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

Gendarmerie nationale

IGC de la Gendarmerie Nationale

Conditions Générales d'utilisation

AC « Personnes » V4

Version 624 mise à jour le 30-04-2024

1 Objet du document

Ce document définit les Conditions Générales d'Utilisation (CGU) des certificats délivrés par les Autorités de Certification suivantes de l'IGC de la Gendarmerie nationale :

AC	OID	Usage
AC GN Personnes Authentification v4	1.2.250.1.189.1.1.1.2.1	Authentification
AC GN Personnes Confidentialité v4	1.2.250.1.189.1.1.1.3.1	Confidentialité
AC GN Personnes Signature v4	1.2.250.1.189.1.1.1.4.2	Signature

Ces AC sont dénommées AC « Personnes » v4 ou simplement AC dans la suite du document. L'objectif de ce document est de présenter de manière synthétique les exigences à respecter par les Autorités de Certification 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 de ces Autorités de Certification, dont l'adresse de publication est définie ci-après.

Ces CGU sont acceptées par le porteur de certificat durant le processus de remise de ses certificats. Elles sont valables de façon identique pour les trois Autorités de Certification.

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 des Politiques de Certification sus mentionnées.

3 Abréviations

AC	Autorité de Certification
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
GN	Gendarmerie Nationale
IGC	Infrastructure à Gestion de Clés
OID	Object IDentifier
PC	Politique de Certification
PDS	PKI Disclosure Statements
PIN	Personal Identification Number
PKI	Public Key Infrastructure (IGC en français)
LAR	Liste des certificats d'AC Révoqués
LCR	Liste de Certificats Révoqués

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

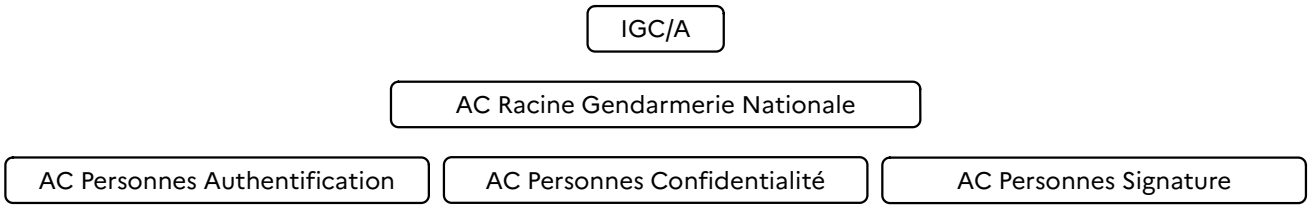
4.2 Type de certificats émis

Ces CGU portent sur les certificats émis pour des personnes physiques, par trois AC, chacune délivrant des certificats pour un usage précis :

AC	OID	Usage
AC GN Personnes Authentification v4	1.2.250.1.189.1.1.1.2.1	Authentification
AC GN Personnes Confidentialité v4	1.2.250.1.189.1.1.1.3.1	Confidentialité
AC GN Personnes Signature v4	1.2.250.1.189.1.1.1.4.2	Signature

Les porteurs pouvant obtenir ces certificats sont des personnes physiques affectés dans une unité relevant de la gendarmerie nationale. Ces certificats sont stockés dans une puce cryptographique présente sur une carte remise au porteur.

Chaque certificat est émis à travers une des chaînes de certification suivantes :



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

4.3 Modalités d'obtention

Un porteur peut obtenir un certificat de chacune des AC s'il est enregistré dans l'annuaire central de la Gendarmerie nationale et qu'il répond à un certain nombre de conditions propres à l'IGC.

Le porteur est prévenu qu'une demande de carte a été faite pour lui, puis reçoit une carte sans certificat. Le porteur se rend auprès de son valideur (notateur ou autre personne habilitée) qui vérifie son identité et exécute la procédure automatisée de génération de clés et de certificats.

Le porteur choisit les codes PIN à saisir par la suite pour utiliser soit la clé privée d'authentification ou de chiffrement, soit la clé privée de signature.

Le porteur est informé que la clé privée de chiffrement est séquestrée par l' « AC GN Personnes Confidentialité v4 ». La fonction de recouvrement de cette clé privée est à l'usage exclusif du porteur lui-même, sauf cas exceptionnel (décès du porteur, enquête judiciaire,. . .).

Le porteur et le valideur vérifient les données affichées à l'écran (informations personnelles, données des certificats, . . .).

Le porteur lit les présentes CGU. La signature électronique des CGU vaut également acceptation des certificats.

4.4 Modalités de renouvellement

Le renouvellement (délivrance d'un nouveau certificat suite à un changement de bi-clé) est réalisé en fin de vie des certificats du porteur ou pour mettre à jour les données personnelles du porteur. Le porteur est ainsi averti de l'arrivée à expiration de ses certificats par courriel avant l'expiration.

