MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

ANFSI

IGC DES FORCES DE SÉCURITÉ INTÉRIEURE

POLITIQUE DE CERTIFICATION
2024 FSI AC Personnes

1.2.250.1.668.1.1.1.2.1
1.2.250.1.668.1.1.1.3.1
1.2.250.1.668.1.1.1.4.1

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

HISTORIQUE DES MODIFICATIONS

Version	Date	Objet de la modification	Auteur	Statut
0.1	12/2023	Version initiale		projet
0.2	03/2024	Compléments	CNE MRDQ	projet
1	22/05/2024	Validation par autorité administrative	ANFSI	Validé

Table des matières

I. Introduction

I.1. Présentation générale

I.1.1. Objet du document

L'ANFSI a mis en place et exploite une infrastructure à gestion de 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) des autorités de certification (AC) subordonnées suivantes :

- 2024 FSI AC Personnes Authentification (1.2.250.1.668.1.1.1.2.1)
- 2024 FSI AC Personnes Chiffrement (1.2.250.1.668.1.1.1.3.1)
- 2024 FSI AC Personnes Signature (1.2.250.1.668.1.1.1.4.1)

Dans le cadre de cette politique de certification, ces AC émettent des certificats pour les personnes physiques relevant de l'ANFSI (personnels gendarmerie, aumôniers militaires de la GN ou personnels civil relevant du P152), chacune pour l'usage unique spécifié dans son nom.

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

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

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/FSI.

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/FSI, 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 et a été élaborée à partir de la PC Type du RGS. Concernant spécifiquement le certificat de signature, cette PC vise la conformité aux exigences de signature eIDAS selon la norme *ETSI EN 319 411-2* au niveau *QCP-n-qscd*.

I.1.2. Architecture de l'IGC

L'architecture de l'IGC/FSI est composée de :

- l'AC racine FSI dont le certificat est auto-signé ;

- trois AC subordonnées internes pour la production de certificats pour les personnes physiques :
  - une AC subordonnée « 2024 FSI AC Personnes Authentification » pour l'authentification,
  - une AC subordonnée « 2024 FSI AC Personnes Chiffrement » pour le chiffrement,
  - une AC subordonnée « 2024 FSI AC Personnes Signature » pour la signature ;
- une AC subordonnée interne « 2024 FSI AC Cachet Serveur » pour la production de certificats de signature pour les machines ;
- une AC subordonnée interne « 2024 FSI AC Machines » pour la production de certificats pour les machines ;
- une AC non signée par la racine, servant à la production de certificats de tests.

Les certificats issus d'AC subordonnées à l'AC Racine sont limités à un usage professionnel dans le cadre des échanges internes au ministère de l'Intérieur, ou dans le cadre d'échanges avec d'autres organismes.

En ce qui concerne les certificats issus des AC « 2024 FSI AC Cachet Serveur » et « 2024 FSI AC Machines », leur usage n'est autorisé que :

- sur les équipements des forces de sécurité intérieure mis en place par le STIG ou l'ANFSI et ne contrevenant pas aux dispositions de la PSSI,
- sur des équipements relevant de la sécurité intérieure administrés par la gendarmerie.

I.2. Identification du document

Ce document constitue la Politique de Certification (PC) pour les 3 AC subordonnées ci-dessous, qui partagent une grande majorité de leurs processus de gestion des certificats. Cette même PC est identifiée indifféremment par chacun des OID associés aux AC données le tableau ci-dessous :

AC	OID	Usage
2024 FSI AC Personnes Authentification	1.2.250.1.668.1.1.1.2.1	Authentification
2024 FSI AC Personnes Chiffrement	1.2.250.1.668.1.1.1.3.1	Confidentialité
2024 FSI AC Personnes Signature	1.2.250.1.668.1.1.1.4.1	Signature

L'OID est ainsi construit :

{iso(1) member-body(2) fr(250) type-org(1) ANFSI(668) igc(1) documentation(1) PC(1) Usage(X) révision(1)]

I.3. Définitions et acronymes

I.3.1. Acronymes

AA	Autorité Administrative
AC	Autorité de Certification
AGECAPE	Application de Gestion des Cartes Professionnelles Électroniques
AE	Autorité d'Enregistrement
APSE	Automate de Personnalisation des *Secure Elements*
ANFSI	Agence nationale des forces de sécurité intérieures

ANSSI	Agence nationale de la sécurité des systèmes d'information
BASSI	Bureau de l'audit de la sécurité des systèmes d'information
BEJ	Bureau des Enquêtes Judiciaires
CGU	Conditions Générales d'Utilisation
CNAU	Centre National d'Assistance aux Utilisateurs
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*
GCMP	Groupe des Chargés de Mission et de Projets
GN	Gendarmerie nationale
IGC	Infrastructure de Gestion de Clés
IPMS	Infrastructure de Production Mutualisée et Secourue
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
OC	Opérateur de Certification
OCSP	*Online Certificate Status Protocol*
OID	Object Identifier
OSSIN	Officier de Sécurité des Systèmes d'Information National
PC	Politique de Certification
PSCE	Prestataire de Services de Certification Électronique
RC	Responsable du Certificat de service applicatif
RSA	Rivest Shamir Adleman
SCT	Section Contrôle Technique
SDAC	Sous-Directeur des Applications de Commandement
SGDC	Section de la Gestion de la Donnée Classifiée
SGI	Section de la Gestion des Identités
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 de cachet du service applicatif auquel le certificat est rattaché.

Autorité responsable d'application (ARA) - Une ARA est l'autorité responsable d'une infrastructure de gestion de clés (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'agence du numérique des forces de sécurité intérieure, par délégation du directeur général de la gendarmerie nationale (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 direction de la sécurité et de l'architecture ANFSI.

Autorité de certification racine (ACR) - L'ACR est l'autorité qui dispose d'une infrastructure de gestion de clés lui permettant d'enregistrer, de générer, d'émettre et de révoquer des certificats, principalement des certificats d'autorités de certification subordonnées, conformément à la PC et à la DPC définies par son AA. L'ACR de l'ANFSI est auto-certifiée, c'est-à-dire que son certificat est auto-signé. 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 département des services socles DSA ANFSI.

Autorité de certification subordonnée (AC subordonnée) - L'AC subordonnée est l'autorité qui dispose d'une infrastructure de gestion de clés (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. Les autorités de certification subordonnées sont représentées par le chef du département des services socles DSA ANFSI.

Cachet serveur – Signature numérique effectuée par un serveur applicatif sur des données dans le but de pouvoir être utilisée soit dans le cadre d'un service d'authentification de l'origine des données, soit dans le cadre d'un service de non répudiation dans le cadre d'échanges dématérialisés entre usagers et l'administration ou entre différentes administrations.

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 prestataire de service de certification électronique (PSCE). Il est délivré par une Autorité de Certification. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Les usages des certificats électroniques régis par le présent document sont la signature électronique, l'authentification, la confidentialité ainsi que le double usage signature électronique + authentification.

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 également à une AC délivrant des certificats à une machine, il faut interpréter le terme porteur comme le Responsable du certificat.

Responsable du certificat – Personne en charge et responsable du certificat électronique de service applicatif de cachet ou d'authentification du serveur.

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.

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

Valideur - Opérateur de l'IGC, au contact des porteurs, réalisant des tâches de contrôle d'identité des porteurs, de remise de carte, de révocation. Il s'agit dans le cadre de la présente PC du notateur du personnel et ses délégataires ainsi que des personnels gradés de l'unité.

