

Manuel utilisateur
CLEO CPS
Commande de certificat serveur

Sommaire

1	Objet du document.....	3
2	Certificats serveurs.....	4
2.1	A quoi sert un certificat serveur de l'ASIP Santé ?	4
2.2	Les types de certificats serveur	4
2.3	Que contient le certificat serveur de l'ASIP Santé ?.....	4
2.4	Comment obtenir un certificat serveur ?	5
2.4.1	Phase administrative	5
2.4.1.1	But	5
2.4.1.2	Mise en œuvre	5
2.4.2	Phase technique	6
2.4.2.1	But	6
2.4.2.2	Mise en œuvre	6
3	L'utilitaire CleoCPS	7
3.1	Pré-requis	7
3.2	Qu'est-ce que CleoCPS ?	7
3.2.1	Première méthode : procédure automatique avec CleoWizard	8
3.2.2	Deuxième méthode : procédure manuelle	11
4	Foire aux questions	19

1 Objet du document

Ce document a pour but d'accompagner les utilisateurs dans leur procédure de demande de certificat serveur auprès de l'ASIP Santé :

- La première partie rappelle l'intérêt et l'usage des certificats serveur.
- La seconde décrit la procédure simplifiée à suivre pour obtenir un certificat serveur délivré par l'ASIP Santé à l'aide de l'outil CleoCPS.

Il s'agit d'une version simplifiée du manuel disponible sur le poste de travail¹ suite à l'installation du logiciel CleoCPS qui ne retient que les éléments essentiels associés aux certificats serveurs.

¹ Menu « Démarrer/Tous les programmes/Santé social/CleoCPS/Manuel CleoCPS.pdf »

2 Certificats serveurs

2.1 A quoi sert un certificat serveur de l'ASIP Santé ?

Un certificat serveur sert à la sécurisation des échanges d'informations entre un utilisateur et un système informatique, ou entre deux systèmes informatiques dans le domaine de la santé.

Un certificat peut aussi être associé à une machine ou un système informatique, c'est le cas d'un certificat serveur qui permet d'assurer l'identification du serveur, mais aussi la reconnaissance (par la signature de l'ASIP Santé) et la sécurisation (cryptographie) des échanges d'informations.

En particulier, certaines opérations nécessitant un interfaçage avec le DMP sont réalisables grâce à aux deux types de certificats serveur décrits ci-dessous.

2.2 Les types de certificats serveur

Il existe deux types de certificats serveurs délivrés par l'ASIP Santé :

- Un certificat serveur, dit « **certificat SSL** », qui permet la sécurisation d'une voie d'échange avec un correspondant, par exemple une liaison https sur SSL avec un serveur, ceci pendant la durée de la connexion; la sécurisation consiste en l'authentification réciproque du serveur vis-à-vis des utilisateurs (ou d'autres serveurs), ainsi qu'à garantir la confidentialité et l'intégrité des données échangées. Ce certificat contient le nom du domaine du serveur (DNS), permettant d'établir une connexion avec lui ;
- Un certificat serveur, dit « **certificat S/MIME** », qui permet la sécurisation des objets échangés, avant ou au moment de l'échange, par exemple par un outil de messagerie mettant en œuvre le protocole S/MIME; la sécurisation consiste en la signature de l'objet par le serveur, garantissant ainsi l'identité de ce serveur et l'intégrité du contenu de l'objet, et éventuellement en un chiffrement du contenu pour en assurer la confidentialité. Ce certificat contient l'adresse e-mail du serveur, permettant de lui expédier des objets.

2.3 Que contient le certificat serveur de l'ASIP Santé ?

Le certificat serveur fourni par l'ASIP Santé est constitué d'une clé publique, de données portant sur la structure et le domaine Internet ou l'adresse e-mail associé au serveur.

L'ensemble est validé et signé par une autorité de certification : l'ASIP Santé.

2.4 Comment obtenir un certificat serveur ?

La procédure d'obtention d'un certificat serveur se décompose en 2 étapes détaillées ci-dessous : une phase administrative suivie d'une phase technique

2.4.1 Phase administrative

2.4.1.1 But

La légitimité de la mise à disposition d'un certificat serveur de l'ASIP Santé est conditionnée par l'existence pour le responsable légal de la structure, d'une carte de la famille CPS (CDE, CPA Directeur ou CPS) afin de valider son identité et sa qualité de responsable de la structure.

Ce dernier peut déléguer la demande technique de certificats serveurs à un membre de son personnel (ou d'une autre structure), lui-même détenteur d'une carte de la famille CPS. Dans la suite du document, cette personne est dénommée « administrateur ».

2.4.1.2 Mise en œuvre

Tout d'abord, il faut avoir fait une demande administrative auprès de l'ASIP Santé : voir sur le site E-santé pour la procédure :

<http://esante.gouv.fr/services/espace-cps/guide/procedure-d-obtention-d-un-certificat-serveur-applicatif-phase-administrat>

Pour mener à bien ces opérations, vous devez disposer au préalable, pour chaque serveur à sécuriser :

- Des informations techniques contenues dans le dossier administratif de « Demande de certificats de serveur applicatif » adressé à l'ASIP Santé par le Responsable de la Structure :
 - L'identification nationale de la structure dans laquelle le serveur est déclaré.
 - Le nom de domaine pleinement qualifié (FQDN) du serveur qui va être sécurisé.
- D'une carte, de la famille CPS, appartenant à une personne enregistrée à l'ASIP Santé comme ayant le rôle d'administrateur du serveur pour lequel vous effectuez les demandes de certificats.

Une fois la phase administrative validée par l'ASIP Santé, le responsable d'établissement ou l'administrateur désigné reçoit un mail de notification. La phase technique décrite dans le paragraphe suivant, peut ensuite être exécutée.

2.4.2 Phase technique

2.4.2.1 But

Les opérations techniques réalisées lors de cette phase consistent à :

- Générer les éléments cryptographiques nécessaires à la sécurisation des échanges au niveau du serveur ciblé : il s'agit du jeu de clés RSA (dénommé aussi bi-clé) dont la partie secrète sera conservée par le serveur et dont la partie publique sera intégrée à une demande de certificat.
- Emettre la demande de certificat vers le Serveur d'Inscription de l'ASIP Santé. Il sera contrôlé que le domaine Internet déclaré est la propriété de la structure et que la demande est bien effectuée par la personne habilitée.

2.4.2.2 Mise en œuvre

Cette phase étant relativement complexe techniquement, l'ASIP Santé met à disposition un utilitaire permettant de mener à bien l'ensemble des opérations sans nécessiter de connaissances techniques particulières.

L'utilisation de cet utilitaire est détaillée dans la suite de ce document.

3 L'utilitaire CleoCPS

3.1 Pré-requis

Pour pouvoir utiliser CleoCPS, les pré-requis suivants doivent être remplis au niveau du poste de travail utilisé :

- Un lecteur de cartes à puce doit être connecté et correctement configuré.
- Les Cryptolib CPS doivent être installées. Si ce n'est pas le cas, utilisez l'outil d'installation mis à disposition par l'ASIP Santé à l'adresse suivante :

<http://www.outil-diagnostic.dmp.gouv.fr/>

- Il faut aussi que l'utilisateur dispose de sa carte CPx et soit déclaré en tant qu'administrateur de son serveur auprès de l'ASIP Santé, ce qui matérialise la fin de la procédure administrative.

