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

Introduction

Dans le cadre du déploiement de Diapason, l'ASIP Santé propose cette fiche pratique destinée aux services informatiques des établissements de santé souhaitant mettre en œuvre la solution.

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 pouvoir mettre en œuvre Diapason, les établissements de santé doivent commander deux certificats logiciels 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).

NB : Pour déployer Diapason en environnement de test, les établissements de santé doivent commander deux certificats logiciels de test (client et serveur). Pour cela, se référer à la Fiche « DIAPASON_Deploiement_Procedure_d_obtention_des_certificats_logiciels_de_test »

En annexe 1 sont présentés les schémas synthétisant les certificats et mécanismes de sécurité mis en œuvre 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 suit trois étapes :

1. Vérification des prérequis
2. Demande d'habilitation à la commande de certificats
3. Commande et installation des certificats logiciels

1. Prérequis à la commande des certificats logiciels

Afin de commander les deux certificats logiciels, les prérequis suivants doivent être respectés :

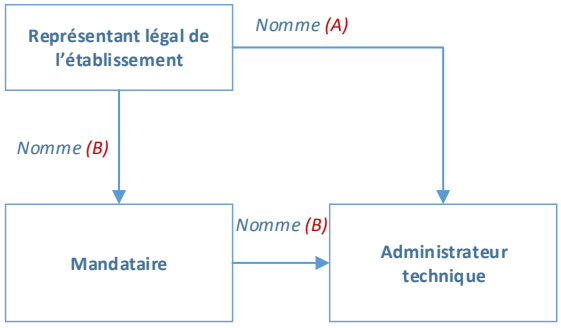
Le représentant légal de l'établissement de santé, ou les mandataires de produits de certification désignés par le représentant légal, doivent disposer d'un contrat avec l'ASIP Santé et être équipés d'une carte CDE active.

Si le représentant légal de la structure n'a pas de contrat et/ou de carte CDE (ou CPS responsable), ce dernier doit signer un contrat de structure[1] et compléter une demande d'attribution d'une carte de représentant légal de structure accessible au téléchargement sur l'Espace CPS[2], rubrique « Vos Commandes » (formulaire de contrat de structure et formulaire n°101).

Le représentant légal de l'établissement de santé a deux possibilités. Il peut désigner :

- **un (ou plusieurs) administrateur(s) technique(s) et s'assurer qu'il est (sont) porteur(s) d'une carte CPx nominative et active (A) ;**
- **un (ou plusieurs) mandataire(s) qui aura (auront) pour mission de conduire, pour le compte de l'établissement, la procédure de commande jusqu'à son terme et de gérer, le cas échéant, le cycle de vie des certificats (B).**

Schéma récapitulatif



[1] Se référer à l'Annexe 2 pour l'identification de l'entité signataire du contrat de structure.

[2] L'Espace CPS dédié aux produits de certification de l'IGC-Santé est accessible sur le site internet de l'ASIP Santé, dans la rubrique « Services » : http://esante.gouv.fr/services/espace-cps

Information sur l'administrateur technique

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

Pour désigner un administrateur technique, deux cas de figure peuvent se présenter au représentant légal de l'établissement :

- si le désigné n'a pas de carte CPx, le représentant légal doit faire une demande d'attribution de carte de personnel de structure accessible au téléchargement sur l'Espace CPS, rubrique « Vos Commandes » (formulaire n°301).
  ***NB :** 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, puis une demande d'habilitation étape 2 ;*
- si le désigné a déjà une carte CPx, il est uniquement nécessaire de faire une demande d'habilitation (étape 2).

Nommer un éditeur en tant qu'administrateur technique ?

Les établissements de santé souhaitant confier le rôle d'administrateur technique à un éditeur peuvent le faire. La procédure à suivre est celle décrite ci-dessus.

Information sur le mandataire

Il est également possible pour le représentant légal d'une structure de désigner un ou plusieurs mandataires pour sa structure.

Le mandataire a pour mission de **conduire, pour le compte de l'établissement, la procédure de commande jusqu'à son terme** et de gérer, le cas échéant, le cycle de vie des produits de certification.

