Génération de CSR

AGENCE
DU NUMÉRIQUE
EN SANTÉ

V1.7.0 du 17/09/2021

Génération de CSR

Version 1.7.0 du 17/09/2021

Historique du document			
Version	Date	Auteur	Commentaires
1.0.0	01/06/2016	ASIP Santé	Création
1.0.1	01/06/2016	ASIP Santé	Relecture
1.1.0	01/06/2016	ASIP Santé	Version initiale
1.2.0	21/06/2016	ASIP Santé	Procédure "Java - Porteclé"
1.3.0	11/07/2016	ASIP Santé	Précision commandes OpenSSL
1.4.0	22/07/2016	ASIP Santé	Précision méthode "CertReq" Création PKCS12 avec ACI et ACR avec le magasin Windows
1.5.0	25/07/2016	ASIP Santé	Création PKCS12 avec ACI et ACR avec Firefox
1.6.0	04/09/2017	ASIP Santé	Ajout commande OpenSSL : conversion Mise à jour URLs et informations obsolètes
1.7.0	17/09/2021	ANS	Changement de nom ANS

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

1 Références

N°	Version	Date	Auteur	Document
[1]				
[2]				
[3]				
[4]				

Tableau 1 : Références

2 Résumé

Ce document décrit différentes manières de générer une CSR sur un poste client du portail PFC afin de :

- documenter une alternative à la "génération de CSR assistée" implémentée via JavaScript sur le portail PFC[1]
- documenter une méthode basée sur les lignes de commandes à destination d'utilisateurs finaux "experts"

Accompagnement	Pour toute question et échange sur ce document : editeurs@esante.gouv.fr

Tableau 2 : contact accompagnement ANS

[1] L'ancienne méthode d'implémentation de la génération de CSR assistée sur le portail PFC, qui utilisait une applet Java et posait des problèmes de compatibilité avec certains navigateurs, a été abandonnée au profit du JavaScript en mars 2017.

3 Sommaire

4 Glossaire

Abréviation	Signification
ANS	Agence du numérique en santé
CSR	Certificate Signing Request
PEM	Primary Email Mime-Type
PFC	Plate-forme de certification : **https://pfc.eservices.esante.gouv.fr/**
PKCS#12	12ème norme de la série des "Public Key Cryptography Standards" définissant le format de stockage des clés privées
RSA	Sigle formé à partir des noms des cryptologues : Ronald Rivest, Adi Shamir et Leonard Adleman

Tableau 3 : Glossaire

5 Liste des entreprises citées

Le présent document cite les produits des entreprises ou organismes suivants :

Nom	Site Web	Lien avec le document
Apple		Editeur de Mac OS X
ANS	esante.gouv.fr	CPx, IGC-Santé, PFC
Microsoft		Editeur de Windows
OpenSSL		Editeur de la librairie cryptographique OpenSSL
Oracle		Editeur de Java
XCA		Editeur du logiciel libre XCA

Tableau 4 : Entreprises citées

6 Avertissements

Sur le nécessaire strict respect des procédures décrites dans le document L'attention de l'utilisateur est attirée sur l'importance de respecter strictement les procédures décrites dans le présent document. Toutes les procédures qui y sont décrites ont été préalablement testées par l'ANS. En cas de non-respect de ces procédures, des dysfonctionnements dans l'environnement de travail de l'utilisateur peuvent apparaître. En cas de dysfonctionnement, quel qu'il soit, l'ANS prêtera dans la mesure du possible assistance à l'utilisateur, qui ne pourra rechercher sa responsabilité en cas de non-respect des procédures décrites dans le présent document.
Sur les liens externes Le présent document contient des liens vers des sites Internet. Ces liens ne visent qu'à informer l'utilisateur. Ces sites Web ne sont pas gérés par l'ANS et l'ANS n'exerce sur eux aucun contrôle : leur mention ne saurait engager l'ANS quant à leur contenu. L'utilisation des sites tiers mentionnés relève de la seule responsabilité du lecteur ou de l'utilisateur des produits documentés.
Sur les copies d'écran Les copies d'écran présentées dans ce document sont données à titre illustratif. Les pages ou écrans réellement affichés peuvent être différents, notamment en raison de montées de version ou de configurations d'environnements différentes.
Citations L'ANS est contrainte de citer le nom de certaines entreprises recensées au Tableau 4 afin d'apporter toute l'aide nécessaire au lecteur. Les entreprises citées peuvent prendre contact avec l'ANS à l'adresse email editeurs@esante.gouv.fr pour toute demande en lien avec la citation les concernant. Les entreprises non citées dans ce manuel et ayant une activité en lien avec la carte CPx ou les IGC peuvent également se faire connaître auprès de l'ANS en la contactant à la même adresse.

Tableau 5 : Avertissements

7 Procédure OpenSSL

Conseil

- Utiliser des mots de passe conformes aux préconisations en vigueur (>8 caractères,..)
- Utiliser des identifiants de clés et des noms de fichiers discriminants

Tableau 6

7.1 Générer une nouvelle clé privée

```
%OPENSSL_HOME%\openssl.exe genpkey -out "d:\_pfcng\.private-key.pem" -outform PEM -pass "pass:motdepasse" -des3 -algorithm RSA -pkeyopt rsa_keygen_bits:2048
```

Tableau 7

Génération de la clé privée	
%OPENSSL_HOME%\openssl.exe genpkey	https://www.openssl.org/docs/manmaster/man1/genpkey.html Génération de clé privée RSA
-out "d:_pfcng\.private-key.pem"	Fichier de sortie
-outform PEM	Format du fichier de sortie
-pass "pass:motdepasse"	Mot de passe qui protège l'accès à la clé privée
-des3	Algorithme utilisé pour chiffrer le fichier qui contient la clé privée
-algorithm RSA	Algorithme utilisé pour produire la clé privée
-pkeyopt rsa_keygen_bits:2048	Caractéristique de la clé privée: longueur de la clé privée 2048 bits

Tableau 8

7.2 Générer la CSR

%OPENSSL_HOME%\openssl.exe req -out "d:_pfcng\csr.pem" -outform PEM -passin "pass:motdepasse" -new -key "d:_pfcng\.private-key.pem" -keyform PEM -subj /countryName=FR/ -SHA256

Tableau 9

Génération de la CSR	
%OPENSSL_HOME%\openssl.exe req	https://www.openssl.org/docs/manmaster/man1/req.html Génération de CSR
-out "d:_pfcng\csr.pem"	Fichier de sortie
-outform PEM	Format du fichier de sortie
-passin "pass:motdepasse"	Mot de passe qui protège l'accès à la clé privée
-new	Nouvelle CSR
-key "d:_pfcng\.private-key.pem"	Fichier contenant la clé privée
-keyform PEM	Format du fichier de clé privée
-subj /countryName=FR/	Paramètre du DN
-SHA256	Type de fonction de hachage utilisé pour signer la requête

Tableau 10

7.3 Importer la CSR sur le portail PFC

Figure 1

« Vous avez déjà réalisé votre CSR > Charger la CSR > choisir D:_pfcng\csr.pem > OK > Finaliser »

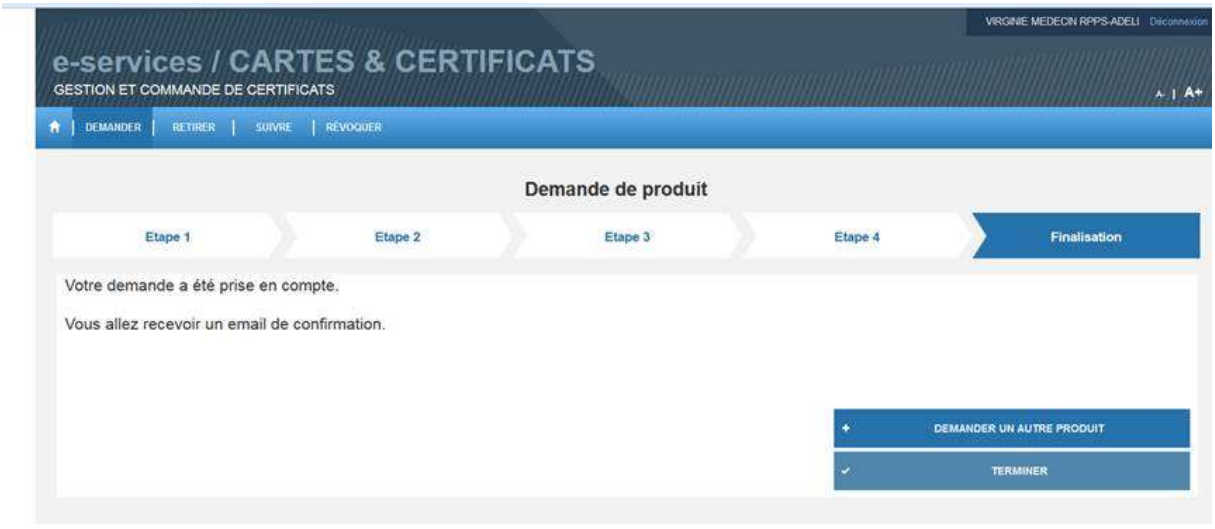


Figure 2

7.4 Attendre le mail de retrait

Agence du numérique en santé

Bonjour,

Nous avons le plaisir de vous informer que le certificat logiciel correspondant à la demande enregistrée sous la référence **N° 6397** est disponible.

Pour le retirer, connectez-vous à **https://pfc-qualif.eservices.esante.gouv.fr/pfcng-ihm/authentication.xhtml** ou copier le lien dans votre navigateur. N'oubliez pas de vous munir de votre carte de la famille CPS et de son code porteur.

Nous vous remercions de l'intérêt que vous portez aux *« e-services CARTES et CERTIFICATS »* de l'Agence du numérique en santé et restons à votre disposition pour tout complément d'information à l'adresse monserviceclient.certificats@asipsante.fr.

Cordialement,
L'équipe Produits de Certification

Figure 3

7.5 Retirer le certificat

Dans « code de révocation » : entrer un mot de passe de 12 caractères, 1 majuscule, 1 caractère non alpha :

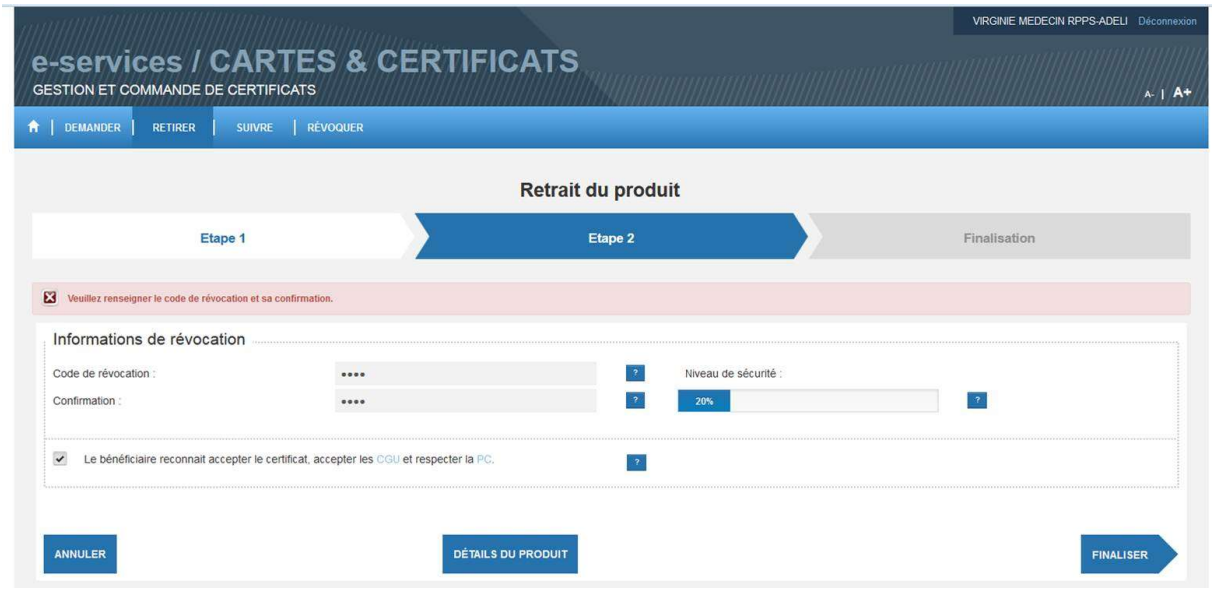


Figure 4

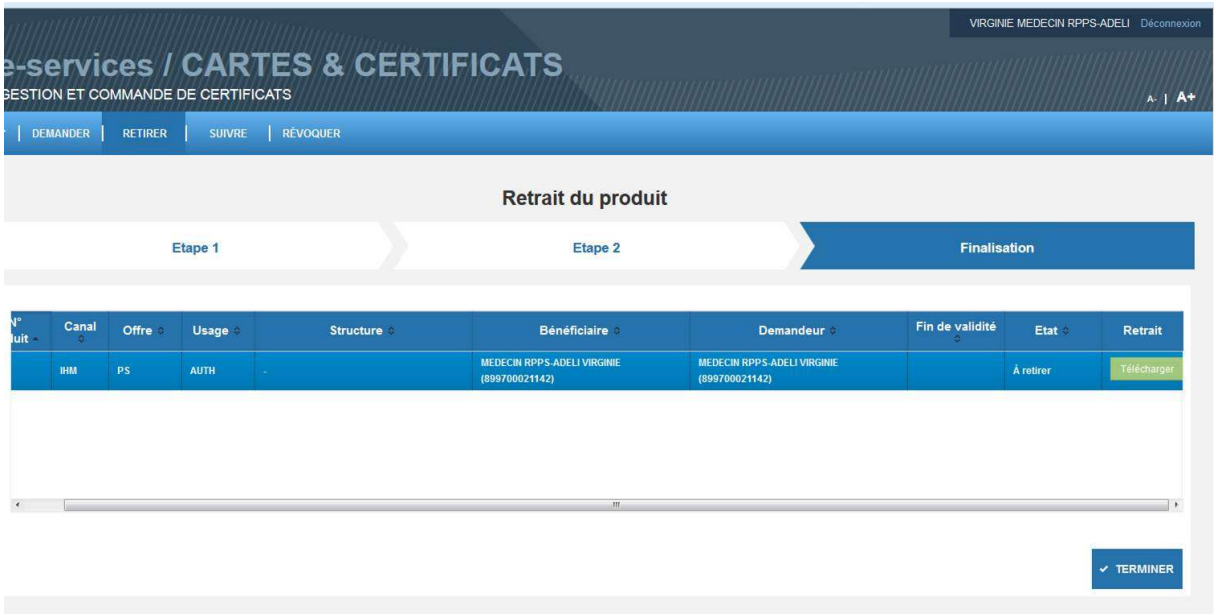


Figure 5

Cliquer sur « Télécharger »

7.6 Convertir le certificat de DER en PEM

Le certificat téléchargé à l'étape précédente (ici renommé en certificate.crt) est au format DER (binaire). Il doit être converti au format PEM (texte) :

```
%OPENSSL_HOME%\openssl x509 -inform DER -in "d:\_pfcng\certificate.crt" -out
"d:\_pfcng\certificate.pem"
```

Tableau 11

Génération de la clé privée	
%OPENSSL_HOME%\openssl.exe x509	https://www.openssl.org/docs/manmaster/man1/x509.html Conversion de format
-inform DER	Format du certificat en entrée : DER
-in "d:_pfcng\certificate.crt"	Chemin du fichier en entrée : certificat au format DER
-out "d:_pfcng\certificate.pem"	Chemin du fichier de sortie : certificat au format PEM

Tableau 12

7.7 Générer le bi-clé au format PKCS#12

Cette étape consiste à réconcilier la clé privée (générée sur votre poste) et le certificat (téléchargé sur le portail PFC). Elle permet d'obtenir un fichier PKCS#12 contenant ces deux éléments :

```
%OPENSSL_HOME%\openssl pkcs12 -export -out "d:\_pfcng\keypair.p12" -in "d:\_pfcng\certificate.pem" -inkey "d:\_pfcng\.private-key.pem" -name exemple-p12 -passout "pass:motdepasse" -passin "pass:motdepasse" -macalg SHA1
```

Tableau 13

Génération de la clé privée	
%OPENSSL_HOME%\openssl.exe pkcs12	https://www.openssl.org/docs/manmaster/man1/x509.html Génération de bi-clé PKCS#12
-export	Création d'un fichier PKCS#12
-out "d:_pfcng\keypair.p12"	Chemin du fichier de sortie PKCS#12
-in "d:_pfcng\certificate.pem"	Fichier contenant le certificat reçu de l'IGC Santé
-inkey "d:_pfcng\.private-key.pem"	Fichier contenant la clé privée
-name exemple-p12	Alias du bi-clé dans le keystore (« Nom convivial » sous Microsoft)
-passout "pass:motdepasse"	Mot de passe protégeant le fichier PKCS#12 de sortie
-passin "pass:motdepasse"	Mot de passe protégeant la clé privée
-macalg SHA1 (valeur par défaut)	Eviter SHA256 (qui fonctionne à l'export du PKCS#12, mais pose des problèmes d'interopérabilité : l'import échoue sous Firefox et Microsoft)[2]

Tableau 14

PKCS#12

Les fichiers PKCS#12 contiennent des données sensibles. Leur transmission et leur sauvegarde doivent se faire en conséquence.

Tableau 15

[2] De même, « openssl pkcs12 -export » devrait être fait avec des options du type « -certpbe AES-256-CBC -keypbe AES-256-CBC » qui « sécurisent » mieux le PKCS#12 :

- utilisation de PKCS#5v2 et de AES-256-CBC, au lieu de pbewithSHAAnd40BitRC2-CBC, utilisé par défaut.
- Ce paramétrage fonctionne à l'export, mais pose des problèmes d'interopérabilité.

7.8 Recommencer la procédure

Pour recommander un produit de certification, il est important de suivre la recommandation suivante:

Recommencer	Pour obtenir un nouveau produit, il faut repartir depuis l'étape "générer une nouvelle clé privée" afin d'utiliser autant de bi-clés que de certificats et d'usage.

Tableau 16 : Recommencer la procédure

8 Procédure "XCA complète"

8.1 Télécharger et installer XCA (Microsoft Windows, Apple Mac OS X ou Linux)

https://sourceforge.net/projects/xca/files/xca/1.3.2/

8.2 Créer une nouvelle base de données

(noter l'emplacement du fichier et noter le mot de passe !!).

