de l'enregistrement du RC.

III.3. Identification et validation d'une demande de renouvellement des clés

Le renouvellement de la bi-clé d'un service applicatif entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat de service applicatif ne peut pas être fourni au RC sans renouvellement de la bi-clé correspondante (cf. chapitre IV.6).

III.3.1. Identification et validation pour un renouvellement courant

À chaque renouvellement, l'AE, saisie de la demande, identifie le RC et le service applicatif selon la même procédure que pour l'enregistrement initial.

III.3.2. Identification et validation pour un renouvellement après révocation

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial.

III.4. Identification et validation d'une demande de révocation

Les exigences concernant les informations à fournir dans une demande de révocation sont décrites au chapitre IV.9.3

La demande de révocation peut être effectuée par tout personnel de l'unité de rattachement du certificat. Elle est réalisée par écrit dans un formulaire signé (manuellement ou éventuellement de manière électronique), et transmise à un administrateur de l'AC.

IV. Exigences opérationnelles sur le cycle de vie des certificats

IV.1. Demande de certificat

IV.1.1. Origine d'une demande de certificat

Un certificat peut être demandé par tout personnel SIC de la Gendarmerie nationale et de l'ANFSI.

De façon exceptionnelle, quand un demandeur n'est pas affecté dans une unité SIC de la Gendarmerie ou à l'ANFSI, il transmet aux administrateurs de l'AE technique par courriel sa demande de certificat au format *PKCS#10*, accompagnée du formulaire de demande signé (manuellement ou éventuellement de manière électronique). Un administrateur de l'AE technique endosse alors le rôle de RC pour procéder à l'enregistrement de la demande et à la génération du certificat. Il modifie ensuite l'unité de rattachement de la demande, afin d'assurer le suivi du cycle de vie du certificat par l'unité d'affectation du demandeur.

IV.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat

Le processus est détaillé au chapitre III.2.

IV.2. Traitement d'une demande de certificat

IV.2.1. Exécution des processus d'identification et de validation de la demande

Les identités « personne physique » sont vérifiées conformément aux exigences du chapitre III.2. L'AE effectue les opérations suivantes :

- validation de l'identité du RC ;
- vérification de la cohérence du formulaire renseigné en ligne ;
- vérification de la prise de connaissance par le RC des modalités applicables pour l'utilisation du certificat ;
- [A-Clt][A-Srv] vérification de la cohérence du nom de domaine totalement qualifié que présentera le certificat avec la politique des noms de domaine de l'ANFSI.

Une fois ces opérations effectuées, l'AE technique enregistre la demande de génération du certificat. Elle conserve le formulaire de demande signé électroniquement ainsi que, le cas échéant, la requête de certificat au format *PKCS#10*.

IV.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le RC en justifiant le rejet.

IV.2.3. Durée d'établissement du certificat

Les certificats sont générés immédiatement à la réception de la demande, en cas d'acceptation de celle-ci.

IV.3. Délivrance du certificat

IV.3.1. Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande (notamment vérification de l'intégrité de la requête *PKCS#10* constituant la preuve de possession de la clé privée), l'AE technique déclenche la fonction de génération du certificat par l'AC.

Lorsque le demandeur n'est pas administrateur du serveur sur lequel le certificat sera déployé, le certificat et sa clé privée sont générés directement dans le boîtier cryptographique et mis à disposition de l'administrateur grâce au double chiffrement évoqué au chapitre III.2.1.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres D et E de [MESURES_IGC], notamment la séparation des rôles de confiance (*cf.* chapitre D.2).

IV.3.2. Notification par l'AC de la délivrance du certificat au RC

L'AC transmet automatiquement le certificat généré à l'AE technique. Celle-ci envoie par courrier électronique le certificat au RC et le rend également disponible à tous les membres de son unité via un lien de téléchargement dans l'application.

IV.4. Acceptation du certificat

IV.4.1. Démarche d'acceptation du certificat

Dès l'envoi du courriel évoqué au chapitre IV.3.2, le RC peut signaler son refus du certificat aux administrateurs de l'AE technique, ce qui aura pour conséquence sa révocation. Il lui revient donc d'en vérifier le contenu avant toute installation.