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 infrastructure de gestion de clés (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, la décomposition *fonctionnelle* de l'IGC qui est retenue dans la présente PC est la suivante :

- **Autorité d'enregistrement technique (AE)** - Cette fonction génère les demandes de cartes (qui contiendront les certificats) de façon automatique à partir des informations des futurs porteurs présentes dans le Système d'Information des Ressources Humaines de la Gendarmerie (AGORHA). Ceci concerne à la fois les demandes initiales (sur arrivée d'une nouvelle personne physique) et les renouvellements, causés par la modification d'informations du porteur ou l'arrivée à l'échéance de la carte.
- **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 porteur provenant soit du porteur, soit de la fonction de génération des éléments secrets du porteur, si c'est cette dernière qui génère la bi-clé du porteur.
- **Fonction de génération des éléments secrets du porteur** - Cette fonction génère des éléments secrets à destination du porteur et les prépare en vue de leur remise au porteur. Ces secrets sont les bi-clés d'authentification et de confidentialité, les codes d'activation et de déblocage de la carte du porteur.
- **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 porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats.
- **Fonction de gestion des révocations** - Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.
- **Fonction d'information sur l'état des certificats** - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction est mise en œuvre par une publication à intervalles réguliers de LCR.
- **Fonction de gestion des recouvrements** - Cette fonction traite les demandes de recouvrement de clés privées de confidentialité des porteurs (notamment identification et authentification du demandeur) et détermine les actions à mener. Dans le cas d'une décision positive, le recouvrement est réalisé par la fonction de séquestre et recouvrement.
- **Fonction de séquestre et recouvrement** - Cette fonction fournit la capacité de séquestrer de manière sécurisée les clés privées de confidentialité des porteurs, puis de les recouvrer en cas de besoin, sur la base de demandes authentifiées et traitées par la fonction de gestion des recouvrements.

D'autres fonctions de l'IGC (contrôles d'identité, remise, révocation…) sont mises en œuvre par les valideurs et 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 §I.3.2) :

- Porteur
- 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, à respecter les exigences suivantes :

- Être une entité légale au sens de la loi française.
- Rendre accessible, de manière non-discriminatoires, l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux porteurs, 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 porteur, 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 porteurs 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. Valideurs

Les valideurs sont des personnes physiques des forces de sécurité intérieure qui disposent de droits fonctionnels spécifiques dans l'IGC. Un valideur peut réaliser des actions relatives à un ensemble restreint de porteurs. Les valideurs et leur périmètre d'intervention sont définis automatiquement par l'AC en fonction de leur position dans l'organisation, de leur grade et de leur rôle au sein de l'unité. Ainsi tout porteur est toujours sous la responsabilité d'un ou plusieurs valideurs, et un valideur est responsable pour un périmètre fini de porteurs.

Ces fonctions sont :

- **Fonction de remise au porteur** - Cette opération, en présence obligatoire du porteur en face à face, comprend :
  - vérification et validation des informations d'identification du futur porteur de certificats avant la génération de bi-clés et de certificats ;
  - établissement d'un dossier (papier ou électronique) de demande et de remise de carte, mentionnant l'acceptation des certificats par le porteur, avec signature par le futur porteur et par le valideur ;
  - transmission du dossier de demande et de remise de carte au service RH pour archivage ;
  - personnalisation de la carte, comprenant la génération de bi-clés (par le porteur et par l'AC), l'envoi des demandes de certificats à l'AC, le choix des codes d'activation de la carte par le porteur ;
  - remise au porteur de sa carte contenant les certificats.

- **Fonction de renouvellement anticipé** – À l'initiative du porteur afin d'éviter d'avoir à le faire dans des conditions dégradées (stage, mission dans des endroits où les accès à l'intranet sont erratiques).
- **Fonction de demande de révocation** – Envoi d'une demande de révocation à l'AC concernant la carte d'un porteur ;

Le valideur peut remettre au porteur une carte professionnelle contenant des certificats valides 3 ans ou, dans certaines conditions, une carte provisoire dont les certificats sont valides un jour (dépannage) ou un an (attente d'une carte personnalisée graphiquement avec les éléments relatifs à son identité).

I.4.3. Porteurs de certificats

Dans le contexte de cette PC, un porteur de certificats ne peut être qu'une personne physique qui utilise sa clé privée et le certificat électronique associé pour ses activités en lien avec l'ANFSI, avec laquelle il a une relation contractuelle, hiérarchique ou réglementaire.

Le porteur participe directement aux fonctions de remise de carte, de renouvellement et de révocation de ses certificats.

Le porteur respecte les obligations qui lui incombent et définies dans cette PC et aux chapitres G.6.3 et G.6.4 de [MESURES_IGC].

I.4.4. Utilisateurs de certificats

Un utilisateur de certificats électroniques peut être notamment :

- Un service en ligne qui utilise un certificat et un dispositif de vérification d'authentification soit pour valider une demande d'accès faite par le porteur du certificat dans le cadre d'un contrôle d'accès, soit pour authentifier l'origine d'un message ou de données transmises par le porteur du certificat ;
- Un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification d'authentification afin d'en authentifier l'origine.
- Un service en ligne qui utilise un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message par le porteur du certificat ;
- Un usager qui signe électroniquement un document ou un message ;
- Un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par le porteur du certificat sur ce message ou sur ces données ;
- Un service en ligne qui utilise un dispositif de chiffrement pour chiffrer des données ou un message à destination du porteur du certificat ;
- Une personne qui émet un message chiffré à l'intention du porteur du certificat électronique.

Les utilisateurs de certificats doivent prendre toutes autres précautions prescrites dans les éventuels accords ou tout autre document, notamment ceux précisés aux chapitres G.6.3 et G.6.4 de [MESURES_IGC].

I.4.5. Autres participants

L'IGC ne fait pas appel à des mandataires de certification.

I.5. Usage des certificats

I.5.1. Domaines d'utilisation applicables

I.5.1.1 Bi-clés et certificats des porteurs

Les usages des certificats électroniques d'authentification délivrés par l'AC « 2024 FSI AC Personnes Authentification » sont l'authentification des porteurs auprès de serveurs distants dans le cadre d'un contrôle d'accès à un serveur ou une application.

Les usages des certificats électroniques de signature délivrés par les AC « 2024 FSI AC Personnes Signature » sont la signature électronique de données.

Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

Les usages des certificats électroniques de confidentialité délivrés par l'AC « 2024 FSI AC Personnes Chiffrement » sont :

- Déchiffrement : à l'aide de sa clé privée, un porteur déchiffre les données qui lui ont été transmises dans le cadre d'échanges dématérialisés, chiffrées à partir de sa clé publique ;
- Chiffrement : à l'aide de la publique du destinataire, une personne chiffre des données.

Cela couvre notamment le cas de chiffrement par une clé symétrique de fichiers ou de messages, clé elle-même protégée par un mécanisme cryptographique asymétrique, de type RSA (chiffrement de la clé symétrique par la clé publique du porteur et déchiffrement par sa clé privée) ou de type Diffie- Hellman (obtention de la clé symétrique, par l'émetteur d'un message, via un algorithme combinant la clé privée de l'émetteur et la clé publique du destinataire, et inversement pour l'obtention de cette clé symétrique par le destinataire du message).

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 des AC (signature des certificats des porteurs 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.*).