3.2 Qu'est-ce que CleoCPS ?

CleoCPS est un utilitaire distribué gratuitement et librement par l'ASIP Santé pour accompagner l'utilisateur dans sa demande de certificat serveur lors de la phase technique.

Il est récupérable à l'adresse suivante sous forme d'installeur standard :

<http://integrateurs-cps.asipsante.fr/pages/CleoCPS>

Une fois l'installeur téléchargé, il suffit de le lancer et de suivre le processus d'installation.

Rappel : l'ASIP Santé n'est en aucun cas responsable de l'utilisation faite de cette application.

Il est rappelé que le certificat obtenu ainsi que la clé secrète générée, est sous la responsabilité du détenteur.

La seule responsabilité de l'ASIP Santé est, en tant qu'autorité de confiance, de cautionner la véracité des informations contenues dans le certificat.

Utilisation de CleoCPS

3.2.1 Première méthode : procédure automatique avec CleoWizard



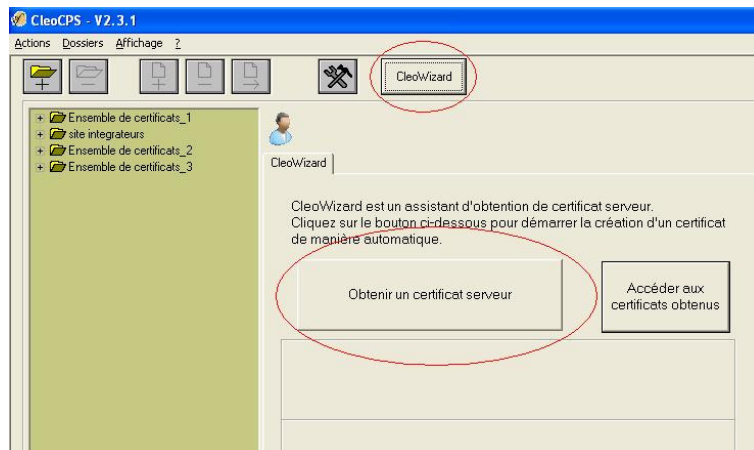
Pour pouvoir exécuter la procédure qui suit :

- Vous devez disposer d'un logiciel de messagerie (Microsoft Outlook par exemple) correctement installé et configuré sur votre poste.
- Le protocole LDAP (port 389) et/ou LDAPS (port 636) doit être autorisé sur votre poste : contactez votre support informatique en cas de problème.

Si vous ne pouvez pas obtenir l'autorisation du protocole LDAP, CleoWizard peut tout de même être utilisé mais certaines données devront être saisies manuellement.

CleoWizard est un assistant de création de certificat serveur (SSL ou S/MIME), qui permet d'obtenir un certificat, de manière simplifiée : toutes les étapes de la génération sont automatisées.

Sur la page d'accueil de CleoCPS, sélectionner « **Accéder à CleoWizard** » (ou le bouton « **CleoWizard** » en haut de l'écran).



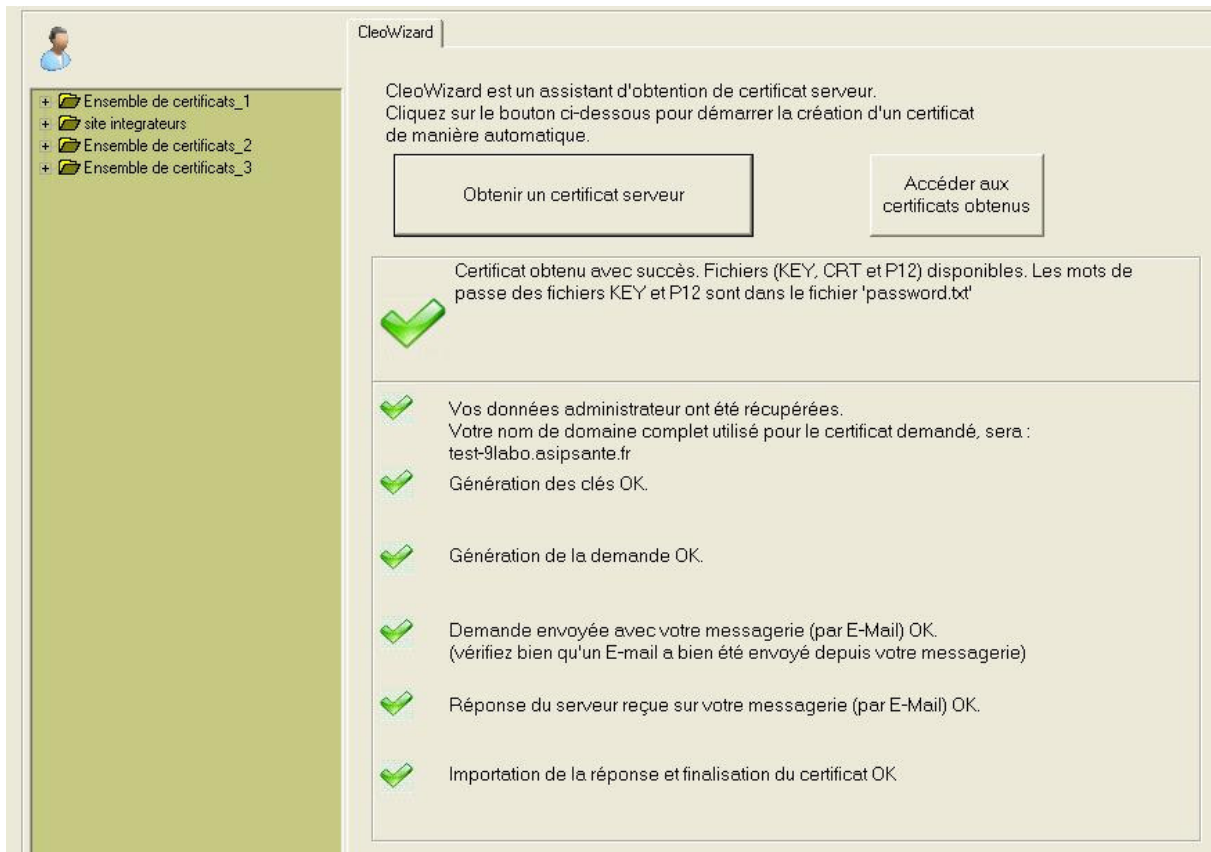
Puis sélectionner « **Obtenir un certificat serveur** », pour démarrer la procédure automatique d'obtention d'un certificat serveur.

Pendant la procédure automatique, il vous sera demandé :

- le type de certificat serveur demandé : SSL ou S/MIME,
- l'adresse E-mail de votre serveur, dans le cas d'un certificat S/MIME,
- si vous désirez sécuriser votre jeu de clés (fichier key) avec un mot de passe ou pas. (fortement recommandé pour protéger vos clés)
- éventuellement, insertion et demande du code PIN de votre carte CPS.