L'absence de retour du RC et, *a fortiori*, l'installation effective du certificat sur le serveur de destination vaut acceptation tacite du certificat.

IV.4.2. Publication du certificat

Le certificat ne fait pas l'objet d'une publication par l'AC. Le RC peut publier le certificat avec ses moyens propres et seulement s'il le souhaite.

IV.4.3. Notification par l'AC aux autres entités de la délivrance du certificat

Cf. chapitre IV.3.2.

IV.5. Usages de la bi-clé et du certificat

IV.5.1. Utilisation de la clé privée et du certificat par le RC

L'utilisation de la clé privée du service applicatif et du certificat associé est strictement limitée à la fonction de sécurité concernée : cf. chapitre I.5.1.1. Les RC doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

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

usage est également clairement explicité dans cette PC, ainsi que dans les conditions générales d'utilisation. Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du RC par l'AC avant d'entrer en relation contractuelle.

IV.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Cf. chapitre précédent et chapitre I.5

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

IV.6. Renouvellement d'un certificat

La notion de renouvellement de certificat, conformément au [RFC3647], correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique du service applicatif).

Cependant, dans la cadre de la présente PC, et comme précisé par les conditions générales d'utilisation, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. L'AC de son côté est configurée afin de refuser toute certification de clé publique pour laquelle elle aurait déjà émis un certificat.

IV.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé

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

IV.7.1. Causes possibles de changement d'une bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des services applicatifs, et les certificats correspondants, seront renouvelés au minimum à une fréquence définie au chapitre VI.3.2.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à :

- la révocation du certificat du service applicatif (cf. chapitre IV.9, notamment le chapitre IV.9.1.1 pour les différentes causes possibles de révocation) ;
- la modification du CN et/ou des noms alternatifs présents dans le certificat.

Nota – Dans la suite du présent chapitre, le terme utilisé est « fourniture d'un nouveau certificat ».

IV.7.2. Origine d'une demande d'un nouveau certificat

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

L'entité peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un service applicatif qui lui est rattaché.

Afin d'éviter l'expiration non anticipée d'un certificat, l'AC peut prévenir le RC de l'approche de la fin de vie du certificat et l'inviter à procéder au renouvellement.

IV.7.3. Procédure de traitement d'une demande d'un nouveau certificat

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre III.3 ci-dessus.

Pour les actions de l'AC, cf. chapitre IV.3.1

IV.7.4. Notification au RC de l'établissement du nouveau certificat

Cf. chapitre IV.3.2

IV.7.5. Démarche d'acceptation du nouveau certificat

Cf. chapitre IV.4.1

IV.7.6. Publication du nouveau certificat

Cf. chapitre IV.4.2

IV.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Cf. chapitre IV.4.3

IV.8. Modification du certificat

La modification d'un certificat, conformément au [RFC3647], correspond à des modifications d'informations sans changement de la clé publique (cf. chapitre IV.7) et autres qu'uniquement la modification des dates de validité (cf. chapitre IV.6).

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

IV.9. Révocation et suspension des certificats

IV.9.1. Causes possibles d'une révocation

IV.9.1.1 Certificats de services applicatifs

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

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

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

IV.9.1.2 Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats ou la signature de LCR) :

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

IV.9.2. Origine d'une demande de révocation

IV.9.2.1 Certificats de services applicatifs

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

- le RC pour le service applicatif considéré ;
- toute personne affectée dans l'unité de rattachement du certificat ;
- l'AC.

IV.9.2.2 Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice. La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

IV.9.3. Procédure de traitement d'une demande de révocation

IV.9.3.1 Révocation d'un certificat électronique

IV.9.3.1.1 Révocation par le RC

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre III.4.

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

- le nom du service applicatif figurant dans le certificat ;
- le nom du demandeur de la révocation ;
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (numéro de série,...) ;
- éventuellement, la cause de révocation.

Le traitement de la demande est décrit au chapitre IV.9.3.1.4 ci-dessous.

IV.9.3.1.2 Révocation par l'AE

Cf. chapitre IV.9.3.1.3.

