CONDITIONS GENERALES D'UTILISATION DES CERTIFICATS SERVEUR CACHET EIDAS

Les présentes CGU précisent vos obligations et engagements pour votre certificat serveur.
Elles doivent être signées lors de la demande de certificats de type cachet eIDAS.

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 certificat serveur cachet de niveau de sécurité conforme au RGS ** et eIDAS.
Cette autorité de certification délivre les certificats aux clients applicatifs.

1. Généralités

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

Ce document doit être connu de tous les RC qu'ils doivent parapher.

La politique de certification de l'autorité de certification déléguée des certificats serveurs de type cachet eIDAS est identifiée comme suit :

AC DELEGUEES MINISTERE DE L'INTERIEUR	OID PC
AC SERVEUR CACHET eIDAS V1	1.2.250.1.152.2.12.5.31

Les certificats serveur de cachet déclinés de ces politiques sont identifiés par les OID suivantes :

AUTORITE CERTIFICATION	CERTIFICATS	OID
AC SERVEUR CACHET eIDAS V1	Certificat Serveur Cachet	1.2.250.1.152.2.12.5.31.5
	Certificat Serveur Horodatage	1.2.250.1.152.2.12.5.31.9

La durée de validité des certificats de type cachet signature est au maximum de 3 ans.
La durée de validité des certificats de type cachet horodatage est au maximum 5 ans.

Les politiques de certification peuvent être consultées sur le site internet :

https://www.interieur.gouv.fr/IGC/PC

2. Usages et consignes d'utilisation

2.2 Désignation et fin d'activité de RC

Au sein des entités susceptibles d'avoir besoin de certificats serveur cachet, le responsable de l'entité désigne un ou des RC en utilisant l'imprimé spécifique. Le RC doit être titulaire d'une adresse de messagerie, et de pouvoir utilisé un conteneur chiffré.

Le RC 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 RC,

Il appartient au RC de fournir au SHFD la preuve qu'il est autorisé à valider les certificats pour les noms de domaines indiqués dans sa demande.

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

En cas d'une prochaine cessation d'activité, le RC en informe le responsable de l'entité afin qu'un nouveau RC 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 RC de ses fonctions et lui désigner un successeur.

Ce nouveau RC 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.

.

La fonction de RC est rôle de confiance. Le RC 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.

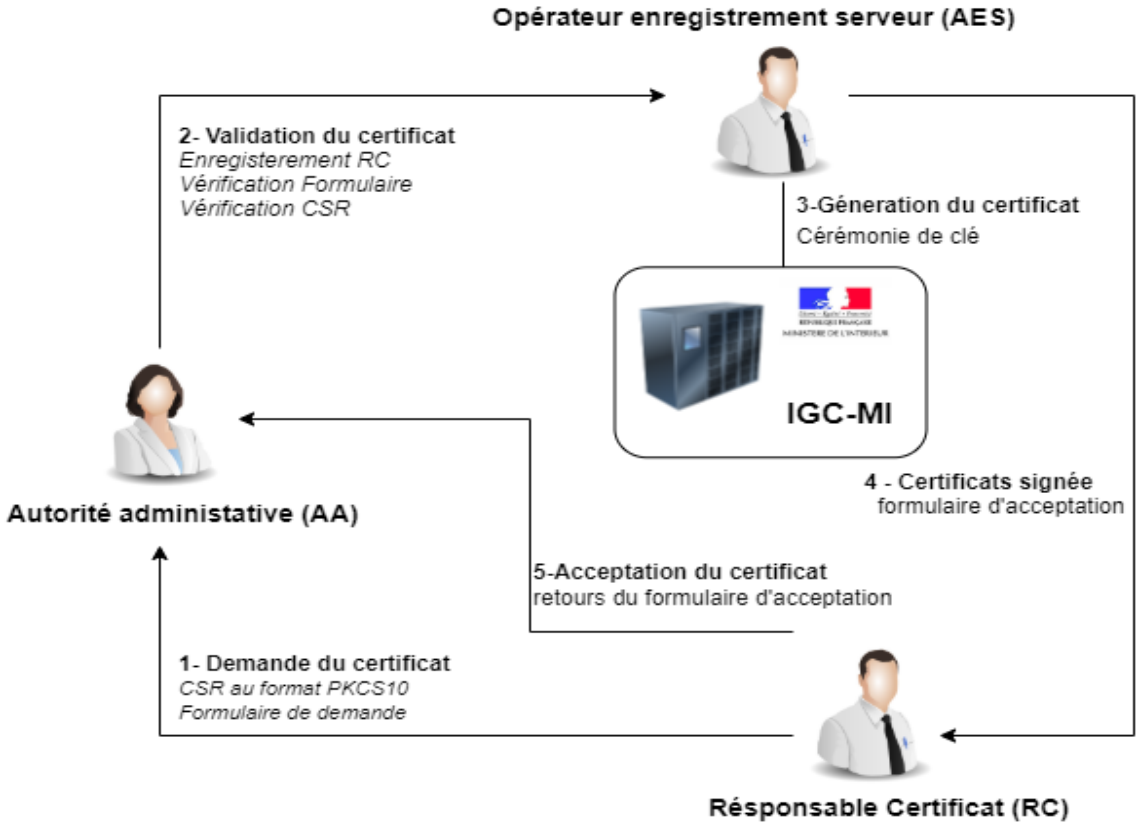
2.3 Demandes de certificats

Aucune demande de certificat ne peut avoir lieu sans RC.

