OFSEP
Observatoire Français
de la Sclérose en Plaques

Mode opératoire d'installation et d'utilisation de GnuPG pour le chiffrage des donées transmises à l'OFSEP

Romain Casey, septembre 2012, v2b

Table des matières

Préambule

Dans le cadre de l'OFSEP, de nombreuses informations à caractère médical sont amenées à circuler. Il s'agit principalement des fichiers d'export que les centres experts envoient au Centre de coordination national de l'OFSEP (CCN) mais aussi des échanges entre centres experts de dossiers médicaux au format EDMUS (déménagement d'un malade d'une région vers une autre, etc.).

Pour assurer la sécurité de ces informations le CCN souhaite à l'avenir que les échanges de fichiers se fassent en chiffrant les données.

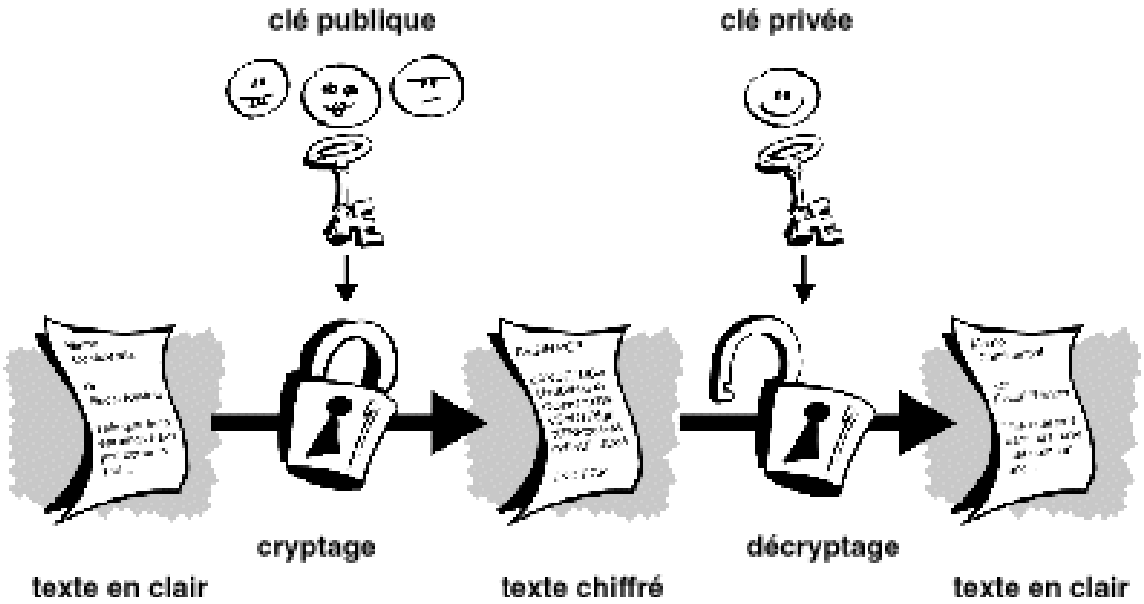
L'outil proposé est GnuPG, un logiciel libre de chiffrage de données utilisant un système de clé publique et clé privée. Ce document vous indiquera :

- le principe de fonctionnement de ce système ;
- comment installer GPG4Win sur votre ordinateur, un logiciel intégrant GPG et une interface graphique fonctionnant sous système Microsoft Windows[1] ;
- comment utiliser GPG4Win : génération des clés publique et privée, partage des clés publiques, chiffrage et déchiffrage des fichiers

Objectif et principe de fonctionnement

L'objectif d'un tel système est de chiffrer un fichier afin que ce dernier ne soit lisible que par le destinataire possédant la clé de déchiffrement.

Ce système repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (que l'utilisateur garde secrète), l'une permettant de coder le message et l'autre de le décoder. Ainsi, l'expéditeur peut utiliser la clé publique du destinataire pour coder un message que seul le destinataire (en possession de la clé privée) peut décoder, garantissant la confidentialité du contenu.



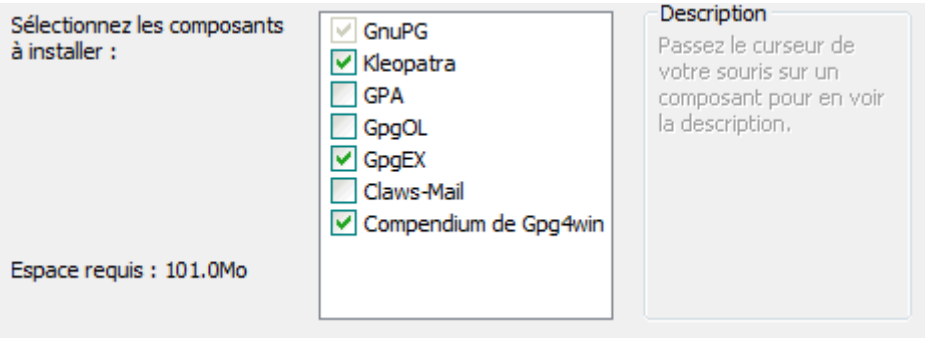
[1] Pour les utilisateurs utilisant un système Mac OS, l'utilisation de GnuPG est possible en utilisant par exemple GPGTools (http://www.gpgtools.org/). Le principe de fonctionnement reste le même. En cas de problème, vous pouvez contacter Bernard Frangoulis (bf@edmus.org).

La clé publique est connue de tout le monde : elle sera distribuée par le CCN à tous les centres experts susceptibles de fournir des données au CCN. Évidemment, si le CCN doit fournir des données sensibles aux centres experts ou si les centres désirent s'échanger des données, les clés publiques devront être partagées.

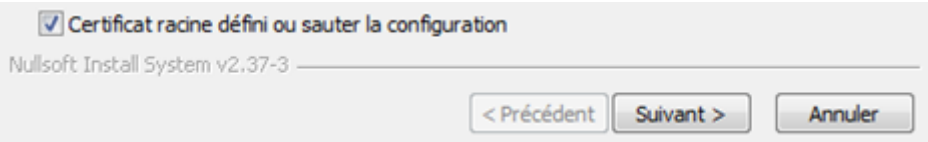
Installation de GPG4Win

Le logiciel peut se télécharger à l'adresse suivante – http://www.gpg4win.org/download.html, ou directement en suivant ce lien : http://files.gpg4win.org/gpg4win-2.1.0.exe.

L'installation nécessite d'avoir les droits administrateurs sur l'ordinateur. Après avoir lancé le fichier d'installation et validé les premières fenêtres, le logiciel nous propose de choisir les composants à installer ; on accepte les choix proposés par défaut, à l'exception de GpgOL, qui est un module qui s'intègre à Outlook et qui peut complexifier son utilisation[2].



Le logiciel demande plus loin de définir les certificats racines dignes de confiance, cochez la case se trouvant en bas de la fenêtre et passez à l'étape suivante.



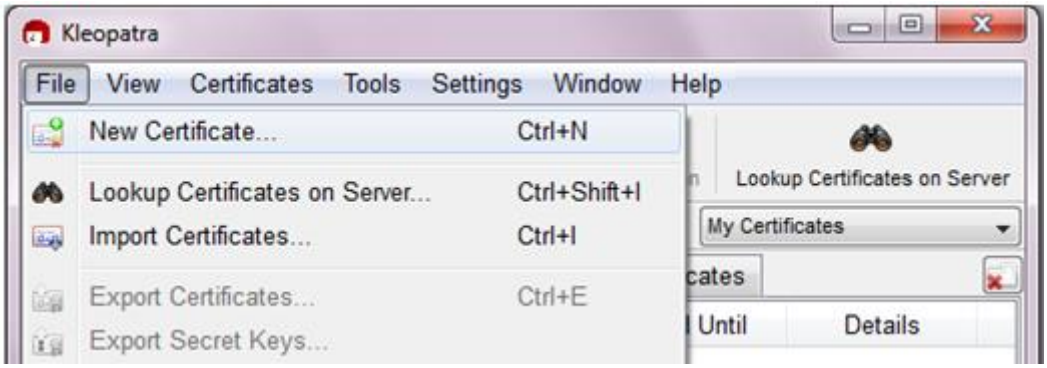
Une fois l'installation terminée, vous pouvez lancer le logiciel Kleopatra (l'interface graphique de GPG).

