MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ANFSI

IGC DES FORCES DE SÉCURITÉ INTÉRIEURE

Conditions Générales d'Utilisation

2024 FSI Machines

Version 1 mise à jour le 15 janvier 2025

Direction Générale de la Gendarmerie Nationale
4, rue Claude Bernard
92130 ISSY LES MOULINEAUX

1 Objet du document

Ce document définit les Conditions Générales d'Utilisation (CGU) des certificats délivrés par l'Autorité de Certification (AC) 2024 FSI AC Machines, parfois simplement désignée « AC » dans la suite du document, de l'Infrastructure de Gestion des Clés (IGC) des Forces de Sécurité Intérieure (IGC/FSI).

L'objectif de ce document est de présenter de manière synthétique les exigences à respecter par l'AC d'une part, et par les porteurs et les utilisateurs des certificats d'autre part. Ces exigences sont définies exhaustivement dans la Politique de Certification (PC) de cette AC, dont l'adresse de publication est définie ci-après. Conformément à la PC, les porteurs de certificats sont ici entendus comme les Responsables de Certificats (RC).

Ces CGU sont acceptées par le RC durant le processus de remise de ses certificats.

2 Identification du document

Ce document est référencé par son numéro de version affiché en page 1. Ce numéro est amené à évoluer de manière indépendante par rapport à l'OID de la PC susmentionnée.

3 Abréviations

AC	Autorité de Certification
AE	Autorité d'Enregistrement
ANFSI	Agence du Numérique des Forces de Sécurité Intérieure
CGU	Conditions Générales d'Utilisation
CNIL	Commission Nationale de l'Informatique et des Libertés
DPC	Déclaration des Pratiques de Certification
ETSI	*European Telecommunications Standards Institute*
FSI	Forces de sécurité intérieure
GN	Gendarmerie Nationale
IGC	Infrastructure de Gestion des Clés
OID	*Object IDentifier*
PC	Politique de Certification
PDS	*PKI Disclosure Statements*
PIN	*Personal Identification Number*

PKCS#10	*Public Key Cryptographic Standards* numéro 10
PKI	*Public Key Infrastructure* (IGC en français)
LAR	Liste des certificats d'AC Révoqués
LCR	Liste de Certificats Révoqués
SIC	Systèmes d'Information et de Communication

4 Conditions Générales d'Utilisation

Les CGU sont structurées conformément aux "PKI Disclosure Statement" (PDS) définis dans la norme ETSI 319 411-1 en annexe A.2.

4.1 Point de contact des Autorités de Certification

Direction Générale de la Gendarmerie Nationale
Agence du Numérique des Forces de Sécurité Intérieure
Direction de la Sécurité et de l'Architecture
Département des Services Socles
4 rue Claude Bernard
CS 60003
92136 Issy les Moulineaux Cedex
FRANCE

4.2 Type de certificats émis

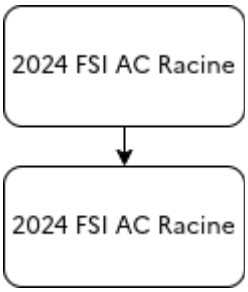
Ces CGU portent sur les certificats émis pour des machines par l'AC pour un usage précis :

AC	OID	Usage
2024 FSI AC Machines	1.2.250.1.668.1.1.1.7.1	Authentification serveur et signature de code

Les RC pouvant obtenir ces certificats sont des personnes physiques affectées à l'ANFSI ou dans une unité SIC relevant de la GN. Ils ne peuvent se connecter à l'AE technique qu'à l'aide de leur certificat électronique d'authentification conforme aux exigences du niveau [RGS] ** contenu dans leur carte professionnelle, garantissant ainsi la validation initiale de leur identité.

Dans la plupart des cas, ces certificats sont stockés dans des machines de type « serveurs » : serveurs physiques, serveurs virtuels, etc. Exceptionnellement, ils peuvent être stockés dans une clef USB stockée de façon sécurisée -- cas des certificats de signature de code -- ou dans une boîte noire cryptographique.

Chaque certificat est émis à travers la chaîne de certification suivante :



Les certificats de la chaîne de certification sont disponibles à l'adresse suivante : `https://igc.gendarmerie.fr`

Les certificats émis par l'AC 2024 FSI AC Machines sont rattachés à l'unité dans laquelle le RC se trouve au moment où il effectue sa demande, quelle que soit l'évolution ultérieure du statut ou de l'affectation du RC. Cette unité est ci-après désignée « unité de rattachement ».

4.3 Modalités d'obtention

Les certificats sont obtenus à la suite d'une demande formulée dans l'application Certilibre, AE technique de l'AC.