Le RC ne peut pas demander de certificat

- 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. Le responsable du certificat cachet serveur (RC) doit transmettre le formulaire de demande de certificat cachet eIDAS avec toutes les informations demandées, joint d'une CSR au format PKSC10 préalablement généré en respect avec la PC.
2. Le responsable de l'Autorité Administrative (AA) vérifie la demande puis rejette la demande en cas de non-conformité ou la valide. La demande de certificat est transmise à l'autorité d'enregistrement serveur.
3. L'opérateur AES organise la cérémonie de génération du certificat par l'Autorité l'AC SERVEUR CACHET eIDAS V1 qui signe la CSR du demandeur.
4. L'AES transmet le certificat signé au RC en format électronique
5. Le RC accepte ou refuse le certificat en transmettant le formulaire d'acceptation a l'AA. En cas de refus, une demande de révocation du certificat est transmise à l'AES qui organise la révocation du certificat dans les délais impartis.

Dispositions:

- Une demande au format papier est renseignée et envoyée au SHFD pour étude car ce type de certificat nécessite **un boîtier cryptographique qualifiée**.
- Le SHFD étudie le dossier et répond au RC s'il autorise ou non la création du certificat. Les échanges se font par mail dont les pièces jointes sont chiffrées.

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

2.4 Usage des certificats

Les certificats émis selon la politique de certification de l'AC serveur de cachet permettent :

- de signer des données, afin que les utilisateurs de certificats puissent en vérifier la signature (le cachet). Ces données peuvent être, par exemple, la signature d'un jeton d'horodatage.

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 sur un jeton OCSP pour vérifier l'état d'un certificat en ligne.

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.
- 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.

2.5 Obligations du RC

- Le RC s'engage, pour chaque certificat à respecter des dispositions de la PC correspondante, en particulier le paragraphe IX.6.3.
- Le RC doit vérifier les identités des opérateurs demandeurs qu'il enregistre.
- Le RC doit s'assurer du respect strict des usages autorisés des bi-clés et des certificats au niveau des serveurs. 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 RC est implicite. À partir de la date de la validation de la demande du certificat par l'AA, le RC 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 RC 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 RC surveille les dates de validité des certificats qui lui ont été remis de façon à déclencher leur renouvellement au minimum 45 jours francs avant la date d'expiration du certificat.
- Le RC 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 RC 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
- 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 RC (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.

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 le responsable de certificat RC.
- 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.

2.6 Obligations de l'autorité de certification Serveur

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

- 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 RC la déclaration des pratiques de certification. Ce document étant de niveau Diffusion Restreinte, il est fourni sous une forme numérique chiffrée. Le RC 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.

2 .7 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 RC n'a pas respecté les modalités applicables d'utilisation du certificat,
- Le RC ou l'entité n'a pas respecté son obligation découlant de la PC serveur,
- 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 RC, 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 RC 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 RC 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,

- 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 :

dnum-mpssi@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 RC, sont informés par mail du bon déroulement de l'opération et de la révocation effective du certificat.
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.

2.8 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 RC 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 « V.4.1 Type d'évènements à enregistrer » de la PC serveur de cachet eIDAS seront archivés pendant 7 ans après leur génération.

3. Autres dispositions

Les politiques de certification des autorités de certification émettrices des certificats électroniques de la carte agent ministérielle sont disponibles à l'adresse https://www.interieur.gouv.fr/IGC.
Les PC sont diffusés sur le site https://www.interieur.gouv.fr/IGC/PC
Les CRL sont diffusés sur le site http://crl.interieur.gouv.fr/ et http://crl2.interieur.gouv.fr/
Les certificats des AC sont diffusés sur le site https://www.interieur.gouv.fr/IGC/Certificat.
Les formulaires sont disponibles sur le site http://ssi.minint.fr/index.php/services/certificats-serveurs-de-ligc-mi

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

4. Responsabilités

Le ministère décline toute responsabilité à l'égard de l'usage de ce certificat 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 des présentes conditions générales 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.

5. Politique de protection des données personnelles

Le système d'information utilisé a fait l'objet d'une déclaration auprès de la CNIL.

Conformément à la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée et au Règlement général sur la protection des données RGPD), le responsable du traitement, le Secrétaire Général, met en œuvre le traitement « Certificat serveur » qui vise aux finalités suivantes : délivrer des certificats serveurs.

Ce traitement collecte les catégories de données suivantes :

- Données d'identification des personnes ;
- Journaux d'évènement de l'application de gestion des certificats serveur.

Ces données sont conservées pour une durée de :

- Données d'identification des personnes : 7 ans après le départ définitif de l'agent du ministère ;
- Journaux d'évènement de l'application gestion des cartes : 7 ans après leur génération.

Elles ne sont accessibles qu'aux personnes suivantes : opérateurs-demandeurs, responsables de certificats, opérateurs AE Serveur.

Pour exercer vos droits d'accès, de rectification, de limitation et d'effacement (sous certaines conditions, art.17 du RGPD), vous devez vous adresser au point de contact ministériel (Cf. chapitre 3 « Autres dispositions »).

Conformément à l'article 21 du RGPD, vous avez le droit de vous opposer à tout moment au traitement des données vous concernant, en justifiant de raisons tenant à votre situation particulière. Le responsable du traitement peut toutefois refuser cette opposition s'il dispose de motifs légitimes et impérieux. Ce droit s'exerce de la même manière.

Ce traitement est contrôlé par le délégué ministériel à la protection des données du ministère de l'intérieur (Délégué ministériel à la protection des données – Ministère de l'intérieur – Place Beauvau – 75800 Paris Cedex 08). Vous pouvez aussi déposer une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL – 3 place de Fontenoy – TSA 80715 – 75334 Paris Cedex 07). »

Le Préfet,
Haut fonctionnaire de défense adjoint