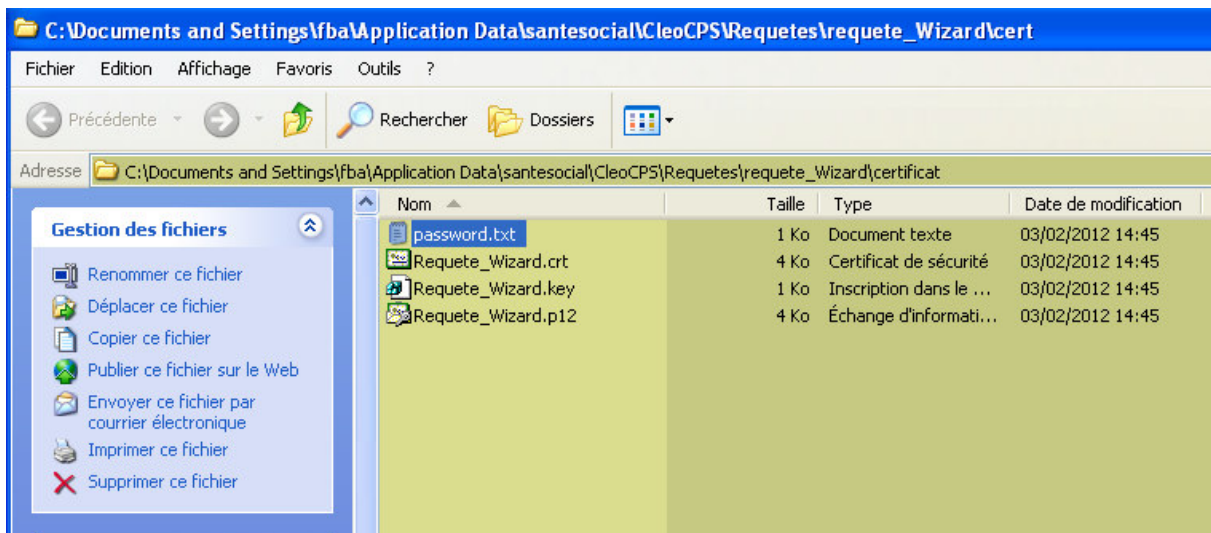
Remarque : dans le cas où l'assistant CleoWizard ne peut pas se connecter à l'annuaire CPS, il vous proposera une procédure dégradée qui consiste à rentrer vous-même manuellement, le nom complet de votre serveur.

(Dans ce cas, il faut que votre serveur fasse partie de votre structure (la même que celle de votre carte CPx), autrement votre demande échouera)



En fin de procédure, si tout s'est bien déroulé, un répertoire s'ouvrira. Il contient :

- Le certificat (au format p12 : **Requete_Wizard.p12**, et crt : **Requete_Wizard.crt**),
- Les clés RSA (**Requete_Wizard.key**),
- Ainsi que le fichier **password.txt** contenant les mots de passe des fichiers .key et .p12.



=> Le bouton « **accéder aux certificats obtenus** » permet d'ouvrir le répertoire contenant le certificat obtenu.

(Les certificats précédemment obtenus, sont automatiquement sauvegardés dans des sous-répertoires)

Remarque : en fonction de votre logiciel de messagerie, vous aurez peut-être un message d'avertissement de Windows concernant l'envoi du mail (« **autorisez cet envoi** »), ainsi que la réception de mails (« **autorisez aussi l'utilisation automatique de votre client de messagerie** »).

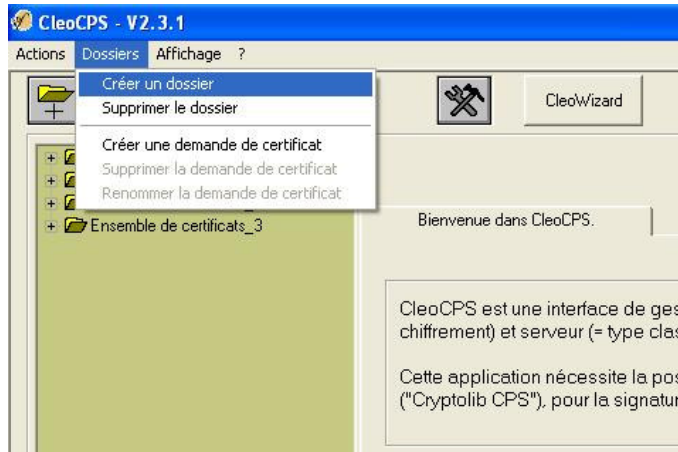
Il faudra alors valider impérativement ces messages pour continuer la procédure.



Dans le cas où la procédure automatique CleoWizard échoue, vous devrez alors passer à la procédure manuelle pour obtenir votre certificat.

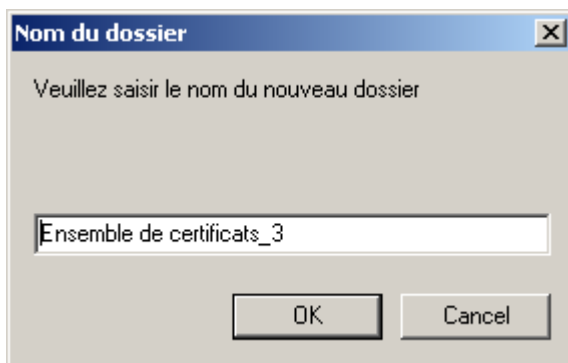
3.2.2 Deuxième méthode : procédure manuelle

Voici la procédure pas-à-pas à suivre pour obtenir un certificat :

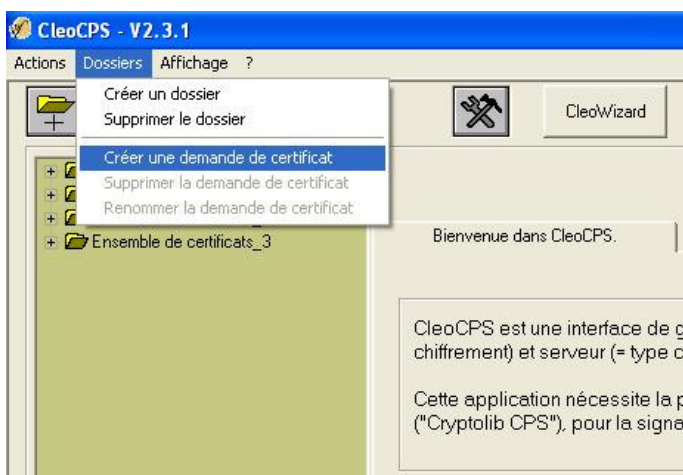


Création d'un nouveau dossier :

Dans le menu « **Dossiers** », sélectionner « **Créer un dossier** » :

