Procédure d'obtention des certificats logiciels de test pour le raccordement des éditeurs à ROC

Introduction

Dans le cadre de la mise en service de ROC, l'ASIP Santé propose cette fiche pratique destinée aux éditeurs de SIH souhaitant mettre en œuvre le dispositif ROC.

L'ASIP Santé propose une offre de services de confiance et de produits de certification (IGC-Santé) visant à sécuriser les échanges et le partage de données entre les acteurs du monde de la santé.
Pour qualifier leurs logiciels, les éditeurs doivent commander deux certificats logiciels spécifiques émis par l'IGC-Santé :

2 certificats logiciels

- un **certificat de type ORG AUTH_CLI** ;
- un **certificat de type ORG_SIGN**.

En annexe sont présentés les schémas synthétisant les certificats et mécanismes de sécurité mis en œuvre dans les échanges entre les ETS, AMC et annuaire.

La procédure d'obtention des certificats logiciels suit deux étapes :

1. Vérification des pré-requis : cartes CPx de test et habilitations
2. Commande et installation des certificats logiciels

1. Vérification des prérequis : cartes CPx de test et habilitations

L'éditeur a la possibilité de commander des cartes de professionnel de santé de test, de les désigner en tant qu'administrateur technique et d'ouvrir les habilitations sur les offres de certificat de test nécessaires.

Deux cas de figure peuvent se présenter : l'éditeur ne dispose pas de cartes CPx de test (A) : l'éditeur dispose de cartes CPx de test (B).

(A) <u>L'éditeur ne dispose pas de cartes CPx de test :</u>

- L'éditeur commande des cartes CPx de test sur l'Espace CPS, rubrique « Vos Commandes » (*formulaire n°414 – section 3*) :

Etape 3.1 Renseigner l'usage suivant « **Projet ROC – Authentification** ».

Etape 3.2 Cocher « Offre kit d'intégration » et indiquer la quantité souhaitée dans la colonne « IGC Santé ».

- L'éditeur demande des habilitations sur les offres de certificats de test nécessaires (*formulaire n°414 – section 4)* :

Etape 4.1 Renseigner les usages suivants « **Projet ROC – usage signature d'un jeton SAML pour répondre au cas d'usage de l'authentification directe d'une personne morale (ES ou assimilé) conformément au Cadre d'interopérabilité technique des services AMC. Usage visé par l'équipe projet ASIP Santé N3 »** <u>et</u> « **Projet ROC – usage authentification TLS mutuelle pour répondre au cas d'usage de l'authentification directe d'une personne morale (ES ou assimilé) conformément aux spécifications de l'annuaire AMC. Usage visé par l'équipe projet ASIP Santé N3** ».

Etape 4.2 Cocher « **Offre certificat logiciel ORG (Personne morale) usage AUTH_CLI, SIGN, CONF ».**

Etape 4.3 Cocher « Non, les cartes de test à associer sont celles commandées dans la partie 3 de ce formulaire ». Dans ce cas, Il est nécessaire d'indiquer que l'on souhaite habiliter 1 des 5 cartes du kit, par exemple la carte CDE.

(B) <u>L'éditeur dispose de cartes CPx de test désignées en tant qu'administrateur technique:</u>

- L'éditeur peut vérifier les offres de certificat de test sur lesquelles ses cartes sont habilitées de deux façons :
  - par mail à l'adresse monserviceclient.developpement@asipsante.fr ;
  - sur la plateforme IGC-Santé à l'adresse https://pfc.eservices.esante.gouv.fr/pfcng-ihm/authentication.xhtml.

- Si les cartes CPx de test ne possèdent aucune habilitation sur les offres de certificat de test, l'éditeur doit les demander sur l'Espace CPS, rubrique « Vos Commandes » (*formulaire n°414 – section 4)* :

Etapes 4.1 et 4.2 Suivre la même procédure que précisé ci-dessus pour les éditeurs ne disposant pas de cartes CPx de test (A).

Etape 4.3 Cocher « Oui » et renseigner les numéros des cartes CPx de test à habiliter.

2. Commande et installation des certificats logiciels

Pour la commande des certificats logiciels de test, l'éditeur suit la même procédure qu'un établissement pour la commande de ses certificats réels.

Commande du produit sur PFCNG[1] :

Etape 3

- pour la demande **ORG_AUTH_CLI**, indiquer la valeur « **Client_ROC_Annuaire_AMC** » ;
- pour la demande **ORG_SIGN**, indiquer la valeur «**Client_ROC_WebServices_AMC** ».