[2] Pour les utilisateurs qui ont installé ce module, ils peuvent s'ils le souhaitent le désactiver en suivant la procédure décrite dans la documentation de GPG4Win (gpg4win-compendium-en.pdf, accessible le menu GPG4Win/Documentation du « menu Démarrer »), notamment à la page 127.

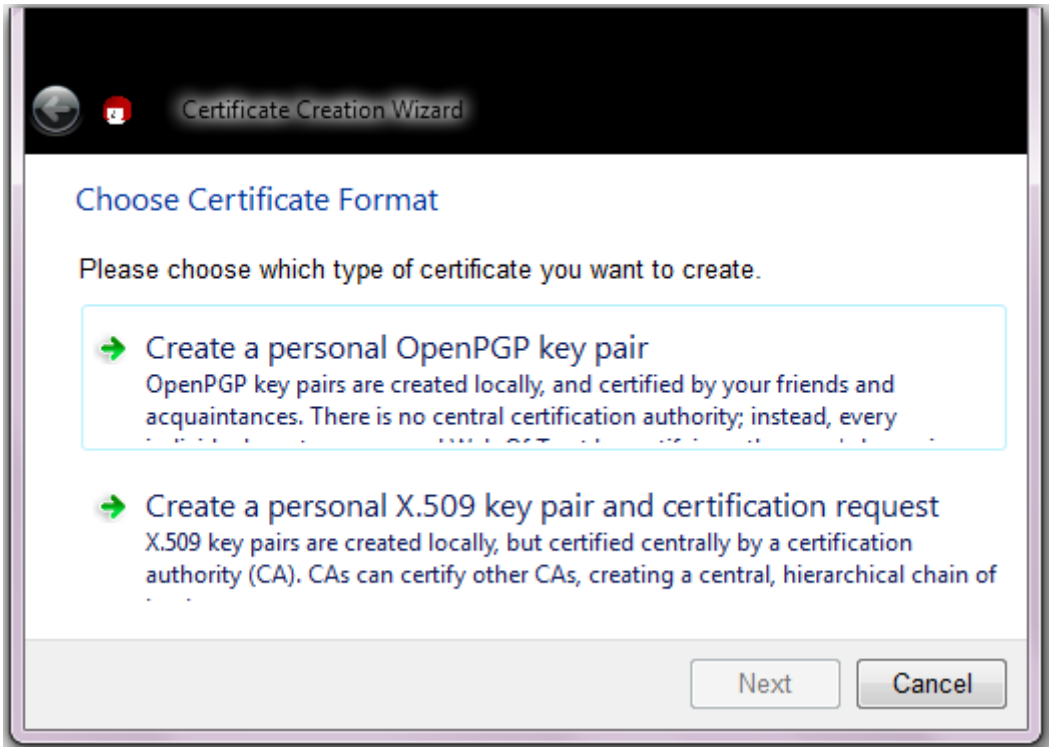
Gestion des clés publique et privé

Génération des clés publique et privé

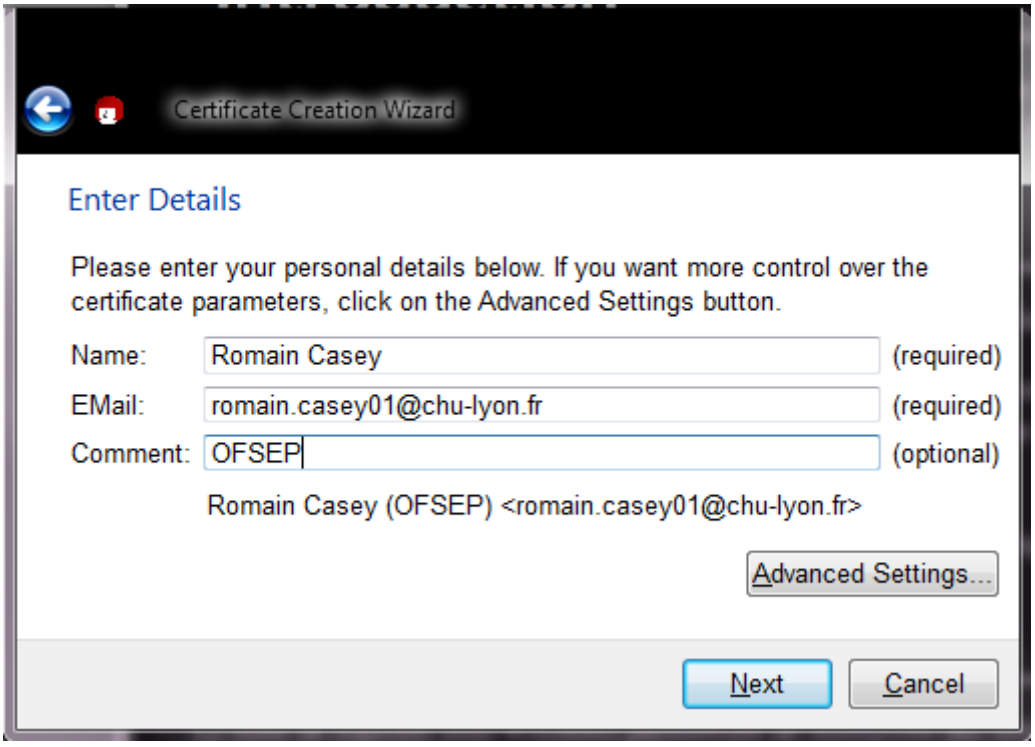
Lors du premier lancement de Kleopatra, aucune clé n'est présente dans la liste des certificats. Pour créer votre propre clé, allez dans le menu « File » et sélectionner « New certificate… ».



Sélectionner l'option « Create a personal OpenPGP key pair ».