IV.9.3.1.3 Révocation par l'AC émettrice du certificat

Un opérateur de l'AC peut directement révoquer, de façon exceptionnelle, un certificat émis par cette AC.

La demande de révocation est enregistrée dans le système, avec les données suivantes :

- le nom du service applicatif figurant dans le certificat ;
- l'identité de l'opérateur agissant pour le compte de l'AC ;
- le numéro de certificat à révoquer ;
- la cause de la révocation (obligatoire dans ce cas)

Le traitement de la demande est décrit au chapitre IV.9.3.1.4 ci-dessous.

IV.9.3.1.4 Traitement de la demande de révocation

Une fois la demande authentifiée et contrôlée, un administrateur l'AC (via sa fonction de gestion des révocations) révoque le certificat correspondant en changeant son statut. Ce nouveau statut est communiqué à la fonction d'information sur l'état des certificats et l'information de révocation est diffusée via une LCR signée par l'AC elle-même.

Le demandeur de la révocation et le RC sont informés du bon déroulement de l'opération et de la révocation effective du certificat.

L'opération est enregistrée dans les journaux d'événements avec toutes les informations disponibles sur les causes initiales ayant entraîné la révocation du certificat (ces causes ne sont pas publiées).

IV.9.3.2 Révocation d'un certificat d'une composante de l'IGC

Le document [MESURES_IGC] précise les procédures mises en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.

IV.9.4. Délai accordé au RC pour formuler la demande de révocation

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

IV.9.5. Délai de traitement par l'AC d'une demande de révocation

IV.9.5.1 Révocation d'un certificat de service applicatif

Par nature, une demande de révocation doit être traitée en urgence.

IV.9.5.2 Disponibilité du système de traitement des demandes de révocation

La fonction de gestion des révocations est disponible 24h/24 et 7j/7. Cette fonction a une durée maximale d'indisponibilité de 4h par interruption de service (panne ou maintenance) et de 12 incidents cumulés sur un an.

Toute demande de révocation d'un certificat est traitée dans un délai inférieur à 72h. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs (publication de la LCR).

IV.9.5.3 Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un événement décrit dans les causes de révocation possibles pour ce type de certificat. La

révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat, et que cette liste est accessible au téléchargement.

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

IV.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat électronique est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante par consultation des LCR et LAR appropriées.

IV.9.7. Fréquence d'établissement et durée de validité des LCR

Les LCR sont publiées avec une fréquence minimale de 24h.

Afin d'assurer une continuité du service dans le cas où un incident sur la publication des LCR survienne, la durée de validité des LCR est de 6 jours.

L'AC objet de cette PC n'a pas d'AC subordonnées et ne publie donc pas de LAR. Se référer à [PC_AC_RACINE] pour obtenir des informations sur les fréquence et durée de vie des LAR concernant l'AC de cette PC.

IV.9.8. Délai maximum de publication d'une LCR

Une fois générées, les LCR sont publiées immédiatement et en tout état de cause dans un délai maximum de 30 minutes suivant leur génération.

IV.9.9. Exigences sur la vérification en ligne de la révocation et de l'état des certificats

Sans objet : l'AC ne propose pas de service en ligne OCSP.

IV.9.10. Autres moyens disponibles d'information sur les révocations

Sans objet.

IV.9.11. Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de services applicatifs, les entités autorisées à effectuer une demande de révocation sont tenues de le faire sans délai après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC, outre les exigences du chapitre IV.9.3.2, la révocation suite à une compromission de la clé privée doit faire l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

IV.9.12. Causes possibles d'une suspension

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

IV.9.13. Origine d'une demande de suspension

Sans objet.

IV.9.14. Procédure de traitement d'une demande de suspension

Sans objet.

IV.9.15. Limites de la période de suspension d'un certificat

Sans objet.

IV.10. Fonction d'information sur l'état des certificats

IV.10.1. Caractéristiques opérationnelles

Des LCR et des LAR sont mises à la disposition des utilisateurs de certificats pour vérifier le statut d'un certificat final, y compris celui des AC de sa chaîne de certification. Ces LCR / LAR sont au format V2.