Il est possible de :

Etape 4

- **générer en ligne la biclé et le CSR** si besoin. Dans ce cas, le certificat et la biclé sont générés en ligne au format PKCS12 ;
- **charger son CSR** si ce dernier et la biclé 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.

*En cas de doute, contactez notre support technique à l'adresse **editeurs@asipsante.fr**.*

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.

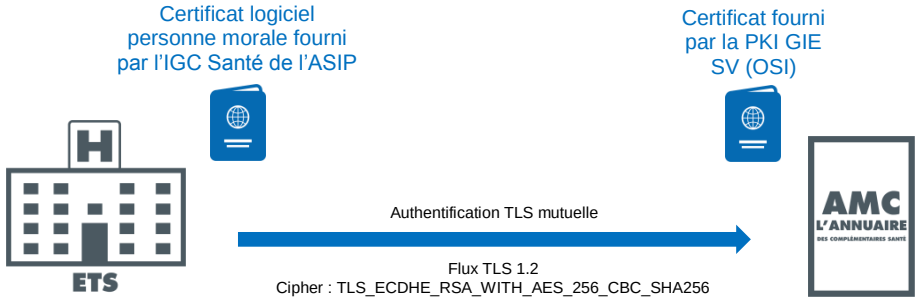
Durant les 3 ans de validité, le représentant légal de la structure ou ses mandataires ont la possibilité de gérer les habilitations (ajout ou suppression) des administrateurs techniques de certificat. (cf. L'Espace CPS, rubrique « Vos démarches »).

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 Plateforme IGC-Santé.

[1] Accès : **https://pfc-auth.eservices.esante.gouv.fr**

Annexe : sécurisation des échanges

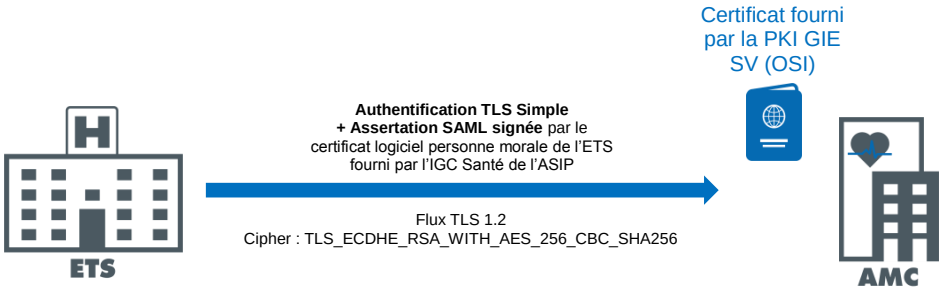
- **Échanges entre les ETS et le service d'annuaire : le schéma ci-dessous synthétise les certificats et mécanismes de sécurité mis en œuvre dans les échanges entre les ETS et le service d'annuaire**



Vérifications réalisées lors de l'établissement du flux TLS
- ► Validité du certificat serveur
  - Parenté (autorité)
  - Dates de début et de fin de validité
  - Etat de révocation (optionnel)

Vérifications réalisées lors de l'établissement du flux TLS
- ► Validité du certificat client
  - Parenté (autorité)
  - Dates de début et de fin de validité
  - Etat de révocation (optionnel)

- **Échanges entre les ETS et les AMC : le schéma ci-dessous synthétise les certificats et mécanismes de sécurité mis en œuvre dans les échanges entre les ETS et les AMC**



Vérifications réalisées lors de l'établissement du flux TLS
- ► Validité du certificat serveur
  - Parenté (autorité)
  - Dates de début et de fin de validité
  - Etat de révocation (optionnel)

Vérifications réalisées lors de la réception de la réponse de l'AMC
- ► Validité de la signature du document métier
- ► Validité du certificat de signature du document
  - Parenté (autorité)
  - Dates de début et de fin de validité
  - Etat de révocation (optionnel)
  - Valeur de l'extension keyusage (nonRepudiation)
- ► Identification de l'AMC

Vérifications réalisées lors de la réception de la requête
- ► Validité de la signature de l'assertion SAML
- ► Validité du certificat de signature de l'assertion
  - Parenté (autorité)
  - Dates de début et de fin de validité
  - Etat de révocation (optionnel)

Remarque : l'assertion SAML ne contient pas d'élément fonctionnel. Elle est exploitée pour authentifier l'ETS, pour autoriser l'exécution du service et elle peut être conservée comme preuve d'accès.