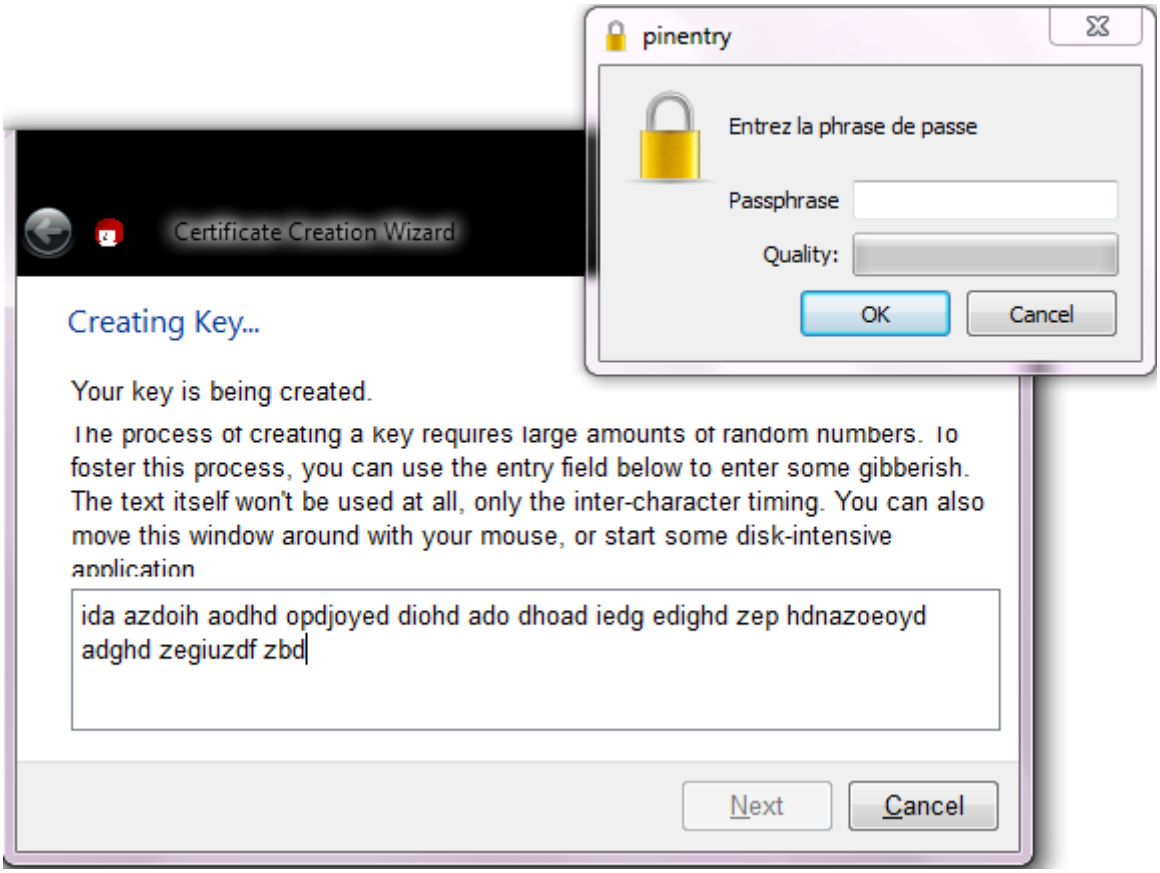
Entrez votre nom, votre adresse email et dans le champ « Comment », le centre auquel vous êtes rattaché. Cliquez sur « Next ».



Dans la fenêtre « Creating key », saisissez du texte au hasard ; le seul but de ceci est de générer des nombres aléatoires pour renforcer la sécurité de la clé.

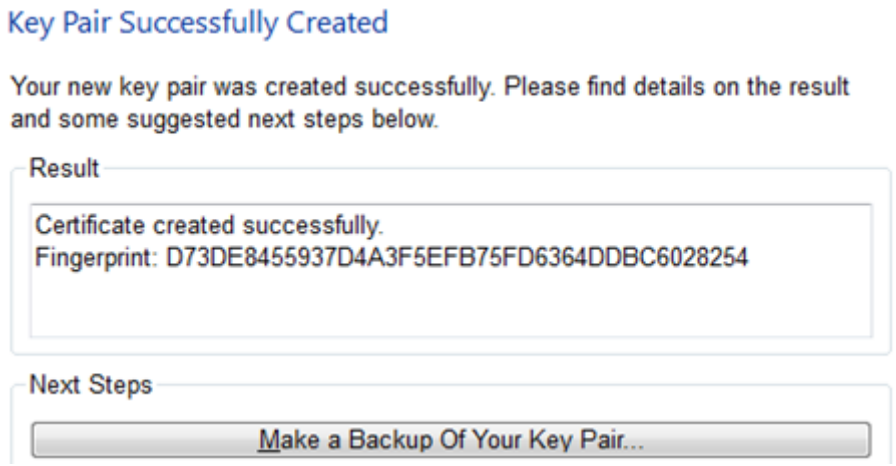
Dans la fenêtre « pinentry », saisissez votre phrase de passe (« passphrase »). Il s'agit d'un long mot de passe permettant de protéger la clé privée (au cas où…) et de signer des messages ou fichiers.

- Lors d'un déchiffrement (utilisation de votre clé privée) GPG vous demandera votre passphrase.
- Lors du chiffrement d'un fichier, vous avez également la possibilité de le « signer » : le logiciel vous demandera avec quelle clé publique chiffrer le message (celle du destinataire) ainsi que votre phrase de passe (pour la signature).



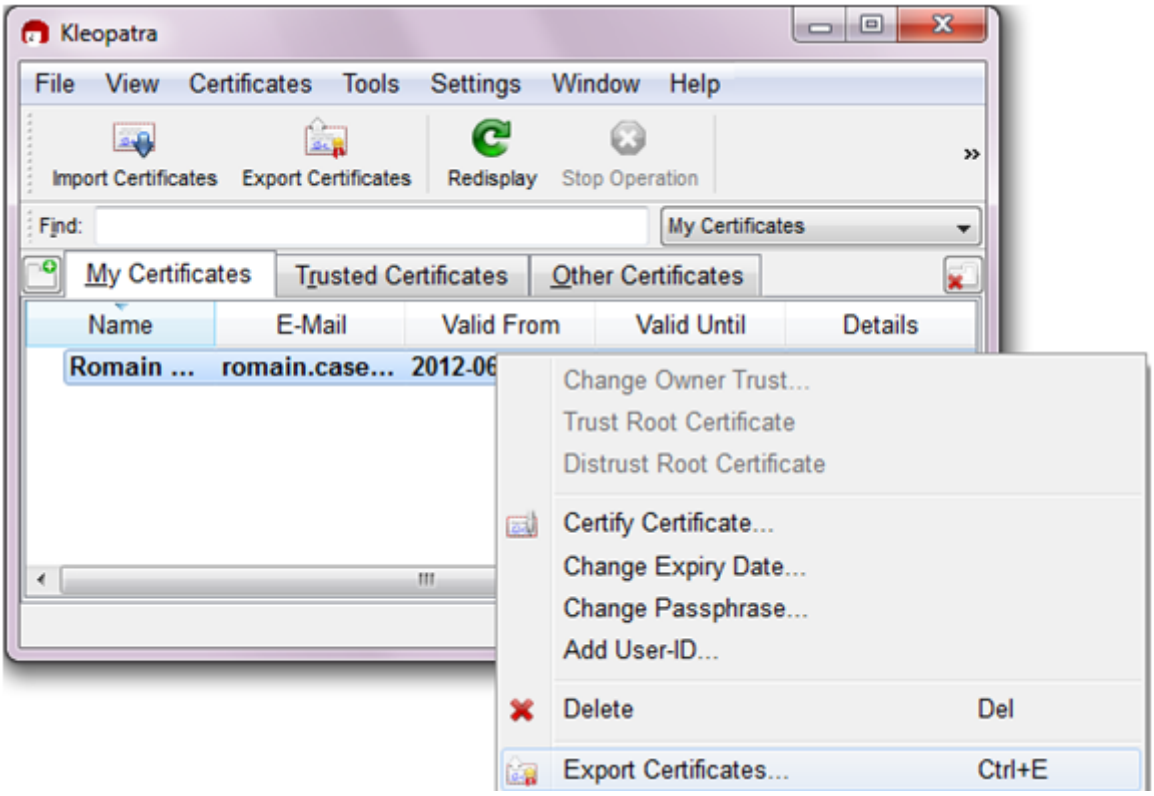
Une fois cette étape terminée, vous devez obtenir un écran indiquant que la génération de votre clé s'est terminée correctement.

Pour plus de sécurité, vous pouvez faire une sauvegarde de votre paire de clés via le bouton « Make a Backup Of Your Key Pair… ». Attention à effectuer cette sauvegarde sur un emplacement de l'ordinateur aussi confidentiel que possible pour garantir la sécurité de votre paire de clés et donc des échanges que vous allez faire à l'aide de ces clés.



Exporter sa clé publique et la transmettre

Pour permettre à vos correspondants de chiffrer des fichiers à votre intention, ils ont besoin de connaitre votre clé publique. Dans Kleopatra, faites un clic-droit sur votre certificat et faites « Export certificates… ». Kleopatra vous demandera alors d'enregistrer un fichier contenant votre clé publique ; vous pouvez nommer ce fichier « pubkey_votre_nom.asc ».