Le mandataire acquiert alors certaines prérogatives du responsable légal de l'établissement, et peut ainsi représenter ce dernier pour :

- commander des cartes CPx distribuées par l'ASIP Santé ;
- **habiliter les administrateurs techniques de certificats logiciels** ;
- mettre en opposition des cartes en cas de perte, vol ou dysfonctionnement ou révoquer des certificats ;
- demander la réfection des codes confidentiels perdus (réédition des plis sécurisés) ;
- actualiser les données relatives aux porteurs de produits.

Pour désigner un mandataire, deux cas de figure peuvent se présenter au représentant légal de l'établissement :

- si le désigné n'a pas de carte CPx, le représentant légal doit faire une demande d'attribution de carte de personnel de structure accessible au téléchargement sur l'Espace CPS, rubrique « Vos Commandes » (formulaire n°301). ***NB :*** *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, puis une demande de désignation de mandataire accessible au téléchargement sur l'Espace CPS, rubrique « Vos Commandes » (formulaire n°502) ;*
- si le désigné a déjà une carte CPx, il est uniquement nécessaire de faire une demande de désignation de mandataire (formulaire n°502).

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 à la commande des certificats logiciels

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

***NB** : un administrateur technique est peut-être déjà habilité à la commande des certificats. Afin de le vérifier, vous avez accès à la plateforme IGC-Santé[3]. Elle vous permettra de déterminer si votre administrateur technique est déjà habilité à la commande des certificats nécessaires dans le cadre de Diapason et, pour les certificats serveur, sur quels domaines.*

Attention :

L'administrateur technique peut n'être habilité que pour un sous-domaine et/ou un serveur spécifique. Dans ce cas, il suffit de renvoyer le formulaire n°413 en suivant la procédure ci-dessous pour élargir ses droits à l'ensemble du domaine de l'établissement.

L'établissement de santé complète, signe et envoie à monserviceclient.certificats@asipsante.fr le formulaire n°413 de commande de certificats logiciels figurant en annexe de cette procédure. Le formulaire est également téléchargeable sur l'Espace CPS, rubrique « Vos Commandes ».

[3] Se rendre sur https://pfc.eservices.esante.gouv.fr/pfcng-ihm/authentication.xhtml, cliquer sur « Demander ». Pour voir les noms de domaine couverts par l'habilitation, sélectionner l'offre SERV, cliquer sur « Demander un nouveau produit » puis sélectionner l'usage SSL_Serveur.

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

Etape 4.1

- pour le certificat client : **« Projet Diapason – usage authentification TLS mutuelle pour répondre au cas d'usage de l'authentification directe d'une personne morale (ES ou assimilé) vis-à-vis du PSP conformément aux spécifications du dispositif Diapason. Usage visé par l'équipe projet ASIP Santé N3 » ;**
- pour le certificat serveur : **« Projet Diapason – usage authentification TLS mutuelle pour répondre au cas d'usage de l'authentification directe d'un serveur (GAP) vis-à-vis du TPE conformément aux spécifications du dispositif Diapason. Usage visé par l'équipe projet ASIP Santé N3 ».**

Pour la partie « Offre de certificat souhaitée » :

Etape 4.2

- cocher **« Offre certificat logiciel ORG (Personne morale) usage AUTH_CLI »** ;
- cocher **« Offre certificat logiciel SERVEUR usage SSL_serveur ».**

*Attention : Dans le champ « Nom de domaine » du certificat serveur, saisir le nom du domaine le plus large, du type *<nom de domaine> (ne pas mentionner de sous-domaine ou de nom de serveur). De cette façon, l'habilitation de l'administrateur technique portera sur l'ensemble du domaine, sans restrictions.*

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.ch-ville.fr » mais «*****ch-ville.fr ».

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

3. Commande et installation des certificats logiciels

L'administrateur technique de votre 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 biclé :

- **le guide d'utilisation des services IHM Plateforme IGC-Santé** (document ASIP_IGC-Sante_Guide-IHM) ;
- **la procédure de génération de CSR** (document ASIP-PUSC-PSCE_generation-de-csr). Il est possible de générer la biclé et le CSR en ligne pendant le commande du certificat et la biclé sont générés au format PKCS12 avec les 2 certificats ACI et ACR.

