Procédure d'obtention des certificats logiciels de test pour la mise en œuvre de Diapason

Introduction

Dans le cadre du déploiement de Diapason, l'ASIP Santé propose cette fiche pratique destinée aux éditeurs et établissements souhaitant mettre en œuvre la solution en environnement de test.

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 tester Diapason, les éditeurs et établissements doivent commander deux certificats logiciels de test spécifiques émis par l'IGC-Santé :

2 certificats logiciels

- un **certificat client de type ORG AUTH_CLI** pour authentifier la GAP auprès du Fournisseur de service de paiement (Payment Service Provider – PSP) ;
- un **certificat serveur de type SSL_SERVEUR** pour authentifier la GAP auprès du Terminal de Paiement Electronique (TPE).

En annexe sont présentés les schémas synthétisant le fonctionnement des certificats et les mécanismes de sécurité dans les échanges entre les établissements, le TPE et le PSP :

- *le TPE s'authentifie auprès de la GAP avec des certificats d'authentification X509 avec clé privée émis par l'IGC IngeTrust de la société Ingenico ;*
- *le PSP s'authentifie auprès de la GAP avec un certificat serveur X509 avec clé privée émis par Geotrust.*

Des AC (Autorités de Certification) IngeTrust et Geotrust doivent être installées au préalable.

Pour plus de précisions, il est conseillé de se rapprocher d'Ingenico.

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

1. Vérification des prérequis : 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 / l'établissement 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 / l'établissement ne dispose pas de cartes CPx de test (A) : l'éditeur / l'établissement dispose de cartes CPx de test (B).

(A) L'éditeur / l'établissement ne dispose pas de cartes CPx de test

- L'éditeur / l'établissement 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 Diapason – usage authentification TLS mutuelle ».

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

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

Etape 4.1 : Renseigner l'usage suivant « Projet Diapason – usage authentification TLS mutuelle vis-à-vis du PSP et des TPE ».

Etape 4.2 : Cocher :

- **offre certificat logiciel SERVEUR usage SSL_SERVEUR**

NB : Renseigner un *nom de domaine réel. L'ASIP Santé vérifiera l'existence de ce domaine. Egalement, renseigner le nom de domaine le plus large, du type *<nom de domaine>, (éviter le nom du sous-domaine et/ou du serveur) pour ne pas restreindre les habilitations.*

Exemple : Le service GAP/Diapason qui assure la communication avec les TPE est hébergé sur un serveur X. Le nom de domaine renseigné pour l'habilitation ne doit pas être « serveurX.domaineEditeur.fr » mais «*domaineEditeur.fr ».

- **offre certificat logiciel ORG (Personne morale) usage AUTH_CLI.**

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 de préciser (à côté) que l'on souhaite habiliter 1 des 5 cartes du kit, par exemple la carte CDE.

(B) L'éditeur / l'établissement dispose de cartes CPx de test désignées en tant qu'administrateur technique

- L'éditeur / l'établissement 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.

Attention : *S'agissant du certificat SERVEUR, les cartes de test peuvent n'être habilitées que sur un sous-domaine et/ou un serveur spécifique. Dans ce cas, il suffit de renvoyer le formulaire n°414 (étape 4.2) pour élargir les habilitations à l'ensemble du domaine de l'éditeur / l'établissement, sans restrictions.*

- Si les cartes CPx de test ne possèdent aucune habilitation sur les offres de certificat de test, l'éditeur / l'établissement 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 / l'établissement 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_Diapason_PSP** » ;
- pour la demande **SSL_Serveur**, indiquer la valeur « **<nom de serveur>.<nom de domaine> ».**
  Le serveur mentionné est le serveur GAP/Diapason assurant la communication avec les TPE.

Attention : Le TPE Diapason prévoit un paramétrage dédié qui permet de spécifier le FQDN du serveur GAP/Diapason. Le FQDN saisi dans le TPE doit être identique à la valeur du CN du certificat serveur installé sur le serveur GAP/Diapason.

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*** *(pour les éditeurs)*
- ***monserviceclient.certificats@asipsante.fr*** *(pour les établissements)*

Cycle de vie des certificats logiciels

Le certificat logiciel de test, une fois généré, a une **validité de 3 ans**. Vous serez alertés par courrier électronique de l'arrivée à échéance du certificat un mois avant que ce dernier ne soit plus valide.

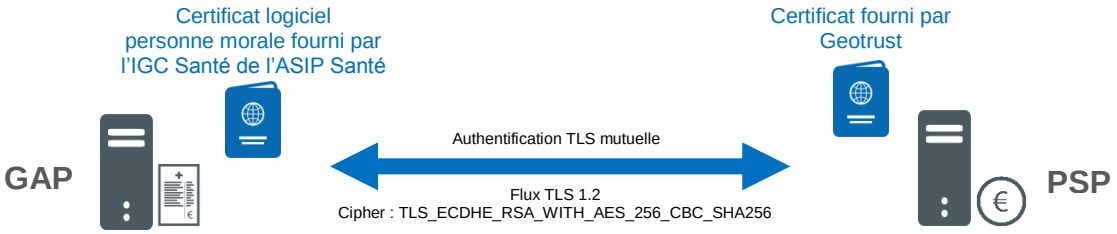
Durant les 3 ans de validité, l'éditeur / l'établissement a la possibilité de gérer les habilitations (ajout ou suppression) liées aux cartes CPx de test. (cf. L'Espace CPS, rubrique « Vos démarches »).

Si vous générez un certificat comportant des erreurs ou en cas de perte ou de vol de certificat, il est nécessaire de **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 établissements et le PSP : certificats et mécanismes de sécurité mis en œuvre**



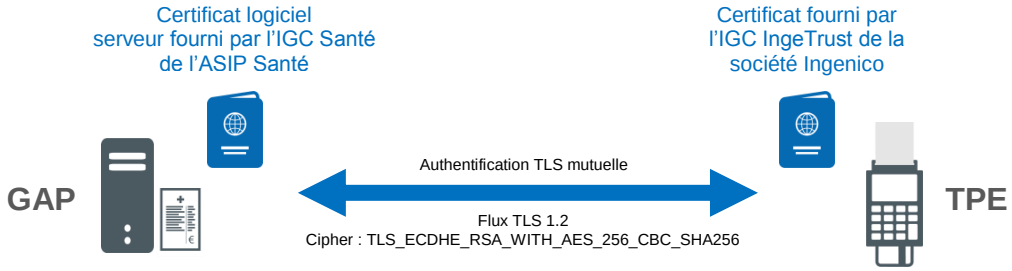
Vérifications réalisées lors de l'établissement du flux TLS

- 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 (obligatoire)

- **Échanges entre les établissements et le TPE : certificats et mécanismes de sécurité mis en œuvre**



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 (obligatoire)