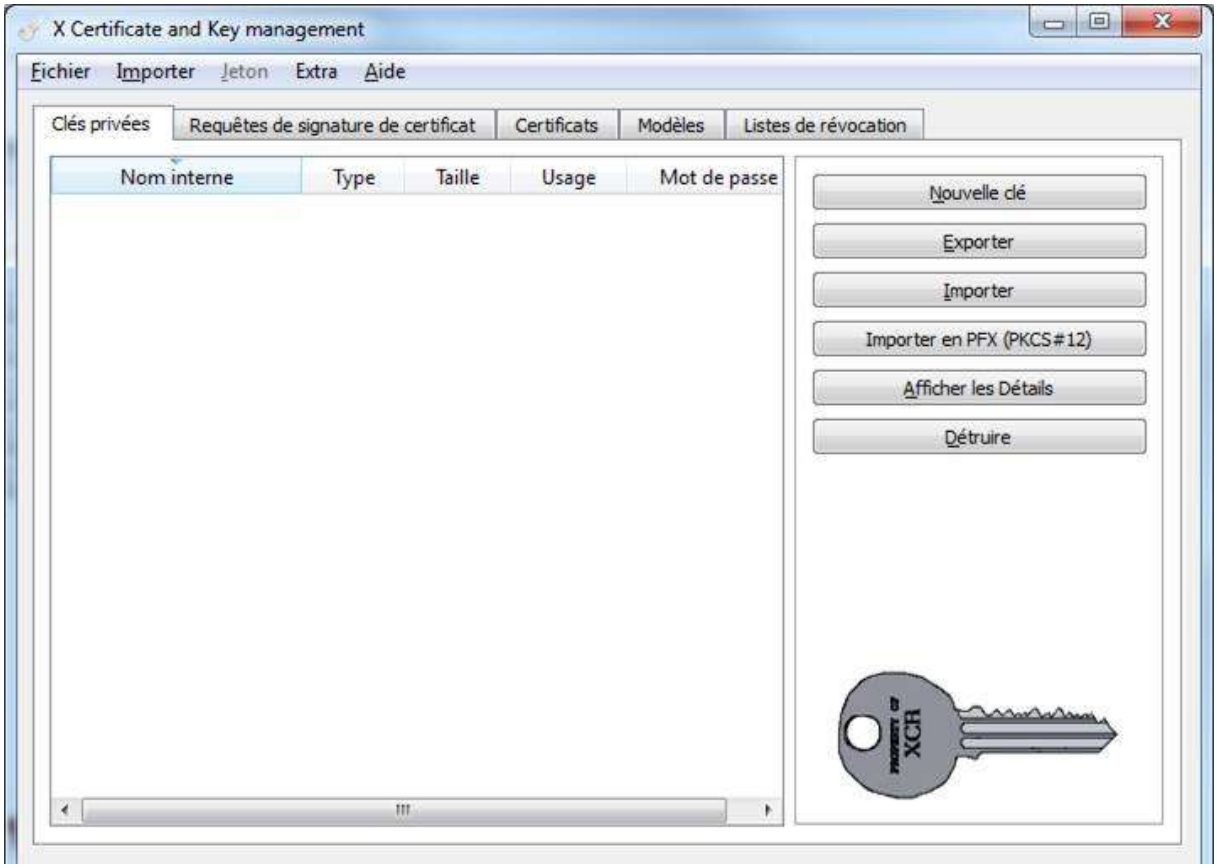


Figure 6

8.3 Générer une nouvelle clé privée

Nom : IGCSanté-AUTH_CLI-privatekey

Taille : 2048 bits

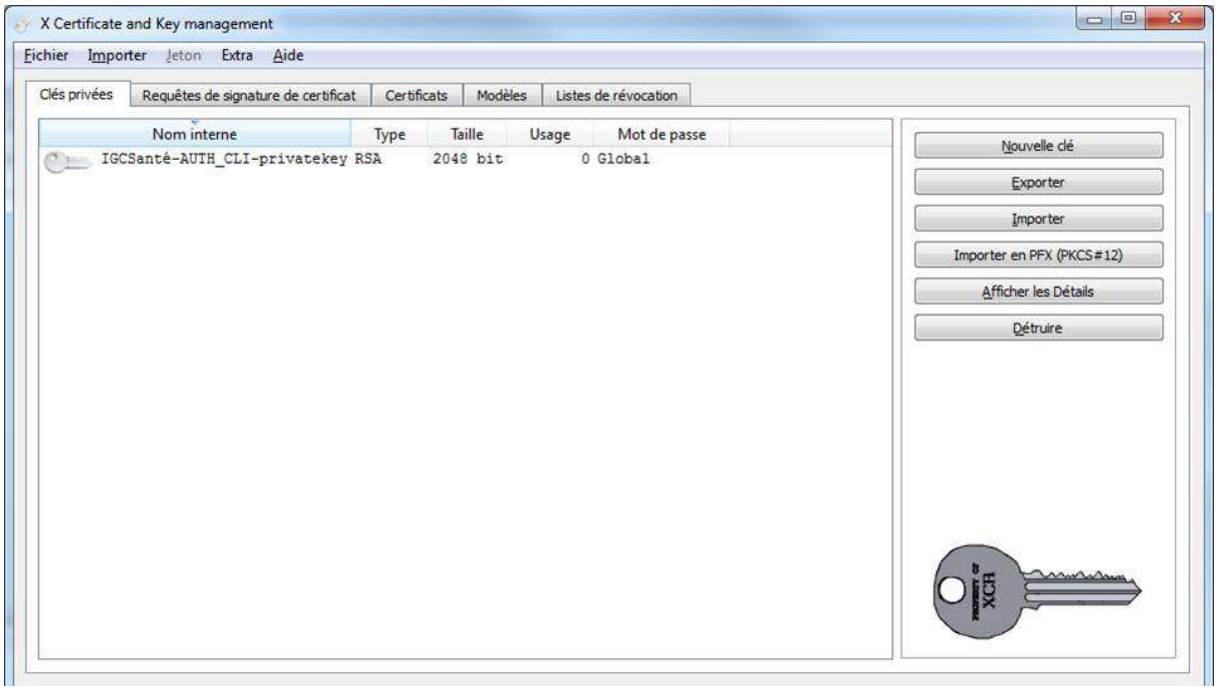


Figure 7

8.4 Générer une requête de signature de certificat

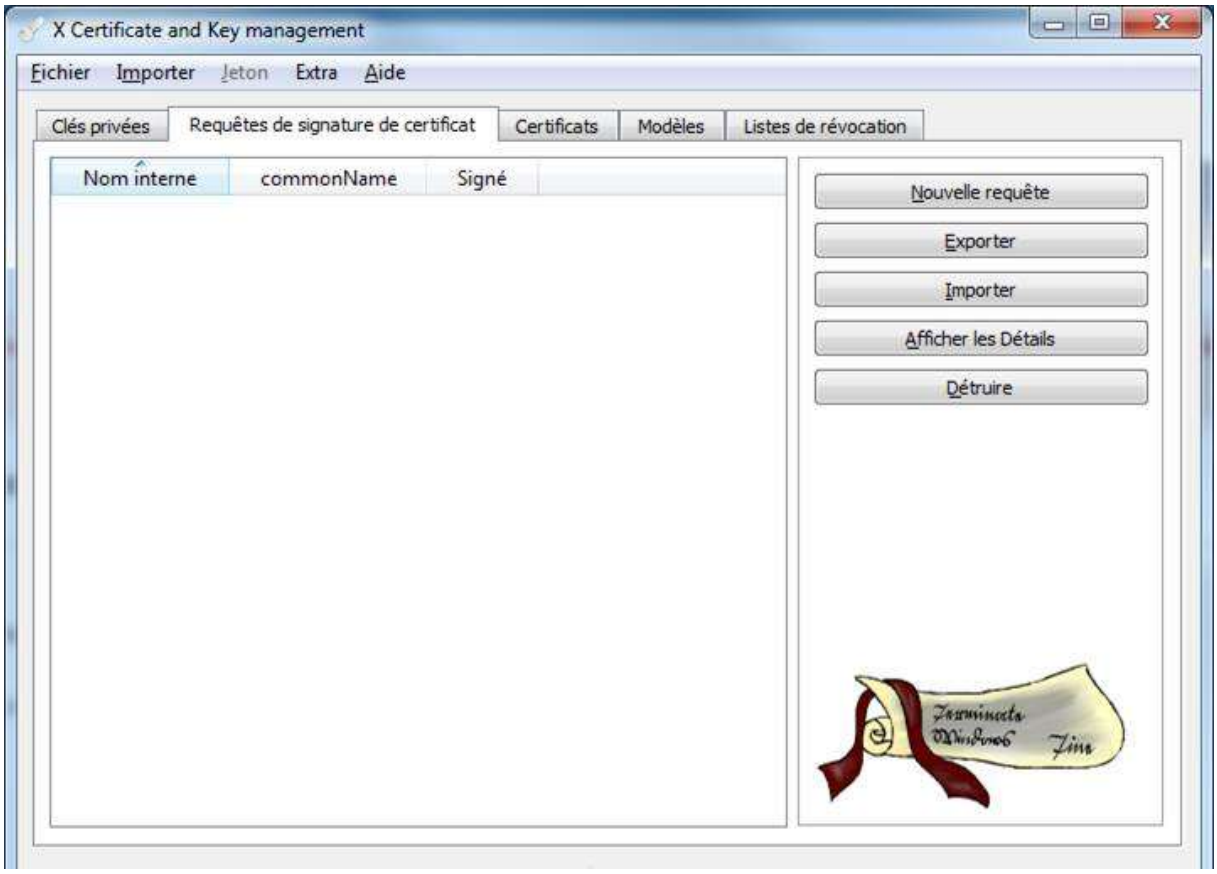


Figure 8

Cliquer sur « nouvelle requête ».

Dans l'onglet « Source », spécifier :

- Signature : SHA 256
- Modèle : default HTTPS_Client

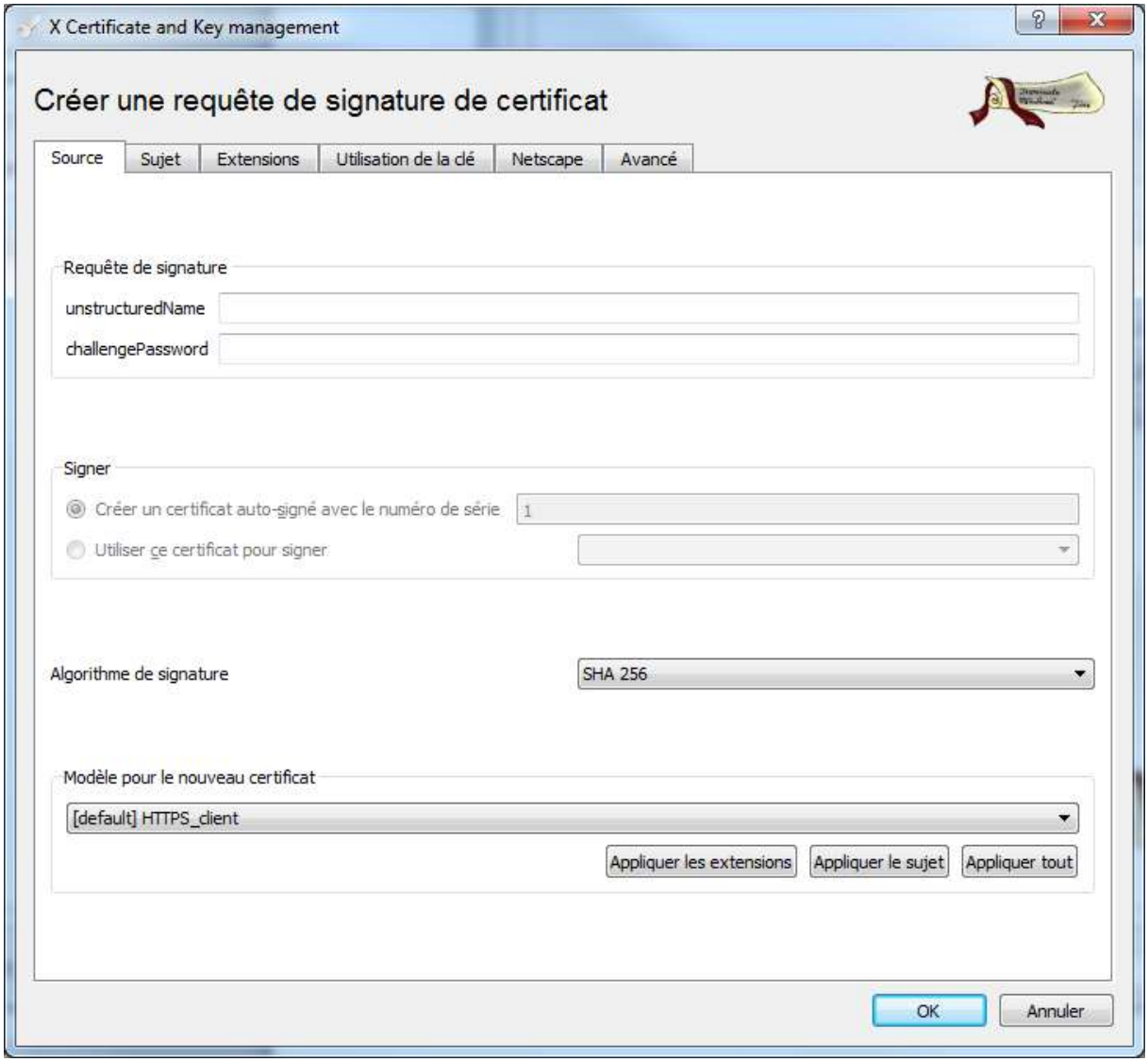


Figure 9

Dans l'onglet « Sujet », spécifier :

- Nom interne : IGCSanté-AUTH_CLI-csr
- Remplir : cn, st, ln, on, ou, cn, ea (attention : ces valeurs ne sont pas utilisées pour générer le certificat, mais elles doivent être non vides)
- Clé privée : IGCSanté-AUTH_CLI-privatekey

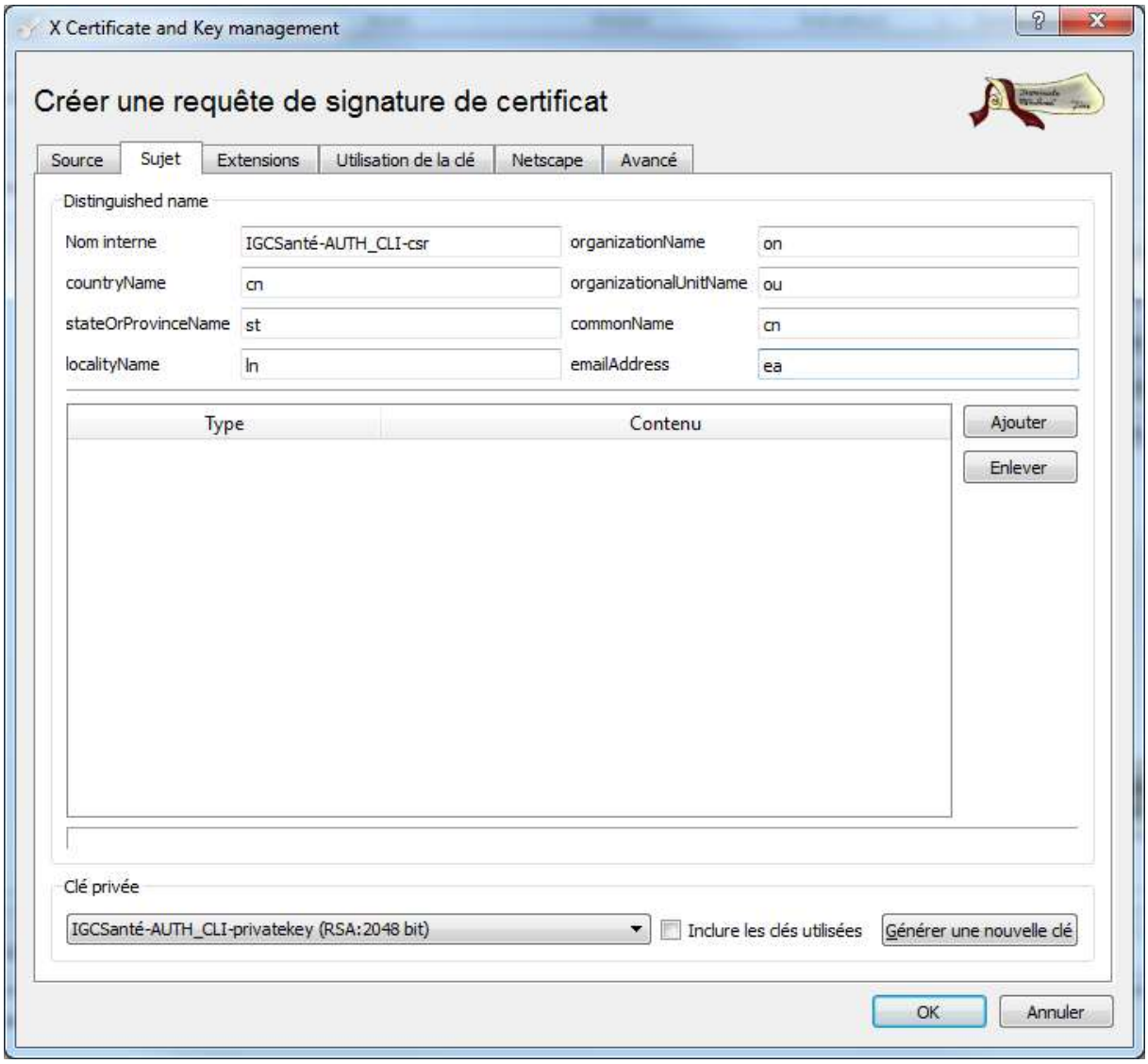


Figure 10

Cliquer sur « OK ».

