IGC de la Gendarmerie Nationale

Conditions Générales d'utilisation
AC GN « Machines Cachet serveur »

version 3.0 du 10 avril 2022

1 Objet du document

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

AC	OID	Usage
AC GN Machines Cachet Serveur	1.2.250.1.189.1.1.1.5.1	Signature Cachet Serveur

Cette AC est dénommée « AC GN Machines Cachet Serveur » ou simplement AC dans la suite du document.
L'objectif de ce document est de présenter de manière synthétique les exigences à respecter par l'Autorité de Certification d'une part, et par les demandeurs et les responsables des certificats d'autre part. Ces exigences sont définies exhaustivement dans la Politique de Certification de cette Autorité de Certification, dont l'adresse de publication est définie ci-après.
Ces CGU sont acceptées par le demandeur de certificat lors de la demande.

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 Politique de Certification sus mentionnée.

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
HSM	Hardware Security Module

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
Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure
Sous-Direction des Applications de Commandement
Bureau du Contrôle Opérationnel des Fichiers
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 une AC, délivrant des certificats pour un usage précis :

AC	OID	Usage
AC GN Machines Cachet Serveur	1.2.250.1.189.1.1.1.5.1	Signature Cachet Serveur

Les demandeurs pouvant obtenir ces certificats sont des personnes physiques relevant de la gendarmerie nationale ou de la police nationale. La délivrance de certificat se fait sur présentation d'une requête de certification. Cette dernière est fournie par les administrateurs du HSM (boîtier cryptographique) protégeant les clés de la solution de signature. Cette opération est un préalable à toute demande.

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

IGC/A

AC Racine Gendarmerie Nationale

AC GN Machines Cachet Serveur

Les certificats de la chaîne de certification sont disponibles à l'adresse suivante :

`https://stsisi.psi.minint.fr/securite/1598/igc`

ainsi que sur internet à l'adresse suivante :

`https://www.gendarmerie.interieur.gouv.fr/igc`

4.3 Modalités d'obtention

Les modalités d'obtention sont décrites dans le document : demande de certificat cachet serveur, disponible à l'adresse suivante :

`https://stsisi.psi.minint.fr/sites/default/files/redacteurs/transfert_files/Demande%20de%20certificat%20Cachet%20serveur.pdf`

La demande est faite au nom d'une entité appartenant à la gendarmerie nationale. Cette demande est établie par le commandant d'unité. Elle porte un numéro de courrier avec un timbre correspondant à l'unité au profit de laquelle la demande est établie. Elle est signée par le commandant d'unité.
Cette demande est établie dans le cadre :

- de la déclaration des pratiques de certification portant l'OID 1.2.250.1.189.1.1.2.2 ;
- de la politique de certification Cachet serveur portant l'OID 1.2.250.1.189.1.1.1.5.1.

La procédure de génération de certificat nécessite une rencontre physique entre la personne délivrant le certificat et celle le demandant. Cependant, le demandeur peut désigner un responsable de certificat appartenant à son unité. Ce dernier le représente dans le cadre de la délivrance du certificat demandé. Cette délégation n'est valable que pour cette seule demande.

4.4 Modalités de renouvellement

Le renouvellement consiste à délivrer un nouveau certificat contenant les mêmes informations que le précédent mais associé à un nouveau bi-clé. Cette opération est réalisée au plus tard deux mois avant la fin de vie des certificats (3 ans). Le demandeur devra suivre la démarche décrite dans la section 4.3 pour en obtenir un autre.

4.5 Modalité de révocation

Les modalités de révocation sont décrites dans le document : demande de révocation cachet serveur, disponible à l'adresse suivante :

`https://stsisi.psi.minint.fr/sites/default/files/redacteurs/transfert_files/Demande_revocation_certificat_machine-v1.0.pdf`

La révocation du certificat cachet serveur va entraîner la nullité de toutes les pièces qui viendraient à être signées par le certificat dès lors qu'il aura été révoqué. Il est donc important de s'assurer que le nécessaire a été fait en amont pour qu'il ne soit plus utilisé par le socle de signature de la gendarmerie nationale.

La demande est faite au nom de l'entité ayant fait la demande initiale. En cas de réorganisation, il s'agit de l'unité ayant pris la suite de l'unité initiale. Cette demande est établie par le commandant d'unité. Elle porte un numéro de courrier avec un timbre correspondant à l'unité au profit de laquelle la demande est établie. Elle est signée par le commandant d'unité.

Il est demandé de fournir tous les éléments permettant d'identifier le certificat à révoquer. Toute demande ambiguë pouvant rendre la révocation impossible sera rejetée. Par ailleurs, une demande établie avec des éléments inexactes risque d'entraîner la révocation d'un autre certificat avec tous les effets de bords induits.

4.6 Limites d'usages

Les certificats ne sont utilisables que pour l'usage prévu spécifiquement pour l'AC : Signature numérique effectuée par un serveur applicatif sur des données dans le but de pouvoir être utilisée pour l'authentification de l'origine des données, soit aux fins de non répudiation d'échanges dématérialisés entre usagers et l'administration ou entre différentes administrations.

Tout usage non explicitement permis est interdit et engage la responsabilité du demandeur. Les certificats sont émis pour une durée de 3 ans et les clés privées correspondantes ne sont plus utilisables après l'expiration ou la révocation des certificats.

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 10 ans.

4.7 Obligations des demandeurs

Les demandeurs de certificats doivent présenter :
— un formulaire papier de demande intégralement renseigné, daté, numéroté et signé par le demandeur et le responsable de certificat désigné ;
— la pièce d'identité du demandeur s'il se déplace et celle de son responsable de certificat s'il se fait représenter.

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 citée 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 l'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

L'AC ne pourra pas être tenue responsable 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 :

`https://stsisi.psi.minint.fr/securite/1598/igc`
Et sur internet à l'adresse suivante:
`https://www.gendarmerie.interieur.gouv.fr/igc`

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 et des demandeurs de certificat cachet serveur sont archivés 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 pourra être effectué, sur demande de l'une des Autorités de Certification, 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.

L'AC GN « Machines Cachet Serveur » a obtenu la qualification de son offre de certificats électroniques vis-à-vis du Référentiel Général de Sécurité v2 pour le niveau **.

L'AC GN « Machines Cachet Serveur » a obtenu la qualification de son offre de certificats électroniques vis-à-vis de l'eIDAS pour la signature électronique qualifiée (QCP-n-qscd).