Ce fichier contient du texte et se présente sous la forme suivante :

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.17 (MingW32)

mQENBE/Mse8BCAC9r3fBWYNf9QknU/+RJuDs36W4qSoV5YDaYbRx7kHNGx0F90+j
rppu4Uz+w1pvW0EDSCcPJN9lvZNzSve60B+Z8ZuaGfCjVYsF2VBfVy1ncEpEe+QX
oOQC+Sw9cP10Z7cZS5c82InqvSzfjqYii6Wf5s7tZpToNPSgK1Vp1Yw597wCEkO7
PKbg3lfelALdZkqYAmlPh4iGr45ZL1Gpuk7pEmEQKQpuL/2Te4aKBVZs/dCef6vd
3zU4aCjS5WWwDswLnLAm0xrkZxLzc+80ahQHPvl/DjZipVfl6HDYsODme/QTYGac
jMJQML7KUacgodMvOlchOZfjRf8tDGP+OAWrABEBAAG0NVJvbWFpbiBDYXNleSAo
Q0NOIE9GU0VQKSA8cm9tYWluLmNhc2V5MDFAY2h1LWx5b24uZnI+iQE4BBMBAgAi
BQJPzLHvAhsPBgsJCAcDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRBCsWCO4NVFIzSH
CACI5nOJR2bJhFM+mwrDTT4ndXV0AZurcuIN6heK/xI2t0uddwjahXPkkXKFbmc4
2jDPcbbvI3Ml6Dvsp0hH1a3VW2blNGyIkac0ZzYgJBDs7Q882HC/3D+P/H+2wb5S
5W24YSi0T4vPdb4lVV70fvXiThWWT5+2nEr77hBy8brdboqcS+Kdyv/p8LVG8e9J
/tTCN3LCa839nOiMTnmafI0NF6BPBgfHvAC4vTQI4MdF8J1ZAY2FVjv8uG1ySlh7