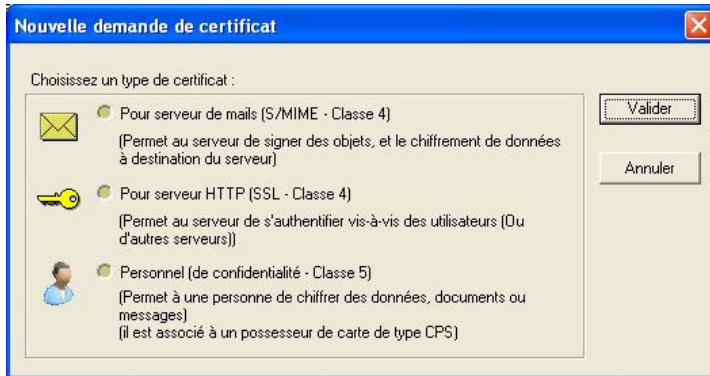


Indiquer le nom de dossier, ou laisser le nom par défaut, puis sélectionner « **OK** »

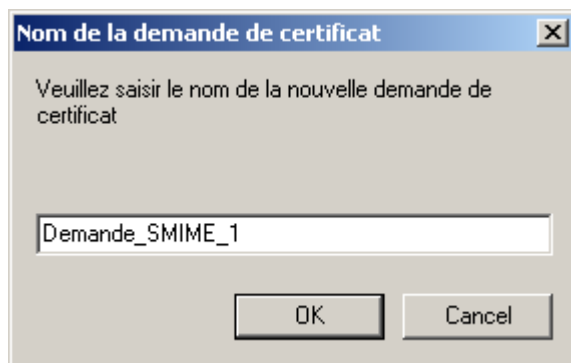


Ensuite, création d'une nouvelle demande de certificat :

Dans le menu « **Dossiers** », sélectionner « **Créer une demande de certificat** ».

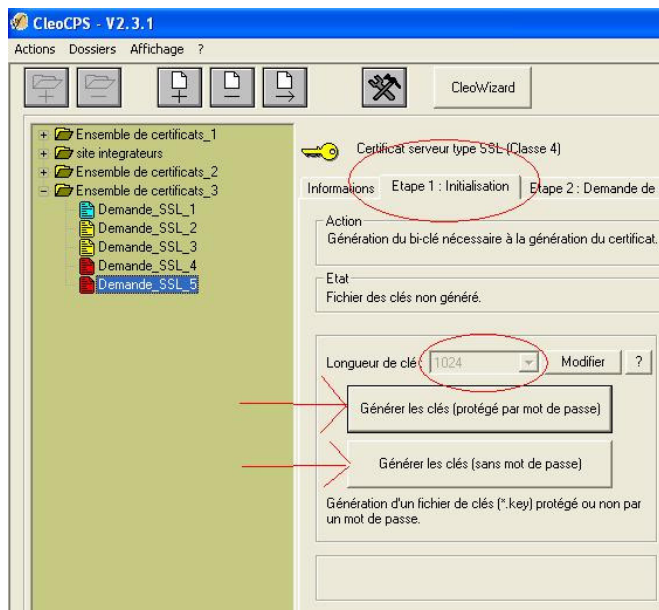


Choisir le type de certificat désiré :
Serveur S/MIME ou SSL.



Indiquer le nom de la demande, ou laisser le nom par défaut, puis sélectionner « **OK** »

Une fois la nouvelle demande créée, sélectionner l'onglet « **Etape 1 : Initialisation** ».

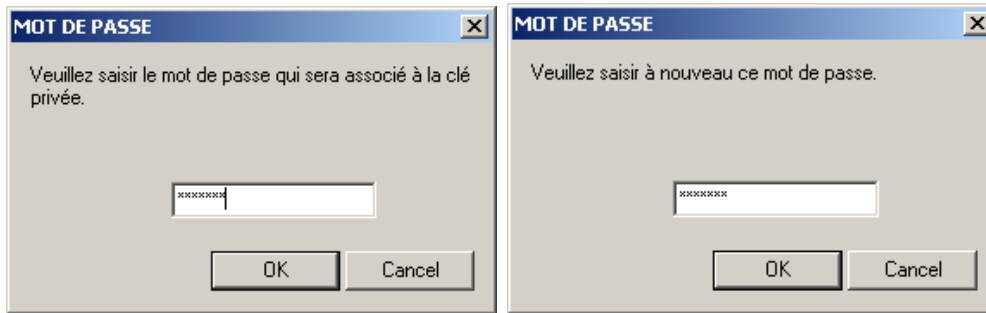


C'est l'étape permettant de créer les clés du certificat demandé :

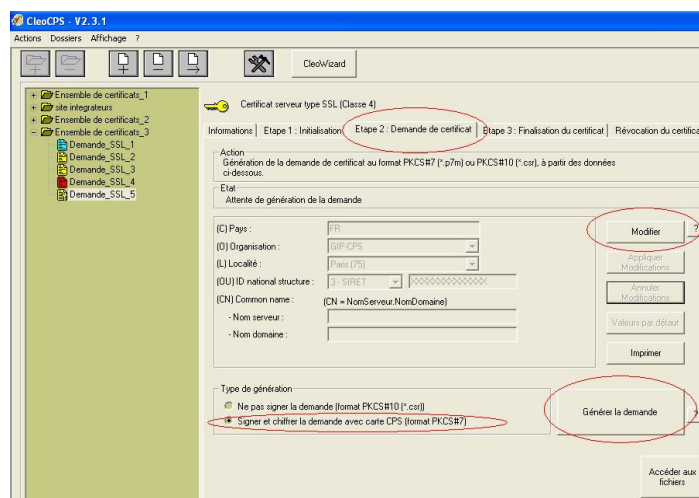
Sélectionner « **générer les clés** » avec ou sans mot de passe.

(Mot de passe fortement recommandé)

(Laisser la longueur de clé à 1024)



Une fois les clés générées, sélectionner l'onglet « **Etape 2 : Demande de certificat** ».



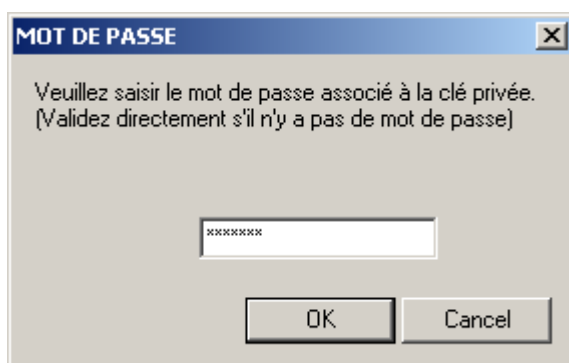
Sélectionner « **Modifier** »,

Remplir les différents champs du formulaire avec les données correspondantes au certificat demandé (notamment le nom de serveur/domaine qui doit être identique à celui donné dans votre dossier administratif de « Demande de certificats de serveur applicatif » déposé auprès de l'ASIP Santé.

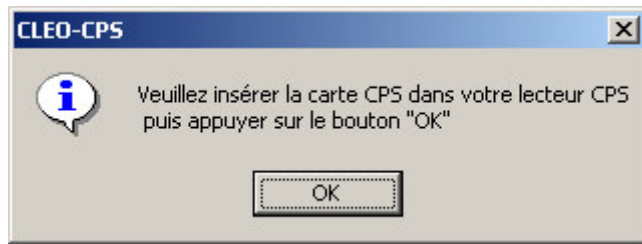
Puis valider les données en sélectionnant « **Appliquer modifications** »

Sélectionner ensuite « **génération la demande** » pour finaliser et envoyer la demande.