IV.10.2. Disponibilité de la fonction d'information sur l'état des certificats

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

Cette fonction a une durée maximale d'indisponibilité de 1h par interruption de service (panne ou maintenance) et de 12 incidents cumulés sur un an.

IV.10.3. Dispositifs optionnels

Sans objet.

IV.11. Fin de la relation entre le RC et l'AC

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

De plus, l'AC doit révoquer un certificat électronique pour lequel il n'y a plus de RC explicitement identifié. Pour éviter cela, les certificats sont rattachés à une unité, et tous les personnels de cette unité ont une vision des certificats générés dans l'interface de l'AE technique.

IV.12. Séquestre de clé et recouvrement

Les clés privées des services applicatifs et les clés privées d'AC ne sont en aucun cas séquestrées.

IV.12.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

IV.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

V. Mesures de sécurité non techniques

Voir [MESURES_IGC].

VI. Mesures de sécurité techniques

Pour tout ce qui concerne les clés d'AC, se référer à [MESURES_IGC].

VI.1. Génération et installation de bi-clés

VI.1.1. Génération des bi-clés

VI.1.1.1 Clés du service applicatif générées par l'AE technique

Les bi-clés des services applicatifs sont générés par l'AE technique dans un module cryptographique qualifié au niveau renforcé. La clé privée sera ensuite transférée de manière sécurisée au service applicatif : cf. chapitre VI.1.2. La requête de certificat au format *PKCS#10* est récupérée par l'AE technique pour être transmise à l'AC : cf. chapitre VI.1.3.

VI.1.1.2 Clés du service applicatif générées au niveau du service applicatif

Les bi-clés du service applicatif générées au niveau du service applicatif sont générées par le RC sur l'équipement administré par le RC et sur lequel le certificat sera déployé. Seule la requête de certificat au format *PKCS#10* est extraite pour être transmise à l'AE technique.

Les conditions générales d'utilisation précisent les modalités à mettre en œuvre pour sécuriser la clé privée.

VI.1.2. Transmission de la clé privée à son propriétaire

Les bi-clés des services applicatifs générés par l'AE technique sont transmises aux personnels autorisés à les déchiffrer de façon sécurisée conformément aux modalités décrites au chapitre III.2.1.

Une fois déchiffrées, elles sont remises sur un support chiffré au personnel administrant l'équipement sur lequel le certificat sera déployé.

La traçabilité de ces étapes est assurée par un outil de gestion de tickets.

Le présent paragraphe ne concerne que les clés générées par l'AE technique conformément au chapitre VI.1.1.1

VI.1.3. Transmission de la clé publique à l'AC

Qu'elles soient générées par le RC ou directement par l'AE technique, les requêtes de certification *PKCS#10* transitent toutes par cette dernière.

Afin de protéger la clé publique en intégrité et d'authentifier son origine, les communications entre l'AE technique et l'AC sont effectuées selon le protocole TLS avec authentification du client par un certificat.

VI.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats

Les clés publiques de vérification de signature de l'AC sont diffusées auprès des utilisateurs de certificats via le certificat de l'AC publié conformément aux dispositions du chapitre II. La chaîne de certification remonte jusqu'au certificat de l'ACR.

VI.1.5. Tailles des clés

Les clés d'AC sont des clés RSA 4096 bits.

Les clés des services applicatifs sont des clés RSA de 2048 ou de 3072 bits.

Ces caractéristiques sont conformes à l'état de l'art et respectent les exigences de sécurité du [RGS].

VI.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité

Les bi-clés générées conformément au chapitre VI.1.1.1 le sont dans des composants qualifiés (HSM). La qualité des bi-clés et leurs paramètres de génération dépendant des équipements utilisés et ces derniers étant qualifiés dans ce cadre, elles sont réputées conformes à l'état de l'art tant que la qualification est maintenue.

Pour les autres, l'AE technique vérifie au travers de la fourniture de la demande de certificat au format *PKCS#10* que l'algorithme utilisé est conforme aux attendus. Comme indiqué dans les conditions générales d'utilisation, le RC s'engage à n'utiliser que la bibliothèque système `openssl`, dans une version à jour et toujours maintenue, pour générer ses bi-clés.