Information

Nous attirons votre attention sur les prérequis nécessaires à cette étape figurant 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**).*

Lors de la commande du produit sur PFCNG, nous recommandons de suivre les règles de nommage suivantes pour le « service applicatif » :

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 celui sur lequel le service GAP/Diapason qui assure la communication avec les TPE est hébergé.
  Exemple : <monserveur>.ch-ville.fr

Attention : Le CN d'un certificat SSL_Serveur contient un FQDN (Fully Qualified Domaine Name). Ce FQDN doit être conforme à la RFC 1035[4] et donc être de la forme : <nom de serveur>.[nom de sous-domaine].<nom de domaine>

Le sous-domaine est facultatif.

Le TPE doit être configuré afin de le faire communiquer avec le serveur GAP/Diapason. 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. La configuration réseau de l'établissement doit permettre au TPE d'atteindre le serveur GAP/Diapason en utilisant la valeur de FQDN saisie dans le TPE.

Il est possible de générer la biclé et le CSR en ligne pendant la commande, ou de charger son CSR si ce dernier a déjà été généré :

Etape 4

- Il est possible de **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. Il est nécessaire de voir avec votre éditeur de SIH sous quel format seront utilisés le certificat et la biclé ;
- Il est possible de **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 :

- ***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 biclés 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.

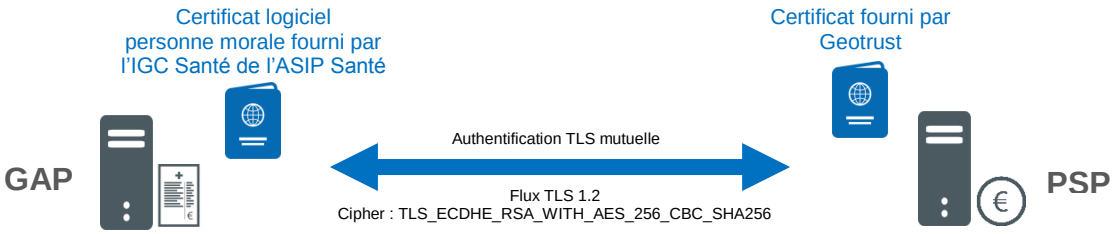
Durant les 3 ans de validité, le représentant légal de la structure ou ses mandataires ont la possibilité de gérer les habilitations (ajout ou suppression) des administrateurs techniques de certificat. (cf. L'Espace CPS, rubrique « Vos démarches »).

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.

[4] Se référer à la documentation IETF (https://www.ietf.org/rfc/rfc1035.txt)

Annexe 1 : sécurisation des échanges

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



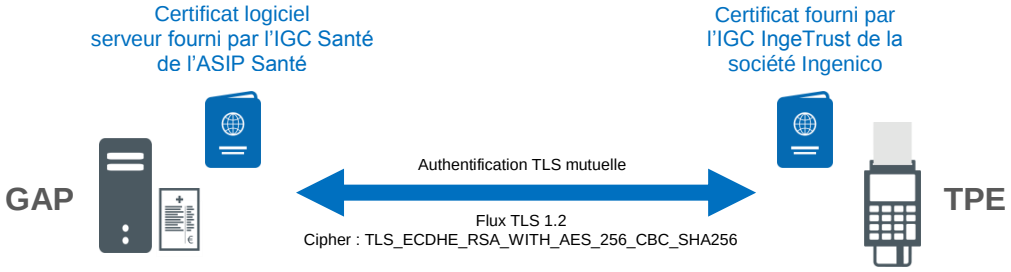
Vérifications réalisées lors de l'établissement du flux TLS

- 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**



Annexe 2 : identification de la structure signataire du contrat

- **Votre établissement de santé n'a pas de contrat de structure avec l'ASIP Santé :**
  - votre établissement de santé compte-t-il plusieurs EG ?
    - si oui :
      - vous pouvez signer à l'EG mais les certificats logiciels seront rattachés à cet EG : c'est donc cet EG qui sera présenté à l'extérieur ;
    - si non :
      - vous pouvez signer à l'EJ ou à l'EG. Il est préconisé de signer à l'EJ.

- **Votre établissement de santé a un contrat de structure avec l'ASIP Santé :**
  - le contrat est signé à l'EJ : vous n'avez rien à faire ;
  - le contrat est signé à l'EG : les certificats logiciels seront rattachés à cet EG, c'est donc cet EG qui sera présenté à l'extérieur.