On obtient:

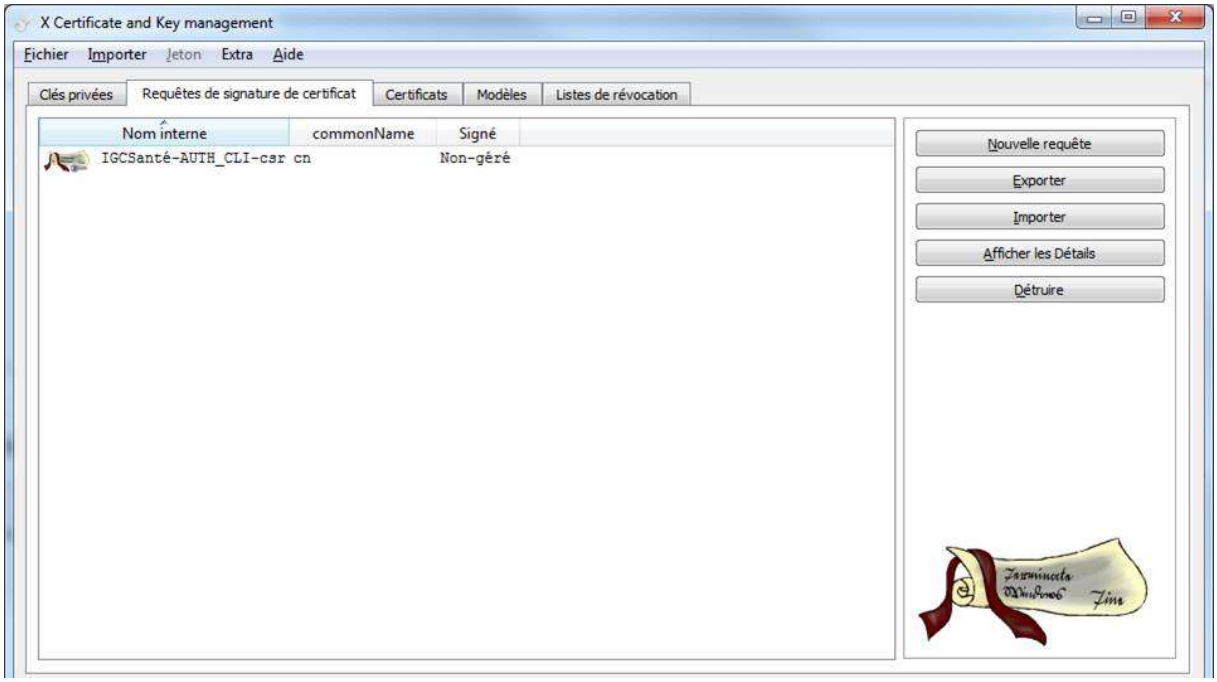


Figure 11

8.5 Exporter la CSR au format PEM

Sélectionner la CSR à exporter puis cliquer sur « Exporter » > « Format PEM »

Figure 12

Dans ce cas, la CSR est dans D:\IGCSanté-AUTH_CLI-csr.pem

8.6 Importer la CSR sur le portail PFC

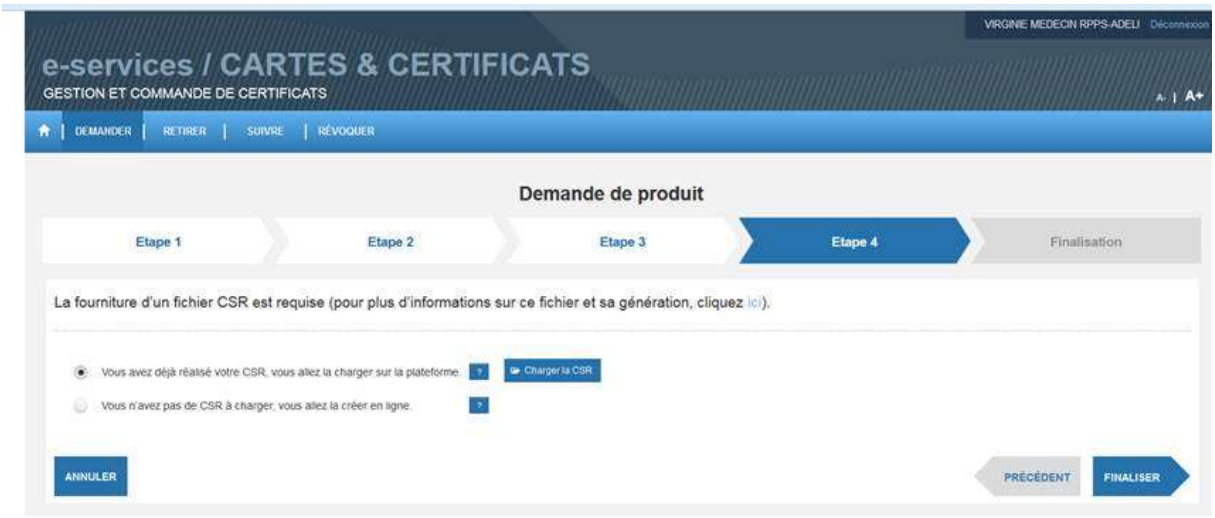


Figure 13

« Vous avez déjà réalisé votre CSR > Charger la CSR > choisir D:\IGCSanté-AUTH_CLI-csr.pem > OK > Finaliser »

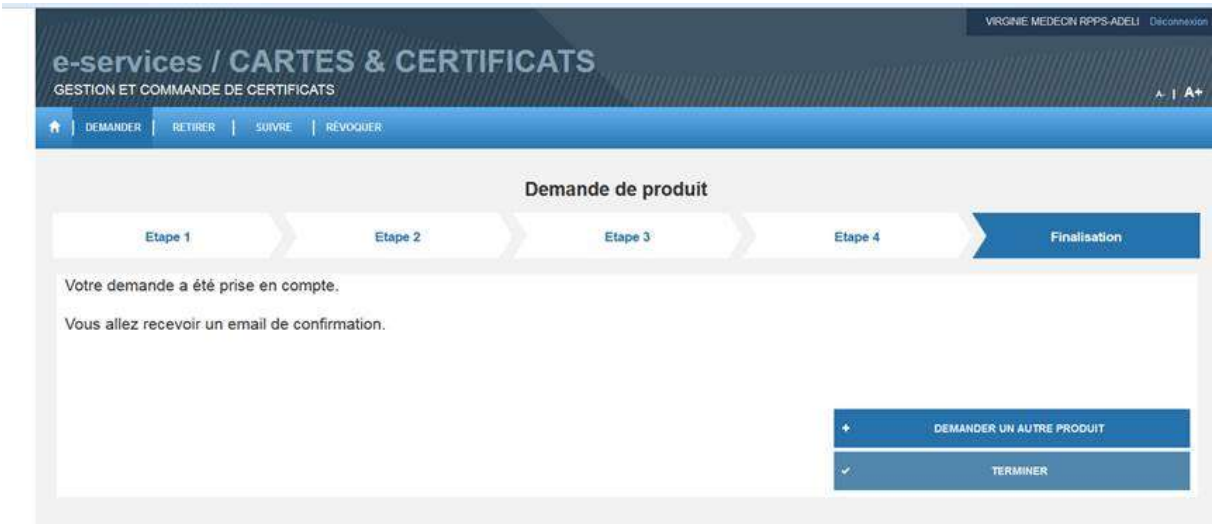


Figure 14

8.7 Attendre le mail de retrait

Agence du numérique en santé

Bonjour,

Nous avons le plaisir de vous informer que le certificat logiciel correspondant à la demande enregistrée sous la référence **N° 6397** est disponible.

Pour le retirer, connectez-vous à **https://pfc-qualif.eservices.esante.gouv.fr/pfcng-ihm/authentication.xhtml** ou copier le lien dans votre navigateur. N'oubliez pas de vous munir de votre carte de la famille CPS et de son code porteur.

Nous vous remercions de l'intérêt que vous portez aux *« e-services CARTES et CERTIFICATS »* de l'Agence du numérique en santé et restons à votre disposition pour tout complément d'information à l'adresse monserviceclient.certificats@asipsante.fr.

Cordialement,
L'équipe Produits de Certification

Figure 15

8.8 Retirer le certificat

Dans « code de révocation » : entrer un mot de passe de 12 caractères, 1 majuscule, 1 caractère non alpha :

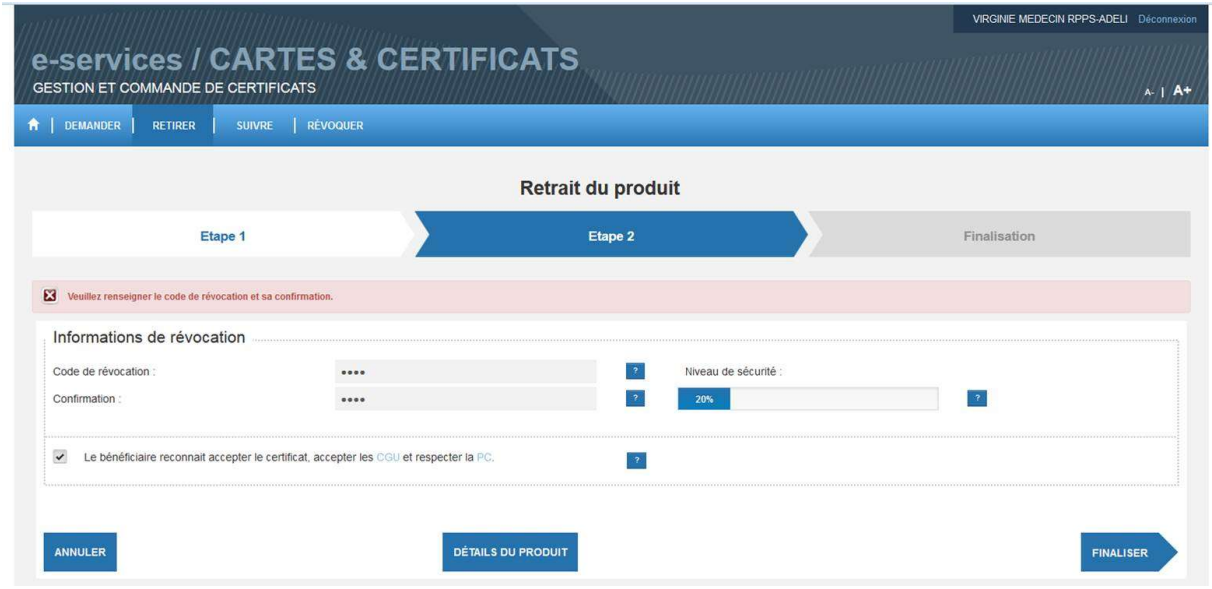


Figure 16

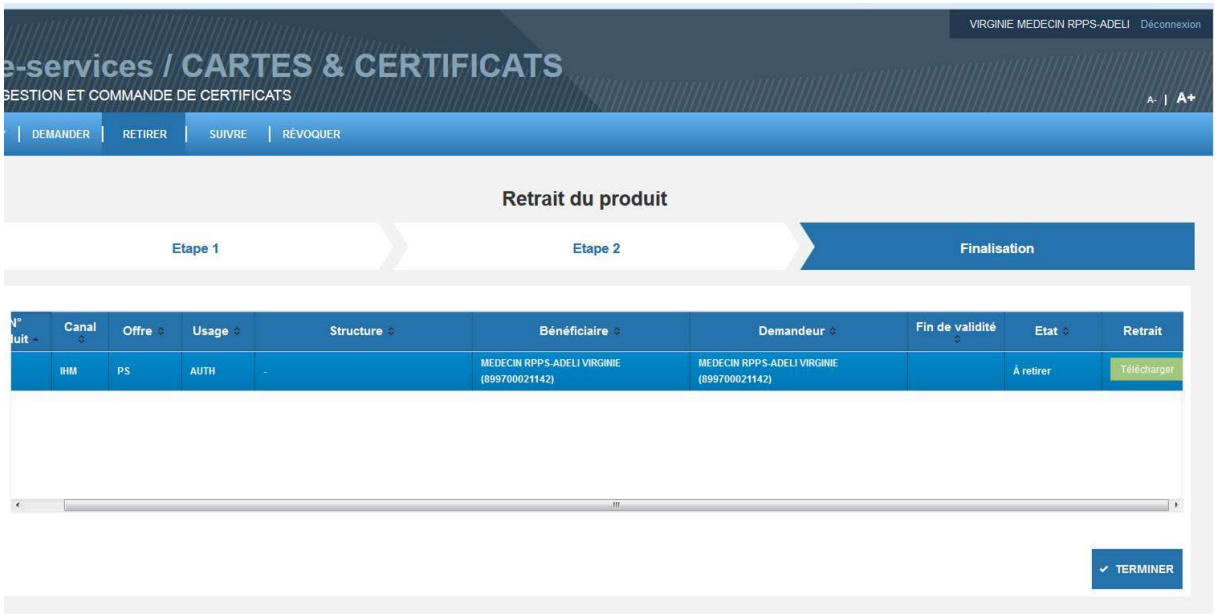


Figure 17

Cliquer sur « Télécharger »

8.9 Réconcilier clé privée et certificat

XCA > Certificat > Importer :

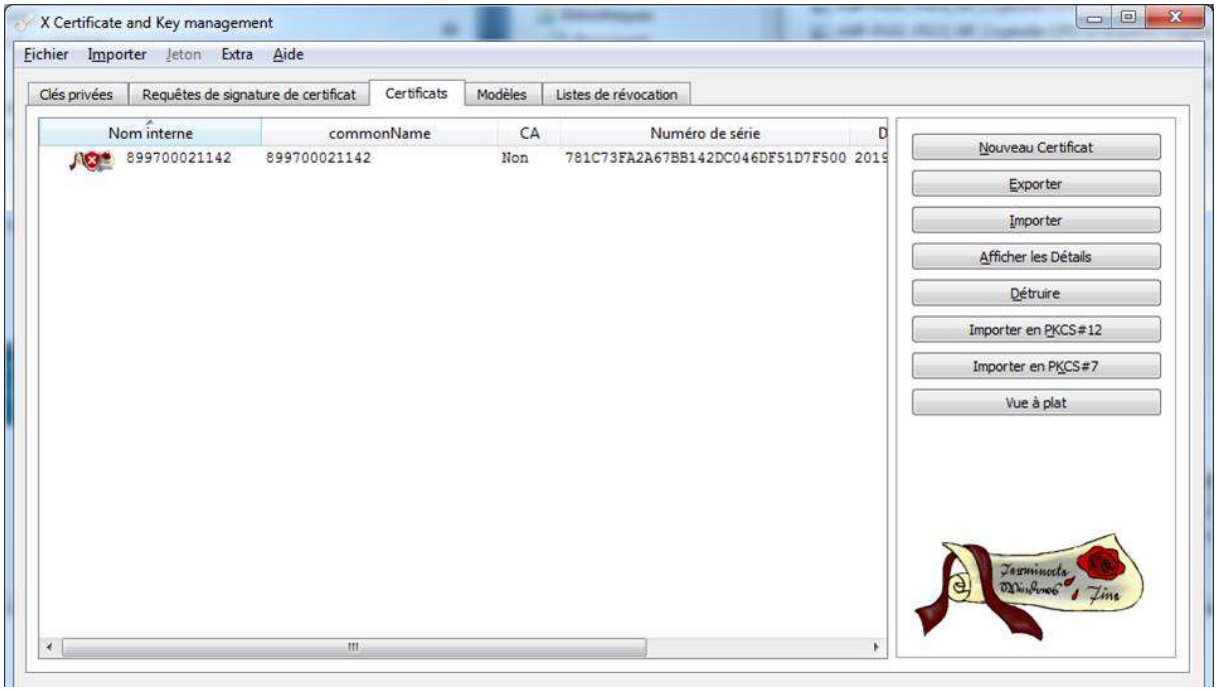


Figure 18

XCA retrouve la clé privée associée au certificat tout seul :

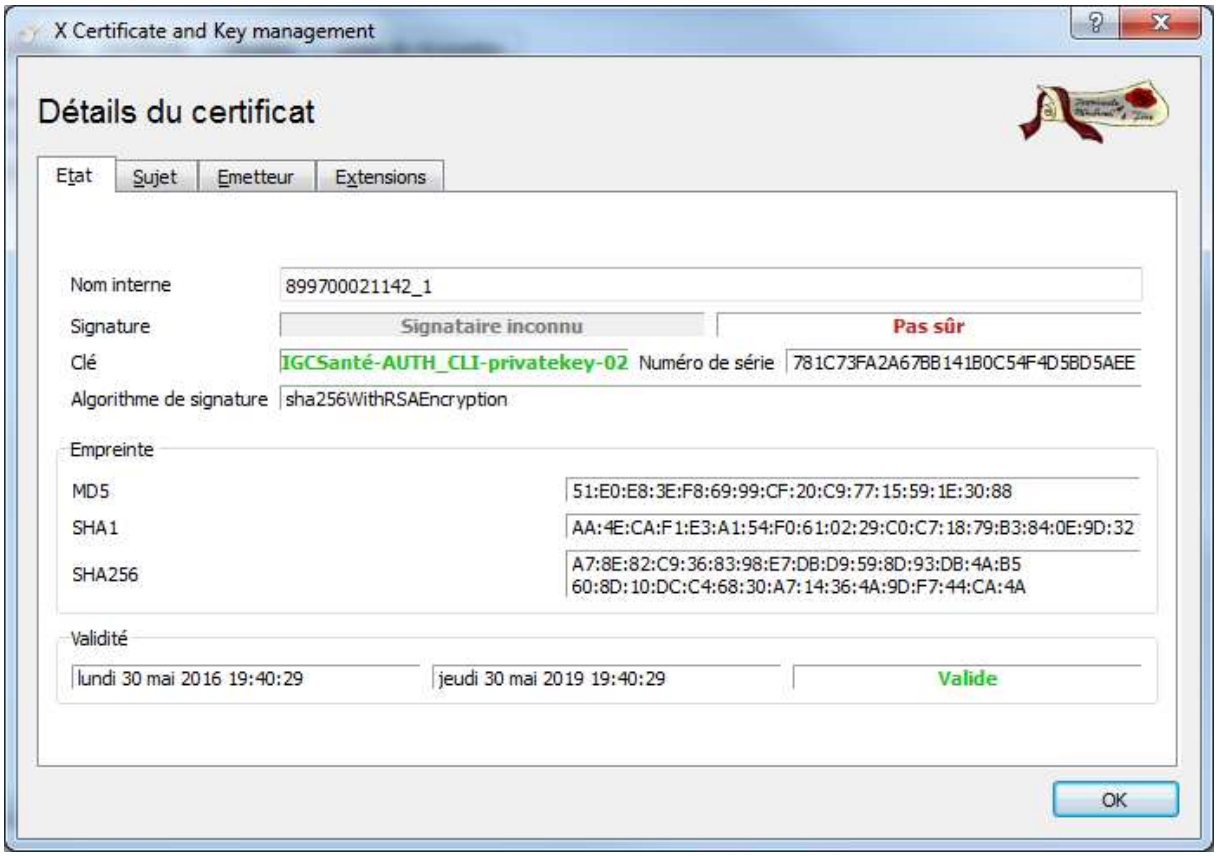


Figure 19

Le bi-clé ainsi reconstitué est noté "pas sûr". Ceci provient du fait que les ACR et ACI ASIP Santé n'ont pas été importés dans XCA.

Clé "pas sûre"

Cette opération peut se faire en allant dans l'onglet "certificat" option "importer" et en important les certificats au format DER (fichiers .cer) depuis http://igc-sante.esante.gouv.fr/PC/#ca et http://igc-sante.esante.gouv.fr/PC%20TEST/#ca puis en ajustant le niveau de confiance pour chaque certificat (clic droit > "Niveau de confiance" > "Toujours se fier à ce certificat")

Tableau 17

Après import et ajustement de la confiance, on obtient:

Vue arborescente:

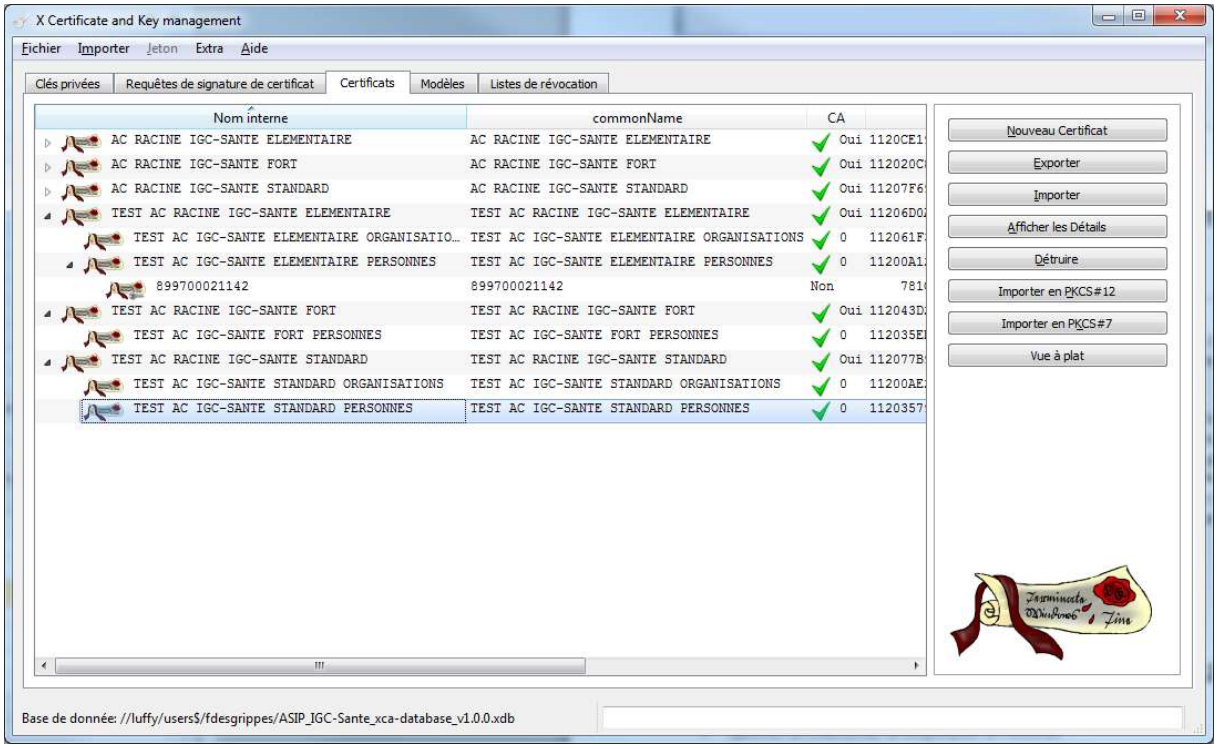


Figure 20

Vue à plat:

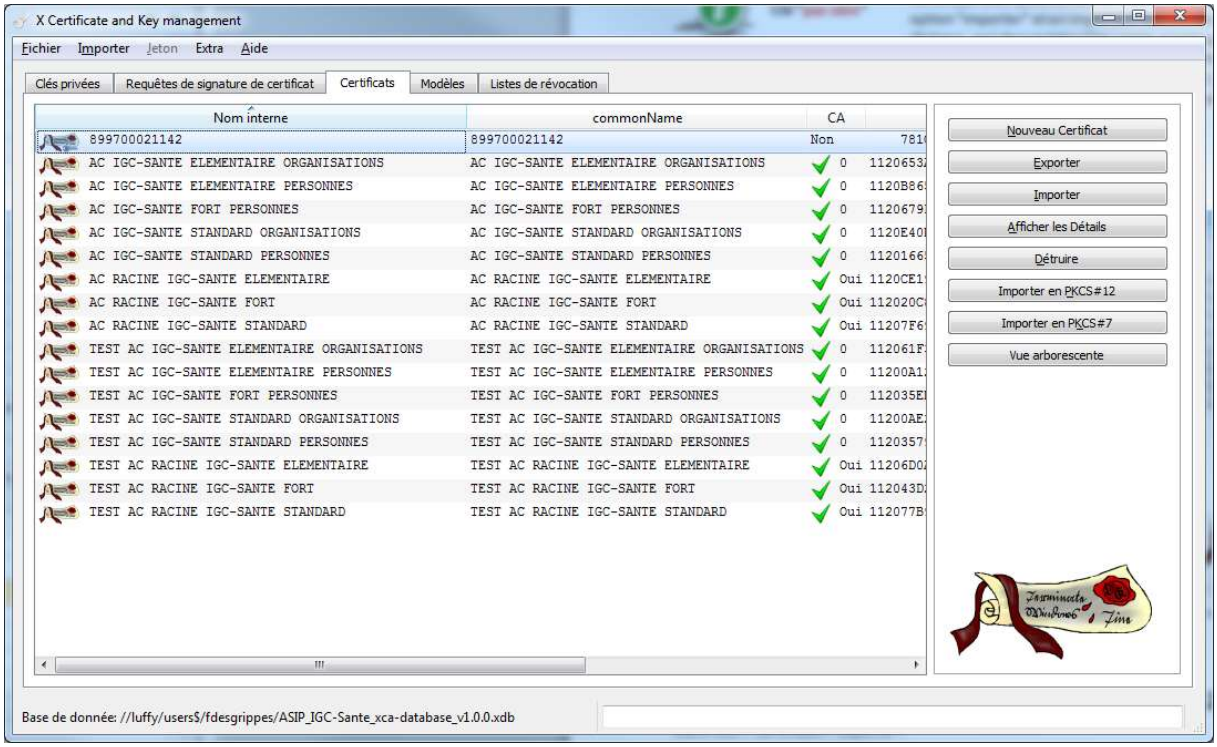


Figure 21

Certificat final marqué comme sûr avec un émetteur identifié:

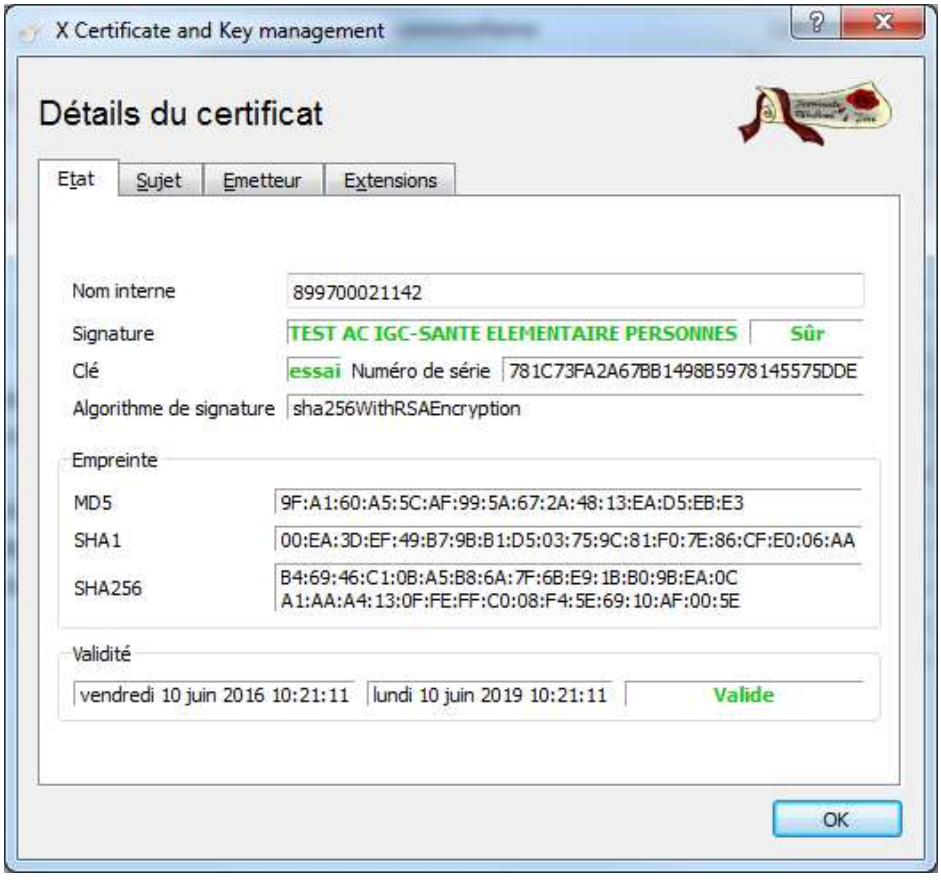


Figure 22

8.10 Exporter le bi-clé au format PKCS#12

Dans XCA > Certificats > Exporter :

- Spécifier un chemin sur le disque pour le PKCS#12.
- Choisir le format d'export « PKCS#12 »

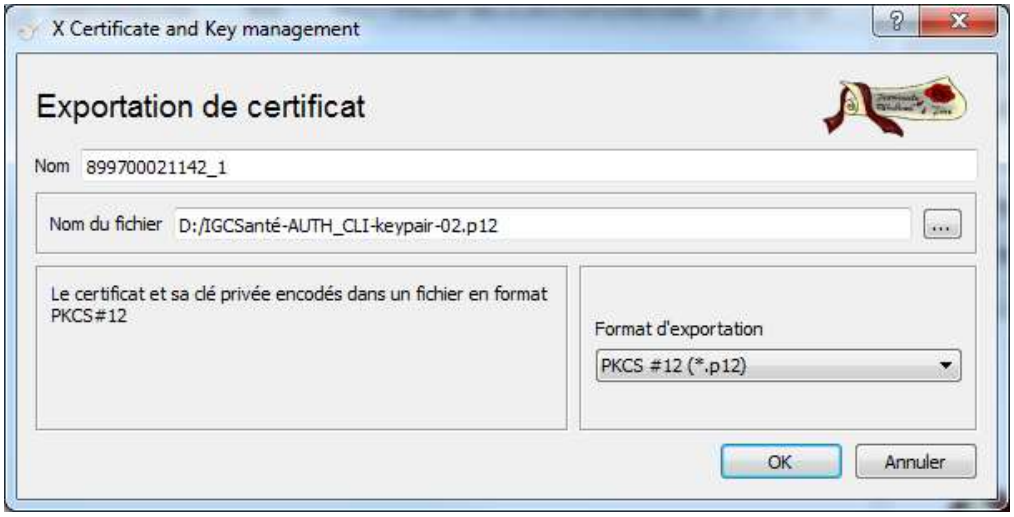


Figure 23

Entrer un mot de passe pour protéger le fichier PKCS#12 :

Figure 24

PKCS#12	Les fichiers PKCS#12 contiennent des données sensibles. Leur transmission et leur sauvegarde doivent se faire en conséquence. Il en est de même pour le mot de passe protégeant le PKCS#12.

Tableau 18

8.11 Recommencer la procédure

Pour recommander un produit de certification, il est important de suivre la recommandation suivante:

Recommencer	Pour obtenir un nouveau produit, il faut repartir depuis l'étape "générer une nouvelle clé privée" afin d'utiliser autant de bi-clés que de certificats et d'usage.

Tableau 19 : Recommencer la procédure

9 Procédure "XCA IGC Santé"

9.1 Installer XCA

9.2 Télécharger la base de données ANS pour XCA

Le fichier de type ".xdb" est disponible sur le site https://tech.esante.gouv.fr/outils-services/igc-sante/manuels-utilisateurs.

Le mot de passe est "**changeit**" (à changer via "Extra" > "Changer le mot de passe de la base de données").

Ce fichier intègre le ACR et ACI de l'IGC-Santé:

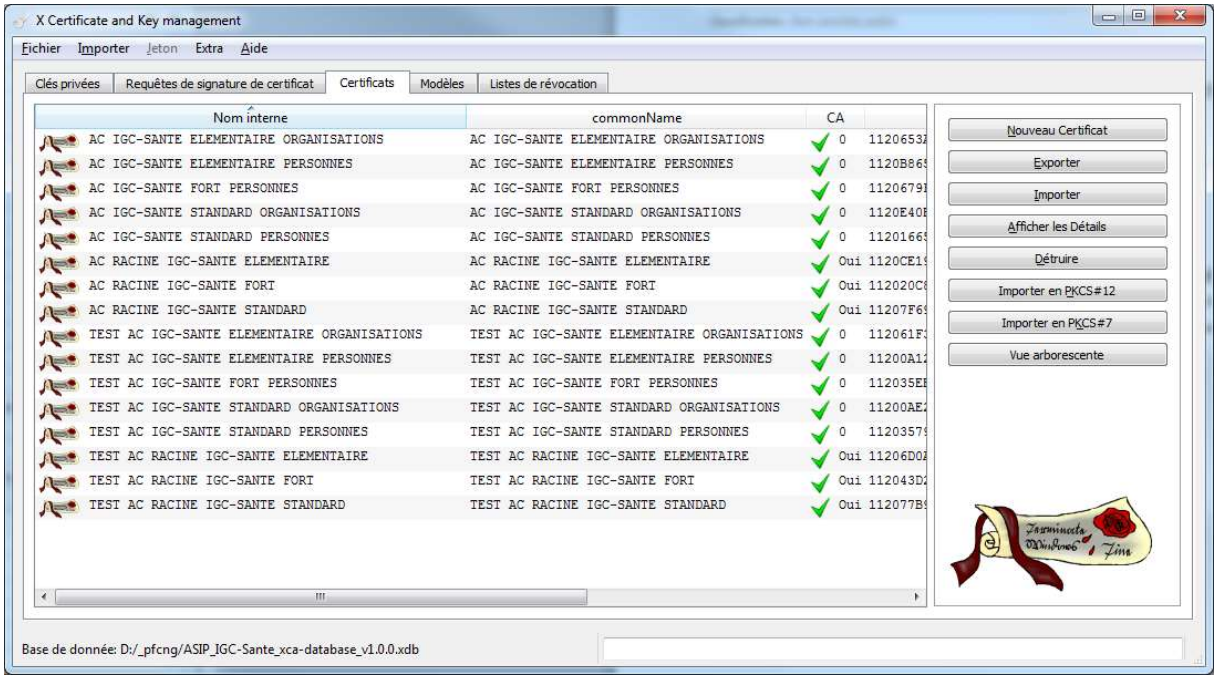


Figure 25

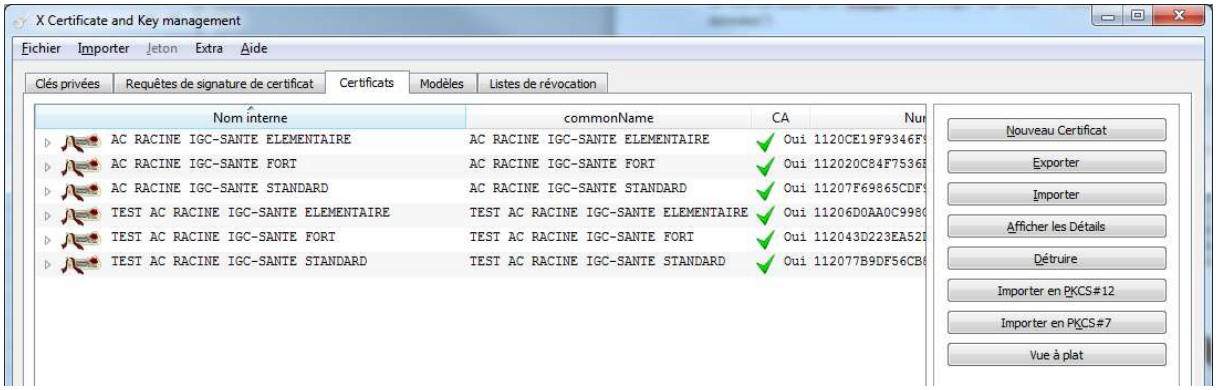


Figure 26

9.3 Appliquer la procédure "XCA complète"

En utilisant le template "IGC-Santé IHM Générique":

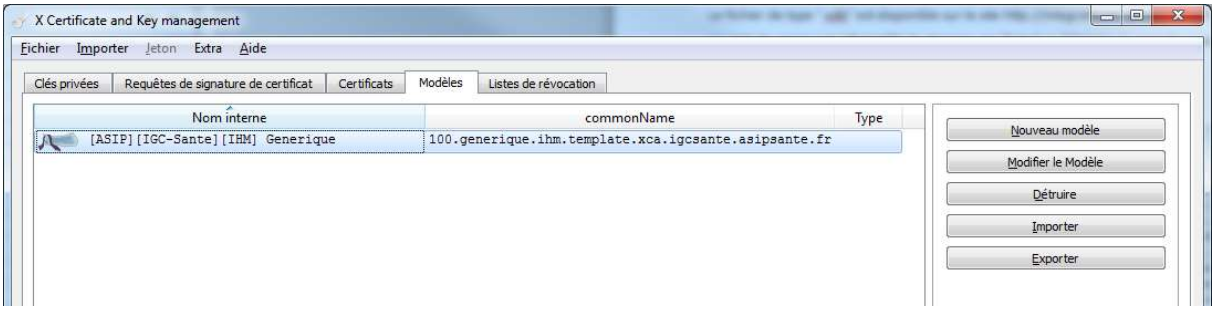


Figure 27

Figure 28

Cliquer sur "Appliquer tout":

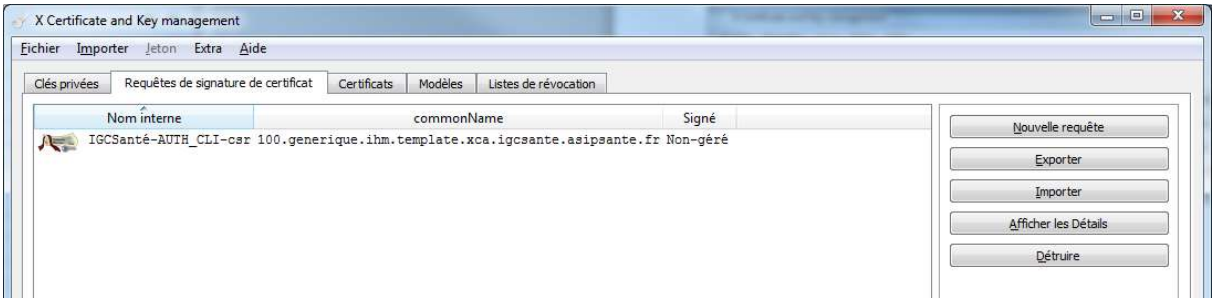


Figure 29

10Procédure "CertReq" sous Microsoft Windows

10.1 Pré-requis: installer les ACR IGC-Santé

Action utilisateur: Touche Windows > "Rechercher les programmes et fichiers" > inetcpl.cpl > touche "entrée":

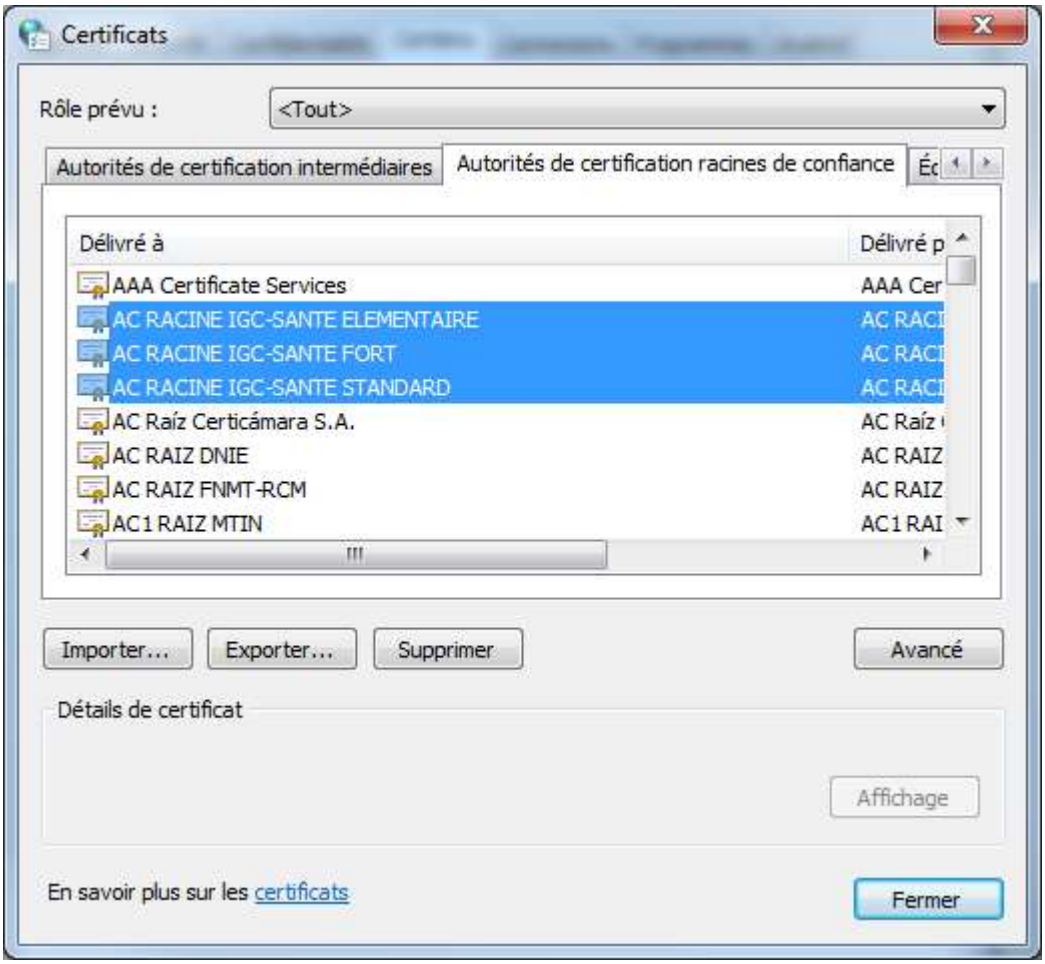


Figure 30

Branche TEST	Faire de même avec la branche "TEST" si utilisation des produits de test il y a