VI.1.7. Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats ou de LCR / LAR.

L'utilisation de la clé privée du service applicatif et du certificat associé est strictement limitée à la fonction de sécurité concernée (cf. section I.5.1.1).

VI.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

VI.2.1. Standards et mesures de sécurité pour les modules cryptographiques

VI.2.1.1 Modules cryptographiques de l'AC

Les clés privées des AC sont générées et restent protégées par un dispositif cryptographique qualifié (HSM) au niveau renforcé.

VI.2.1.2 Dispositifs de protection des éléments secrets du service applicatif

Le RC s'engage contractuellement à protéger les clés privées relevant de leur responsabilité, conformément aux dispositions des conditions générales d'utilisation.

VI.2.2. Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC doit être assuré par un personnel de confiance : porteur de secrets d'IGC.

VI.2.3. Séquestre de la clé privée

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

VI.2.4. Copie de secours de la clé privée

La clé privée de l'AC ne peut être exportée du module cryptographique qualifié au niveau renforcé qui la contient que sous forme chiffrée. Seul le secret dudit module permet de la déchiffrer à la restauration.

Les clés privées des services applicatifs peuvent faire l'objet de copie de secours, à la discrétion du RC.

Une sauvegarde des clés privées générées par l'AE technique est présente dans le poste chiffré et déconnecté de tout réseau évoqué au chapitre III.2.1.

VI.2.5. Archivage de la clé privée

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

VI.2.6. Transfert de la clé privée vers / depuis le module cryptographique

Tout transfert (sauvegarde, restauration) se fait sous forme chiffrée.

VI.2.7. Stockage de la clé privée dans un module cryptographique

Les clés privées d'AC sont stockées dans un module cryptographique qualifié au niveau renforcé, excepté leurs sauvegardes qui respectent des exigences du chapitre VI.2.4.

VI.2.8. Méthode d'activation de la clé privée

VI.2.8.1 Clés privées d'AC

La méthode d'activation des clés privées d'AC dépend du module cryptographique qualifié au niveau renforcé utilisé pour conserver ces clés. Elle répond ainsi aux exigences réglementaires en vigueur. Elle fait intervenir en outre au moins une personne ayant au moins un rôle de confiance : officier de sécurité.

VI.2.8.2 Clés privées des services applicatifs

Les clés privées générées par l'AE technique sont transmises chiffrées au RC, sans donnée d'activation associée.

VI.2.9. Méthode de désactivation de la clé privée

VI.2.9.1 Clés privées des d'AC

La désactivation des clés privées d'AC dans le module cryptographique est automatique dès l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

VI.2.9.2 Clés privées des services applicatifs

Sans objet.

VI.2.10. Méthode de destruction des clés privées

VI.2.10.1 Clés privées des d'AC

La destruction des clés privées d'AC dans le matériel cryptographique est réalisée par une fonction nominale du matériel qui garantit un effacement sécurisé. La destruction des sauvegardes est réalisée de façon systématique et sécurisée en fin de vie d'une clé privée d'AC, normale ou anticipée (révocation).

VI.2.10.2 Clés privées des services applicatifs

En fin de vie de la clé privée d'un service applicatif, il est de la responsabilité du RC de s'assurer de sa suppression effective de l'équipement sur lequel elle était déployée.

VI.2.11. Niveau de qualification du module cryptographique et des dispositifs de protection des éléments secrets

Sans objet en l'absence de délivrance de tout dispositif de protection par le prestataire de service de certification électronique.

VI.3. Autres aspects de la gestion des bi-clés

VI.3.1. Archivage des clés publiques

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

VI.3.2. Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des services applicatifs couverts par la présente PC ont une durée de vie maximale de 3 ans.

L'AC s'interdit d'émettre des certificats dont la durée de vie dépasse celle du certificat de l'AC.