Un RC peut obtenir un certificat si les conditions cumulatives suivantes sont remplies :

- au choix :
  - il est enregistré dans l'annuaire central de la GN comme personnel SIC ;
  - il est enregistré dans l'annuaire de l'ANFSI ;
- le CN demandé est conforme à la PC ;
- la demande est validée par un valideur, tel que défini par la PC.

Le RC a le choix entre deux types de demande :

- cas numéro 1, le RC est administrateur du serveur sur lequel le certificat sollicité sera déployé :
  - il génère lui-même la bi-clé sur le serveur concerné en n'utilisant que la bibliothèque système `openssl` dans une version maintenue ;
  - il ajoute la demande de certificat au format *PKCS#10* au formulaire en ligne de demande de certificat
- cas numéro 2, le RC n'est pas administrateur du serveur sur lequel le certificat sollicité sera déployé :
  - la bi-clé sera automatiquement générée par l'autorité d'enregistrement technique ;
  - il en sera de même de la requête au format *PKCS#10*, transmise ensuite à l'AC.

Dans tous les cas, le RC appose sa signature électronique personnelle, horodatée et validée, sur le document PDF récapitulant sa demande. Il est ensuite prévenu par courriel qu'une demande de certificat a bien été enregistrée et est en attente de validation.

Également informé par courriel, le valideur vérifie le contenu de la demande et, s'il la juge opportune, la valide. Pour ce faire, il appose également sa propre signature électronique personnelle, horodatée et validée, sur ledit document PDF récapitulant la demande.

Dans le cas où est nécessaire la contre-validation par un des administrateurs, ceux-ci en sont informés par courriel. L'un d'eux peut alors vérifier le contenu de la demande et, s'il la juge opportune, la contre-valider. Pour ce faire, il appose également sa propre signature électronique personnelle, horodatée et validée, sur ledit document PDF récapitulant la demande.

Avant toute signature, RC, valideur et contre-valideur vérifient les données affichées à l'écran qui seront ensuite reprises dans le PDF signé : informations personnelles, données du certificat sollicité, lien vers les présentes CGU, etc.

Après validation simple ou double, selon le cas, la demande est transmise à l'AC en vue de la génération du certificat.

La fourniture du certificat est réalisée par envoi d'un courriel au RC et mise à disposition de tous les membres de son unité dans l'interface web de l'autorité d'enregistrement technique. En outre, dans le cas 2 évoqué *supra*, la bi-clé générée est transmise, via un support chiffré, aux personnels chargés de son déploiement sur l'équipement concerné.

4.4 Modalités de renouvellement

Il ne sera procédé à aucun renouvellement de certificat sans renouvellement de la bi-clé.

Le renouvellement (délivrance d'un nouveau certificat suite à un changement de bi-clé) est réalisé en fin de vie du certificat ou pour mettre à jour les données qu'il contient : *e.g.* ajout d'un nom alternatif dans un certificat. Le RC et l'unité de rattachement du certificat sont ainsi avertis de l'arrivée à expiration de leur certificat par courriel avant l'expiration.

Tout personnel de l'unité de rattachement du certificat peut effectuer une demande de renouvellement de ce dernier. Le processus est alors identique à celui de la génération initiale du certificat.

Afin d'éviter toute interruption de service, la génération d'un nouveau certificat avec un DN déjà existant est autorisée, à la seule condition que le service applicatif concerné par le certificat soit le même. En conséquence, toute demande de renouvellement par un RC non affecté dans l'unité de rattachement du certificat fera l'objet d'une contre-validation par un administrateur.

4.5 Modalité de révocation

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

- le RC ayant sollicité la génération du certificat initial ;
- tout membre de l'unité de rattachement du certificat initial, alors considéré comme RC du certificat à révoquer ;
- un administrateur de l'IGC.

Révocation par le RC ou tout membre de l'unité de rattachement du certificat :

Le RC peut demander la révocation du certificat dans l'AE technique. Cette demande fait l'objet d'un formulaire PDF signé par le RC. Ce dernier transmet ce document à un administrateur de l'AC.

Révocation par un administrateur de l'IGC :

Exceptionnellement, un administrateur habilité de l'IGC peut révoquer le certificat d'un RC, pour une raison telle qu'une erreur dans les informations ou dans le formulaire de demande du certificat, une suspicion de compromission de la clé privée ou la fin de vie du service applicatif.

Dans tous les cas, le RC et l'unité de rattachement du certificat concerné sont notifiés de sa révocation.

4.6 Limites d'usages

Les certificats ne sont utilisables que pour un usage prévu par l'AC dans sa PC :

- authentification d'un service applicatif serveur ;
- authentification d'un service applicatif client ;
- signature de code.