Tableau 20

Récupération des certifications IGC-Santé	http://igc-sante.esante.gouv.fr/PC/ ou http://igc-sante.esante.gouv.fr/PC%20TEST/

Tableau 21

10.2 Pré-requis: Installer les ACI IGC-Santé

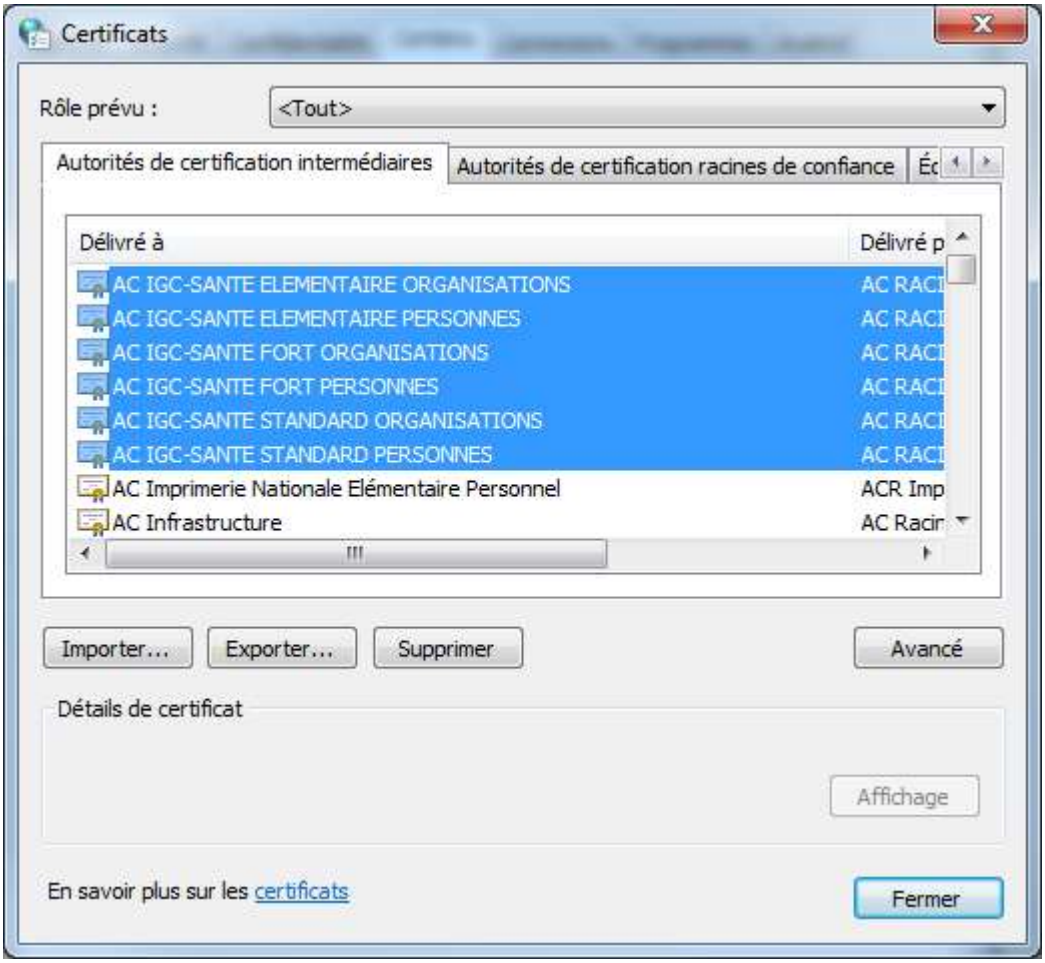


Figure 31

	Branche TEST	Faire de même avec la branche "TEST" si utilisation des produits de test il y a

Tableau 22

10.3 Créer un fichier .inf de génération de clé

La documentation de référence est :

https://technet.microsoft.com/en-us/library/dn296456%28v=ws.11%29.aspx

Créer un fichier igcsante-cerreq.inf contenant les champs suivants:

```
[NewRequest]
Subject = "CN=monbiclé"
Exportable = TRUE
KeyLength = 2048
```

10.4 Générer une nouvelle clé privée et la CSR

La documentation de référence est :

https://technet.microsoft.com/en-us/library/dn296456%28v=ws.11%29.aspx

Générer une nouvelle clé privée et la CSR:

```
CertReq -New d:\_pfcng\igcsante\cerreq.inf d:\_pfcng\igcsante\cerreq.req
```

Clé privée	La clé privée générée est stockée, sécurisée, dans le magasin Microsoft sur le Poste de Travail

Tableau 23

10.5 Importer la CSR sur le portail PFC

Reproduire la démarche décrite plus haut avec d:_pfcng\igcsante cerreq.req

10.6 Attendre le mail de retrait

Cf. aperçus d'écran plus haut

10.7 Retirer le certificat

Cf. aperçus d'écran plus haut

10.8 Importer le certificat obtenu de la PFC dans le magasin personnel

Import et clé privée	Le certificat obtenu doit être importé sur le même Poste de Travail qui a généré la clé privée

Tableau 24

La documentation de référence est :

https://technet.microsoft.com/en-us/library/dn296456%28v=ws.11%29.aspx

```
CertReq -accept d:\_pfcng\igcsante-cerreq.crt
```

Chaines de confiance	Pour l'import sous cette forme, les chaines de confiance doivent avoir été préalablement correctement installées.

Tableau 25

10.9 Exporter le bi-clé sous forme de fichier PKCS#12

Depuis "inetcpl.cpl", double-cliquer sur le certificat correspondant au bi-clé à exporter:

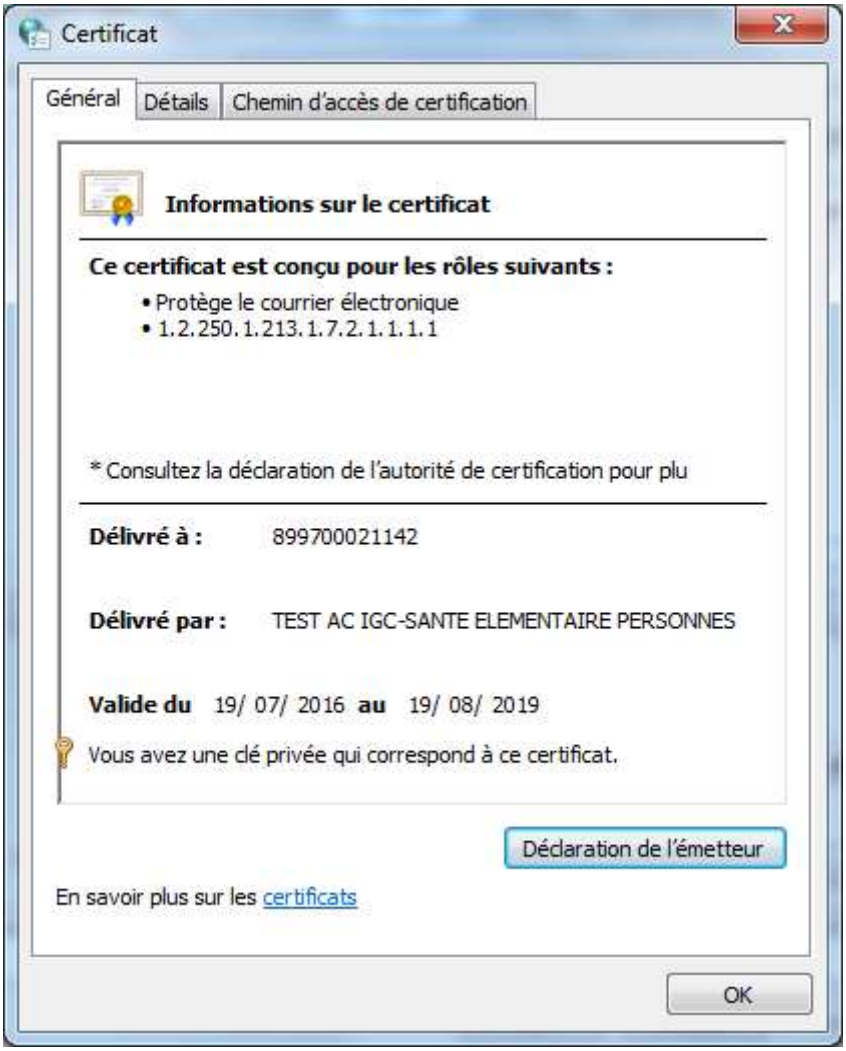


Figure 32

Cliquer sur l'onglet "Détails"

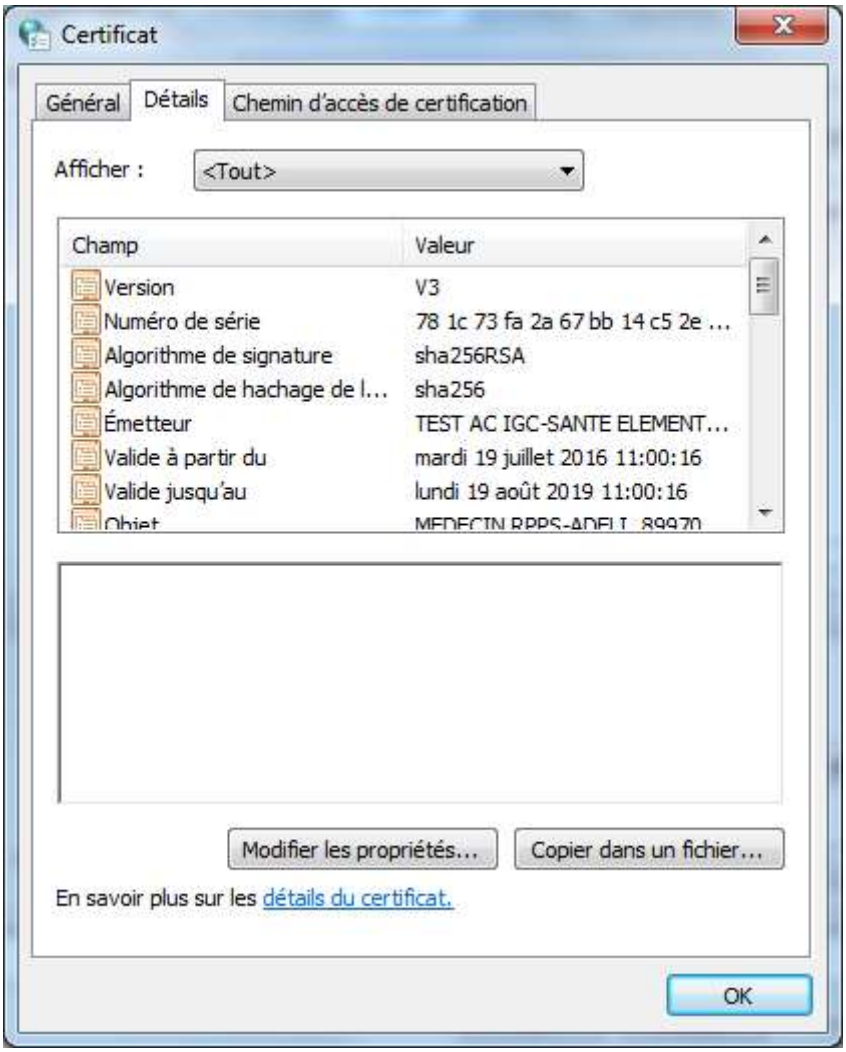


Figure 33

Choisir: "Copier dans un fichier…"

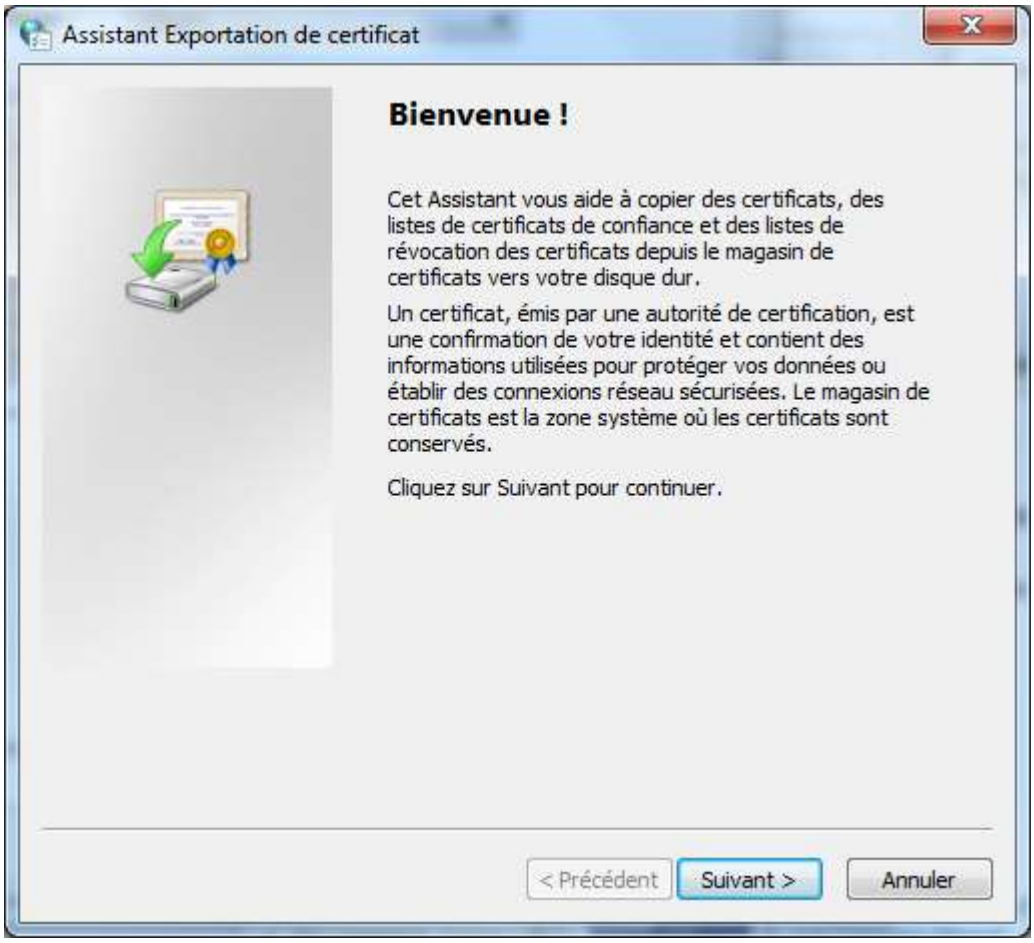
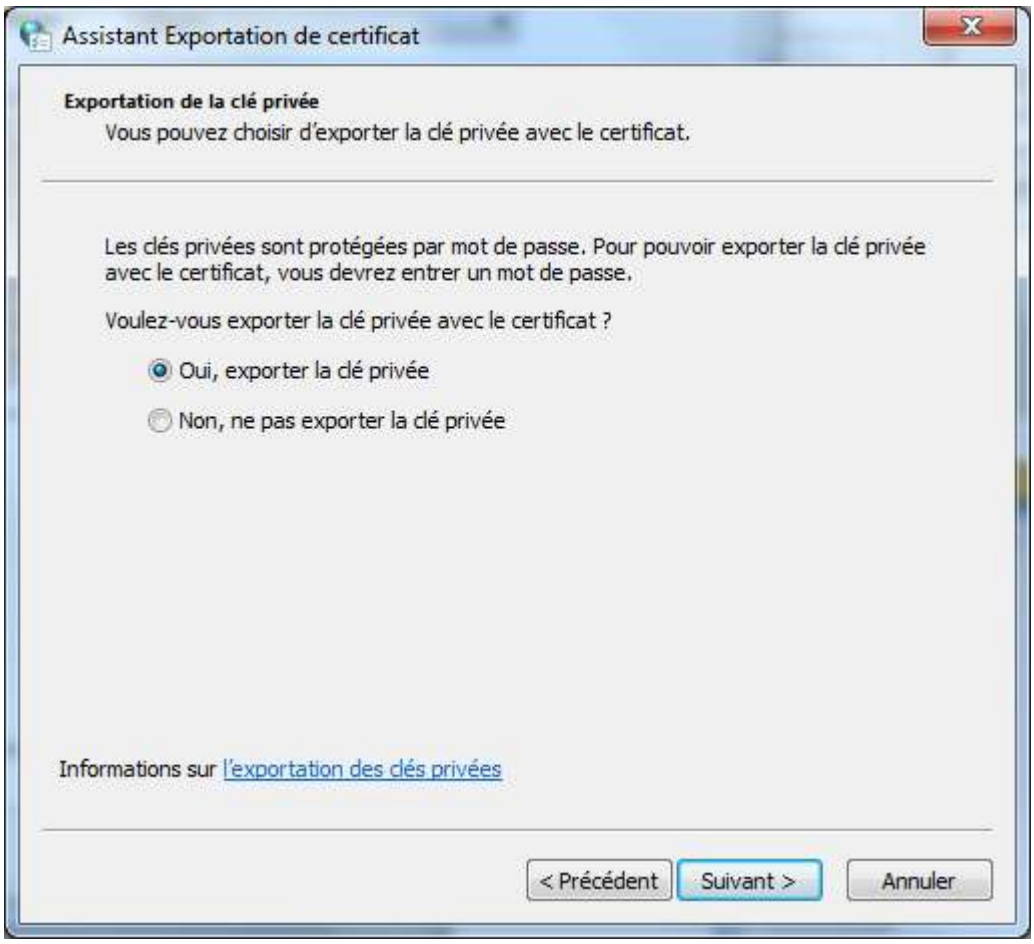
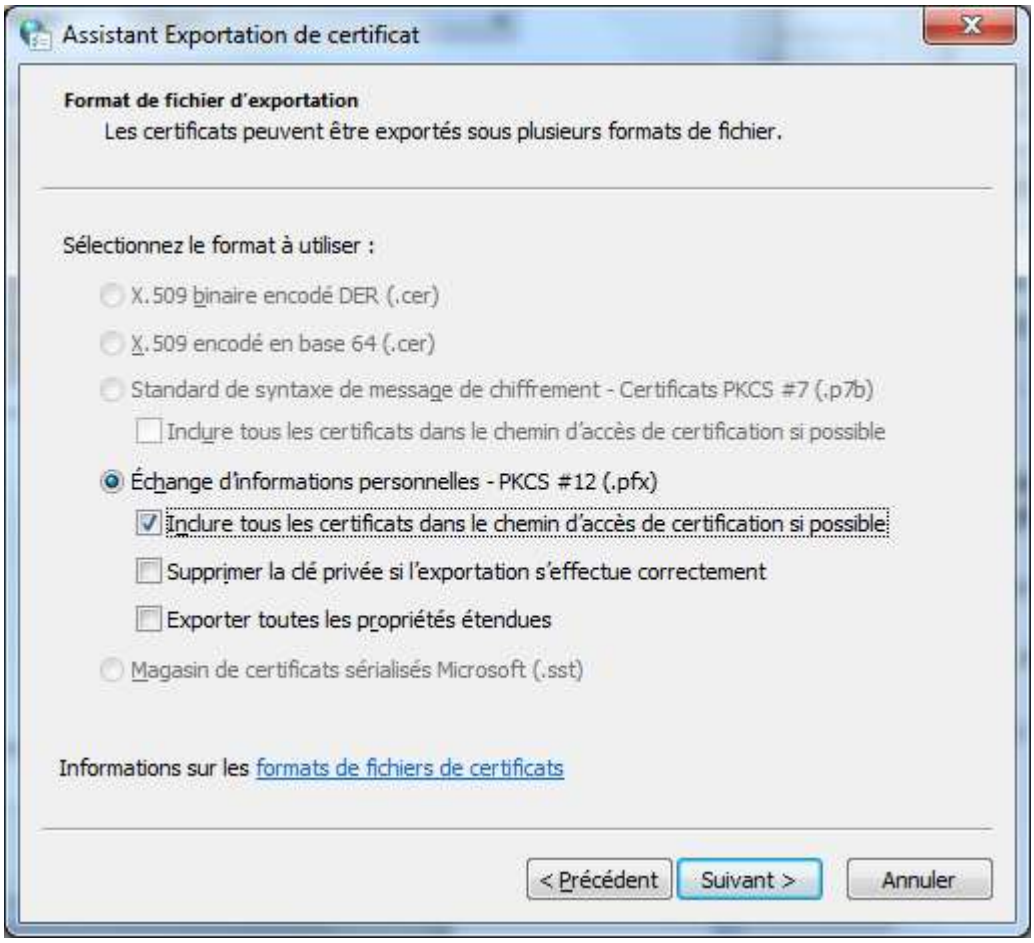

