CONDITIONS GENERALES D'UTILISATION DE L'IGC-MI CERTIFICATS SERVEURS

1. Introduction

Le présent document résume les informations pertinentes de la politique de certification de l'autorité de certification déléguée du ministère, relative à la délivrance de certificats serveurs de niveau de sécurité conforme au RGS *.
Cette autorité de certification délivre les certificats aux serveurs, aux clients applicatifs et aux équipements réseaux du ministère de l'Intérieur.

2. Généralités

RCAS : le responsable de certificat d'authentification serveur est une personne physique qui est responsable de l'utilisation du certificat d'authentification du serveur identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'entité également identifiée dans ce certificat.

RCC : le responsable du certificat de cachet est la personne physique responsable de l'utilisation du certificat de cachet du serveur identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'entité également identifiée dans ce certificat.

Opérateur demandeur : personnel désigné au sein d'une entité du ministère chargé d'initialiser la demande de certificats qui est transmis à un RCAS/RCC.

Administrateur demandeur : Rôle confié au RCAS/RCC chargé au sein du système de gestion des cartes et des certificats, de gérer (création, suppression) les opérateurs demandeurs.

Ce document doit être connu de tous les RCAS/RCC qu'ils doivent parapher.

Les politiques de certification sont identifiées par les OIDs suivantes :

autorité de certification	CERTIFICATS	OID
SERVEUR 1E 2018	Certificat SSL Serveur 1* MultiSAN	1.2.250.1.152.2.12.41.1.21
	Certificat SSL Serveur 1*	1.2.250.1.152.2.12.41.1.2
	Certificat SSL Client 1*	1.2.250.1.152.2.12.41.1.3
	Certificat Serveur Cachet 1	1.2.250.1.152.2.12.41.1.5
	Certificat Contrôleur Domaine AD 1*	1.2.250.1.152.2.12.41.1.4
	Certificat Serveur OCSP 1*	1.2.250.1.152.2.12.41.1.6
	Certificat Signature de code 1*	1.2.250.1.152.2.12.41.1.8
	Certificat Serveur Horodatage 1*	1.2.250.1.152.2.12.41.1.11

Les politiques de certification peuvent être consultées sur le site internet : https://www.interieur.gouv.fr/IGC/PC

3. Désignation et fin d'activité des opérateurs demandeurs

Au sein des entités susceptibles d'avoir besoin de certificats serveurs, le responsable de l'entité désigne des opérateurs demandeurs en utilisant l'imprimé spécifique.

L'opérateur demandeur doit être titulaire d'une carte agent ministérielle.
L'imprimé est transmis à l'administrateur des opérateurs (RCAS/RCC de l'entité).
La fin d'activité d'un opérateur demandeur est signalée de la même façon.

4. Désignation et fin d'activité de RCAS/RCC

Au sein des entités susceptibles d'avoir besoin de certificats serveurs, le responsable de l'entité désigne un ou des RCAS/RCC en utilisant l'imprimé spécifique. Le RCAS/RCC doit être titulaire d'une adresse de messagerie, d'une carte agent ministérielle et d'une clé Acid.

Le RCAS/RCC prend connaissance des présentes CGU qu'il signe.

Le dossier complet doit comprendre :

- l'imprimé de désignation dûment complété,
- le document CGU signé,
- la copie recto verso de la carte nationale d'identité du RCAS/RCC,
- le certificat d'authentification du RCAS/RCC.

Le dossier est transmis par mail au SHFD, chiffré par ACID qui étudie la complétude et la faisabilité de la demande et procède à l'accréditation ou non du RCAS/RCC. La décision est communiquée au demandeur.

En cas d'une prochaine cessation d'activité, le RCAS/RCC en informe le responsable de l'entité afin qu'un nouveau RCAS/RCC soit désigné et enregistré auprès du service du haut-fonctionnaire de défense. L'entité administrative doit signaler au SHFD, préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RCAS/RCC de ses fonctions et lui désigner un successeur.

Ce nouveau RCAS/RCC doit bénéficier au minimum des mêmes autorisations en termes de noms de domaine et de types de certificats car il devient automatiquement responsable des certificats de son prédécesseur.

