

## PROCEDURE D'OBTENTION DES CERTIFICATS LOGICIELS CONTEXTE ROR POUR UNE APPLICATION METIER

### INTRODUCTION

Cette fiche pratique est destinée aux services informatiques qui souhaitent mettre en œuvre une connexion sécurisée TLS/SSL, en conformité avec la politique de sécurité définie dans la Doctrine d'Urbanisation autour du ROR, dans l'échange suivant :

- Consommation des données du ROR national par une application métier ;
- Consommation des données

Pour répondre à ce besoin où les ROR et les applications consommatrices s'authentifient en tant que client TLS/SSL, l'offre de l'IGC-Santé est la suivante :

certificat d'authentification Client SSL de l'offre ELEMENTAIRE  
ORG AUTH\_CLI

Le serveur doit faire confiance à l'IGC-Santé en installant le certificat d'autorité de l'IGC-Santé racine dans le magasin de confiance du serveur. Seul le certificat racine doit être « trusté », lors de la réception d'une requête de connexion d'un client, la chaîne de confiance sera reconstituée avec le certificat d'ACI « organisations » poussée par le client avec son certificat d'authentification.

La procédure d'obtention du certificat logiciel de l'offre ORG AUTH\_CLI suit trois étapes :

- vérification des prérequis ;
- demande d'habilitation à la commande du certificat ;
- commande et installation du certificat logiciel.

### 1. PREREQUIS A LA COMMANDE DU CERTIFICAT LOGICIEL

Afin de commander le certificat logiciel, les prérequis suivants doivent être respectés :

Le représentant légal de la structure (ou de son délégataire dûment habilité à le représenter) doit disposer d'un contrat avec l'ANS et être équipé d'une carte CPE ou CPA responsable active.

Si le représentant légal de la structure n'a pas de contrat et/ou de carte CPE, CPA responsable, ce dernier doit compléter une demande d'attribution d'une carte de représentant légal de structure accessible au téléchargement sur le site web de l'ANS<sup>1</sup>, rubrique « Commandes » (formulaire n°101).

Le représentant légal de la structure désigne un (ou plusieurs) administrateur(s) technique(s) et s'assure qu'il est (sont) porteur(s) d'une carte CPE ou d'une carte CPA nominative et active.

L'administrateur technique est une personne de confiance à qui le représentant légal de la structure délègue le droit de gérer le cycle de vie (demande, retrait, révocation et suivi) des certificats logiciels commandés pour le programme ROR.

Si le désigné n'a pas de carte CPE/A, le représentant légal doit faire une demande d'attribution de carte de personnel de structure accessible au téléchargement sur le site

[https://esante.gouv.fr/sites/default/files/media\\_entity/documents/F301.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/F301.pdf) (formulaire n°301).

N. B. Il est également possible de se rendre sur le portail TOM à l'adresse <https://tom.eservices.esante.gouv.fr/tom/> afin de réaliser cette démarche de manière dématérialisée.

**POUR TOUTE INFORMATION COMPLEMENTAIRE**, contactez notre service client à l'adresse : [monserviceclient.cartes@esante.gouv.fr](mailto:monserviceclient.cartes@esante.gouv.fr)

ou au **08 25 85 20 00** Service 0,06 € / min + prix appel

### 2. DEMANDE D'HABILITATION A LA COMMANDE DU CERTIFICAT LOGICIEL

Une fois les prérequis réunis, il est nécessaire d'habilitier votre administrateur technique à la commande des certificats délivrés par l'ANS.

(N. B. un administrateur technique est peut-être déjà habilité à la commande des certificats. Dans ce cas, pour déterminer si votre administrateur technique est déjà habilité à la commande de certificats nécessaires dans le cadre du programme ROR, vous avez accès à la plateforme IGC Santé afin de vérifier l'existence de ses droits.)

Le représentant légal de la structure :

- télécharge une demande d'habilitation sur le site ([formulaire n°413 en annexe de cette procédure](#)).
- complète, signe et envoie à [monserviceclient.cartes@esante.gouv.fr](mailto:monserviceclient.cartes@esante.gouv.fr) le formulaire n°413 de commande du certificat logiciel.