Chaque 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'AC Racine. 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 chapitre IV.5 ci-dessous, en fonction du niveau de sécurité. L'AC doit respecter ces restrictions et imposer leur respect par ses porteurs et ses utilisateurs de certificats.

À cette fin, elle doit communiquer à tous les porteurs 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] et de l'[ETSI EN 319 412].

Dans chaque certificat, l'AC émettrice (*issuer*) et le porteur *(subject)* sont identifiés par un *Distinguished Name (DN)*.

III.1.2. Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les porteurs de certificats sont explicites. Le DN du porteur est construit à partir des informations présentées lors de son enregistrement dans AGORHA.

III.1.2.1 Nommage des Autorités de Certification

Le DN des AC émettrice est construit comme suit :

Attribut	Valeur	Commentaires
C	FR	Pays
O	ANFSI	Organisation
OU	0002 130031404	Numéro SIREN de l'ANFSI, obligatoire pour le respect du RGS
CN	Nom de l'AC, voir ci-dessous	Identification de l'AC parmi celles de l'IGC/FSI

Les différentes AC de l'IGC/GN, objet de cette PC, portent les noms suivants :

- 2024 FSI AC Personnes Authentification
- 2024 FSI AC Personnes Signature
- 2024 FSI AC Personnes Chiffrement

Par exemple, le DN de l'autorité émettant des certificats de signature est :

C = FR, O = ANFSI, OU = 0002 130031404, CN = 2024 FSI AC Personnes Signature

III.1.2.2 Nommage des porteurs de type « Personnes »

Le DN des porteurs de type personne physique est construit comme suit :

Attribut	Valeur	Commentaires
C	FR	Pays
O	Gendarmerie nationale	Organisation
organizationIdentifier	NTRFR-157000019	(certificat signature uniquement) Obligatoire pour le eIDAS
OU	0002 157000019	Numéro SIREN de la DGGN, obligatoire pour le respect du RGS
OU	Personnes *usage*	Indication de l'AC émettrice du

		certificat
SN	Nom	Nom de l'état civil ou nom d'usage de la personne
GN	Prénom	L'un des prénoms de la personne
CN	nom.prenom	Nom et prénom en minuscules séparés par un point, un indice x pouvant être ajouté en cas d'homonymes
UID	Identifiant	Identifiant unique interne de la personne provenant de l'annuaire de la Gendarmerie (NIGEND) sur 8 chiffres
E	Courriel	Courriel de messagerie professionnelle, pour la signature et le chiffrement.

Note - L'OID de l'attribut UID est 0.9.2342.19200300.100.1.1.

Par exemple, un DN de porteur peut être :

C = FR, O = Gendarmerie nationale, OU = 0002 157000019, OU = Personnes Signature, SN = Martin, GN = Michel, CN=martin.michel, UID = 12345678, E=martin.michel@gendarmerie.interieur.gouv.fr

III.1.3. Pseudonymisation des porteurs

Cette PC interdit la pseudonymisation pour les certificats des porteurs de type Personnes.

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

Sans objet.

III.1.5. Unicité des noms

L'attribut UID, présent dans le DN du champ « *subject* » de chaque certificat de porteur, identifie de façon unique un porteur dans le domaine de l'AC. Il s'agit de son NIGEND. Cet attribut est propre à une personne physique et ne peut pas être attribué à une autre personne pendant toute la durée de vie de l'AC. Il est de toute façon défini dès l'entrée en gendarmerie.

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

L'AC est responsable de l'unicité des noms de ses porteurs 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 porteur dans l'IGC se fait automatiquement par l'AE technique, à partir des informations d'AGORHA.

La vérification et la validation initiales de l'identité de la personne physique sont réalisées par le valideur dans les conditions décrites au chapitre III.2.

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

Lorsque c'est le porteur qui génère sa bi-clé (cas du bi-clés de signature), il prouve à l'AC la possession de la clé privée correspondant à la clé publique par la signature de sa demande de certificat avec sa clé privée.

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

Sans objet.

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

L'enregistrement d'un porteur dans l'IGC se fait automatiquement par l'AE technique, à partir des informations d'AGORHA qui est réputée fiable. La présence du porteur dans AGORHA prouve son lien avec l'ANFSI, et l'AE Technique ne crée la demande que si le porteur est effectivement éligible pour recevoir un certificat.

Le valideur, qui s'apprête à remettre une carte à un porteur, identifie le porteur, en face à face, par le recoupement entre les informations contenues dans la demande, le dossier personnel du porteur et par sa connaissance préalable de la personne dont il est en général le notateur. Si le valideur ne connaît pas personnellement le futur porteur, alors il lui demande de présenter les éléments suivants :

- un document officiel d'identité, original et en cours de validité : carte d'identité, ou passeport ou document officiel équivalent.

III.2.4. Informations non vérifiées du porteur

Toutes les informations présentes dans les certificats sont issues du système d'information RH Agorha. Ce système assure la garantie de l'intégrité des informations .

III.2.5. Validation de l'autorité du demandeur

Sans objet.

III.2.6. Critères d'interopérabilité

Les AC « Personnes physiques », objet de cette PC, n'ont pas d'accord spécifique de reconnaissance avec des AC extérieures.

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

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

Ce chapitre concerne aussi bien les bi-clés générées par le porteur que celles générées par l'AC.

III.3.1. Identification et validation pour un renouvellement courant

Deux types de renouvellement peuvent se produire :

- La carte du porteur doit être renouvelée (remplacée par une nouvelle carte) parce qu'elle a atteint sa durée de vie maximale ou parce que le visuel de la carte doit être changé. Dans ce cas, le porteur se verra remettre la nouvelle carte par un valideur,

avec un processus identique à une demande initiale, en particulier l'identification du porteur. Les certificats actifs de la carte à renouveler sont révoqués lors de la remise de la nouvelle carte.

- Seuls les certificats doivent être renouvelés (le porteur conserve sa carte) parce qu'ils arrivent à expiration ou contiennent une donnée à mettre à jour (sans nécessiter un changement de carte). Dans ce cas, le porteur peut réaliser ce renouvellement auprès d'un valideur ou seul si le précédent renouvellement a été effectué auprès d'un valideur.
  - Si le porteur se rend auprès d'un valideur, l'identification du porteur est identique à celle effectuée lors de la remise initiale (cf. §III.2.3).
  - Si le porteur réalise son renouvellement seul, il est identifié et authentifié sur le système IGC par son certificat d'authentification valide à sa connexion.

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

Suite à la révocation définitive de ses certificats, quelle qu'en soit la cause, le porteur ne peut obtenir de nouveaux certificats qu'en effectuant le processus nominal de demande initiale de certificats.

La procédure d'identification et de validation de cette demande est donc celle décrite au §III.2.

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

Un porteur peut demander lui-même l'invalidation de sa propre carte (donc la révocation de tous ses certificats actifs) en face à face avec un opérateur ou à distance.

- Dans le premier cas, l'identification du porteur se fait par un face à face avec un valideur et, si besoin, par la présentation d'un document officiel d'identité.
- Dans les autres cas, le porteur est authentifié en répondant aux trois questions secrètes personnelles qu'il avait renseignées au préalable dans AGECAPE.

Lorsque la demande de révocation est réalisée par un opérateur, celui-ci s'authentifie avec son certificat d'authentification sur le système.