Le RCAS/RCC doit être titulaire d'une carte agent ministérielle.

La fonction de RCAS/RCC est rôle de confiance. Le RCAS/RCC ne doit notamment pas avoir de condamnation de justice en contradiction avec ses attributions. La désignation par l'autorité signifie que cette vérification a été faite.

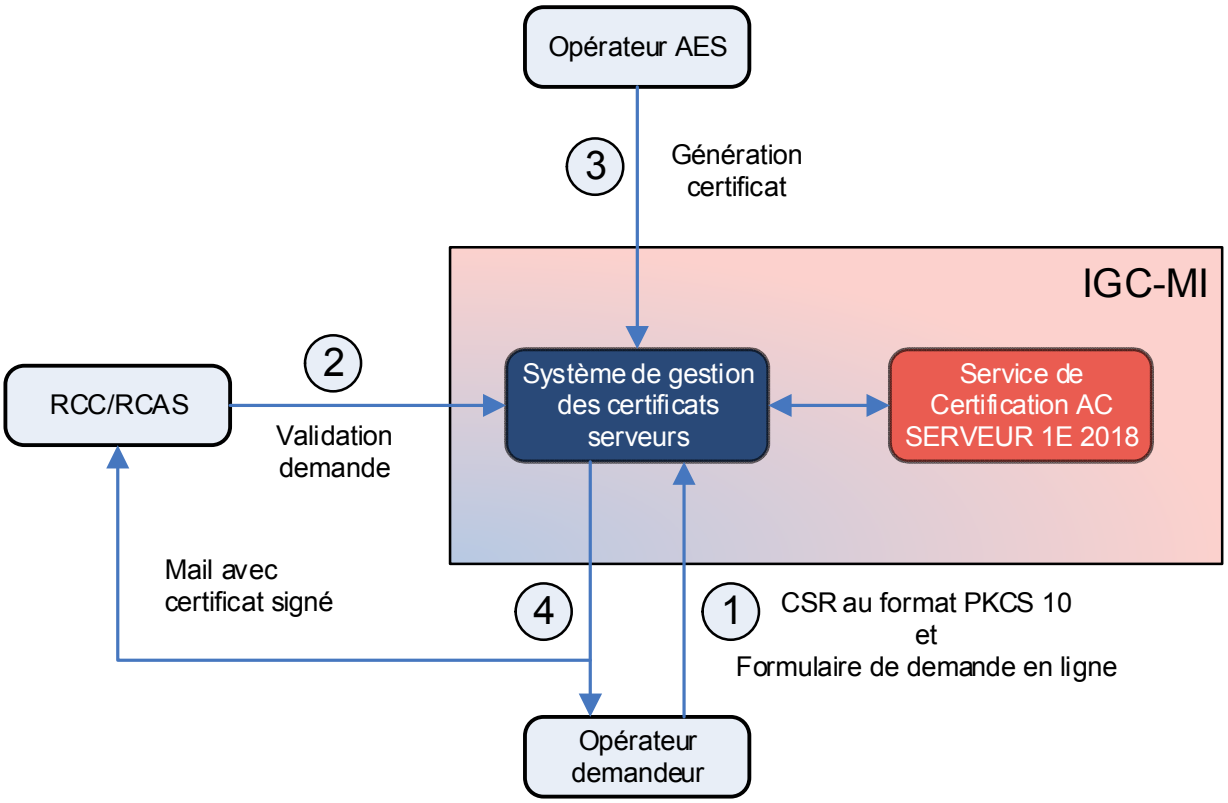
5. Demandes de certificats

Aucune demande de certificat ne peut avoir lieu sans opérateur demandeur et sans RCAS/RCC.

Le RCAS/RCC ne peut pas demander de certificat

- pour un nom de domaine n'appartenant pas au ministère de l'intérieur,
- pour un nom de domaine ou un type de certificat pour lequel il n'a pas été autorisé par le responsable de l'entité dans le formulaire de désignation.