Pour la partie 4.2 « Usage des certificats et solution utilisée », indiquer dans le champ « Précisions sur l'usage des certificats et sur votre projet » :

- **Pour authentifier votre application consommatrice des données du ROR, « Programme ROR – usage pour une application consommatrice du ROR pour s'authentifier en tant que client TLS/SSL. »**

Pour la partie 4.3 « Type de certificat souhaité » :

- **Cocher « Certificat ORG (Personne morale) usage AUTH\_CLI, SIGN, CONF (Ex : DMP, ROR, Annuaire Santé...) »**

Le ou les administrateurs techniques de la structure seront notifiés par courriel qu'ils sont habilités à commander les certificats logiciels choisis sur la Plateforme IGC-Santé.

<sup>1</sup> Le contenu dédié aux produits de certification de l'IGC-Santé est accessible sur le site internet de l'ANS, dans la rubrique

### 3. COMMANDE ET INSTALLATION DU CERTIFICAT LOGICIEL

L'administrateur technique de l'établissement prend connaissance de la documentation disponible sur le site <https://industriels.esante.gouv.fr/produits-services/jgc-sante-certificats-personnes-morales-et-serveurs>.

Les documents clés pour générer et installer le CSR et la bi-clé :

- [Le guide d'utilisation des services IHM Plateforme IGC-Santé](#) (document ANS\_IGC-Sante\_Guide-IHM) ;
- [La procédure de génération de CSR](#) (document ANS-PUSC-PSCE\_generation-de-csr). Il est possible de générer le bi-clé et la CSR en ligne pendant la commande ; le certificat et le bi-clé sont générés au format PKCS12 avec les 2 certificats ACI et ACR.

**Les prérequis pour générer et installer le CSR et la bi-clé figurent au chapitre 5 du guide d'utilisation, en particulier :**

- un poste équipé d'un lecteur de carte à puce ;
- un accès à internet pour accéder à la Plateforme IGC-Santé (<https://pfc-auth.eservices.esante.gouv.fr>).

A l'étape n°3 de commande du produit sur PFCNG, nous recommandons de suivre les règles de nommage suivantes pour le « service applicatif » :

**Pour la demande ORG\_AUTH\_CLI :**

- dans la cas de la recherche-interROR, indiquer la valeur « CLIENT\_WS\_ROR »,
- dans le cas de la consommation du ROR national, indiquer la valeur « CLIENT\_WS\_RORN »,
- dans le cas de la consommation de l'annuaire santé par les ROR régionaux, indiquer la valeur « CLIENT\_WS\_ANNUAIRE ».

A l'étape 4 de commande du produit, il est possible de générer la bi-clé et le CSR en ligne pendant la commande, ou de charger son CSR si ce dernier a déjà été généré :

- **Il est possible de générer en ligne la bi-clé et le CSR si besoin. Dans ce cas, le certificat et la bi-clé sont générés en ligne au format P12.** Il est nécessaire de voir avec votre solution ROR ou votre éditeur d'application sous quel format seront utilisés le certificat et la bi-clé.
- **Il est possible de charger son CSR si ce dernier et la bi-clé associée ont déjà été générés. Dans ce cas, il est nécessaire de rajouter le certificat d'autorité intermédiaire, que l'on peut télécharger à l'adresse <http://jgc-sante.esante.gouv.fr/AC/ACI-EL-ORG.cer>**

**Remarque :**

Tous les ROR doivent faire confiance à l'AC IGC Santé RACINE ELEMENTAIRE <http://jgc-sante.esante.gouv.fr/AC/ACR-EL.cer>

**EN CAS DE DOUTE**, contactez notre support technique :

- [monserviceclient.cartes@esante.gouv.fr](mailto:monserviceclient.cartes@esante.gouv.fr) pour les questions sur la commande technique sur la plateforme IGC Santé;
- [editeurs@esante.gouv.fr](mailto:editeurs@esante.gouv.fr) pour les questions d'implémentation des bi-clés et des certificats par les éditeurs.

### CYCLE DE VIE DES CERTIFICATS LOGICIELS

Le certificat logiciel, une fois généré, a une **validité de 3 ans**. Le ou les administrateurs techniques désignés seront alertés par courrier électronique de l'arrivée à échéance du certificat un mois avant que ce dernier ne soit plus valide.

Durant les 3 ans de validité, le représentant légal de la structure ou ses mandataires ont la possibilité de gérer les habilitations (ajout ou suppression) des administrateurs techniques de certificat. (Cf. <https://esante.gouv.fr/produits-services/certificats-logiciels> rubrique « La plateforme IGC Santé »).

Si vous générez un certificat comportant des erreurs ou en cas de perte ou de vol de certificat, il est nécessaire de le **révoquer**. Les modalités sont décrites au chapitre 11 du guide d'utilisation des services IHM.