(Vérifier auparavant que « **Signer et chiffrer la demande avec la carte CPS** » est bien sélectionné)

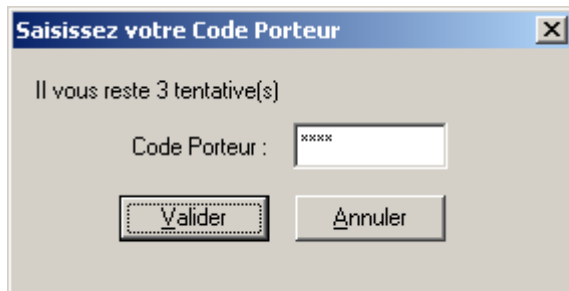


Si vous avez choisi de mettre un mot de passe sur les clés à l'étape 1, celui-ci vous sera alors redemandé.



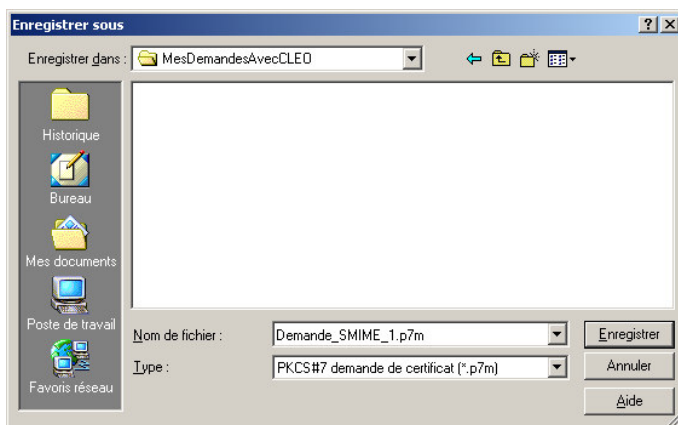
Cette demande doit être signée par votre CPS.

Si la CPS n'est pas présente dans le lecteur, CleoCPS vous demandera alors de l'insérer.



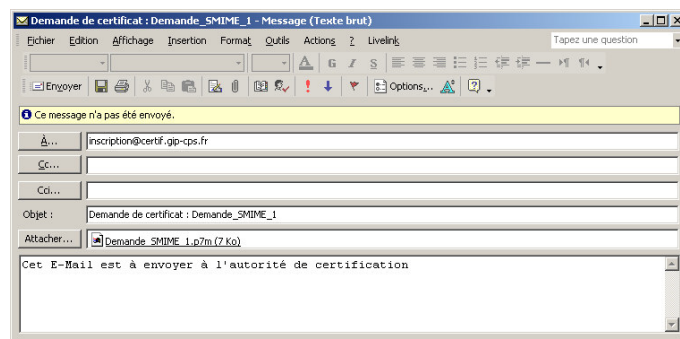
Le code porteur de la carte vous sera alors demandé.

(Sauf si ce code porteur a déjà été rentré)



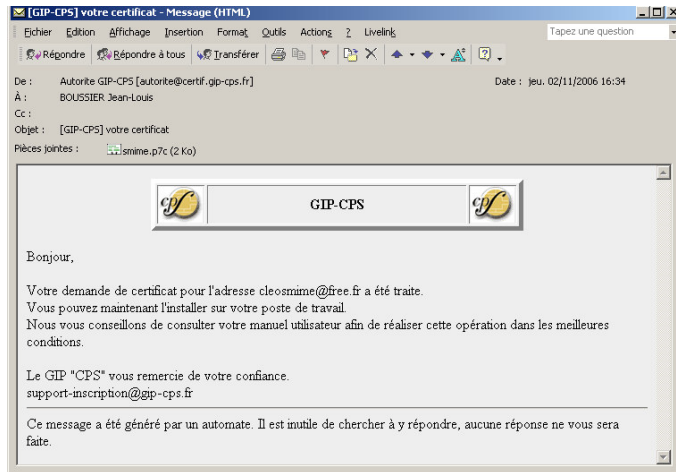
Sauvegarder le fichier résultat, qui constitue la demande générée.

Si votre poste a un logiciel de messagerie installé, CleoCPS l'utilisera pour ouvrir un Email prêt à l'envoi. Exemple :



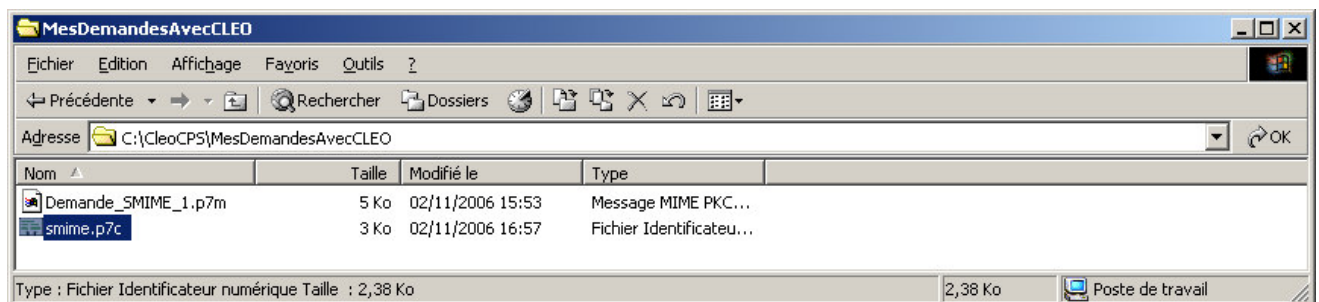
Il ne reste plus alors qu'à l'envoyer directement (ici, bouton « Envoyer »)

Vous devez donc, après avoir envoyé le message avec le fichier « p7m » en pièce jointe, attendre la réponse du serveur d'inscription (quelques minutes d'attente en moyenne), qui arrivera dans votre boîte aux lettres. Vous pouvez ensuite procéder à l'étape suivante.