La demande de certificat suit le processus suivant :



1- L'opérateur demandeur du certificat serveur se connecte au système de gestion des cartes et des certificats en utilisant un certificat d'authentification RGS qualifié au niveau de sécurité RGS 2 étoiles puis remplit le formulaire de demande de certificats avec les informations demandées, joint une CSR au format PKSC10 préalablement généré en respect avec la PC, choisit le type de certificat et valide sa demande, qui est transmise et au RCAS/RCC qui valide la demande.
2- RCAS/RCC se connecte au système de gestion des cartes et des certificats en utilisant un certificat d'authentification RGS qualifié au niveau de sécurité RGS 2 étoiles. Il étudie la demande puis la rejette en cas de non-conformité ou la valide. La demande de certificat est transmise à l'autorité d'enregistrement serveur.
3- l'AES autorise la génération du certificat par l'autorité AC SERVEUR 1E 2018 qui signe la CSR du demandeur.
4- Le système de gestion des cartes et des certificats transmet le certificat signé au RCAS/RCC et à l'opérateur demandeur par courrier électronique.

Dispositions particulières pour une demande de certificat « cachet », « OCSP » ou « horodatage » :
Une demande au format papier est renseignée et envoyée au SHFD pour étude car ce type de certificat nécessite un boîtier cryptographique. Le SHFD étudie le dossier et répond au RCAS/RCC s'il autorise ou non la création du certificat. Les échanges se font par mail dont les pièces jointes sont chiffrés par ACID.

Il est à noter que le certificat étant attaché au serveur informatique et non au RCAS/RCC, ce dernier peut être amené à changer en cours de validité du certificat : départ du RCAS/RCC de l'entité administrative, changement d'affectation et de responsabilités au sein de l'entité, etc.

6. Usage des certificats

Les certificats émis selon la politique de certification **AC SERVEUR 1E 2018** permettent :

- de signer des données, afin que les utilisateurs de certificats puissent en vérifier la signature (le cachet). Ces données peuvent être, par exemple, un accusé de réception suite à la transmission d'informations par un usager à un serveur informatique, une réponse automatique d'un serveur informatique à une demande formulée par un usager ou la signature d'un jeton d'horodatage, une signature de code d'une application développée par les services du ministère de l'intérieur.

Ceci correspond notamment aux relations suivantes :

1. Apposition d'un cachet signature sur des données par un serveur informatique sous la responsabilité d'une autorité administrative du ministère de l'intérieur et vérification de cachet par un usager.
2. Apposition d'un cachet signature sur des données par un serveur informatique sous la responsabilité d'une autorité administrative du ministère de l'intérieur et vérification de ce cachet par un agent.
3. Apposition d'un cachet signature sur des données par un serveur informatique sous la responsabilité d'une autorité administrative du ministère de l'intérieur et vérification de ce cachet par un autre serveur informatique.
4. Apposition d'un cachet signature sur un exécutable ou un script développé par les services du ministère de l'intérieur pour confirmer l'identité de l'auteur du code et garantir que le code n'a pas été modifié ou corrompu après la signature, le RCC est responsable de vérifier l'intégrité du code signé.
5. Apposition d'un cachet signature sur un exécutable sur un jeton OCSP pour vérifier l'état d'un certificat en ligne.

- d'authentifier ces serveurs dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS, avec les catégories d'utilisateurs de certificats identifiées au chapitre 1.3.5 de la politique de certification et établir une clé symétrique de session afin que les échanges au sein de ces sessions soient chiffrés.

Ceci correspond notamment aux relations suivantes :

1. Etablissement d'une session sécurisée entre un serveur sous la responsabilité d'une autorité administrative du ministère de l'intérieur et un usager,
2. Etablissement d'une session sécurisée entre un serveur sous la responsabilité d'une autorité administrative du ministère de l'intérieur et un agent,
3. Etablissement d'une session sécurisée entre deux serveurs dont au moins l'un des deux est sous la responsabilité d'une autorité administrative du ministère de l'intérieur.