XsgVtyX8bqL43aZg8WFnPhMisJNdCFPsb6jqLnPHTfPT1opR+dgqbvQgjcIEBjKY
8k56SzI+66K2Ee+7sC5GW/9Y
```

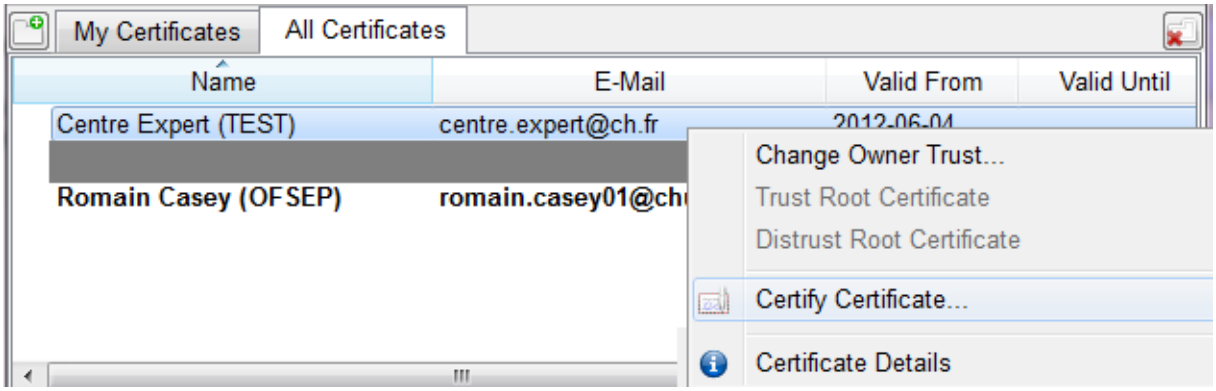
```
=4h2k
-----END PGP PUBLIC KEY BLOCK-----
```

Vous pouvez envoyer ce fichier par mail au CCN et à tous vos correspondants auxquels vous enverrez des fichiers chiffrés.

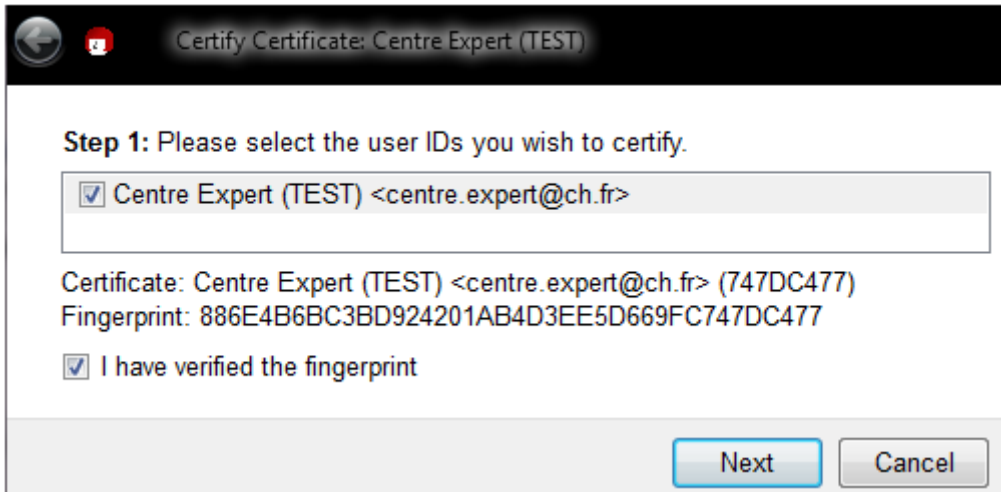
Importer une clé publique et la certifier

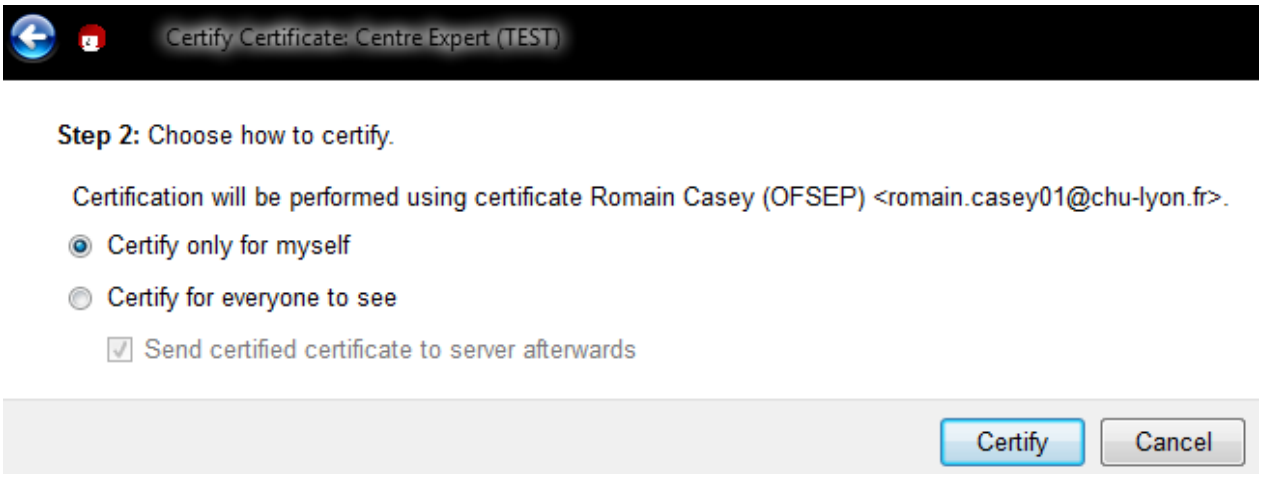
À l'inverse, pour importer la clé publique d'un de vos correspondants, vous devez cliquer sur le bouton « Import certificates » et sélectionner le fichier contenant la clé publique de votre correspondant.

Une fois cette étape réalisée, il convient (même si ce n'est pas obligatoire) de certifier la clé publique. Ceci est une étape très importante qui permet de vous assurer que la clé que vous avez obtenue provient bien de la bonne personne. Il s'agit d'une étape qui peut être faite par téléphone. Appelez la personne qui vous a fourni la clé, et vérifiez que