IV. Exigences opérationnelles sur le cycle de vie des certificats

IV.1. Demande de carte

IV.1.1. Origine d'une demande de carte

La demande de carte est réalisée de façon automatique par l'AE technique. Un valideur peut également initier une demande de carte via un renouvellement anticipé du support dans AGECAPE.

Les certificats des porteurs sont exclusivement fournis sur leur carte personnelle ou sur une carte provisoire qui leur a été préalablement attribuée. Le processus décrit ci-dessous est par conséquent celui de demande, de traitement et de délivrance de carte. Les demandes, traitements et délivrances de certificats sont réalisés pendant le processus de délivrance de la carte.

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

L'AE technique consulte périodiquement l'annuaire AGORHA afin d'identifier les personnes pour lesquelles une carte doit être produite. Les informations trouvées dans AGORHA sont réputées fiables. La demande de carte est établie si au minimum les critères suivants sont vérifiés :

- les données personnelles du futur porteur sont complètes et syntaxiquement valides ;
- la photo de la personne est présente dans les données avec des caractéristiques techniques valables ;
- la personne est éligible à la détention d'une carte (statut…) ;
- la personne ne possède pas déjà une carte en production ou valide ;
- la personne est présente depuis a minima 100 jours.

La demande est enregistrée informatiquement dans AGECAPE et journalisée. Un message électronique est adressé au futur porteur pour l'informer de la demande de carte qui vient d'être effectuée.

IV.2. Traitement d'une demande de carte

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

Sans objet.

IV.2.2. Acceptation ou rejet de la demande

Toutes les demandes effectuées automatiquement par l'AE technique sont présumées valides et donc tacitement acceptées. Les identités des porteurs et les informations portées sur les cartes et dans les certificats seront vérifiées lors de la remise.

IV.2.3. Durée d'établissement des cartes

Les demandes de cartes sont regroupées par lot et font l'objet d'une mise en production de cartes à puce à personnaliser graphiquement.

La durée de production des cartes est de quelques jours, à laquelle il faut ajouter un délai d'acheminement des cartes aux porteurs. Les certificats seront eux produits à la volée durant la remise de la carte.

IV.2.4. Codes PUK

Se reporter à la DPC.

IV.3. Délivrance de la carte et des certificats

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

Lorsqu'un valideur reçoit une carte vierge personnalisée graphiquement, il prévient le porteur concerné pour fixer un rendez-vous afin de se faire délivrer des certificats.

La remise de la carte a lieu lors d'un face à face entre le futur porteur et le valideur. Le futur porteur apporte les justificatifs nécessaires.

En cas de délivrance d'une carte provisoire, il est nécessaire de faire appel à un troisième personnel qui fait office de témoin de l'attribution de la carte provisoire et notamment de la présence physique du demandeur. Ce témoin doit s'authentifier avec sa carte professionnelle.

L'opération de remise comprend les étapes successives suivantes :

- Validation de l'identité du futur porteur conformément aux procédures du chapitre III.2 ;
- Lancement d'AGECAPE par le valideur
- Vérification de la cohérence des justificatifs présentés avec les informations de la demande ;
- Authentification du porteur :
  - Si le porteur dispose d'une carte encore active : authentification du porteur par sa carte actuelle ;
  - *[Cas de la carte professionnelle personnalisée avec les informations du porteur]* Si le porteur n'a pas de carte active, il faut procéder à une remise de carte provisoire.
- *[Cas de la carte provisoire]* Choix du menu « Attribuer une carte provisoire » ;
- *[Cas de la carte provisoire]* Affichage de la cinématique et champ de recherche du porteur ;
- *[Cas de la carte provisoire]* Sélection du porteur ;
- *[Cas de la carte provisoire]* Confirmation du porteur sélectionné ;
- *[Cas de la carte provisoire]* Confirmation de la présence physique du porteur ;
- *[Cas de la carte provisoire]* Authentification du porteur tiers faisant office de témoin ;
- *[Cas de la carte provisoire]* Envoi d'un mail au porteur tiers faisant office de témoin ;
- *[Cas de la carte provisoire]* Journalisation de l'authentification du porteur tiers faisant office de témoin ;
- Révocation des éventuels certificats valides du porteur (carte professionnelle ou provisoire) ;
- Désaffectation de l'éventuelle carte professionnelle ou provisoire du porteur ;
- Envoi d'un message électronique au porteur ;
- Choix du code PIN global et du code PIN de signature par le porteur ;
- Génération du bi-clé de signature sur la puce de la carte ;
- Récupération des bi-clés d'authentification et de chiffrement auprès de l'AC (sauf pour les cartes provisoires de 24h pour lesquelles il n'y a pas génération d'un nouveau bi-clé de confidentialité) ;
- Génération et envoi à l'AC des demandes de certificats signées par les clés privées correspondantes ;

- Génération et signature des certificats par l'AC ;
- Séquestre de la bi-clé et du certificat de chiffrement (s'ils ont été générés)
- Présentation du contenu des certificats générés au porteur ;

  Cet affichage contient :

  - L'identité du porteur ;
  - Les caractéristiques des certificats ;
  - La reconnaissance de remise de la carte au porteur ;
  - L'information de séquestre de la clé privée de chiffrement (le cas échéant) ;
  - Les informations contenues dans le certificat (en particulier les informations nominatives, la durée de validité, l'usage des certificats)
  - L'acceptation des certificats et de leur publication ;
  - L'acceptation des conditions générales d'utilisation des certificats

- Acceptation explicite des certificats par le porteur et des CGU ;
- Inscription des certificats (et du bi-clé d'authentification et de chiffrement) sur la puce de la carte ;
- Les CGU signées sont conservées dans AGeCAPE et servent de preuve d'acceptation des certificats.

Les échanges entre la puce, le lecteur de carte, le valideur et les composantes de l'IGC sont tous sécurisés par l'utilisation de TLS et du *Secure Messaging* (canal sécurisé) pour le dialogue avec la puce. Ainsi les éléments secrets (clés privées, codes d'activation) sont protégés en intégrité et confidentialité pendant tout le processus.

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

La signature des conditions générales d'utilisation vaut notification par l'AC de la délivrance des certificats au porteur.

IV.4. Acceptation du certificat

IV.4.1. Démarche d'acceptation du certificat

L'acceptation des certificats et des CGU vaut récépissé de remise de la carte, signé par le porteur.

IV.4.2. Publication du certificat

Seuls les certificats de confidentialité peuvent être publiés.

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

La délivrance des certificats est immédiatement consultable dans l'IGC par les autres opérateurs ayant accès à cette information.

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

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

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

L'usage autorisé de la bi-clé du porteur et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des clés (*cf.* VII).

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

Voir 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 porteur).

Cependant, dans la cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. En particulier, l'AC garantit que les bi-clés de chiffrement générées par l'AC ne sont utilisées que pour un seul 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 au porteur liée à la génération d'une nouvelle bi-clé.

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

Les bi-clés sont renouvelées au minimum tous les trois ans (durée de vie des certificats), afin de minimiser les possibilités d'attaques cryptographiques.

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

- suite au remplacement de la carte (support des certificats), pour cause de fin de vie de la carte ou de problème sur la carte entraînant sa révocation (*cf.* chapitre IV.9, notamment le chapitre IV.9.1.1 pour les différentes causes possibles de révocation).
- ou pour tenir compte de la modification de données personnelles du porteur n'impliquant pas le changement de la carte. Dans ces cas, les certificats actifs sont révoqués lorsque les nouveaux sont générés.