Les contraintes suivantes sont à respecter:

- Pour les fonctions cachet signature et cachet horodatage, l'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service de cachet de données émises par le serveur.
- Pour les fonctions cachet signature de code le certificat associé est strictement limitée à l'utilisation pour signer des applications développées par les services du ministère de l'intérieur.
- Pour les fonctions authentification client et serveur, l'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service d'authentification et d'établissement d'une session sécurisée : authentification du serveur, échange de la clé symétrique de session.
- Le ministère ne procède pas au renouvellement de certificat sans renouvellement de bi-clé. Une demande de renouvellement de certificat correspond à une nouvelle demande pour un même serveur ayant déjà bénéficié d'un certificat pour le même usage. Une nouvelle CSR est exigée.

7. Obligations du RCAS/RCC

- Le RCAS/RCC est administrateur des opérateurs demandeurs. Il doit à cet effet conserver les formulaires de désignation et de cessation d'activité.
- Le RCAS/RCC s'engage, pour chaque certificat à respecter des dispositions de la PC correspondante, en particulier le paragraphe 12.2.
- Vérifier les identités des opérateurs demandeurs qu'il enregistre.
- Le RCAS/RCC doit s'assurer du respect strict des usages autorisés des bi-clés et des certificats au niveau des serveurs et de l'intégrité du code signée par les certificats de signature de code. Dans le cas contraire, leur responsabilité pourrait être engagée. L'usage autorisé de la bi-clé du serveur et du certificat associé est indiqué dans les extensions du certificat. Les usages des certificats sont listés ci-dessus.
- L'acceptation du certificat par le RCAS/RCC est implicite. À partir de la date de la validation de la demande du certificat, le RCAS/RCC dispose d'un délai de 8 jours ouvrés pour notifier son refus du certificat auprès de l'autorité de certification pour révocation en utilisant le formulaire réservé à cet effet.
- Le RCAS/RCC doit vérifier le contenu du certificat avant toute installation sur un serveur car son installation ou utilisation. L'installation et l'utilisation valent acceptation du certificat.
- Le RCAS/RCC surveille les dates de validité des certificats qui lui ont été remis de façon à déclencher leur renouvellement au minimum 15 jours francs avant la date d'expiration du certificat.
- Le RCAS/RCC doit aviser au plus vite l'AE Serveur en cas de compromission ou de suspicion de compromission de la clé privée correspondante. (Ou de ses données d'activations) et demander la révocation du certificat avec le formulaire adéquat.

Le RCAS/RCC a le devoir de :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat
- Protéger la clé privée du serveur dont il a la responsabilité par des moyens appropriés à son environnement

- Protéger les données d'activation de cette clé privée et, le cas échéant, les mettre en œuvre
- Vérifier l'intégrité du code et des applications signées par un certificat de signature de code sous l'autorité de l'IGC-MI.
- Protéger l'accès à la base de certificats du serveur.
- Informer l'AA et l'AE Serveur de tout événement relatif à ses fonctions de RCAS/RCC (cessation, transfert…)
- Informer l'AA et l'AE serveur de l'arrêt définitif ou de changement de contexte d'emploi du service applicatif pour lequel le certificat a été délivré.
- Le RCAS/RCC s'assure que le certificat de signature de code sera utilisé pour signer des codes développés par des personnels du ministère ou par des prestataires extérieurs dans le cadre d'un marché passé par une entité du ministère de l'intérieur. Ce code devra être exempt de faille de sécurité et son utilisation réservée aux applications internes au ministère de l'Intérieur.

En cas de renouvellement de certificats :

- La demande de renouvellement équivaut à une nouvelle demande pour le serveur considéré.
- La réutilisation des bi-clés est interdite et de nouvelles bi-clés sont générées.
  Le nouveau PKCS# 10 et la demande doit être faite par l'opérateur demandeur et validé par le responsable RCC/RCAS.
- Le nouveau certificat ne pourra être émis au plus tôt que moins de trois mois (90 jours) avant la fin de vie du certificat en cours.

8. Obligations de l'autorité de certification Serveur

L'autorité de certification serveur publie les informations suivantes à destination entre autres des RCAS/RCC:

- Les politiques de certifications
- La liste des certificats révoqués (serveurs et autorités de certification),
- Les certificats d'autorité de certification (AC serveur et AC de la hiérarchie).