VI.4. Données d'activation

VI.4.1. Génération et installation des données d'activation

VI.4.1.1 Génération et installation des données d'activation correspondant à la clé privée de l'AC

La génération et l'installation des données d'activation du module cryptographique de l'AC se font lors de la phase d'initialisation et de personnalisation de ce module, dans le cadre d'une cérémonie de clés. Le porteur de ces données en est le détenteur exclusif : il les reçoit directement en main propre et est responsable de leur confidentialité et de leur intégrité.

VI.4.1.2 Génération et installation des données d'activation correspondant à la clé privée du service applicatif

Sans objet.

VI.4.2. Protection des données d'activation

VI.4.2.1 Protection des données d'activation correspondant aux clés privées de l'AC

Les données d'activation qui sont générées par l'AC pour les modules cryptographiques de l'IGC doivent être protégées en intégrité et en confidentialité jusqu'à la remise à leur

destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

VI.4.2.2 Protection des données d'activation correspondant aux clés privées des services applicatifs

Sans objet.

VI.4.3. Autres aspects liés aux données d'activation

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

VI.5. Mesures de sécurité des systèmes informatiques

Voir [MESURES_IGC].

VI.6. Mesures de sécurité des systèmes durant leur cycle de vie

Voir [MESURES_IGC].

VI.7. Mesures de sécurité réseau

Voir [MESURES_IGC].

VI.8. Horodatage / Système de datation

Voir [MESURES_IGC].

VII. Profils des certificats et des LCR

VII.1. Format du certificat de 2024 FSI AC Machines

Nom du champ	Contenu
Champs de base	
Version **(version)**	2 (version 3)
Numéro de série **(serialNumber)**	Attribué par l'ACR
Algorithme de signature **(signature)**	Algorithme RSA / SHA-2 : • Champ « algorithm » : sha256WithRSAEncryption • Champ « parameters » : non présent
Émetteur **(issuer)**	C = FR O = ANFSI OU = 0002 130031404 CN = 2024 FSI AC Racine
Valide à partir du **(validity/notBefore)**	Date de génération par l'ACR
Valide jusqu'au **(validity/notAfter)**	Maximum 12 ans après la date de génération
Objet **(subject)**	C = FR O = ANFSI OU = 0002 130031404 CN = 2024 FSI AC Machines
Clé publique **(subjectPublicKeyInfo)**	Algorithme RSA : • Champ « algorithm/algorithm » : rsaEncryption • Champ « algorithm/parameters » : non présent • Champ « subjectPublicKey » : clé publique de 4096 bits
Extensions	
Contraintes de base **(basicConstraints)** **Critique**	Champ « cA » : TRUE (certificat d'autorité de certification) Champ « pathLenConstraint » : 0 (cette AC est une AC terminale)
Identifiant de clé d'autorité **(authorityKeyIdentifier)** **Non critique**	Valeur « subjectKeyIdentifier » du certificat de l'ACR de l'IGC/FSI. Seul le champ « keyIdentifier » sera utilisé

Nom du champ	Contenu
Identifiant de clé de sujet (subjectKeyIdentifier) Non critique	Empreinte numérique de la clé publique de l'objet.
Utilisation de clé (keyUsage) Critique	Signature de certificats, Signature de listes des certificats révoqués (keyCertSign, cRLSign)
Politiques de certification (certificatePolicies) Non critique	Champ « policyIdentifier » : contient l'identifiant de la politique de certification régissant cette AC, du type : OID = 1.2.250.1.668.1.1.1.6 Champ « policyQualifiers » : contient un champ « PolicyQualifierInfo » de type « CPS » contenant une adresse web pointant vers la page web des PC : URI = http://igc.gendarmerie.fr
Points d'accès aux LCR/LAR (cRLDistributionPoints) Non critique	URI=http://crl.gendarmerie.fr/2024_fsi_ac_racine.crl URI=http://crl.gendarmerie.interieur.gouv.fr/2024_fsi_ac_racine.crl URI=http://crl.gendarmerie.interieur.ader.gouv.fr/2024_fsi_ac_racine.crl URI=http://crl.gendarmerie.interieur.rie.gouv.fr/2024_fsi_ac_racine.crl
Accès aux informations de l'AC (authorityInfoAccess) Non critique	Champ « accessMethod » : id-ad-calssuers Champ « accessLocation » : http://crl.gendarmerie.fr/2024_fsi_ac_racine.der http://crl.gendarmerie.interieur.gouv.fr/2024_fsi_ac_racine.der http://crl.gendarmerie.interieur.ader.gouv.fr/2024_fsi_ac_racine.der http://crl.gendarmerie.interieur.rie.gouv.fr/2024_fsi_ac_racine.der Non critique