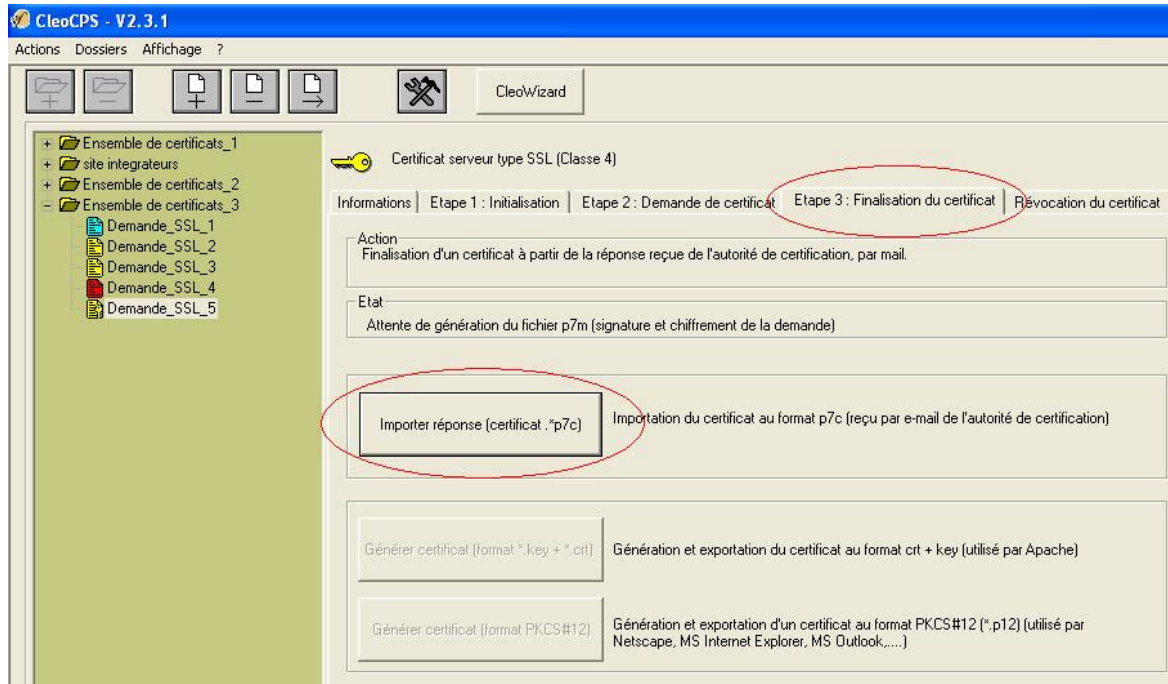
Un exemple d'E-mail reçu du serveur d'inscription dans votre logiciel de messagerie.

Sauvegarder alors la pièce jointe de l'Email reçu (fichier « smime.p7c ») sur votre poste de travail.

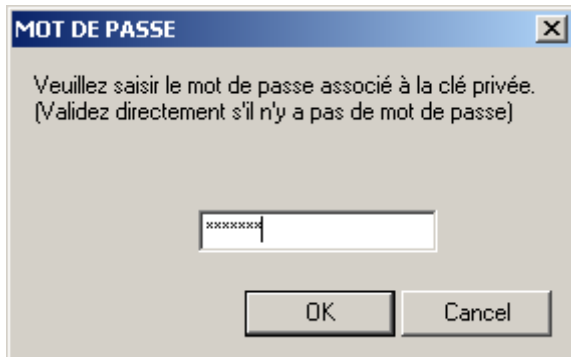


Remarque : si vous recevez une réponse négative par mail, de la part du serveur d'inscription, il vous faudra recommencer une nouvelle demande depuis le début (il n'est pas possible de modifier une demande déjà émise). Si le problème persiste, contactez l'ASIP Santé pour plus d'aide : Certificat.classe4@asipsante.fr

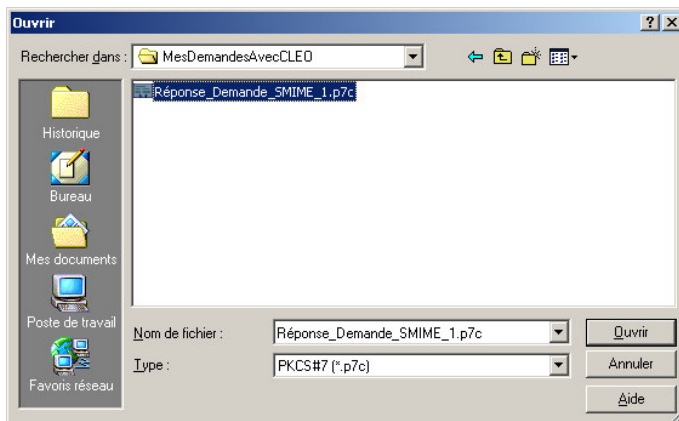
Sélectionner ensuite l'onglet « **Etape 3 : Finalisation du certificat** ».



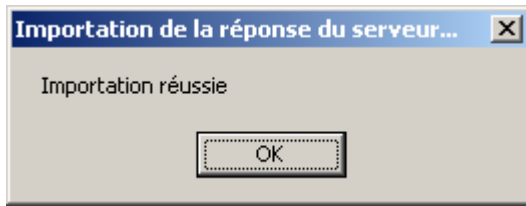
Et sélectionner « **Importer réponse** ».



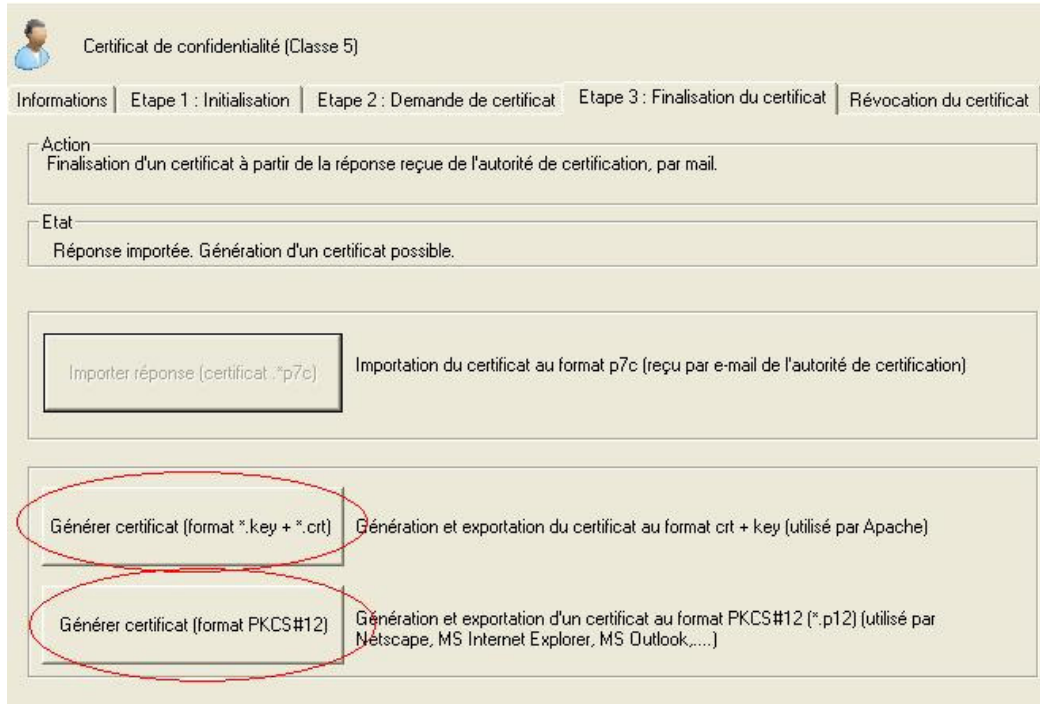
Si vous avez choisi de mettre un mot de passe sur les clés à l'étape 1, celui-ci vous sera alors redemandé.



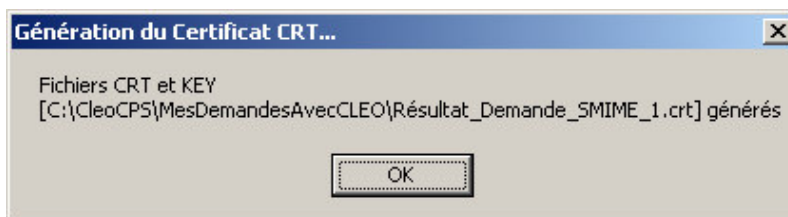
Puis sélectionner le certificat reçu (le fichier p7c reçu par E-mail, et sauvegardé sur votre poste de travail).