l'empreinte (fingerprint) et le Key ID sont celles de la clé de votre correspondant (pour le trouvez, clic-droit sur la clé puis « Certificate details »). Une fois cette vérification effectuée, vous pouvez certifier la clé (clic-droit puis « Certify Certificate »).



Vous sélectionnez l'identifiant de la clé que vous voulez certifier et indiquez que cette certification n'est valable que pour vous.

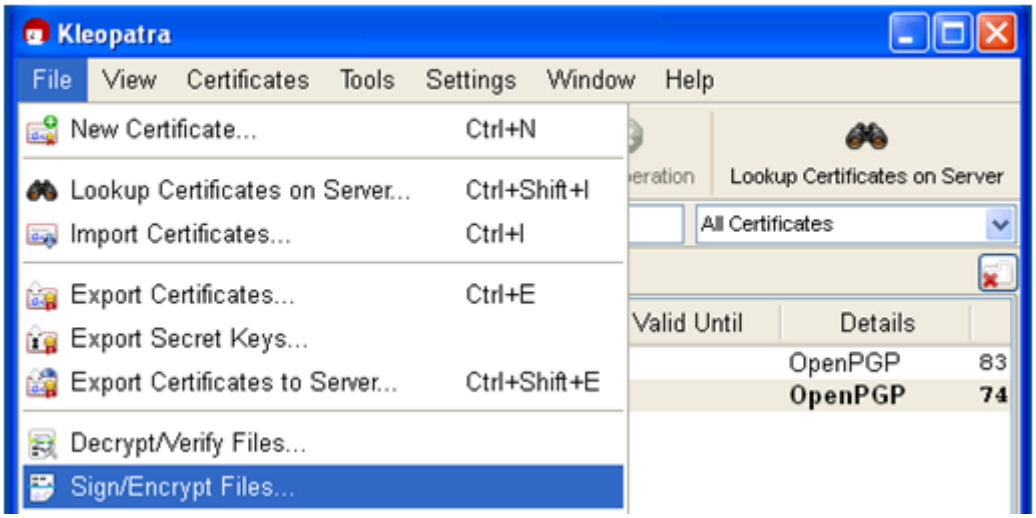




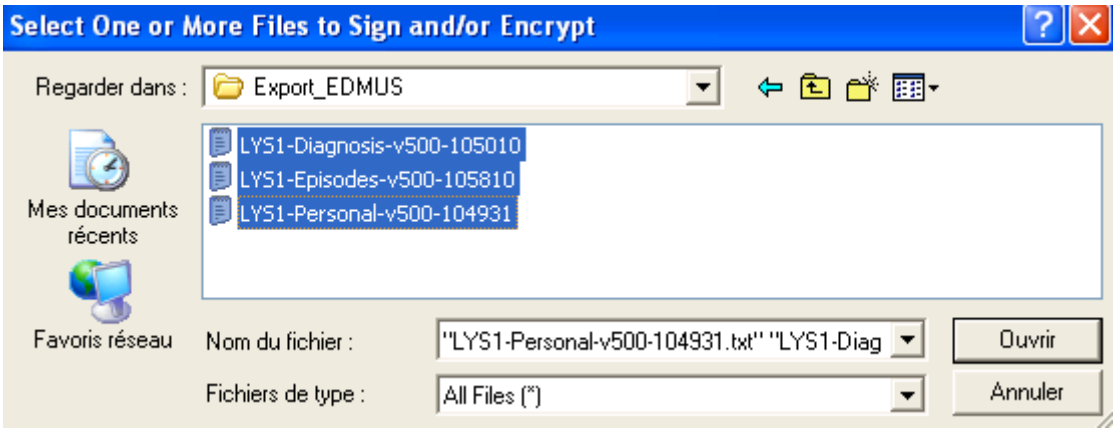
Utilisation du système de chiffrage et déchiffrage

Chiffrer et envoyer des fichiers

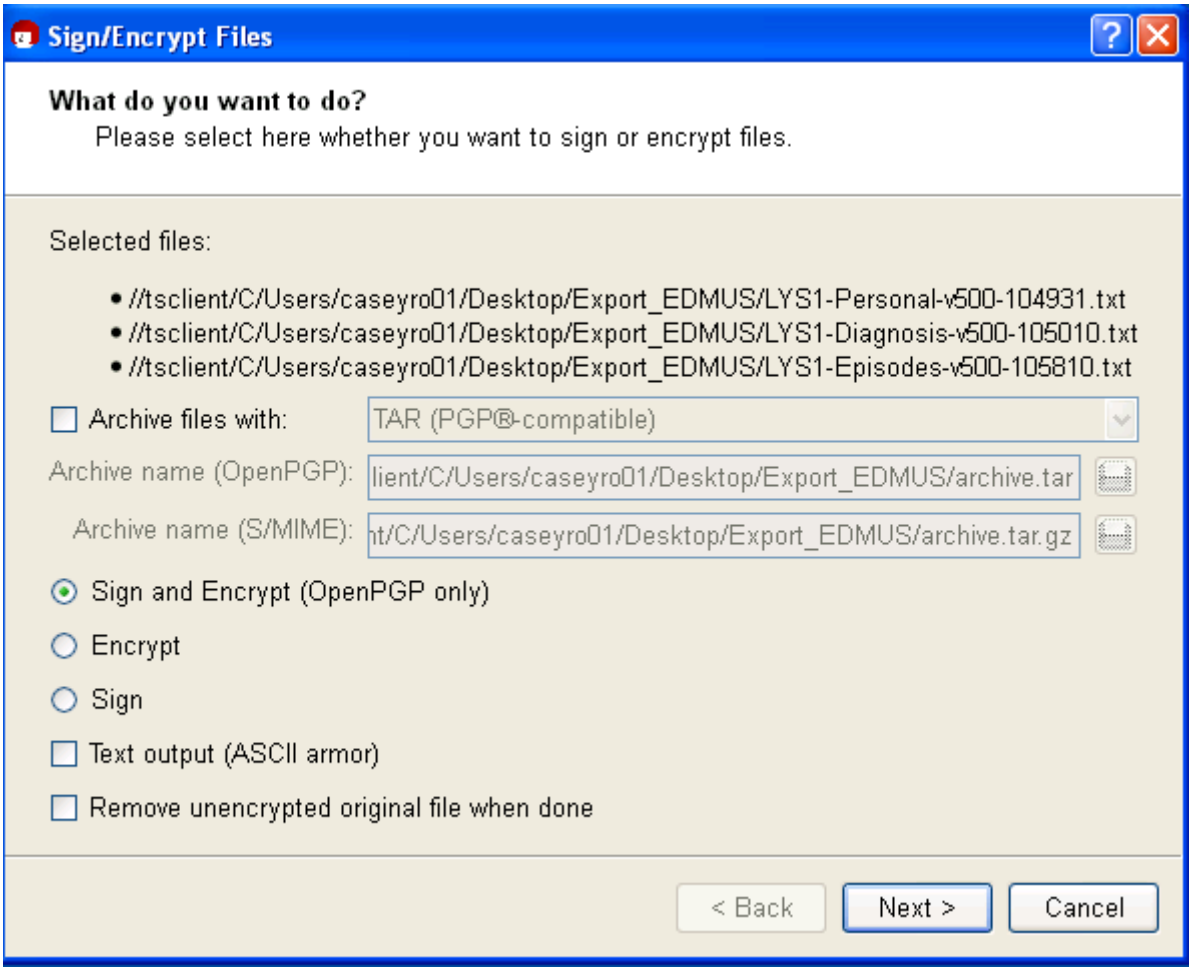
Pour chiffrer des fichiers, allez dans le menu « File » et sélectionnez « Sign/Encrypt Files… ».



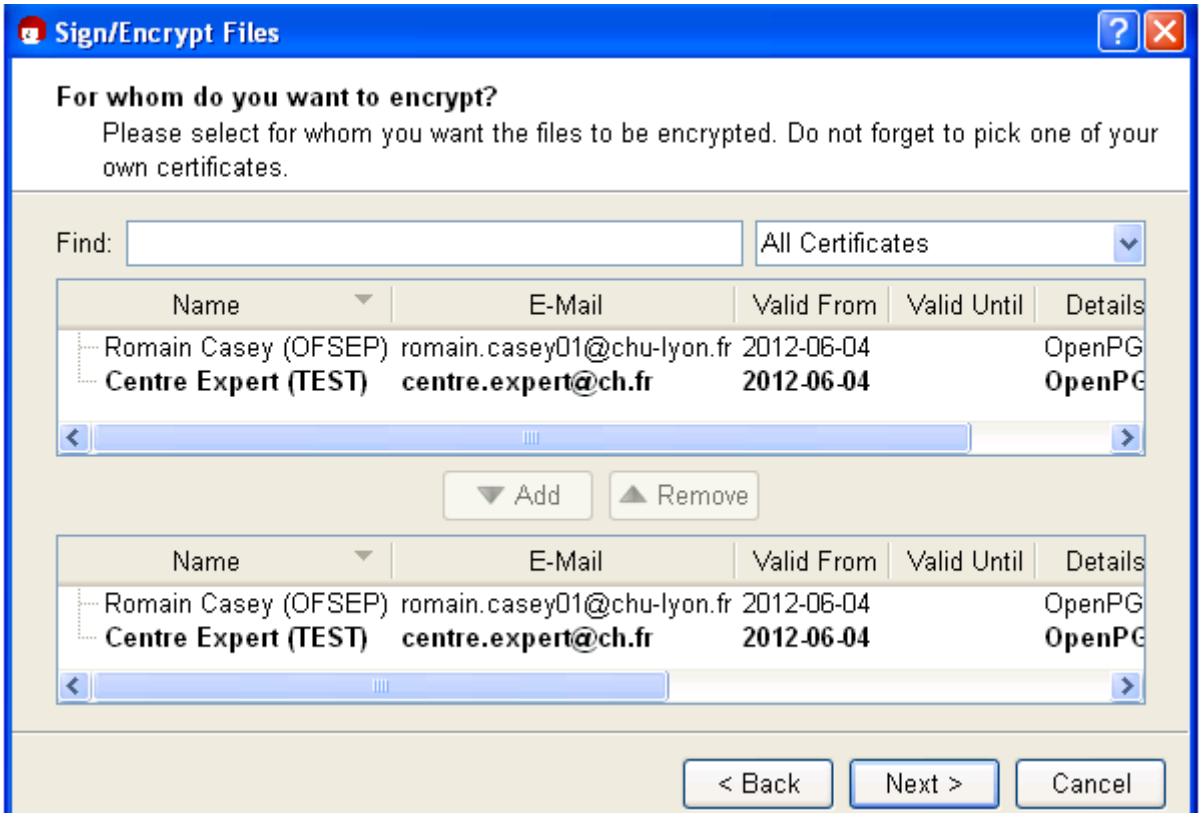
Vous devez alors sélectionner le ou les fichiers que vous souhaitez chiffrer, typiquement des fichiers d'export d'EDMUS.



Sélectionnez le bouton radio « Sign and Encryt » puis appuyez sur « Next ».