VII.2. Format des certificats des services applicatifs

Nom du champ	Contenu
Champs de base	
Version (version)	2 (version 3)

Nom du champ	Contenu
Numéro de série (serialNumber)	Attribué par l'2024 FSI AC Machines
Algorithme de signature (signature)	Algorithme RSA / SHA-2 : • Champ « algorithm » : sha256WithRSAEncryption • Champ « parameters » : non présent
Émetteur (issuer)	C = FR, O = ANFSI, OU = 0002 130031404, CN = 2024 FSI AC Machines
Valide à partir du (validity/notBefore)	Date de génération par l'2024 FSI AC Machines
Valide jusqu'au (validity/notAfter)	Maximum 3 ans après la date de génération
Objet (subject)	C = FR O = ANFSI OU = 0002 130031404 OU = Machines CN= *Le CN est défini de la manière suivante :* • ***[A-Srv]*** : **‹nom de domaine totalement qualifié›** Nom de domaine totalement qualifié du service applicatif pour lequel un certificat est émis, correspondant à la politique des noms de domaine de l'ANFSI. => ex. : igc.gendarmerie.fr => pour les certificats de test : AAAAMMJJ-testX.gendarmerie.fr, AAAAMMJJ-testX.police.fr ou AAAAMMJJ-textX.intranet • ***[A-Clt]*** : **‹nom de domaine totalement qualifié›** Un nom de domaine totalement qualifié explicite pour le RC et correspondant à la politique de noms de domaine de l'ANFSI mais non résolu pour autant. => ex. : appli1-client-appli2.intranet *=> pour les certificats de test : AAAAMMJJ-test-clientX.gendarmerie.fr, AAAAMMJJ-test-clientX.police.fr ou AAAAMMJJ-test-clientX.intranet* • ***[S-Code]*** : **‹nom de l'unité de rattachement du certificat›.signature** Le CN ne doit pas contenir un nom de domaine totalement qualifié, *Fully Qualified Domain Name* ou *FQDN*. => ex. : anfsi.signature => pour les certificats de test : AAAAMMJJ-testX.signature Dans tous les cas, pour les certificats de test : • AAAA : numéro d'année ; • MM : numéro de mois ; • JJ : numéro de jour ;

Nom du champ	Contenu
	• X : numéro d'ordre, si plusieurs tests le même jour.
Clé publique **(subjectPublicKeyInfo)**	Algorithme RSA : • Champ « algorithm/algorithm » : rsaEncryption • Champ « algorithm/parameters » : non présent • Champ « subjectPublicKey » : clé publique de 2048 bits (exception interdite après le 31/12/2025) ou 3072 bits (par défaut)
Extensions	
Contraintes de base **(basicConstraints)** **Critique**	Champ « CA » : FALSE (certificat d'entité finale) Champ « pathLenConstraint » : non présent (pas de signification)
Identifiant de clé d'autorité **(authorityKeyIdentifier)** **Non critique**	Valeur « subjectKeyIdentifier » du certificat de l'AC émettrice Seul le champ « keyIdentifier » sera utilisé
Identifiant de clé de sujet **(subjectKeyIdentifier)** **Non critique**	Empreinte numérique de la clé publique de l'objet.
Utilisation de clé **(keyUsage)** **Critique**	[A-Srv] Digital Signature, Key Encipherment [A-Clt] Digital Signature [S-Code] Digital Signature
Utilisation étendue de clé **(extendedKeyUsage)** **Non critique**	[A-Srv] id-kp-serverAuth [A-Clt] id-kp-clientAuth [S-Code] id-kp-codeSigning
Politiques de certification **(certificatePolicies)** **Non critique**	Champ « policyIdentifier » : contient l'identifiant de la politique de certification régissant cette AC, du type : OID = 1.2.250.1.668.1.1.1.7.1 Champ « policyQualifiers » : contient un champ « PolicyQualifierInfo » de type « CPS » contenant une adresse web pointant vers la page web des PC : URI = http://igc.gendarmerie.fr URI = https://www.gendarmerie.interieur.gouv.fr/igc/pc
Points d'accès aux LCR/LAR **(cRLDistributionPoints)** **Non critique**	URI = http://crl.gendarmerie.fr/2024_fsi_ac_machines.crl URI = http://crl.gendarmerie.interieur.gouv.fr/2024_fsi_ac_machines.crl URI = http://crl.gendarmerie.interieur.ader.gouv.fr/2024_fsi_ac_machines.crl URI =