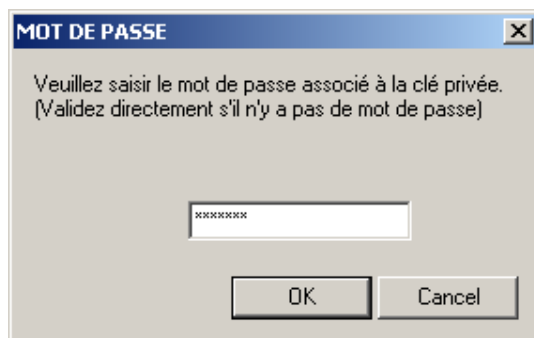
... après quelques secondes, l'importation est terminée.



Il ne reste plus ensuite qu'à choisir sous quelle forme vous voulez obtenir votre certificat.
(Les deux choix peuvent être utilisés)

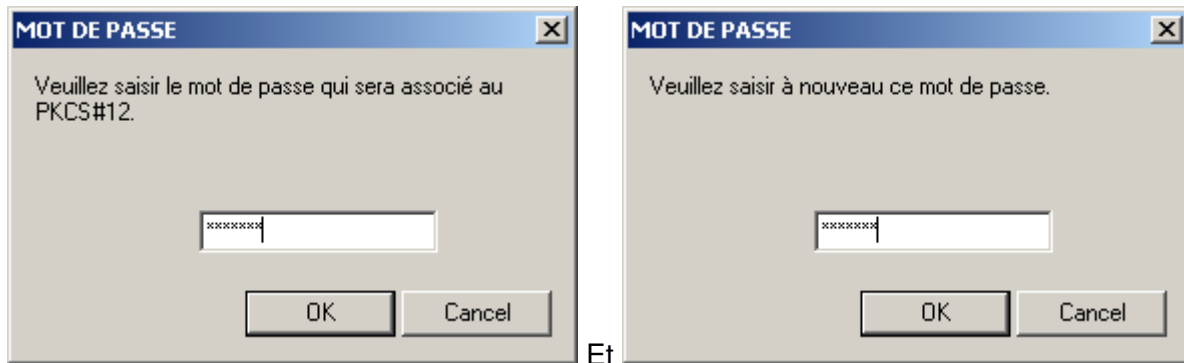


Soit sous forme d'un couple de fichiers « .key » et « .crt »
.....



..... Soit sous forme d'un fichier package « PKCS#12 » (.p12) ; il faut alors saisir le mot de passe de la clé privée (si définie dans l'étape 1).

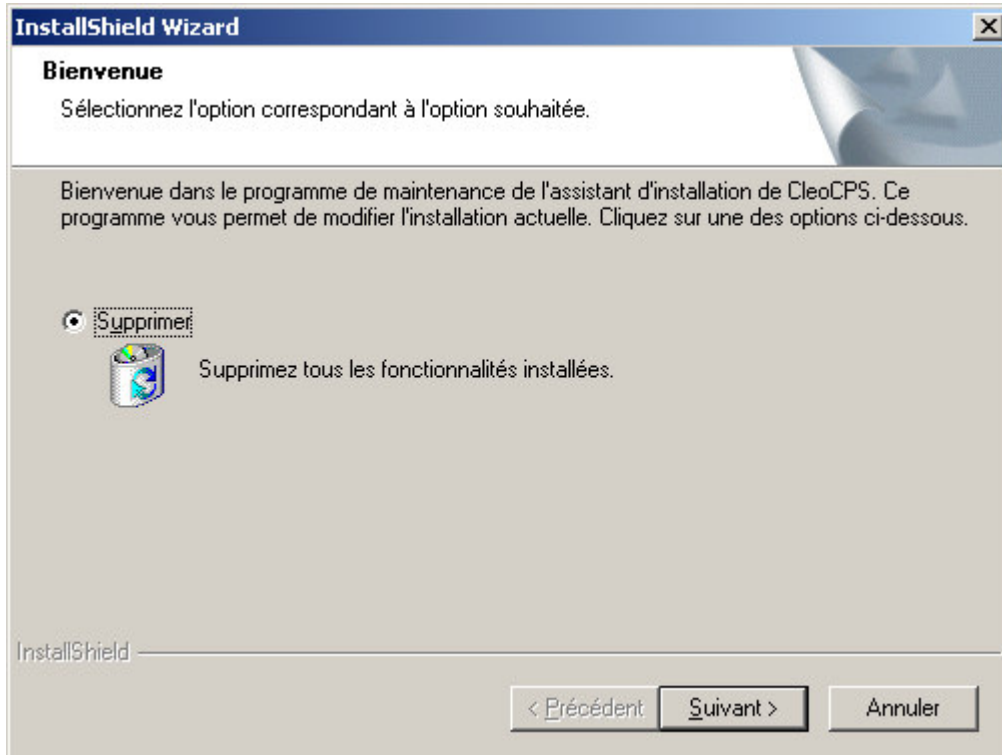
Ce fichier P12 doit être protégé par un AUTRE mot de passe que vous donnerez au récipiendaire pour qu'il puisse l'importer sur le serveur :



Le certificat obtenu peut alors être récupéré en sélectionnant le bouton « **Accéder aux fichiers** ». (Le répertoire contenant les fichiers s'ouvrira)

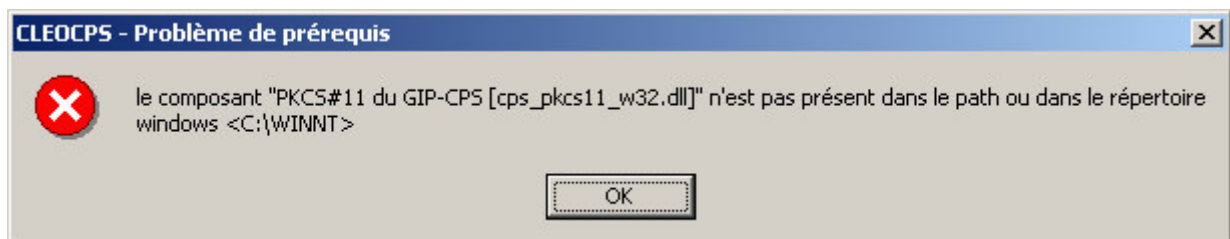
4 Foire aux questions

Q : J'ai lancé l'installation de CleoCPS, celle-ci me propose le choix suivant :



R : Il y a déjà une précédente version de CleoCPS installée sur votre poste. Il est préférable de la désinstaller avant de relancer l'installation.