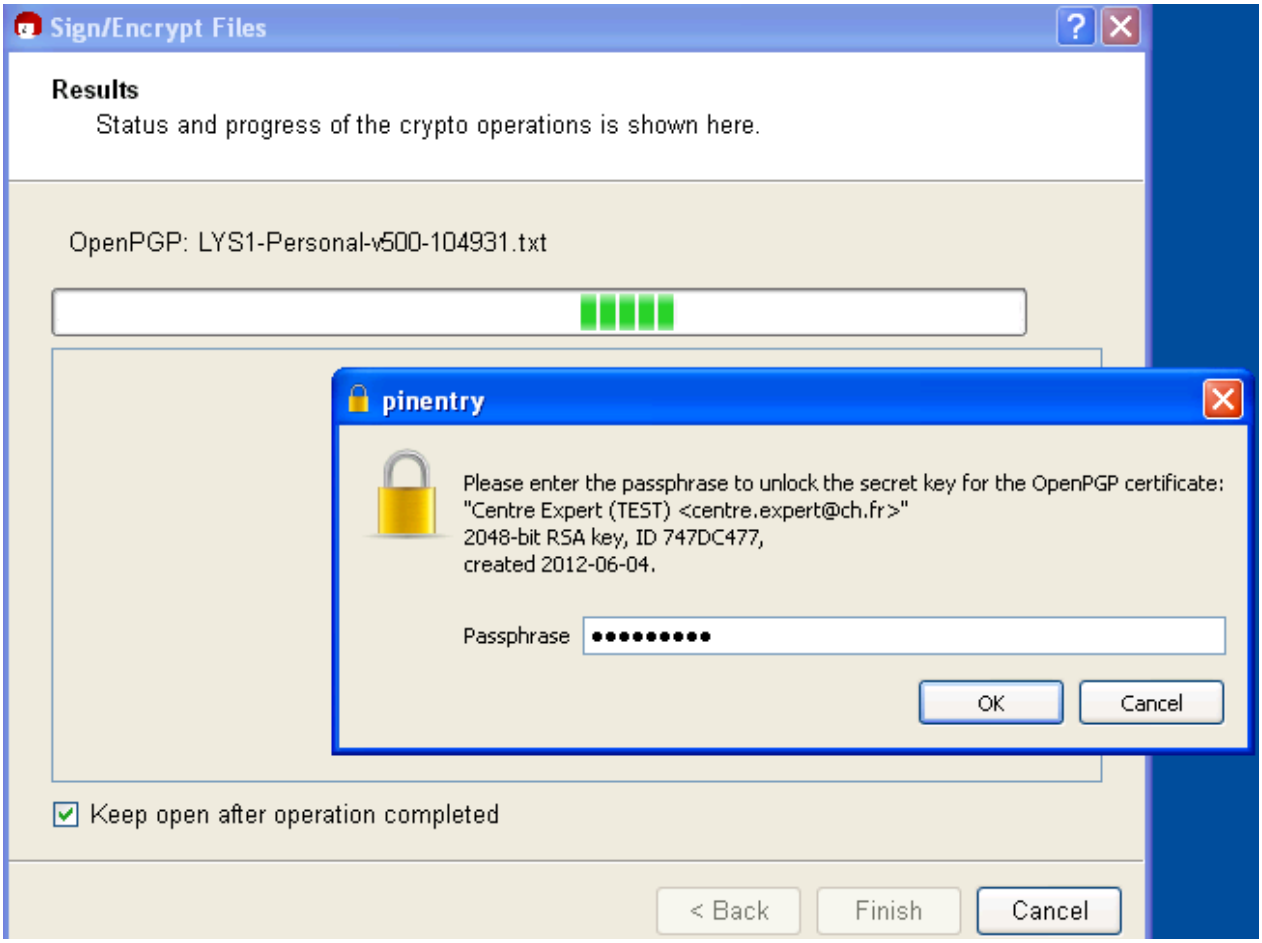


Vous devez ensuite indiquer (à l'aide du bouton « Add ») avec quelle clé vous souhaitez chiffrer les fichiers. Il vous faut indiquer la clé publique de votre correspondant (typiquement celle du CCN) mais aussi votre propre paire de clés, pour que vous puissiez vous aussi déchriffrer le fichier. Appuyez sur « Next ».

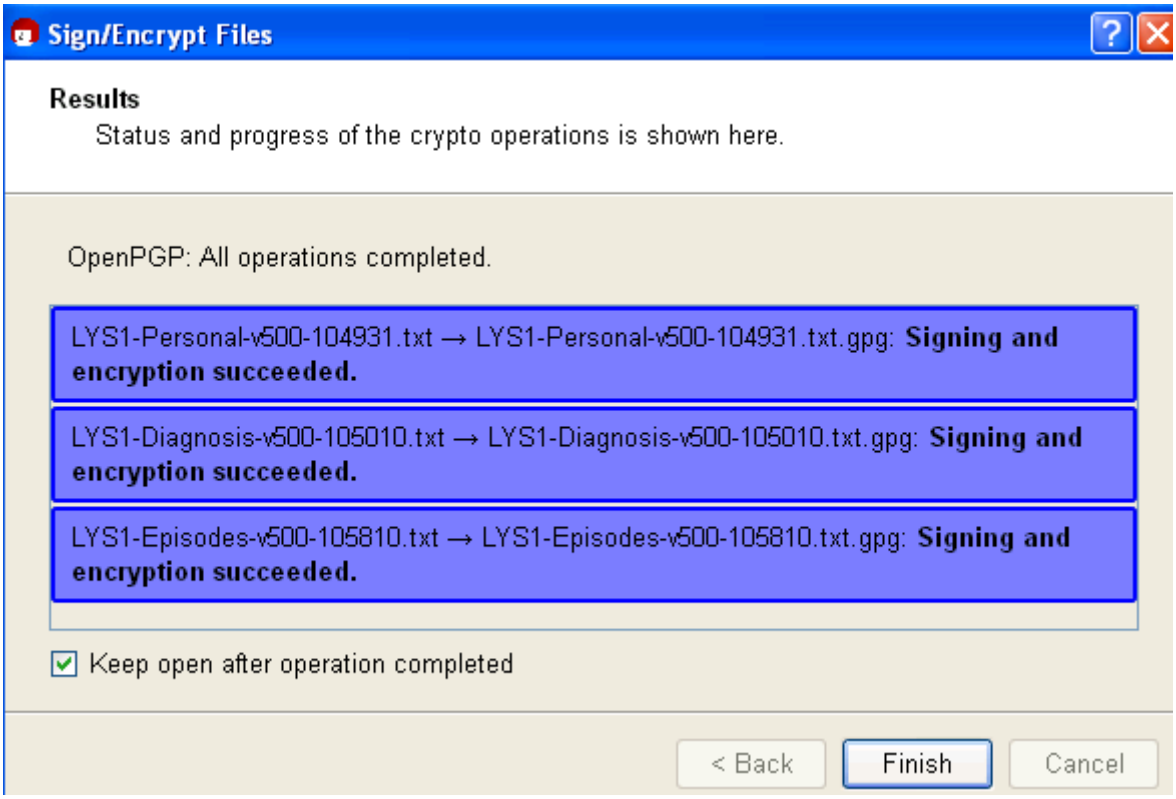


On vous demande avec quelle clé vous souhaitez signer vos fichiers. Si vous n'avez qu'une paire de clés, elle sera sélectionnée par défaut. Appuyez sur « Sign & Encrypt ».

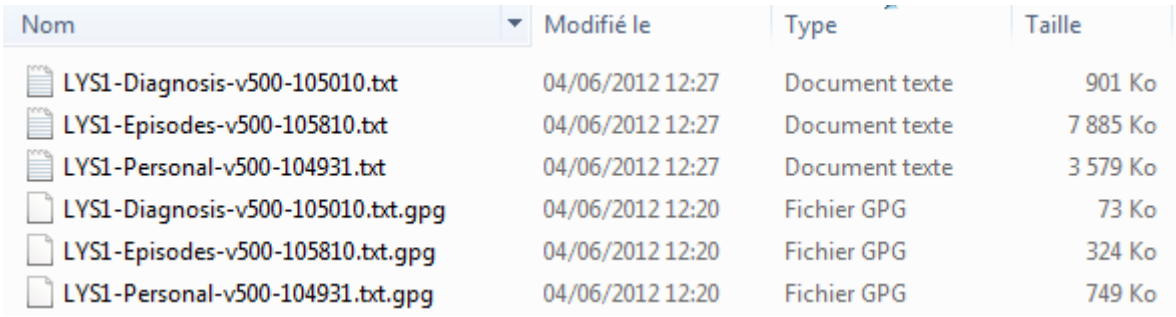
On vous demandera alors d'indiquer votre phrase de passe pour vérifier la validité de votre clé privée et ainsi permettre de signer vos documents.



À la fin de l'opération, vous devez obtenir une fenêtre de la forme suivante vous indiquant que tout s'est bien déroulé.



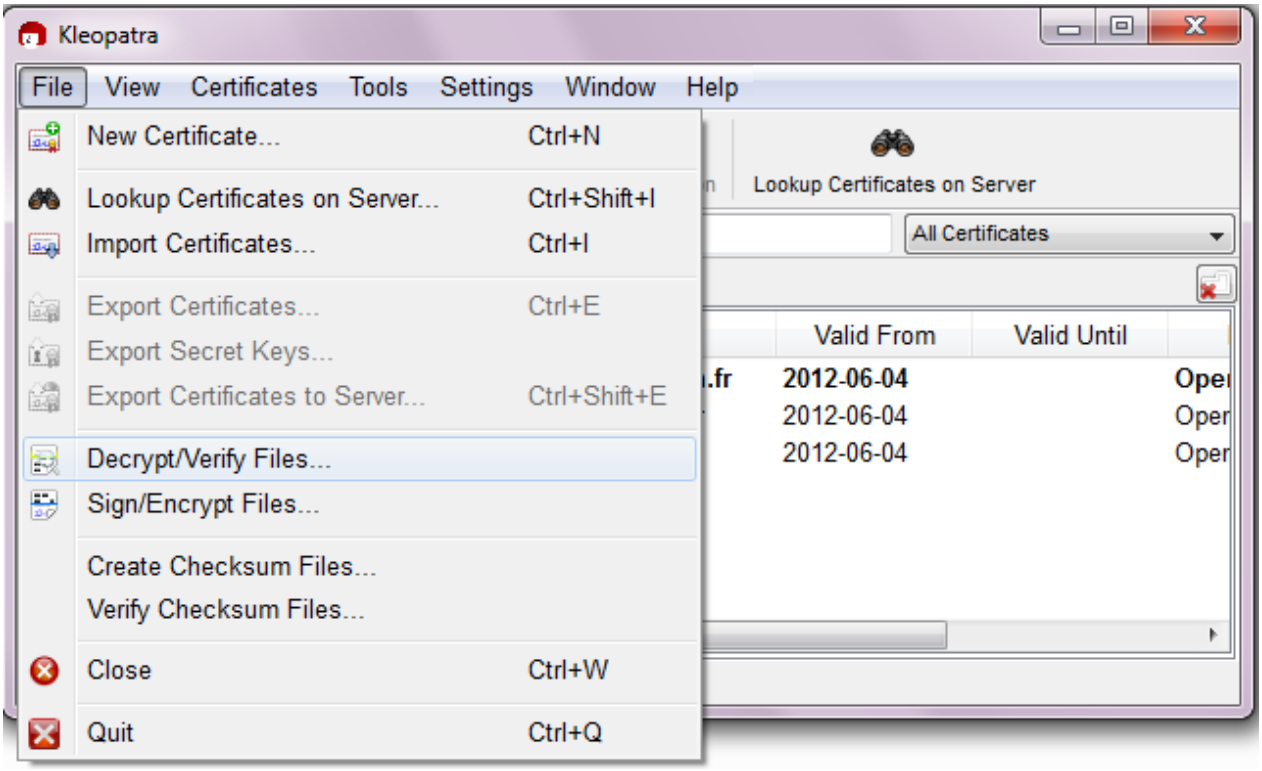