Nom du champ	Contenu
	http://crl.gendarmerie.interieur.rie.gouv.fr/2024_fsi_ac_machines.crl
Accès aux informations de l'AC **(authorityInfoAccess)** **Non critique**	AccessMethod : OID 1.3.6.1.5.5.7.48.2 : id-ad-calssuers accessLocation : URI = http://crl.gendarmerie.fr/2024_fsi_ac_machines.der URI = http://crl.gendarmerie.interieur.gouv.fr/2024_fsi_ac_machines.der URI = http://crl.gendarmerie.interieur.ader.gouv.fr/2024_fsi_ac_machines.der URI = http://crl.gendarmerie.interieur.rie.gouv.fr/2024_fsi_ac_machines.der
Noms alternatifs du sujet **(subjectAlternativeNames)** **Non critique**	[A-Clt][A-Srv] *a minima* le CN, éventuellement accompagnés d'autres noms de domaine totalement qualifiés et/ou adresses IP.

VII.3. Format des listes de révocation (LCR) émises par l'2024 FSI AC Machines

Nom du champ	Contenu
Champs de base	
Version **(version)**	1 (version 2)
Algorithme de signature **(signature)**	Algorithme RSA / SHA-2 : • Champ « algorithm » : sha256WithRSAEncryption • Champ « parameters » : non présent
Émetteur **(issuer)**	C = FR O = ANFSI OU = 0002 130031404 CN= 2024 FSI AC Machines
Date d'émission **(thisUpdate)**	Date de génération par l'AC
Date de prochaine mise à jour **(nextUpdate)**	6 jours après la date de génération
Liste des certificats révoqués	
Numéro de série	Numéro de série du certificat révoqué

Nom du champ	Contenu
(userCertificat)	
Date de révocation (revocationDate)	Date de révocation du certificat
Extensions de la CRL	
Identifiant de clé d'autorité (authorityKeyIdentifier) Non critique	Valeur « subjectKeyIdentifier » du certificat de l'AC émettrice Seul le champ « keyIdentifier » sera utilisé
Numéro de CRL (CRLNumber) Non critique	Numéro séquentiel de la CRL
Empreinte numérique signée (signatureValue)	Suite de bits contenant le bloc de données signé par l'émetteur

VIII. Audit de conformité et autres évaluations

Voir [MESURES_IGC].

IX. Autres problématiques métiers et légales

Voir [MESURES_IGC].

Annexe 1 : Documents cités en référence

I.1. Documents techniques

[RGS]	Référentiel Général de Sécurité – Version 2.0
[RGS_A3]	RGS – Politiques de Certification Type – certificats électroniques de services applicatifs – Version 3.0
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, Version 2.03
[ETSI_NQCP]	ETSI TS 102 042 V1.3.4 (décembre 2007) Policy Requirements for Certification Authorities issuing public key certificates
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version d'août 2005 (complétée par les correctifs techniques Corrigendum 1 de janvier 2007et Corrigendum 2 de novembre 2008)
[PC_AC_RACINE]	Politique de certification de l'AC Racine FSI
[GESTION_ROLES]	Rôles et responsabilités de l'IGC de l'ANFSI
[Cessation d'activité]	Procédure_cessation_activité
[MESURES_IGC]	Mesures de sécurité communes : OID 1.2.250.1.668.1.1.1.8.1