Assistant Exportation de certificat
Bienvenue !
Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats depuis le magasin de certificats vers votre disque dur.
Un certificat, émis par une autorité de certification, est une confirmation de votre identité et contient des informations utilisées pour protéger vos données ou établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.
Cliquez sur Suivant pour continuer.
< Précédent
Suivant >
Annuler

Figure 34

Oui, exporter la clé privée





Inclure tous les certificats dans le chemin d'accès de certification si possible

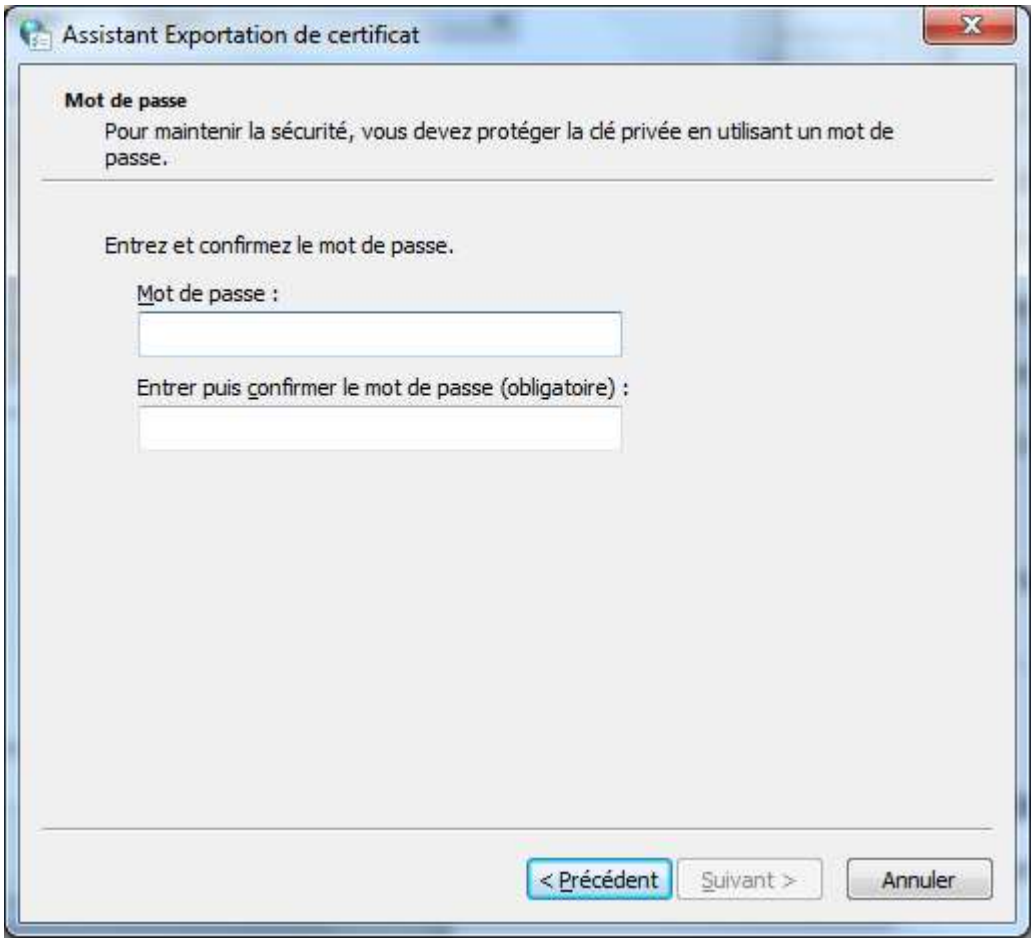

Assistant Exportation de certificat
Mot de passe
Pour maintenir la sécurité, vous devez protéger la clé privée en utilisant un mot de passe.
Entrez et confirmez le mot de passe.
Mot de passe :
Entrer puis confirmer le mot de passe (obligatoire) :
< Précédent
Suivant >
Annuler

Figure 35

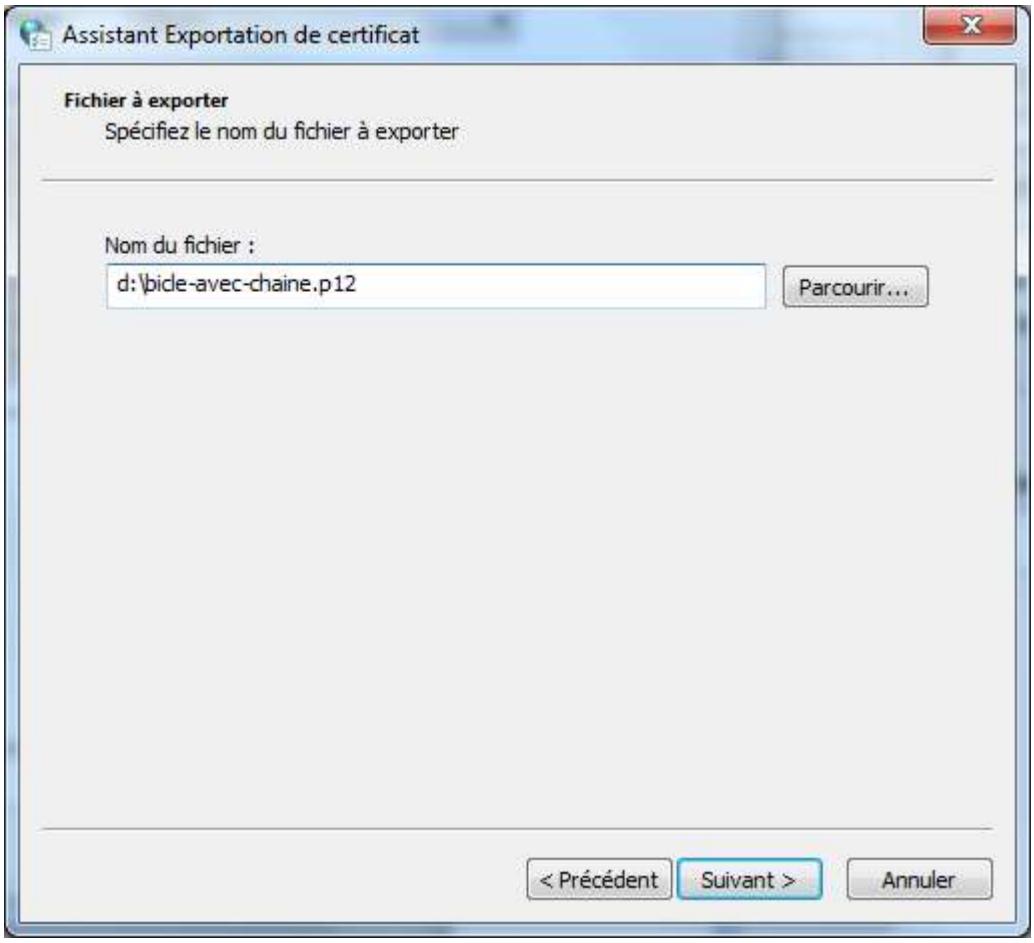

Assistant Exportation de certificat
Fichier à exporter
Spécifiez le nom du fichier à exporter
Nom du fichier :
d:\bide-avec-chaine.p12
Parcourir...
< Précédent
Suivant >
Annuler

Figure 36

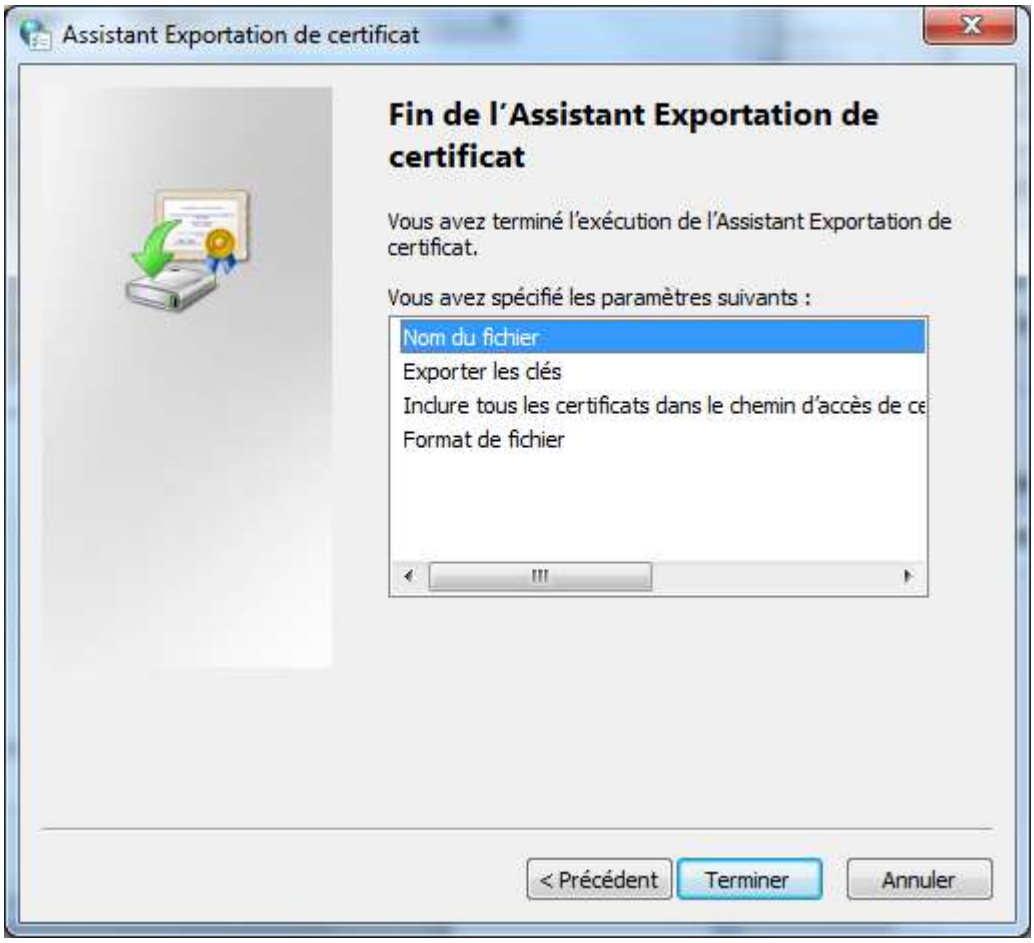


Figure 37

Figure 38

10.10 Recommencer la procédure

Pour recommander un produit de certification, il est important de suivre la recommandation suivante:

Recommencer	Pour obtenir un nouveau produit, il faut repartir depuis l'étape "générer une nouvelle clé privée" afin d'utiliser autant de bi-clés que de certificats et d'usage.

Tableau 26 : Recommencer la procédure

11Transformation du PKCS#12 en .keystore Java

keytool est un outil Java fourni avec le JDK (pas avec le JRE) (mots de passe à changer)

%JDK_HOME%\bin\keytool.exe -importkeystore -deststorepass monmotdepasse -destkeypass monmotdepasse -destkeystore d:\IGCSanté-AUTH_CLI-keypair-02.keystore -srckeystore d:\IGCSanté-AUTH_CLI-keypair-02.p12 -srcstoretype PKCS12 -srcstorepass monmotdepasse -alias 899700021142_1

Tableau 27

Transformation du PKCS#12 en .keystore	
%JDK_HOME%\bin\keytool.exe	https://docs.oracle.com/javase/8/docs/technotes/tools/windows/keytool.html
-importkeystore	
-deststorepass monmotdepasse	
-destkeypass monmotdepasse	
-destkeystore d:\IGCSanté-AUTH_CLI-keypair-02.keystore	
-srckeystore d:\IGCSanté-AUTH_CLI-keypair-02.p12	
-srcstoretype PKCS12	
-srcstorepass monmotdepasse	
-alias 899700021142_1	Nom interne XCA du certificat, ici: 899700021142_1

Tableau 28

Fichiers keystores

Les fichiers Keystore contiennent des données sensibles. Leur transmission et leur sauvegarde doivent se faire en conséquence.

Il en est de même pour le mot de passe protégeant le keystore.

Tableau 29

12Transformation du PKCS#12 en un PKCS#12 contenant le bi-clé ainsi les chaines de certificats IGC-Santé (ACI + ACR)

12.1 Sous Windows avec le gestion de certificats

1. Appliquer Pré-requis: installer les ACR IGC-Santé
2. Appliquer Pré-requis: Installer les ACI IGC-Santé
3. Importer le fichier .p12 obtenu après retrait du produit dans le magasin de certificats en double-cliquant dessus et en suivant les indications du "wizard" d'import Microsoft
4. Appliquer Exporter le bi-clé sous forme de fichier PKCS#12

Export sans ACR	Désinstaller l'ACR Appliquer les 4 étapes

Tableau 30

12.2 Avec Mozilla Firefox

- Importer les ACR et ACI dans le magasin de certificats Firefox ("outils > options > avancé > afficher les certificats > Importer")
- Importer le fichier .p12 obtenu après retrait du produit dans le magasin de certificats Firefox ("outils > options > avancé > afficher les certificats > Importer")

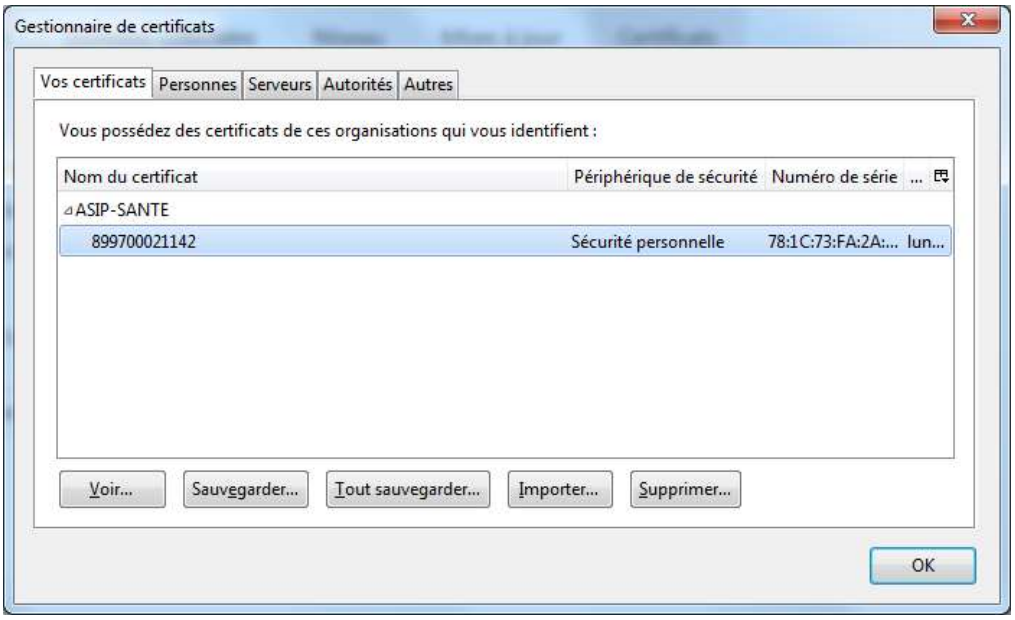


Figure 39

- Exporter le bi-clé et sa chaine:
  - outils > options > avancé > afficher les certificats > Personnel
  - Sélectionner le certificat (pas de double-clic sur le certificat)
  - Sauvegarder…

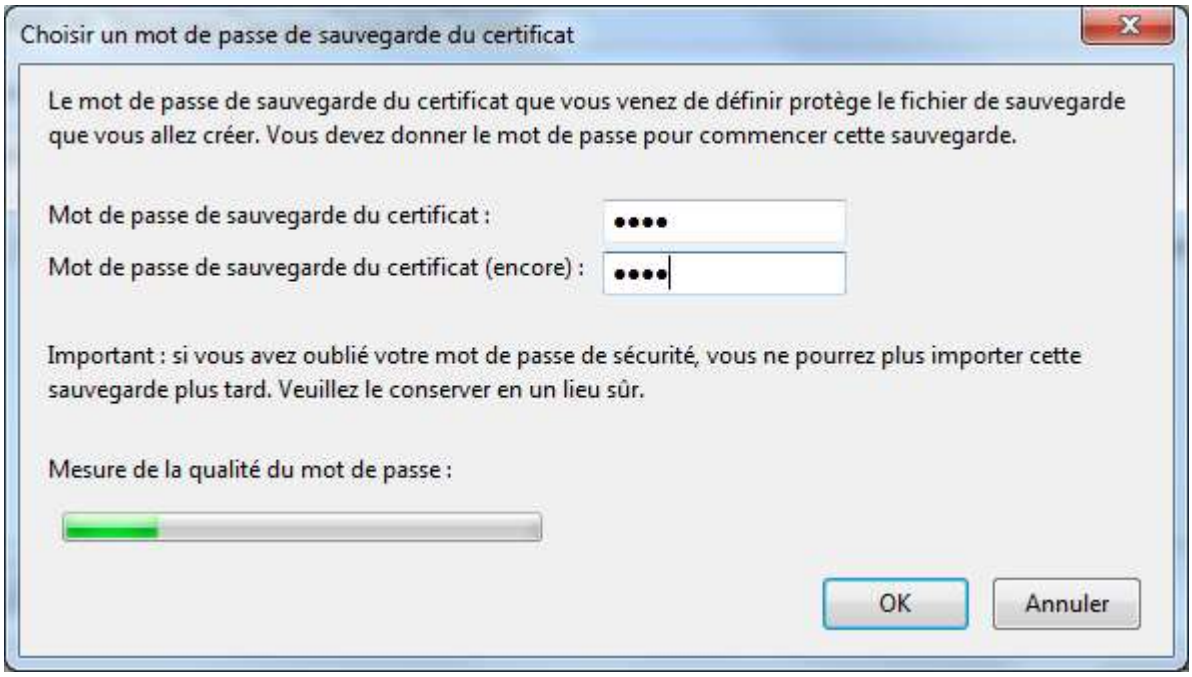


Figure 40

13Procédure "Java Porteclé"

Cette procédure est adapté aux éditeurs / intégrateurs travaillant avec des keystores Java.