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

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

Le déclenchement de la fourniture d'un nouveau certificat du porteur peut-être automatique (cas d'expiration prochaine des certificats, de changement de données du porteur) ou bien à l'initiative du valideur (remplacement de la carte) ou du porteur (par exemple après une notification d'expiration prochaine de ses certificats).

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

Si la carte est remplacée, la production de la carte et sa remise se font par des processus identiques à la demande initiale. Le porteur se rend dans ce cas auprès d'un de ses valideurs.

Si seuls les certificats sont à renouveler, et une fois la demande enregistrée dans le système, la génération des certificats est réalisée par le porteur auprès d'un valideur.

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

IV.7.3.1 Procédure de délivrance de nouveaux certificats en présence du valideur

Lorsque le porteur se rend auprès du valideur, le processus est le suivant :

- Validation de l'identité du porteur conformément aux procédures du chapitre III.3 ;
- Vérification de la cohérence des justificatifs présentés avec les informations de la demande ;
- Authentification de la carte du porteur par le système ;
- Révocation des éventuels certificats valides du porteur (carte professionnelle ou provisoire) ;
- Génération du bi-clé de signature sur la puce de la carte ;
- Récupération des bi-clés d'authentification et de chiffrement auprès de l'AC ;
- Génération et envoi à l'AC des demandes de certificats signées par les clés privées correspondantes ;
- Génération et signature des certificats par l'AC ;
- Séquestre de la bi-clé et du certificat de chiffrement ;
- Présentation du contenu des certificats générés au porteur :

  Cet affichage contient :

  - L'identité du porteur ;
  - Les caractéristiques des certificats ;
  - La reconnaissance de remise de la carte au porteur ;
  - L'information de séquestre de la clé privée de chiffrement (le cas échéant) ;
  - Les informations contenues dans le certificat (en particulier les informations nominatives, la durée de validité, l'usage des certificats)
  - L'acceptation des certificats et de leur publication ;
  - L'acceptation des conditions générales d'utilisation des certificats ;
- Acceptation explicite des certificats par le porteur ;
- Inscription des certificats (et du bi-clé d'authentification et de chiffrement) sur la puce de la carte ;
- Les CGU signées sont conservées dans AGECAPE et servent de preuve d'acceptation des certificats.

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

Voir chapitre IV.3.

IV.7.5. Démarche d'acceptation du nouveau certificat

Voir chapitre IV.4.

IV.7.6. Publication du nouveau certificat

Voir chapitre IV.4.

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

Voir chapitre IV.4.

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 porteurs

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

- les informations du porteur imprimées sur sa carte sont non conformes ;
- le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le porteur et/ou, le valideur n'ont pas respecté leurs obligations découlant de la PC de l'AC ;
- la clé privée du porteur ou la carte du porteur est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- le porteur ou un valideur demande la révocation des certificats de sa carte à cause d'un problème sur la carte (hors service, usée, illisible) ;
- le porteur ne satisfait plus aux conditions de détention d'une carte de l'ANFSI ;
- le décès du porteur.

Lorsqu'une des circonstances ci-dessus se réalise, le porteur ou le valideur ou l'AE technique le déclare et réalise une demande de révocation, qui sera traitée par l'AC.

Note – Lors d'un renouvellement de certificats, les précédents certificats éventuellement encore en cours de validité sont révoqués pour que le porteur ne dispose que d'un seul certificat valide pour un usage donné. Cependant, ceci est fait automatiquement dans le processus de renouvellement et ne correspond pas au processus de révocation décrit dans ce chapitre.

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 pour 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 porteurs

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

- le porteur au nom duquel le certificat a été émis ;
- un valideur du porteur du certificat à révoquer ;
- un opérateur central de l'IGC/GN (support, supervision) sur demande d'un porteur ;
- l'AE technique ;
- un administrateur de l'IGC ;
- l'AC émettrice du certificat.

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 de porteur

IV.9.3.1.1 Révocation par le porteur

Le porteur n'est pas en capacité de révoquer lui-même ses certificats.

Il doit contacter un de ses valideurs. La permanence du commandement et le fait que les valideurs soient dans la chaîne hiérarchique implique qu'au moins un de ces valideurs sera disponible.

IV.9.3.1.2 Révocation par un valideur

Un valideur dispose des droits nécessaires pour demander la révocation d'une carte même en l'absence du porteur.

La valideur s'authentifie sur AGECAPE, recherche le porteur et choisit l'une de ses cartes pour la révoquer. Il spécifie une raison de révocation.

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

- Identité du porteur
- Identité du valideur
- Numéro de carte à révoquer
- Raison de révocation de la carte

Le porteur du certificat est informé par messagerie électronique de la demande de révocation de son certificat. Le traitement de cette demande de révocation est décrit au §IV.9.3.1.6.

En cas d'absence de tous les valideurs et si l'urgence le nécessite (vol par exemple), le porteur peut contacter sa chaîne de technicien SIC, qui en remontant les permanences, peut permettre de réaliser la révocation, par un administrateur (IV.9.3.1.4).

IV.9.3.1.3 Révocation par l'AE technique

L'AE technique peut demander la révocation de certificats porteurs pour les raisons suivantes, à l'occasion de tâches planifiées :

- Cartes arrivées à échéance d'utilisation (durée de vie physique du support atteinte) ;
- Départ d'un porteur du périmètre des unités administrées par l'ANFSI (ou perte de l'éligibilité à une carte) ;

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

- Identité du porteur
- « Système IGC/ANFSI » comme auteur de la révocation
- Numéro de carte à révoquer
- Raison de révocation de la carte (Carte à échéance, non éligibilité)

Le porteur du certificat est informé par messagerie électronique de la demande de révocation de son certificat. Le traitement de cette demande de révocation est décrit au §IV.9.3.1.6.

IV.9.3.1.4 Révocation par un administrateur de l'IGC

L'administrateur de l'IGC ne dispose pas du droit de révocation sur l'AE technique.

IV.9.3.1.5 Révocation par l'AC émettrice du certificat

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

Afin de permettre la révocation en cas d'absence de tous les valideurs, il peut réaliser l'opération de la même manière que le valideur.

Cette opération exceptionnelle est réalisée après des contres-appels permettant de s'assurer de la véracité des faits et des personnes.

IV.9.3.1.6 Traitement de la demande de révocation

Une fois la demande enregistrée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats.

L'information de révocation est diffusée par la génération et la publication d'une nouvelle LCR signée par l'AC elle-même.

L'opération est enregistrée dans les journaux d'évènements 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

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. Le point de contact identifié sur le site www.cyber.gouv.fr doit être immédiatement informé.

La DPC 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 porteur pour formuler la demande de révocation

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

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

IV.9.5.1 Révocation d'un certificat de porteur

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 12h en cumulé sur un an.

Toute demande de révocation d'un certificat porteur est traitée dans un délai inférieur à 24h. 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

En cas de révocation d'un des certificats de la chaîne de certification, l'AC doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs concernés que leurs certificats ne sont plus valides.

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un évènement 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. Le point de contact identifié sur le site www.cyber.gouv.fr doit être immédiatement informé.

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

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

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

Les LCR sont publiées au moins une fois par 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.

Les AC objet de cette PC n'ont pas d'AC subordonnées et ne publient donc pas de LAR. Se référer à la PC de l'AC Racine pour obtenir des informations sur les fréquences et durées de vie des LAR concernant les 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. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

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

IV.9.10. Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Voir chapitre IV.9.5.3 ci-dessus.

