PROCEDURE D'OBTENTION DES CERTIFICATS LOGICIELS CONTEXTE ROR

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 les échanges suivants :

- **Echanges entre ROR ;**
- **Consommations des données du ROR par une application métier ;**
- **Consommation des données des Référentiels Nationaux par les ROR (RPPS, ADELI, AMELI, …).**

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

Remarque : les certificats de l'IGC CPS-2bis ne sont plus distribués. Le serveur doit faire confiance à l'IGC-Santé, en complément de l'IGC-CPS2bis, 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[1], 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 http://esante.gouv.fr/securite/cartes-et-certificats, rubrique « commandes » (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.certificats@asipsante.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'habiliter 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 *http://esante.gouv.fr/securite/cartes-et-certificats*, rubrique « commandes» (formulaire n°413 en annexe de cette procédure).**
- **complète, signe et envoie à *monserviceclient.certificats@asipsante.fr* le formulaire n°413 de commande du certificat logiciel.**

Pour la partie 4.1 « Usage des certificats et solution utilisée », indiquer dans le champ « Précisions sur l'usage des certificats et sur votre projet » :

- **Pour authentifier votre ROR dans la recherche Inter-ROR, « Programme ROR – usage pour authentifier le ROR en tant que client TLS/SSL. »**
- **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. »**

[1] *Le contenu dédié aux produits de certification de l'IGC-Santé est accessible sur le site internet de l'ANS, dans la rubrique « commandes» : http://esante.gouv.fr/securite/cartes-et-certificats*

- **Pour authentifier votre ROR auprès des services de l'annuaire.sante.fr, « Programme ROR – usage pour authentifier le ROR auprès de l'Annuaire Santé. »**

Pour la partie 4.2 « Offre de certificat souhaitée » :

- **Cocher « Offre certificat logiciel ORG (Personne morale) usage AUTH_CLI».**

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.

3. COMMANDE ET INSTALLATION DU CERTIFICAT LOGICIEL

L'administrateur technique de l'établissement prend connaissance de la documentation disponible sur l'**Espace intégrateur CPS** (*http://integrateurs-cps.asipsante.fr/*, rubrique « IGC Santé » puis « Portail Web ») 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, indiquer la valeur « CLIENT_WS_ROR ».**

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://igc-sante.esante.gouv.fr/AC/ACI-EL-ORG.cer***

Remarque :

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

Les premiers ROR qui ont été déployés utilisent toujours en accès client des certificats SSL Serveur émis par l'IGC CPS-2bis donc il faut aussi faire confiance à l'AC IGC CPS-2bis RACINE : http://annuaire.asipsante.fr/dsdgetbinary?Connection=CEduSAA-Meibo&attachmentFile=certificat.cer&typeMime=application/pkix-cert&attribute=cACertificate&type=certificate&index=0

EN CAS DE DOUTE, contactez notre support technique :

- ***monserviceclient.certificats@asipsante.fr*** pour les questions sur la commande technique sur la plateforme IGC Santé;
- *editeurs@asipsante.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. ***http://esante.gouv.fr/securite/cartes-et-certificats*** *rubrique « sécurité » puis « cartes et certificats »*).

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.