Le porteur peut renouveler ses certificats auprès de son valideur (notateur ou autre personne habilitée).

Les anciens certificats sont révoqués et les clés privées détruites, exception faite de la précédente bi-clé de confidentialité conservée pour permettre l'exploitation des données chiffrées par le précédent certificat de confidentialité.

4.5 Modalité de révocation

Lorsqu'une demande de révocation est faite, elle concerne simultanément tous les certificats de sa carte.
Les personnes / 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.

Révocation par le porteur :
Le porteur peut demander la révocation de ses certificats :

- auprès de son valideur ;
- auprès du personnel SIC en dehors des heures ouvrées.

Révocation par le valideur ou un opérateur de l'IGC :
Le valideur (ou exceptionnellement un opérateur habilité de l'IGC) peut révoquer les certificats d'un porteur, pour une raison telle qu'une erreur dans les informations ou dans le dossier d'enregistrement du porteur, une suspicion de compromission des clés privées ou le décès du porteur.

Révocation automatique par l'IGC :

L'IGC révoque automatiquement les certificats renouvelés ou ceux d'un porteur quittant la Gendarmerie nationale (ou ne remplissant plus les conditions de détention des certificats).

Dans tous les cas le porteur et le valideur sont notifiés de la révocation des certificats.

4.6 Limites d'usages

Les certificats ne sont utilisables que pour l'usage prévu spécifique à chaque AC :

L'usage du certificat électronique d'authentification délivrés par l'AC « Personnes Authentification » est l'authentification des porteurs auprès de serveurs distants dans le cadre d'un contrôle d'accès à un serveur ou une application.

L'usage du certificat électronique de signature délivrés par l'AC « Personnes Signature » est 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 « Personnes Confidentialité » 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.

De plus, les certificats ne doivent être utilisés que dans la cadre de l'activité du porteur au sein de la Gendarmerie nationale, ou pour ses relations avec la Gendarmerie nationale pour le cas de porteurs externes.

Tout usage non explicitement permis est interdit et engage la responsabilité du porteur. Les certificats sont émis pour une durée de 3 ans et les clés privées correspondantes (authentification et signature) ne sont plus utilisables après l'expiration ou la révocation des certificats. Les clés privées de chiffrement sont utilisables au moins 6 ans via le recouvrement, et jusqu'à 10 ans par recouvrement du séquestre, pour déchiffrer les données.

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 et au minimum 10 ans après leur génération.

4.7 Obligations des porteurs

Les porteurs de certificats doivent :

- communiquer des informations exactes pour leur enregistrement dans l'annuaire de la Gendarmerie nationale et l'informer de toute modification de celles-ci ;
- protéger la carte contre le vol, la perte ou une détérioration ;
- protéger la confidentialité des codes PIN ;
- respecter les conditions d'usage des certificats ;
- demander sans délai la révocation de ses certificats, par exemple en cas de perte, de vol de sa carte ou de ses codes PIN ;
- accepter les Conditions Générales d'Utilisation et les certificats qui lui sont présentés lors de son enrôlement.

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'une des AC citées dans la description des certificats ci-dessus ;
- vérifier l'usage pour lequel le certificat a été émis ;
- vérifier que le certificat n'est pas présent dans les listes de révocation ;
- vérifier la signature du certificat, et de la chaîne de certification, jusqu'à l'AC « IGC /A » et contrôler la validité des certificats, en vérifiant également que le certificat de l'autorité de certification fait partie de la liste de confiance européenne (TRUSTED LIST) disponible sur le site de l'agence nationale de la sécurité des systèmes d'information.

Les listes de révocation des certificats émis par les AC sont disponibles à l'adresse suivante :

`http://crl.gendarmerie.fr`
`http://crl.gendarmerie.interieur.gouv.fr`
`http://crl.gendarmerie.interieur.ader.gouv.fr`

4.9 Limite de responsabilité

Les AC ne pourront pas être tenues responsables d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées et des données d'activation, des LAR et des LCR ainsi que de tout autre équipement ou logiciel mis à disposition.

4.10 Références documentaires

Les Politiques de Certification des AC sont accessibles à l'adresse suivante :

`http://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 les 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 des personnes ainsi que les événements entrainés par les actions des porteurs 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

Les Politiques de Certification des AC sont soumises au droit français.

Toute réclamation doit être adressée à l'inspection générale de la gendarmerie nationale. L'adresse courriel de l'inspection générale de la gendarmerie nationale est :
`iggn@gendarmerie.interieur.gouv.fr`

4.14 Audits et références applicables

Un contrôle de conformité de l'IGC 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.

Les trois AC « Personnes » ont obtenu la qualification de leur offre de certificats électroniques vis-à-vis du Référentiel Général de Sécurité v2 pour le niveau **. L'AC Personne Signature a obtenue la qualification de ces certificats électroniques vis à vis de l'eIDAS pour la signature électronique qualifiée (QCP-n-qscd).