IV.9.11. Autres moyens disponibles d'information sur les révocations

Sans objet.

IV.9.12. Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de porteur, les entités autorisées à effectuer une demande de révocation sont tenues de le faire sans délais 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 ci-dessus, 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.9.13. Causes possibles d'une suspension

L'AC n'autorise pas les suspensions de certificat.

IV.9.14. Origine d'une demande de suspension

Sans objet.

IV.9.15. Procédure de traitement d'une demande de suspension

Sans objet.

IV.9.16. 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 12h en cumulé sur un an.

IV.10.3. Dispositifs optionnels

Sans objet.

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

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

IV.12. Séquestre de clé et recouvrement

Seules les clés privées associées aux certificats électroniques de confidentialité sont séquestrées à des fins de recouvrement. Les clés privées d'AC et les clés privées associées aux certificats électroniques des autres usages ne sont en aucun cas être séquestrées.

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

Les différentes étapes de séquestre et de recouvrement de clés privées associées aux certificats électroniques dont l'usage est la confidentialité (chiffrement) doivent respecter les exigences des chapitres qui suivent.

IV.12.1.1 Demande de séquestre

Les clés privées de confidentialité sont automatiquement soumises au séquestre pour une durée de 10 ans (durée fixée dans le système), au cours de l'opération de remise de carte (*cf.* §IV.3.1).

Le porteur en est informé lors de la procédure de remise de carte et de génération des certificats. Les CGU signée sont la preuve de l'acceptation du séquestre par le porteur.

IV.12.1.2 Traitement d'une demande de séquestre

Les clés sont conservées sous forme chiffrée en base de données. La clé AES est stockée dans un HSM. Le DN du certificat du porteur et le numéro de série du certificat permettent d'identifier de manière unique une clé du séquestre.

IV.12.1.3 Origine d'une demande de recouvrement

Dans le cadre normal du service, seul le porteur peut demander le recouvrement d'une de ses précédentes bi-clés de confidentialité, via une fonction du portail AGECAPE qui lui est accessible.

Le recouvrement des clés de confidentialité d'un porteur par une tierce personne ne peut être réalisé que dans le cadre d'une enquête judiciaire ou administrative ou en cas de force majeure comme le décès du porteur.

Cette opération est sous le contrôle de l'IGGN par l'intermédiaire de son Bureau de l'audit de la sécurité des systèmes d'information (BASSI). La demande est réalisée par le bureau des enquêtes judiciaires (BEJ) ou par le bureau des enquêtes administratives (BEA).

IV.12.1.4 Identification et validation d'une demande de recouvrement par le porteur

Le porteur s'authentifie par son certificat d'authentification valide sur AGECAPE.

Le porteur choisit alors, parmi ses précédentes bi-clés de confidentialité, connues et listées par le système, celle qu'il veut recouvrer sur sa carte. Cette demande est considérée valide et acceptée automatiquement par le système.

IV.12.1.5 Identification et validation d'une demande de recouvrement par l'IGGN

La SGI reçoit la demande officielle de l'IGGN par l'intermédiaire de son bureau des enquêtes administrative (BEA) ou de son bureau des enquêtes judiciaires (BEJ).

La demande doit comporter :

- une pièce d'identité du demandeur
- l'identité du porteur du certification
- la mention de l'identifiant du ou des certificats à recouvrer

Le ou les personnels de la SGI, après avoir vérifiés la validité de la demande, fixe un rendez-vous avec les auditeurs de l'IGC et le demandeur.

IV.12.1.6 Traitement d'une demande de recouvrement

La bi-clé de confidentialité (la clé privée, la clé publique) et le certificat correspondant sont transmis de façon sécurisée depuis AGECAPE vers la carte du porteur. Le délai est immédiat dans le cadre d'une demande par le porteur.

Cette remise s'effectue avec une sécurité équivalente à la remise de la clé privée lors de la génération du certificat du porteur (cf. chapitres VI.1.1.3 et VI.4).

La demande de recouvrement et le rapport d'exécution du recouvrement sont journalisés par le système.

Dans le cadre d'une enquête judiciaire ou administrative, le ou les personnels de la SGI, après avoir vérifiés la validité de la demande, fixe un rendez-vous avec les auditeurs de l'IGC et le demandeur.

Une fois rassemblés, ils sélectionnent alors, parmi les bi-clés de confidentialité du porteur, connues et listées par le système, celles qu'ils veulent recouvrer.

La ou les bi-clés de confidentialité demandés sont alors remis au demandeur contre signature. La demande est archivée.

Actuellement, cette fonction de recouvrement s'effectue manuellement, sur demande officielle de l'IGGN à la SGI.

Devront être présent :

- au moins un personnel de la SGI ;
- au moins un représentant de l'IGGN ayant le rôle d'auditeur de l'IGC ;
- le représentant du BEJ ou BEA nommément désigné par la demande.

La clé de confidentialité est remise et stockée de manière sécurisée.

La SGI s'engage à proposer un rendez-vous, à réception de la demande valide, dans le mois qui suit la réception de cette demande.

IV.12.1.7 Destruction des clés séquestrées

Dès la fin de la période de conservation d'une clé séquestrée, tout exemplaire de cette clé détenue par AGECAPE est détruit de manière fiable afin de ne pouvoir ni recouvrer ni reconstituer la clé.

IV.12.1.8 Disponibilité des fonctions liées au séquestre et au recouvrement

La disponibilité de la fonction de recouvrement ne fait pas l'objet d'un engagement spécifique.

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

Sans objet.

V. Mesures de sécurité non techniques

Les mesures de sécurité non techniques sont décrites au chapitre D de [MESURE_IGC].

VI. Mesures de sécurité techniques

Les mesures de sécurité non techniques sont décrites au chapitre E de [MESURE_IGC]. Seules les spécificités des AC « Personnes » sont mentionnées ici.

VI.1. Génération et installation de bi-clés

VI.1.1. Génération des bi-clés

VI.1.1.1 Clés d'AC

Voir [MESURE_IGC].

VI.1.1.2 Clés porteurs générées par l'AC

Voir [MESURE_IGC].

VI.1.1.3 Clés porteurs générées par le porteur

La génération de la bi-clé de signature est effectuée dans la carte du porteur, dont la puce est un dispositif cryptographique qualifié au niveau renforcé.

L'AC est assurée que la clé publique exportée réside effectivement dans ce dispositif par la fonction de génération des éléments secrets du porteur qui pilote la génération sur la puce avec le mécanisme de messagerie sécurisée.

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

Les clés privées d'authentification et de confidentialité sont transmises au porteur de manière sécurisée (garantie de confidentialité et d'intégrité) en utilisant la messagerie sécurisée de la puce.

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

Voir [MESURE_IGC].

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

Voir [MESURE_IGC].

VI.1.5. Tailles des clés

Voir [MESURE_IGC].

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

Voir [MESURE_IGC].

VI.1.7. Objectifs d'usage de la clé

Voir [MESURE_IGC].

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

Voir [MESURE_IGC].

VI.2.1.2 Dispositifs de protection des éléments secrets des porteurs

Les dispositifs de protection des éléments secrets des porteurs, pour la mise en œuvre de leurs clés privées de personne, sont des dispositifs cryptographiques qualifiés au niveau renforcé.