13.1 Installer un JDK Java

13.2 Télécharger et installer le logiciel "Porteclé"

Porteclé est disponible via sourceforge:

https://sourceforge.net/projects/portecle/

Dezipper le fichier .zip dans un répertoire C:\Java\portecle\portecle-1.9

Démarrer Porteclé:

touche Windows > rechercher les programmes et fichiers > cmd > entrée

```
set JAVA_HOME=d:\JavaSoft\18045
set PATH=.;%JAVA_HOME%\bin;%PATH%
D:\
cd C:\Java\portecle\portecle-1.9
java -jar portecle.jar
```

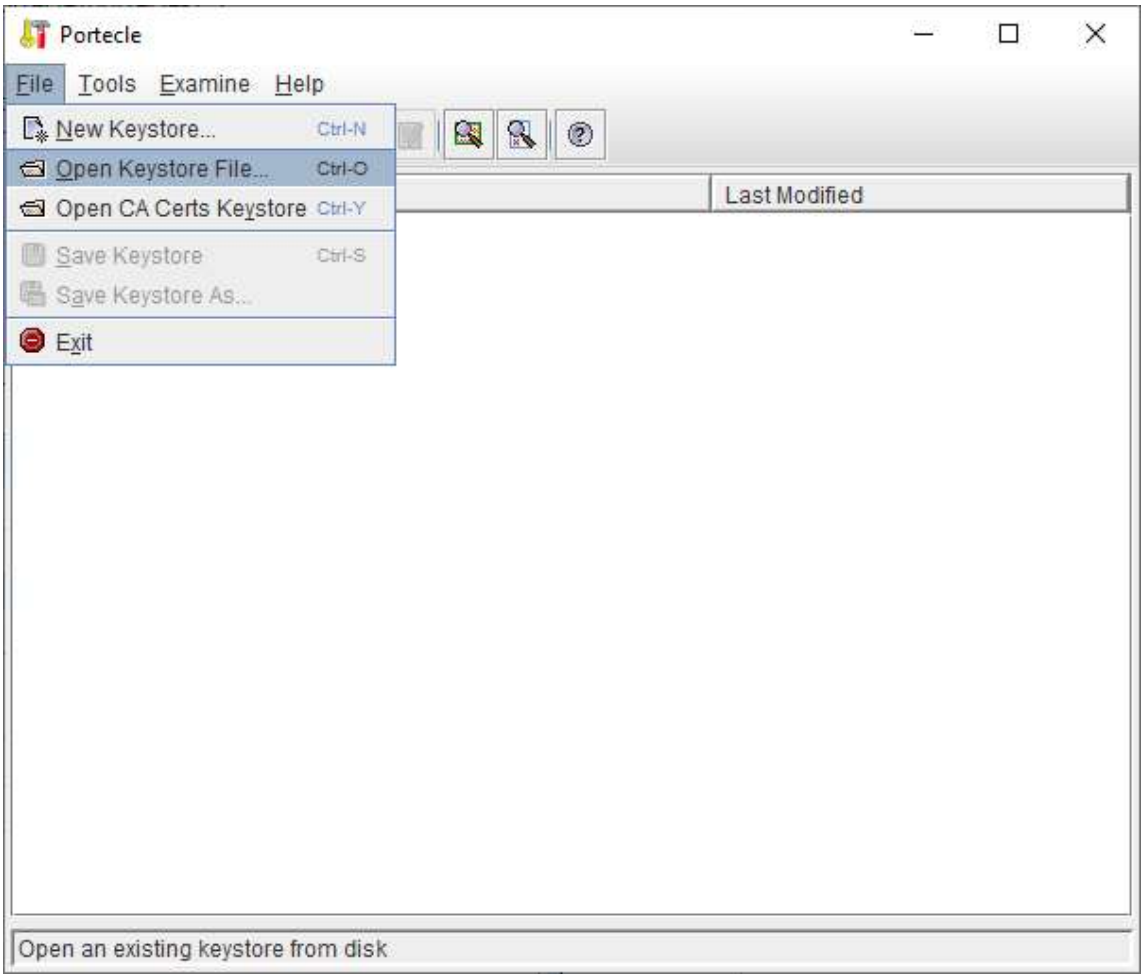


Figure 41

Ouvrir ANS_IGC-Sante_java-database_v1.0.0.jks :

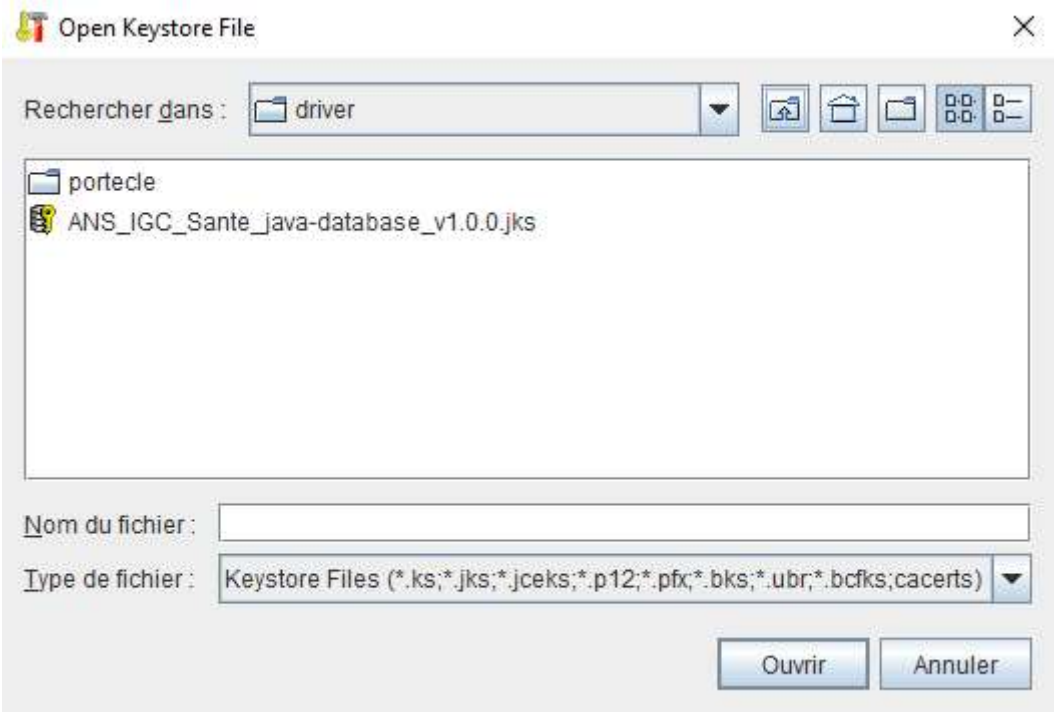


Figure 42

Entrer le mot de passe « changeit » :

Figure 43

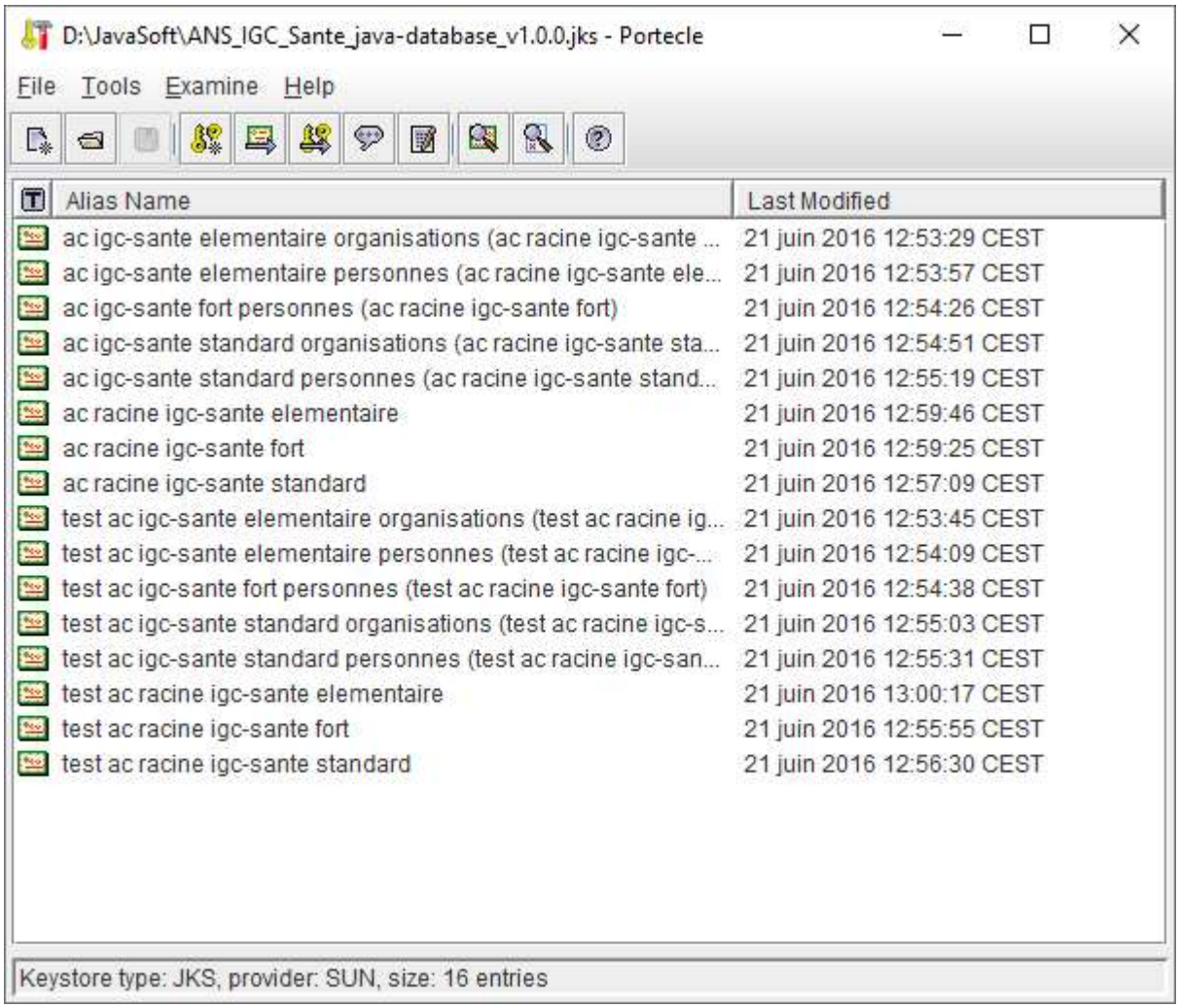

D:\JavaSoft\ANS_IGC_Sante_java-database_v1.0.0.jks - Portecle
File Tools Examine Help
Alias Name
Last Modified
ac igc-sante elementaire organisations (ac racine igc-sante ... 21 juin 2016 12:53:29 CEST
ac igc-sante elementaire personnes (ac racine igc-sante ele... 21 juin 2016 12:53:57 CEST
ac igc-sante fort personnes (ac racine igc-sante fort) 21 juin 2016 12:54:26 CEST
ac igc-sante standard organisations (ac racine igc-sante sta... 21 juin 2016 12:54:51 CEST
ac igc-sante standard personnes (ac racine igc-sante stand... 21 juin 2016 12:55:19 CEST
ac racine igc-sante elementaire 21 juin 2016 12:59:46 CEST
ac racine igc-sante fort 21 juin 2016 12:59:25 CEST
ac racine igc-sante standard 21 juin 2016 12:57:09 CEST
test ac igc-sante elementaire organisations (test ac racine ig... 21 juin 2016 12:53:45 CEST
test ac igc-sante elementaire personnes (test ac racine igc-... 21 juin 2016 12:54:09 CEST
test ac igc-sante fort personnes (test ac racine igc-sante fort) 21 juin 2016 12:54:38 CEST
test ac igc-sante standard organisations (test ac racine igc-s... 21 juin 2016 12:55:03 CEST
test ac igc-sante standard personnes (test ac racine igc-san... 21 juin 2016 12:55:31 CEST
test ac racine igc-sante elementaire 21 juin 2016 13:00:17 CEST
test ac racine igc-sante fort 21 juin 2016 12:55:55 CEST
test ac racine igc-sante standard 21 juin 2016 12:56:30 CEST
Keystore type: JKS, provider: SUN, size: 16 entries