De plus, les certificats ne doivent être utilisés que par un service applicatif des FSI ou par un service applicatif tiers pour ses relations avec les FSI pour le cas de porteurs externes.

Tout usage non explicitement permis est interdit et engage la responsabilité du RC. Tout certificat est émis pour une durée de 3 ans et la clé privée correspondante n'est plus utilisable après l'expiration ou la révocation du certificat.

Les dossiers d'enregistrement, les traces d'application, les journaux d'audit ou procès-verbaux relatifs au cycle de vie des certificats des AC et des porteurs sont conservés sur toute la durée de vie de l'IGC/FSI et au minimum 10 ans après leur génération.

4.7 Obligations des porteurs

Les RC doivent :

- communiquer des informations exactes pour leur enregistrement dans l'annuaire de la Gendarmerie nationale ou de l'ANFSI, et l'informer de toute modification de celles-ci ;
- communiquer des informations exactes et à jour lors de :
  - leur demande de certificat ;
  - leur demande de renouvellement de certificat ;
  - leur demande de révocation de certificat ;
- prendre, ou faire prendre, toutes les mesures nécessaires pour protéger la clé privée associée à leur certificat, tout au long du cycle de vie de ce dernier, et notamment :
  - ne pas la faire transiter en clair ;
  - paramétrer les propriétaires et groupes ainsi que les droits pour en autoriser la lecture par les seuls utilisateurs système strictement requis ;
  - l'effacer en fin de vie, que ce soit après l'installation d'un nouveau certificat à la suite du renouvellement du précédent, à l'expiration d'un certificat non renouvelé ou à la révocation d'un certificat en cours de validité ;
- respecter les conditions d'usage du certificat ;
- accepter les présentes CGU ;
- notifier à l'AE technique leur refus du certificat généré dans les huit jours suivant sa génération, aux fins de révocation dudit certificat. Ils utilisent le formulaire *ad hoc*. L'absence de réaction du RC vaut acceptation implicite du certificat, *a fortiori* en cas d'installation et/ou d'utilisation du certificat ;
- demander sans délai la révocation de son certificat dès que nécessaire, par exemple en cas de perte, de vol ou de compromission de la clé privée associée ;

4.8 Obligations de vérification des certificats par les utilisateurs

Les utilisateurs des certificats doivent :

- vérifier que le certificat utilisé a bien été émis par l'AC ;
- vérifier l'usage pour lequel le certificat a été émis ;
- vérifier que le certificat n'est pas présent dans la LCR de l'AC ;
- vérifier la signature du certificat ;
- vérifier la chaîne de certification jusqu'à l'AC 2024 FSI AC Racine et contrôler la validité des certificats.

La CRL de l'AC 2024 FSI AC Machines est disponible aux adresses suivantes :

- `http://crl.gendarmerie.fr/2024_fsi_ac_machines.crl` ;
- `http://crl.gendarmerie.interieur.gouv.fr/2024_fsi_ac_machines.crl` ;
- `http://crl.gendarmerie.interieur.ader.gouv.fr/2024_fsi_ac_racine.crl` ;
- `http://crl.gendarmerie.interieur.rie.gouv.fr/2024_fsi_ac_racine.crl`

4.9 Limite de responsabilité

L'AC ne saurait être tenue responsable d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées, des LAR et des LCR, ainsi que de tout autre équipement ou logiciel mis à disposition.

4.10 Références documentaires

La PC de l'AC est accessible aux adresses suivantes :

- `https://igc.gendarmerie.fr` ;
- `https://www.gendarmerie.interieur.gouv.fr/igc/pc`

4.11 Politique de confidentialité

Toute collecte et tout usage de données à caractère personnel par l'AC sont réalisés dans le strict respect de la législation en vigueur, en particulier des dispositions de la CNIL (Loi n° 78-17 du 6 janvier 1978 modifiée). Les données à caractère personnel ne sont ni divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre obligation légale.

Les dossiers d'enregistrement ainsi que les événements entraînés par les actions des RC sont conservés 10 ans, dans des conditions garantissant leur intégrité et leur confidentialité.

4.12 Conditions d'indemnisation

Sans objet

4.13 Loi applicable et résolution des conflits

La PC de l'AC est soumise au droit français.

Toute réclamation doit être adressée à l'Inspection générale de la Gendarmerie nationale, dont l'adresse électronique est : `iggn@gendarmerie.interieur.gouv.fr`

4.14 Audits et références applicables

Un contrôle de conformité de l'IGC/FSI à la PC est effectué au minimum une fois tous les 2 ans.

Par ailleurs, avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC fera également procéder à un contrôle de conformité de cette composante.