L'AC fournit ce dispositif au porteur et s'assure que :

- la préparation des dispositifs de protection des éléments secrets est contrôlée de façon sécurisée ;
- les dispositifs de protection des éléments secrets sont stockés et distribués de façon sécurisée ;
- les désactivations et réactivations des dispositifs de protection des éléments secrets sont contrôlées de façon sécurisée.

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

Voir [MESURE_IGC].

VI.2.3. Séquestre de la clé privée

Les clés privées de confidentialité sont séquestrées, conformément aux dispositions prévues au chapitre IV.12. Des mécanismes de sécurité garantissent la confidentialité de ce séquestre, et que les clés privées séquestrées ne sont jamais en clair en dehors d'un module cryptographique.

VI.2.4. Copie de secours de la clé privée

Hormis pour les clés privées de confidentialité, les clés privées des porteurs ne font l'objet d'aucune copie de secours.

Voir [MESURE_IGC].

VI.2.5. Archivage de la clé privée

Voir [MESURE_IGC]. Les clés privées des porteurs 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

Les clés privées d'authentification et de confidentialité des porteurs, générées en dehors du dispositif du porteur, sont transférées dans la puce conformément aux exigences du chapitre VI.1.1.2 ci-dessus.

Pour les clés privées d'AC, voir [MESURE_IGC].

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

Voir [MESURE_IGC].

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

VI.2.8.1 Clés privées d'AC

Voir [MESURE_IGC].

VI.2.8.2 Clés privées des porteurs

L'activation de la clé privée du porteur se fait par utilisation d'un code PIN personnel, défini par le porteur lui-même et connu de lui seul.

Il existe un code PIN pour activer la clé privée d'authentification et la clé de confidentialité, et un second code PIN distinct pour activer spécifiquement la clé privée de signature.

VI.2.9. Méthode de désactivation de la clé privée

VI.2.9.1 Clés privées d'AC

Voir [MESURE_IGC].

VI.2.9.2 Clés privées des porteurs

La désactivation des clés privées d'un porteur est automatique dès la fin de session entre l'application qui a activé la clé privée et la puce (session fermée par l'application, fin du processus de l'application, retrait de la carte…).

VI.2.10. Méthode de destruction des clés privées

VI.2.10.1 Clés privées d'AC

Voir [MESURE_IGC].

VI.2.10.2 Clés privées des porteurs

Les clés privées des porteurs qui sont générées par l'AC dans un module cryptographique sont détruites du module après leur export dans la puce de la carte du porteur par les moyens sécurisés du matériel.

Les clés privées des porteurs, importées depuis l'AC ou générées directement par la puce de la carte du porteur, sont détruites après renouvellement du certificat par les fonctions sécurisées de la puce, à l'exception de la clé privée de confidentialité dont le précédent bi-clé est conservé pour permettre une une période de transition du chiffrement.

Dans les deux cas, l'effacement sécurisé est garanti par la qualification au niveau renforcé du matériel.

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

Le module cryptographique de l'AC et les puces des cartes des porteurs sont qualifiées par l'ANSSI au niveau renforcé.

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 porteurs 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 porteurs 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

Voir [MESURE_IGC].

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

Les clés privées du porteur qui ont été générées par l'AC sont transmises de manière sécurisée à la puce du porteur. Les codes d'activation sont choisis directement par le porteur. Toutes ces opérations sont réalisées lors de la remise de la carte en face à face avec le valideur.

VI.4.2. Protection des données d'activation

VI.4.2.1 Protection des données d'activation correspondant à la clé privée de l'AC

Voir [MESURE_IGC].

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

Les codes d'activation de la puce sont des codes PIN connus des seuls porteurs qui sont garants de leur confidentialité.

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

Il n'y a pas d'autres aspects lié aux données d'activation.

VI.5. Mesures de sécurité des systèmes informatiques

Voir [MESURE_IGC].

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

Voir [MESURE_IGC].

VI.7. Mesures de sécurité réseau

Voir [MESURE_IGC].

VI.8. Horodatage / Système de datation

Voir [MESURE_IGC].

VII. Profils des certificats et des LCR

VII.1. Format du certificat des AC subordonnées « personnes physiques »

Nom du champ	Contenu
Champs de base	
Version **(version)**	2 (version 3)
Numéro de série **(serialNumber)**	Attribué par l'AC racine de l'IGC/FSI
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'AC Racine
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 Personnes *usage* La valeur *usage* est l'un des usages suivants : • Authentification • Chiffrement • Signature
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)

Nom du champ	Contenu
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
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 d'authentification des personnes

Nom du champ	Contenu
Champs de base	

Nom du champ	Contenu
Version (version)	2 (version 3)
Numéro de série (serialNumber)	Attribué par l'AC 2024 FSI AC Personnes Authentification
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 Personnes Authentification
Valide à partir du (validity/notBefore)	Date de génération
Valide jusqu'au (validity/notAfter)	3 ans après la date de génération Pour les certificats des cartes provisoires : - 24h si le porteur possède déjà une carte active possédant des certificats - 1 an si le porteur ne possède pas déjà une carte active possédant des certificats
Objet (subject)	C = FR O = Gendarmerie nationale OU = 0002 157000019 OU = Personnes Authentification SN = *nom (test pour les certificats de test)* GN = *prénom (test pour les certificats de test)* CN=*prenom.nom (test.test pour les certificats de test)* UID = *NIGEND (000000 pour les certificats de test)*
Clé publique (subjectPublicKeyInfo)	Algorithme RSA : • Champ « algorithm/algorithm » : rsaEncryption • Champ « algorithm/parameters » : non présent • Champ « subjectPublicKey » : clé publique de 2048 bits (pour les cartes à puce P60 JCOP3) ou de 3072 bits (pour les autres supports).
Extensions	
Contraintes de base (basicConstraints)	Champ « CA » : FALSE (certificat d'entité finale) Champ « pathLenConstraint » : non présent (pas de

Nom du champ	Contenu
Critique	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**	Authentification (digitalSignature)
Utilisation étendue de clé (extendedKeyUsage) **Non critique**	Authentification du client (OID 1.3.6.1.5.5.7.3.2) secureShellClient (OID 1.3.6.1.5.5.7.3.21) Ouverture de session par carte à puce (OID 1.3.6.1.4.1.311.20.2.2) keyPurposeClientAuth (OID 1.3.6.1.5.2.3.4)
Politiques de certification (certificatePolicies) **Non critique**	Champ «policyIdentifier » : contient l'identifiant de la politique de certification régissant cette AC, du type : OID = 1.2.250.1.668.1.1.1.2.1 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
Nom alternatif de sujet (subjectAltName) **Non critique**	MS UPN = <Identifiant de la forme prenom.nom@KRB.GENDARMERIE.FR> KRB5PrincipalName = <Identifiant de la forme prenom.nom@KRB.GENDARMERIE.FR>
Points d'accès aux LCR/LAR (cRLDistributionPoints) **Non critique**	URI = http://crl.gendarmerie.fr/2024_fsi_ac_personnes_authentification.crl URI = http://crl.gendarmerie.interieur.gouv.fr/2024_fsi_ac_personnes_authentification.crl URI = http://crl.gendarmerie.interieur.ader.gouv.fr/2024_fsi_ac_personnes_authentification.crl