Figure 44

13.3 Générer un bi-clé RSA 2048bits

Figure 45

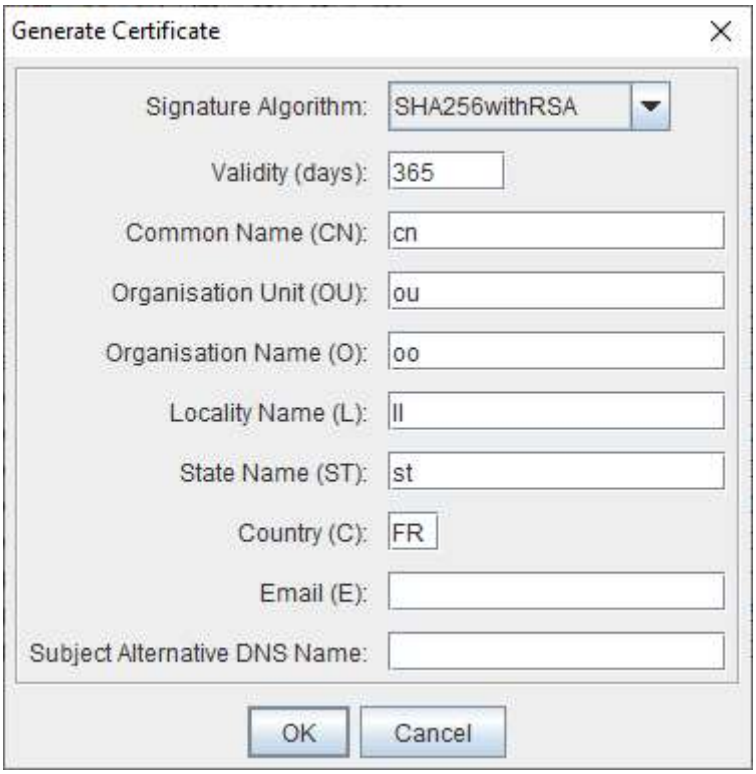


Figure 46

Figure 47

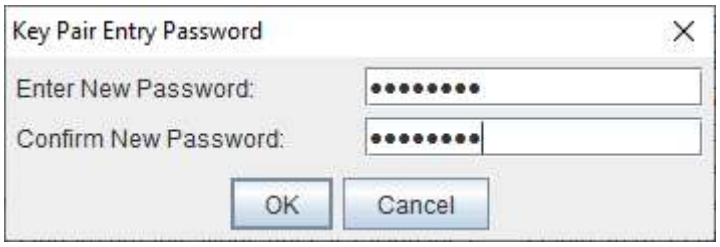


Figure 48

Figure 49

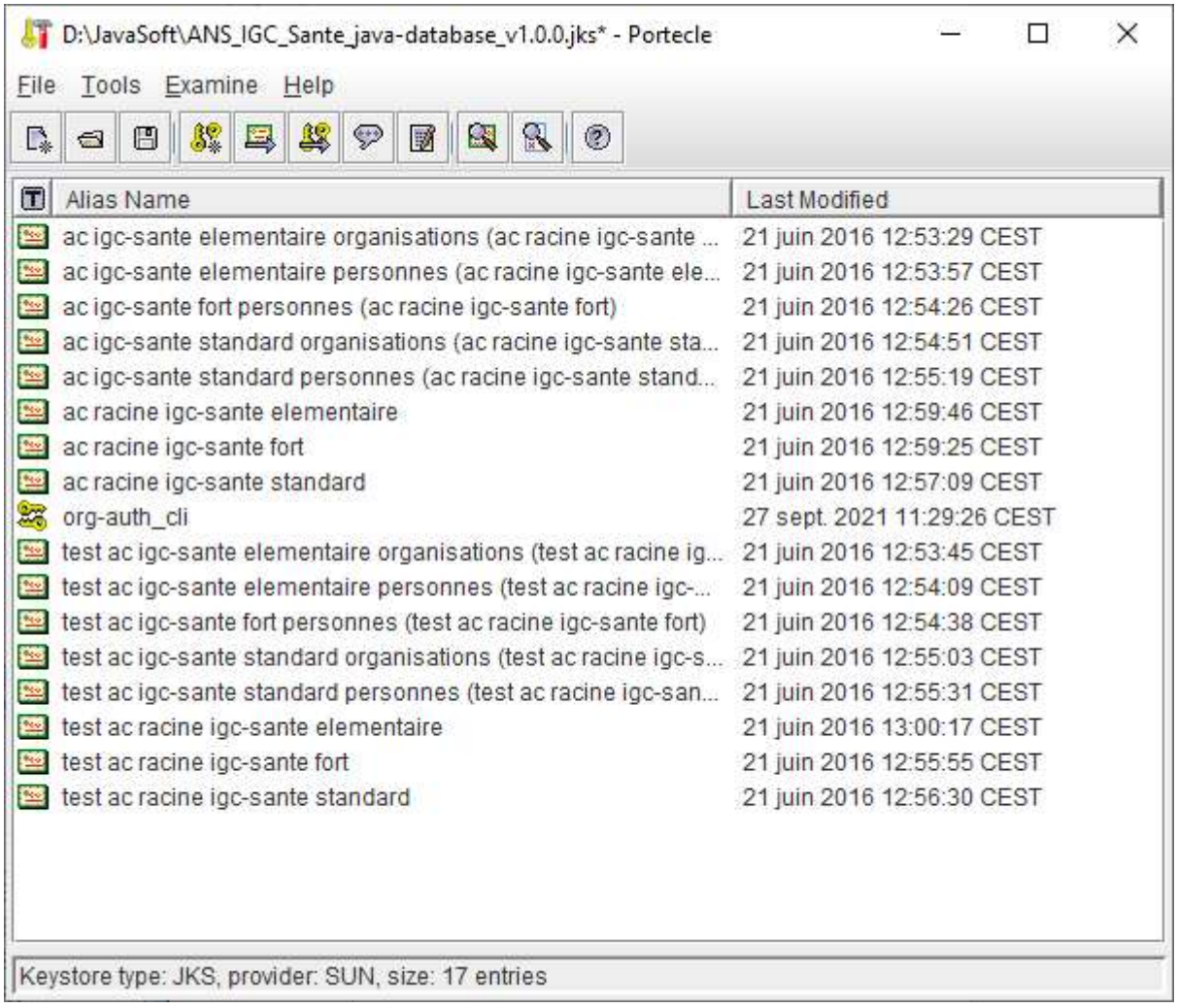


Figure 50

13.4 Générer une requête de signature de certificat

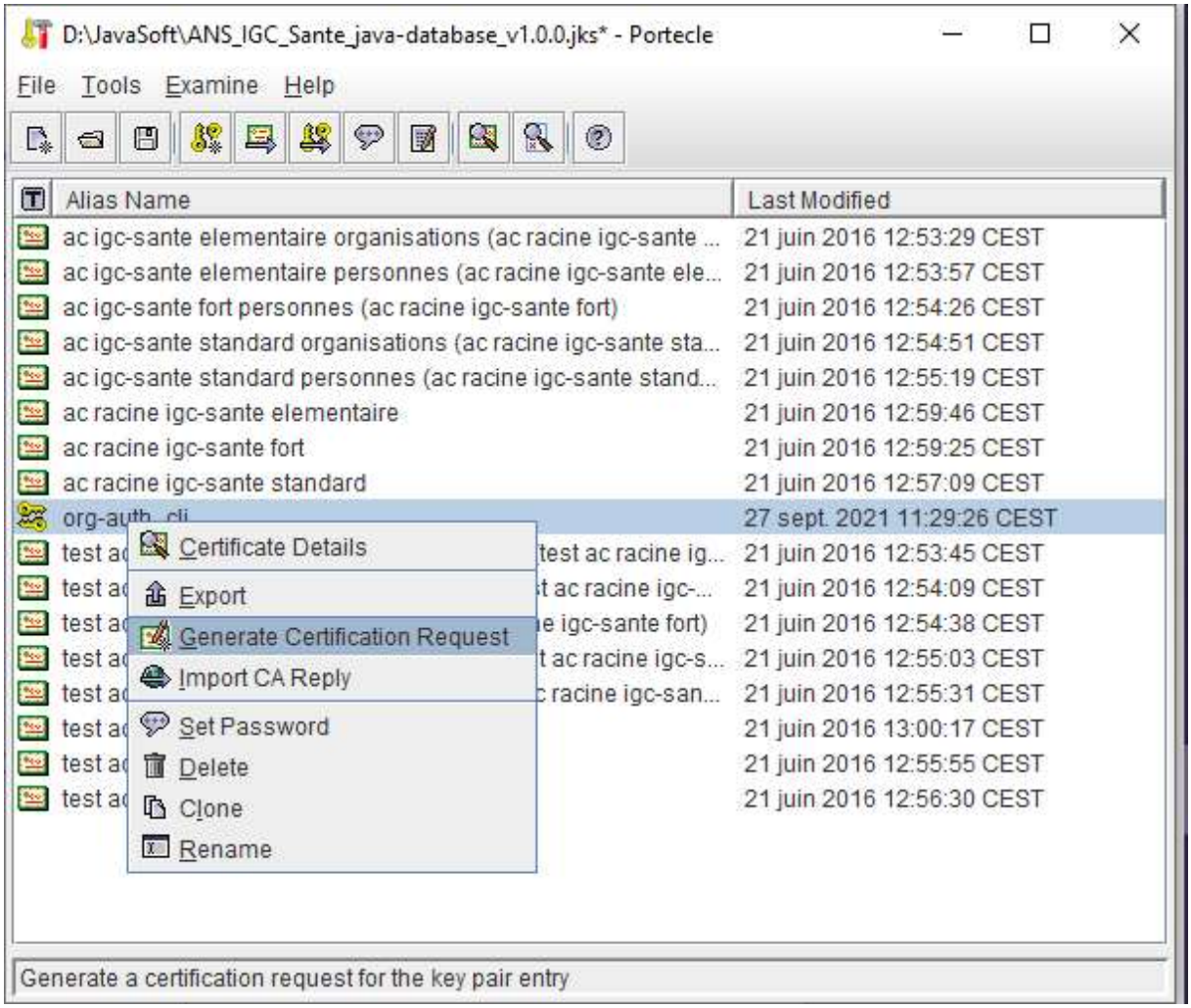


Figure 51

Figure 52

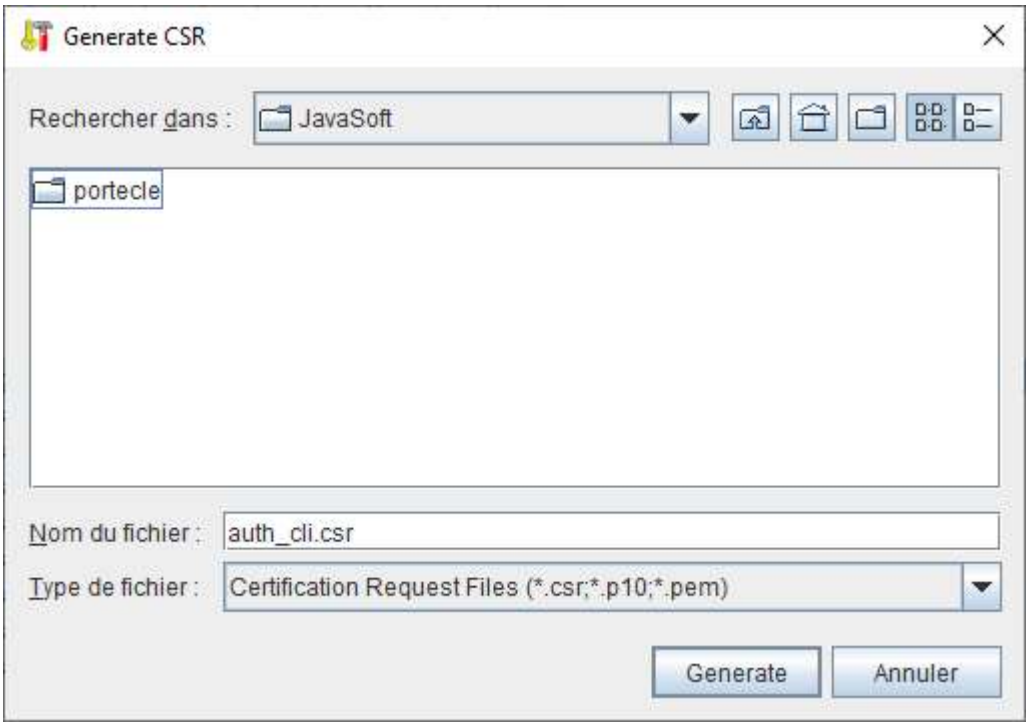


Figure 53

Figure 54

13.5 Importer la CSR sur le portail PFC

Cf. plus haut

13.6 Attendre le mail de retrait

Cf. plus haut

13.7 Retirer le certificat sur le portail PFC

Cf. plus haut

13.8 Réconcilier la clé privée et le certificat dans PorteClé

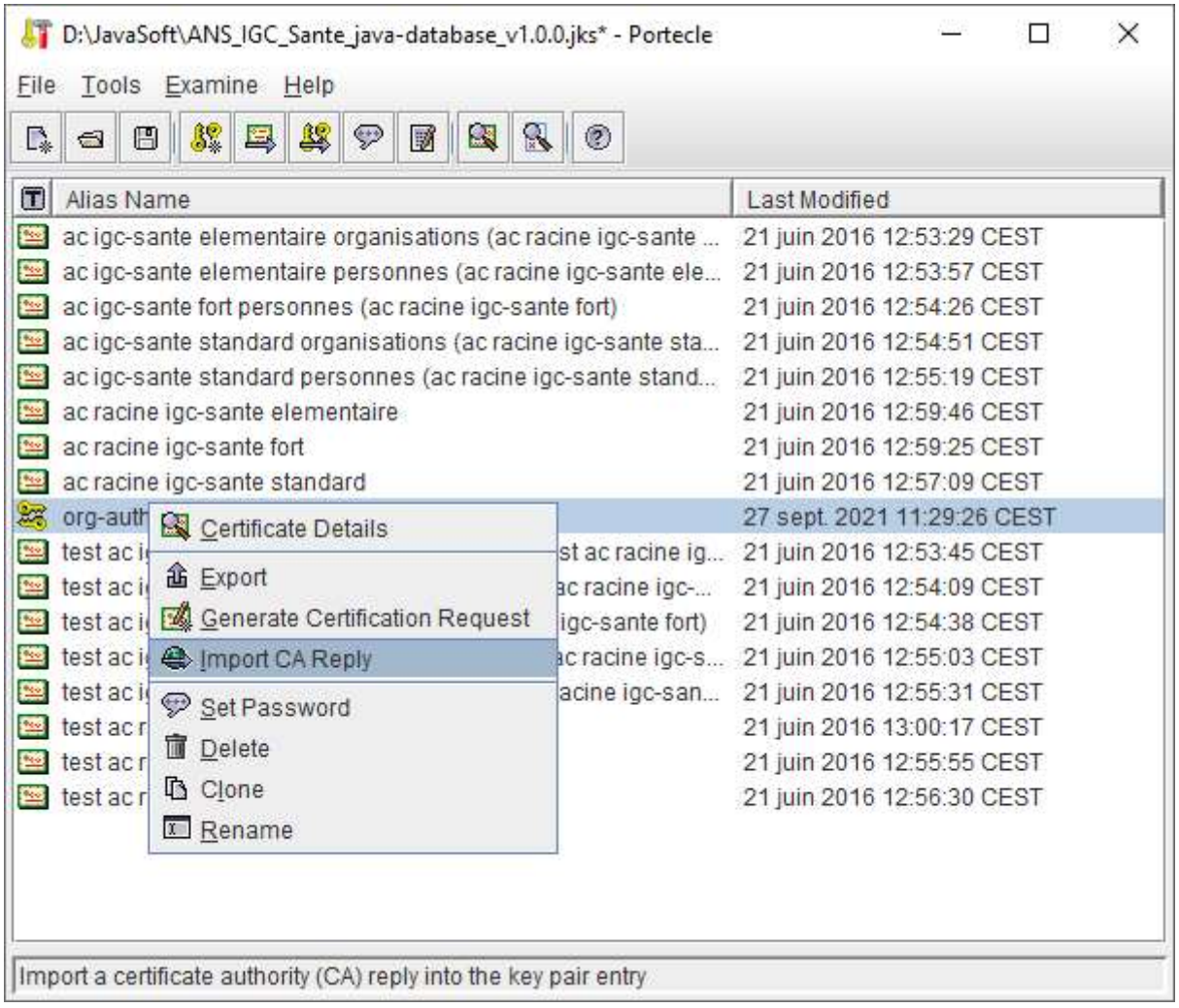


Figure 55

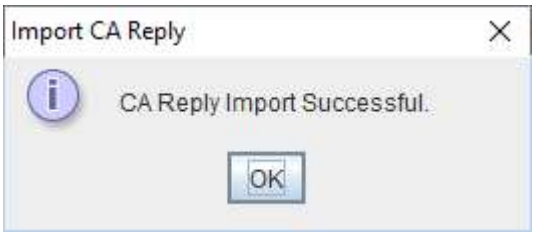


Figure 56

Vérifier la chaine du certificat :

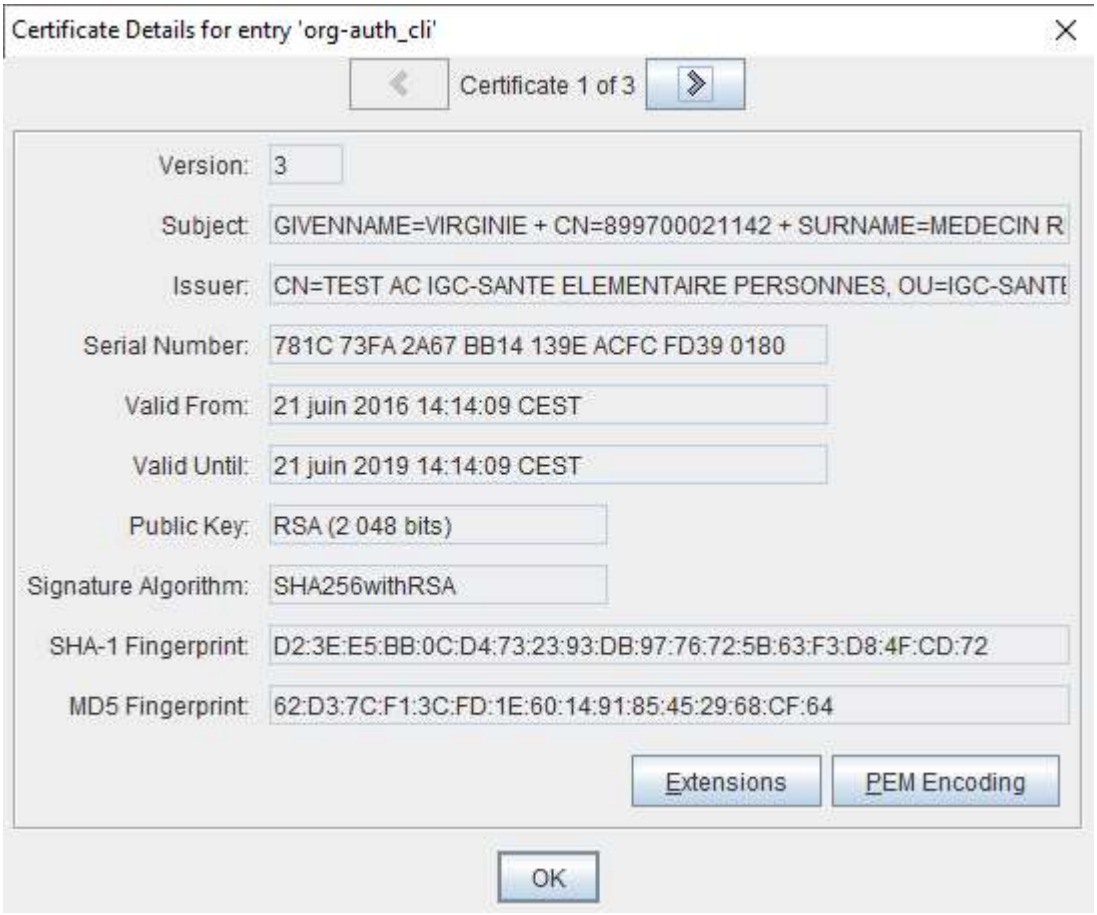


Figure 57

13.9 Exporter au format PKCS#12 (optionnel)

Installer les « unlimited strength jurisdiction policy files for java 8 » dans %JAVA_HOME%\jre\lib\security

Lancer Porteclé

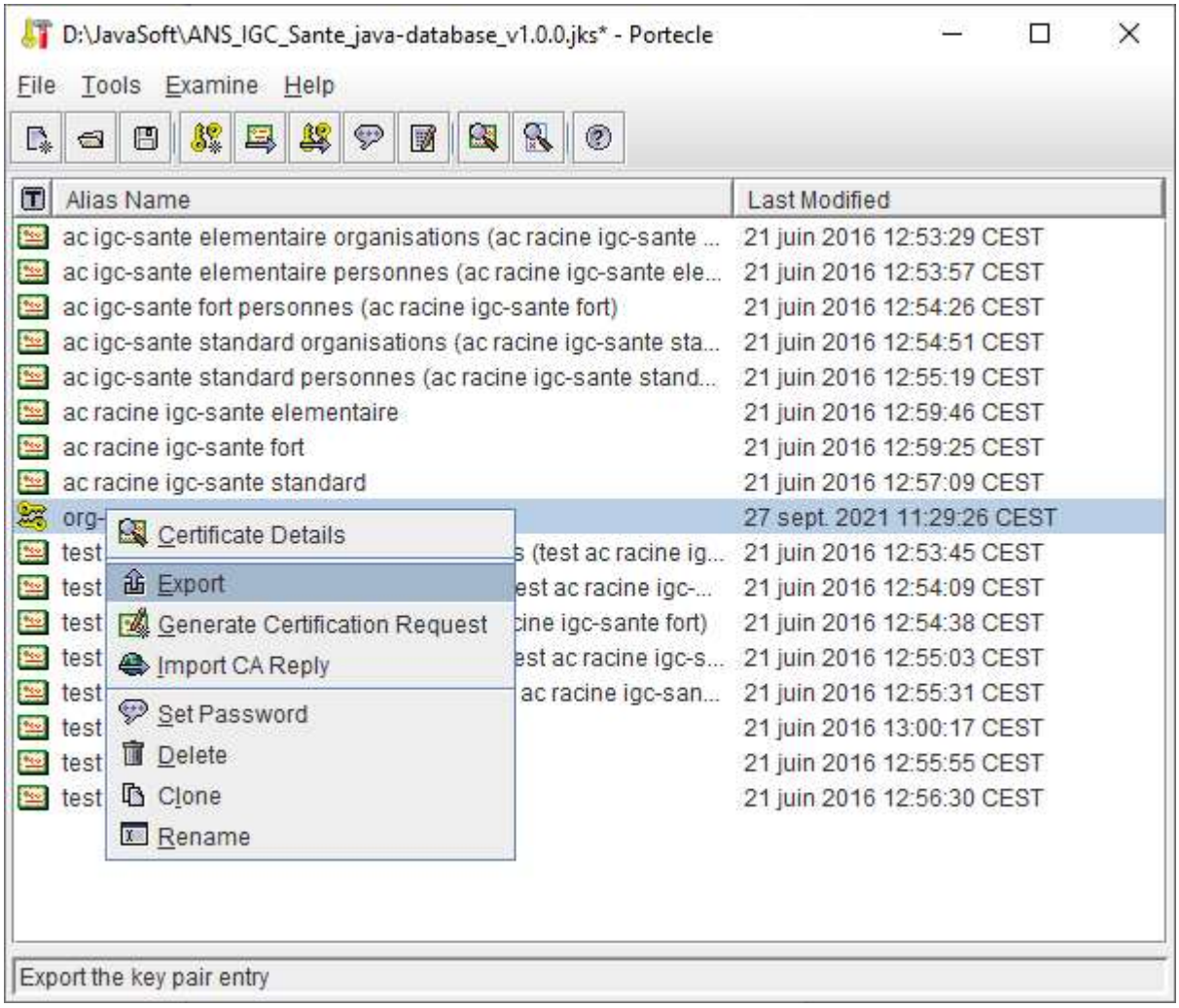


Figure 58

Figure 59

Figure 60

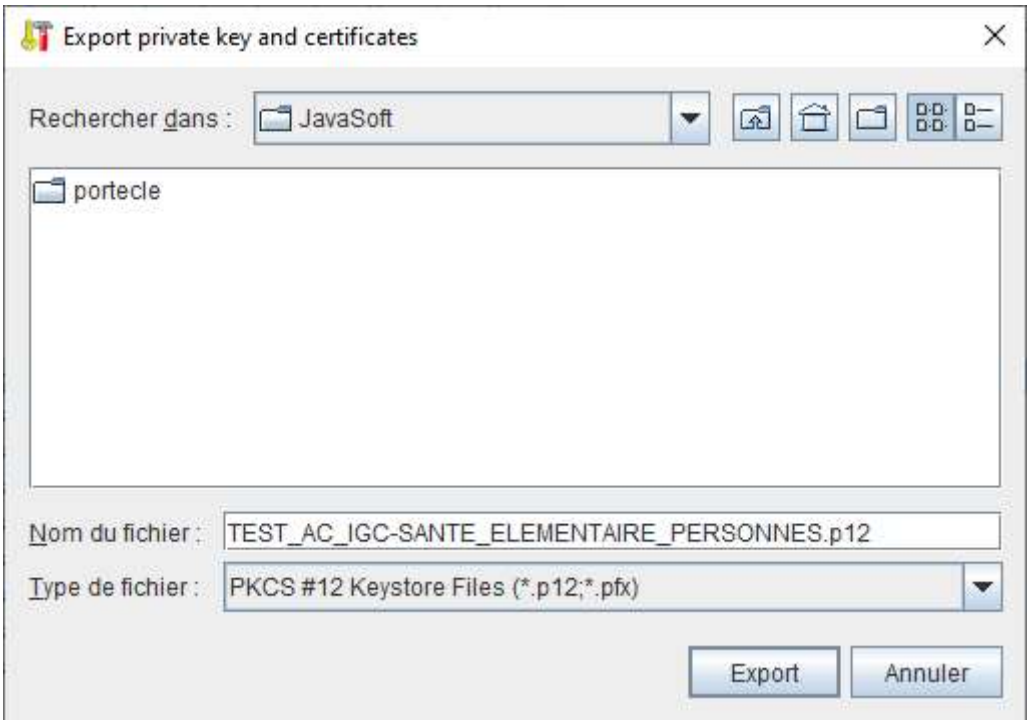


Figure 61

Figure 62

Le PKCS#12 produit est compatible Windows et Firefox.

13.10 Recommencer la procédure

Pour recommander un produit de certification, il est important de suivre la recommandation suivante:

Recommencer	Pour obtenir un nouveau produit, il faut repartir depuis l'étape "générer une nouvelle clé privée" afin d'utiliser autant de bi-clés que de certificats et d'usage.

Tableau 31 : Recommencer la procédure

14Annexe – Liste des figures

15Annexe – Liste des tableaux

16Notes

[fin du document]

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
Tél : 01 58 45 32 50
esante.gouv.fr