L'autorité de certification fournit aux RCAS/RCC la déclaration des pratiques de certification. Ce document étant de niveau Diffusion Restreinte, il est fourni sous une forme numérique chiffrée par ACID. Le RCAS/RCC s'engage à ne pas le diffuser et à le stocker toujours sous la forme chiffrée, sauf à disposer d'un système d'information homologué pour traiter ce type d'informations.

9. Révocation des certificats

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

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du nom du serveur), ceci avant l'expiration normale du certificat,
- Le RCC/RCAS n'a pas respecté les modalités applicables d'utilisation du certificat,
- Le RCC/RCAS ou l'entité n'a pas respecté son obligation découlant de la présente PC,
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement,
- La clé privée du serveur est suspectée de compromission, est compromise, est perdue ou est volée, (éventuellement les données d'activation associées),

- Le RCC/RCAS, ou une entité autorisée (représentant légal de l'entité, par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du serveur et/ou de son support),
- L'arrêt définitif du serveur ou la cessation d'activité de l'entité du RCC/RCAS de rattachement du serveur.

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

Les demandes de révocation sont faites par le RCC/RCAS ou un représentant légal de l'entité en utilisant l'imprimé spécifique.
Les informations suivantes doivent au moins figurer dans la demande de révocation de certificat :

- Le nom du serveur utilisé dans le certificat,
- [A-SER] le FQDN du serveur utilisé dans le certificat,
- Le nom du demandeur de la révocation,
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série,), éventuellement, la cause de révocation.

La demande est envoyée par courriel au pôle SSI à l'adresse suivante :

dsic-polessi@interieur.gouv.fr

Une fois la demande authentifiée et contrôlée, 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 au minimum via une CRL signée par l'autorité de certification.
Le demandeur de la révocation, le RCC/RCAS et l'opérateur demandeur, sont informés par mail du bon déroulement de l'opération et de la révocation effective du certificat par mail.
L'entité est aussi informée de la révocation de tout certificat qui lui est rattaché.
L'opération est enregistrée dans les journaux d'événements de l'IGC-MI.

10. Archivage des données

Les données archivées sont les suivantes :

- Les PC ;
- Les DPC ;
- Les certificats et LCR tels qu'émis ou publiés;
- Les récépissés ou notifications (à titre informatif);
- Les justificatifs d'identité des RCC/RCAS et de leur entité de rattachement;
- Les journaux d'évènements des différentes entités de l'IGC.

Les dossiers de demande de certificat accepté sont archivés aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable.

Les journaux d'évènements traités au chapitre 6.4.1 Type d'évènements à enregistrer de la PC AC SERVEUR 1E 2018 seront archivés pendant 8 ans après leur génération.

11. Aspect légal

Le point de contact ministériel est :

Ministère de l'Intérieur
Secrétaire Général
Service du Haut Fonctionnaire de Défense
Place Beauvau
75800 PARIS CEDEX 08

Adresse pour le courriel : igc-mi@interieur.gouv.fr.

Le système de gestion des cartes et des certificats a fait l'objet d'une déclaration à la CNIL. Les données personnelles sont alors supprimées du système de gestion des cartes et des certificats du ministère 5 ans après le départ définitif de l'agent du ministère.

Le ministère décline toute responsabilité à l'égard de l'usage de cette carte agent dans des conditions ou à des fins autres que celles prévues dans la politique de certification et rappelées ci-dessus et quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, et quant aux retards, à l'altération ou autres erreurs pouvant se produire dans la transmission de toute télécommunication. Il ne saurait être tenu responsable, et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente politique lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'Article 1148 du Code civil.
La responsabilité de l'Etat peut seulement être mise en cause en cas de non-respect des dispositions prévues par les politiques de certification.

Les tribunaux administratifs sont compétents dans la résolution des conflits

12. Diffusion de l'information

- Les PC sont diffusés sur le site https://www.interieur.gouv.fr/IGC/PC
- Les certificats des AC et les CRL sont diffusés sur le site http://crl.interieur.gouv.fr/
- Les formulaires http://ssi.minint.fr/index.php/services/certificats-serveurs-de-ligc-mi
- Le système de gestion des cartes et des certificats https://cartes.minint.fr/cams/

Le Préfet,
Haut fonctionnaire de défense adjoint