Nom du champ	Contenu
Accès aux informations de l'AC (authorityInfoAccess) **Non critique**	accessMethod : OID 1.3.6.1.5.5.7.48.2 : id-ad-caIssuers accessLocation : URI = http://crl.gendarmerie.fr/2024_fsi_ac_personnes_authentification.der URI = http://crl.gendarmerie.interieur.gouv.fr/2024_fsi_ac_personnes_authentification.der URI = http://crl.gendarmerie.interieur.ader.gouv.fr/2024_fsi_ac_personnes_authentification.der

VII.3. Format des certificats de signature des personnes

Nom du champ	Contenu
Champs de base	
Version (version)	2 (version 3)
Numéro de série (serialNumber)	Attribué par l'AC
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 Personnes Signature
Valide à partir du (validity/notBefore)	Date de génération par l'AC
Valide jusqu'au (validity/notAfter)	3 ans après la date de génération Pour les certificats des cartes provisoires : - 24h si le porteur possède déjà une carte active possédant des certificats - 1 an si le porteur ne possède pas déjà une carte active possédant des certificats

Nom du champ	Contenu
Objet (subject)	C = FR O = Gendarmerie nationale OrganizationIdentifier : NTRFR-157000019 OU = 0002 157000019 OU = Personnes Signature SN = *nom (test pour les certificats de test)* GN = *prénom (test pour les certificats de test)* CN=*prenom.nom (test.test pour les certificats de test)* UID = *NIGEND (000000 pour les certificats de test)* *E = prenom.nom@gendarmerie.interieur.gouv.fr (absent pour les cartes à puce P60 JCOP3)* *(test.test@gendarmerie.interieur.gouv.fr pour les certificats de test)*
Clé publique (subjectPublicKeyInfo)	Algorithme RSA : • Champ « algorithm/algorithm » : rsaEncryption • Champ « algorithm/parameters » : non présent • Champ « subjectPublicKey » : clé publique de 2048 bits (pour les cartes à puce P60 JCOP3) ou de 3072 bits (pour les autres supports).
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**	Signature (nonRepudiation)
Utilisation étendue de clé (extendedKeyUsage) **Non critique**	Messagerie électronique sécurisée (1.3.6.1.5.5.7.3.4) Signature de document (1.3.6.1.4.1.311.10.3.12)
Politiques de certification (certificatePolicies) **Non critique**	Champ «policyIdentifier » : contient l'identifiant de la politique de certification régissant cette AC, du type : OID = 1.2.250.1.668.1.1.1.4.1

Nom du champ	Contenu
	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_personnes_signature.crl URI = http://crl.gendarmerie.interieur.gouv.fr/2024_fsi_ac_personnes_signature.crl URI = http://crl.gendarmerie.interieur.ader.gouv.fr/2024_fsi_ac_personnes_signature.crl
Accès aux informations de l'AC (authorityInfoAccess) **Non critique**	accessMethod : OID 1.3.6.1.5.5.7.48.2 : id-ad-caIssuers accessLocation : URI = http://crl.gendarmerie.fr/2024_fsi_ac_personnes_signature.der URI = http://crl.gendarmerie.interieur.gouv.fr/2024_fsi_ac_personnes_signature.der URI = http://crl.gendarmerie.interieur.ader.gouv.fr/2024_fsi_ac_personnes_signature.der
Extensions « QC Statements »	
QC Statements	Déclaration de certificat qualifié
Conformité Certificat qualifié ETSI (QCS-1)	Utilisé
Dispositif qualifié de création de signature (QSCD) ETSI (QCS-4)	Utilisé
Type ETSI (QCS-6)	Signature électronique (eSign)
URL et langue du PDS ETSI (QCS-5)	URI = https://www.gendarmerie.interieur.gouv.fr/igc/pc Langue : Français

VII.4. Format des certificats de confidentialité des personnes

Nom du champ	Contenu
Champs de base	
Version (version)	2 (version 3)
Numéro de série (serialNumber)	Attribué par l'AC
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 Personnes Chiffrement
Valide à partir du (validity/notBefore)	Date de génération par l'AC
Valide jusqu'au (validity/notAfter)	3 ans après la date de génération Pour les certificats des cartes provisoires : - 24h si le porteur possède déjà une carte active possédant des certificats - 1 an si le porteur ne possède pas déjà une carte active possédant des certificats
Objet (subject)	C = FR O = Gendarmerie nationale OU = 0002 157000019 OU = Personnes Confidentialité SN = *nom (test pour les certificats de test)* GN = *prénom (test pour les certificats de test)* CN=*prenom.nom (test.test pour les certificats de test)* UID = *NIGEND (000000 pour les certificats de test)* *E=courriel (test.test@...)*
Clé publique (subjectPublicKeyInfo)	Algorithme RSA : • Champ « algorithm/algorithm » : rsaEncryption • Champ « algorithm/parameters » : non présent • Champ « subjectPublicKey » : clé publique de 2048 bits(pour les cartes à puce P60 JCOP3) ou de 3072 bits (pour les autres supports).
Extensions	

Nom du champ	Contenu
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**	KeyEncipherment
Politiques de certification (certificatePolicies) **Non critique**	Champ «policyIdentifier » : contient l'identifiant de la politique de certification régissant cette AC, du type : OID = 1.2.250.1.668.1.1.1.3.1 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_personnes_chiffrement.crl URI = http://crl.gendarmerie.interieur.gouv.fr/2024_fsi_ac_personnes_chiffrement.crl URI = http://crl.gendarmerie.interieur.ader.gouv.fr/2024_fsi_ac_personnes_chiffrement.crl
Accès aux informations de l'AC (authorityInfoAccess) **Non critique**	accessMethod : OID 1.3.6.1.5.5.7.48.2 : id-ad-caIssuers accessLocation : URI = http://crl.gendarmerie.fr/*2024_fsi_ac_personnes_chiffrement.der* *URI = http://crl.gendarmerie.interieur.gouv.fr/2024_fsi_ac_personnes_chiffrement.der* *URI = http://crl.gendarmerie.interieur.ader.gouv.fr/2024_fsi_ac_person*

Nom du champ	Contenu
	nes_chiffrement.der

VII.5. Format des listes de révocation (LCR) émises par les AC subordonnées « personnes physiques »

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 Personnes usage La valeur usage est l'un des usages suivants : • Authentification • Chiffrement • Signature
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 (userCertificat)	Numéro de série du certificat révoqué
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	Numéro séquentiel de la CRL

Nom du champ	Contenu
(CRLNumber) **Non critique**	
Empreinte numérique signée (signatureValue)	Suite de bits contenant le bloc de données signé par l'émetteur
Laisser les certificats expirés dans la CRL (ExpiredCertsOnCRL)	Utiliser (pour 2024 FSI AC Personnes Signature uniquement) Non présent pour les autres AC.

VII.6. Format des certificats de test d'authentification, de signature et de confidentialité des personnes

Comme indiqué dans les profils de certificat, les certificats de tests reprendront les données suivantes :

SN = *test (éventuellement test2, test3...)*

GN = *test (éventuellement test2, test3...)*

CN=test.test *(test2.test2...)*

UID = *NIGEND (000000 pour les certificats de test)*

E=courriel (test.test@..., test2.test2@...)

Ces certificats ne servent qu'à l'IGC dans le cadre des audits, des tests… et doivent être révoqués au plus tôt après la fin de leur utilisation.

VIII. Audit de conformité et autres évaluations

Voir [MESURES_IGC].

IX. Autres problématiques métiers et légales

Voir [MESURES_IGC].