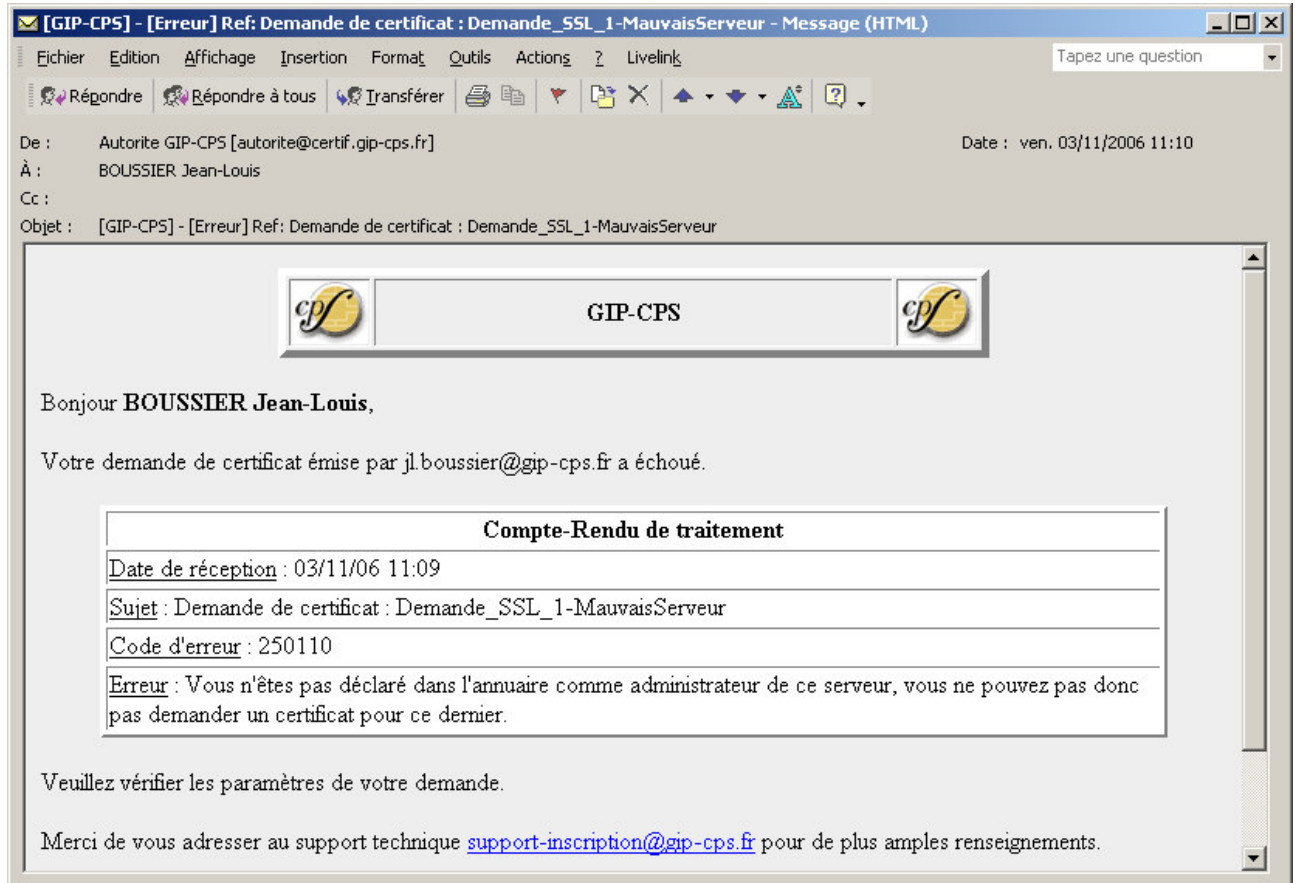
Q : Après avoir installé CleoCPS, au lancement de cet outil, j'ai le message suivant :



R : CleoCPS s'appuie sur un des composants (PKCS#11) des bibliothèques **Cryptolib CPS**. Vous devez donc avoir, au préalable, installé un lecteur de cartes (ce peut être un lecteur PC/SC) et ces bibliothèques **Cryptolib CPS** pour pouvoir utiliser CleoCPS.

Q : Je reçois un message d'erreur de l'autorité du GIP-CPS. Que dois-je faire ?

Exemple de tel message :

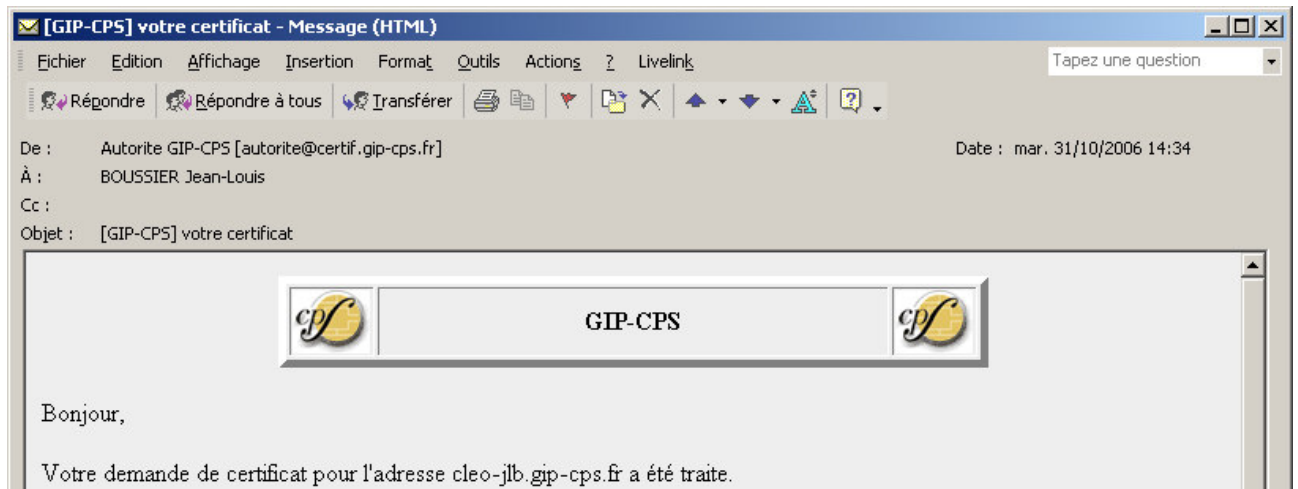


R : Le message d'erreur indique que votre demande n'a pu aboutir.

Dans le cas présenté, ce message indique que le porteur de la carte CPS utilisée pour signer la demande de certificat n'est pas reconnu à l'ASIP Santé comme **administrateur du doublet serveur & domaine** que vous avez saisi dans l'onglet « Demande de certificat » ; il faut donc récupérer une carte et son porteur...

La cause du rejet étant identifiée, il vous faut malheureusement recommencer toute la procédure à partir de la création d'une demande dans un dossier car CleoCPS ne vous autorise pas à rejouer une demande. Vous supprimerez ensuite l'ancienne demande du dossier.

Q : Je reçois bien un message de l'autorité du GIP-CPS m'indiquant que mon certificat est disponible. Mais où est ce certificat ?



R : Le certificat est bien dans le message en pièce jointe, mais vous ne le voyez pas ! Changez des options d'affichage de ce message et enregistrez ces modifications peut le faire apparaître. Ici, par exemple, l'importance du message a été changée vers « Haute »...



Ensuite, en fermant et rouvrant le message, le certificat Smime.p7c (2 Ko) est bien visible en pièce jointe :