Dans le répertoire où se situent vos fichiers initaux, doivent alors se trouver en plus des fichiers portant l'extension .gpg. Ce sont ces fichiers que vous pouvez envoyer par email à votre correspondant. Notez que le fichier d'origine ne bouge pas.



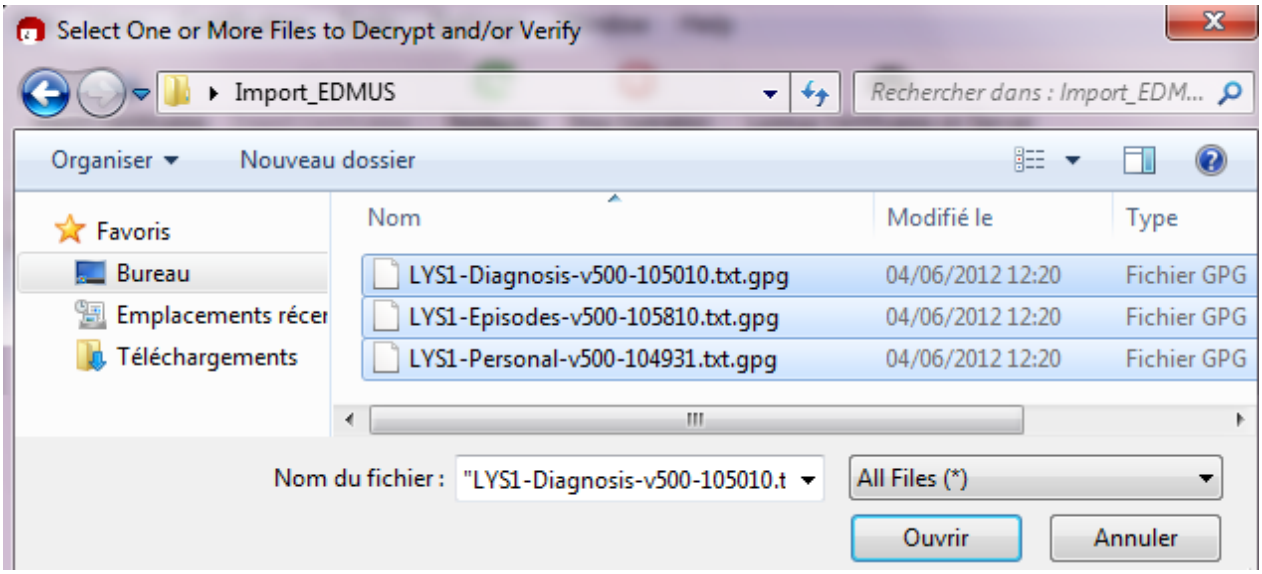
Nom	Modifié le	Type	Taille
LYS1-Diagnosis-v500-105010.txt	04/06/2012 12:27	Document texte	901 Ko
LYS1-Episodes-v500-105810.txt	04/06/2012 12:27	Document texte	7 885 Ko
LYS1-Personal-v500-104931.txt	04/06/2012 12:27	Document texte	3 579 Ko
LYS1-Diagnosis-v500-105010.txt.gpg	04/06/2012 12:20	Fichier GPG	73 Ko
LYS1-Episodes-v500-105810.txt.gpg	04/06/2012 12:20	Fichier GPG	324 Ko
LYS1-Personal-v500-104931.txt.gpg	04/06/2012 12:20	Fichier GPG	749 Ko

Recevoir des fichiers et les déchiffrez

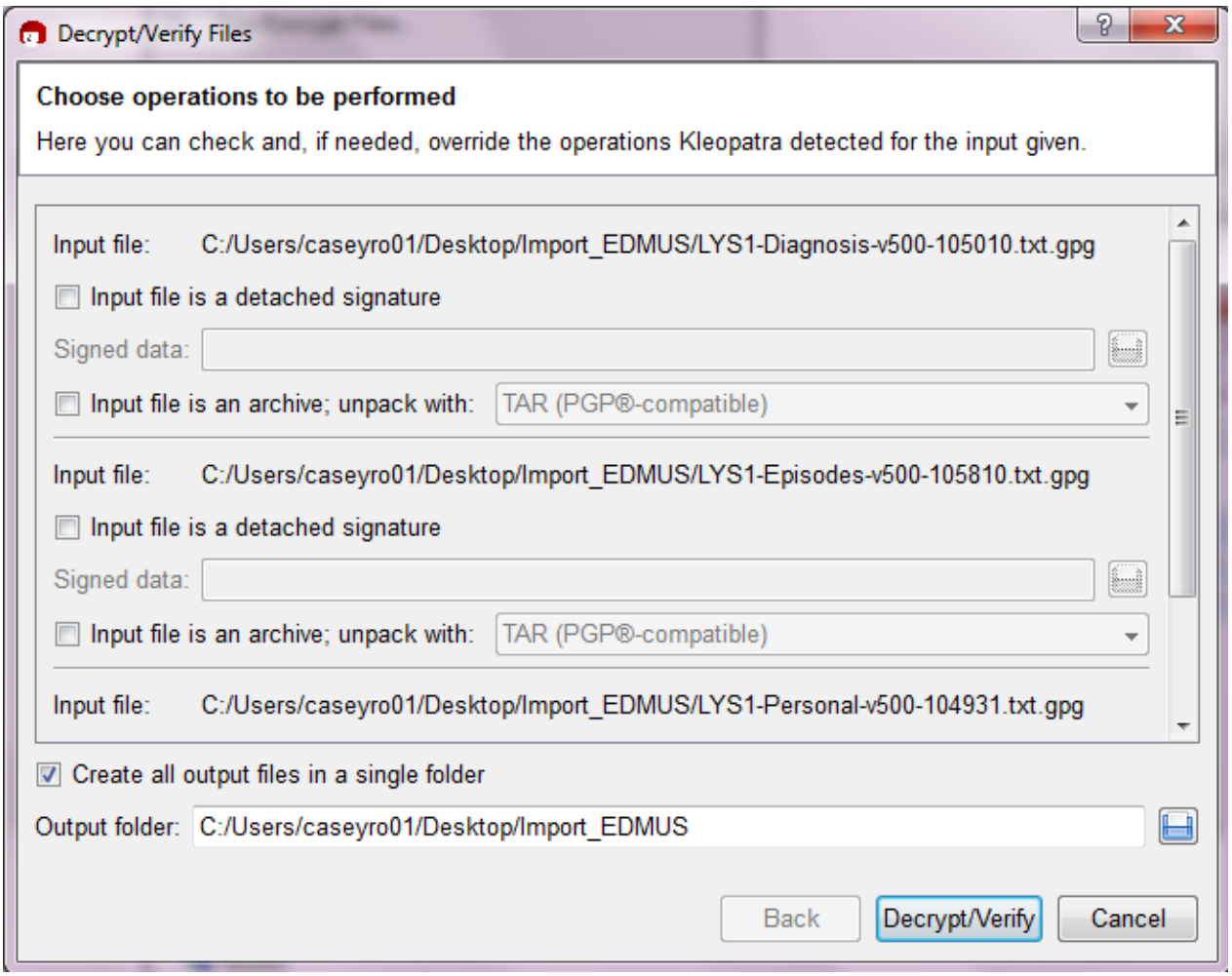
Si vous recevez des fichiers chiffrés par email, vous devez les enregistrer sur votre disque dur puis, dans Kleopatra, aller dans le menu « File » et sélectionner « Decrypt/Verify Files… ».

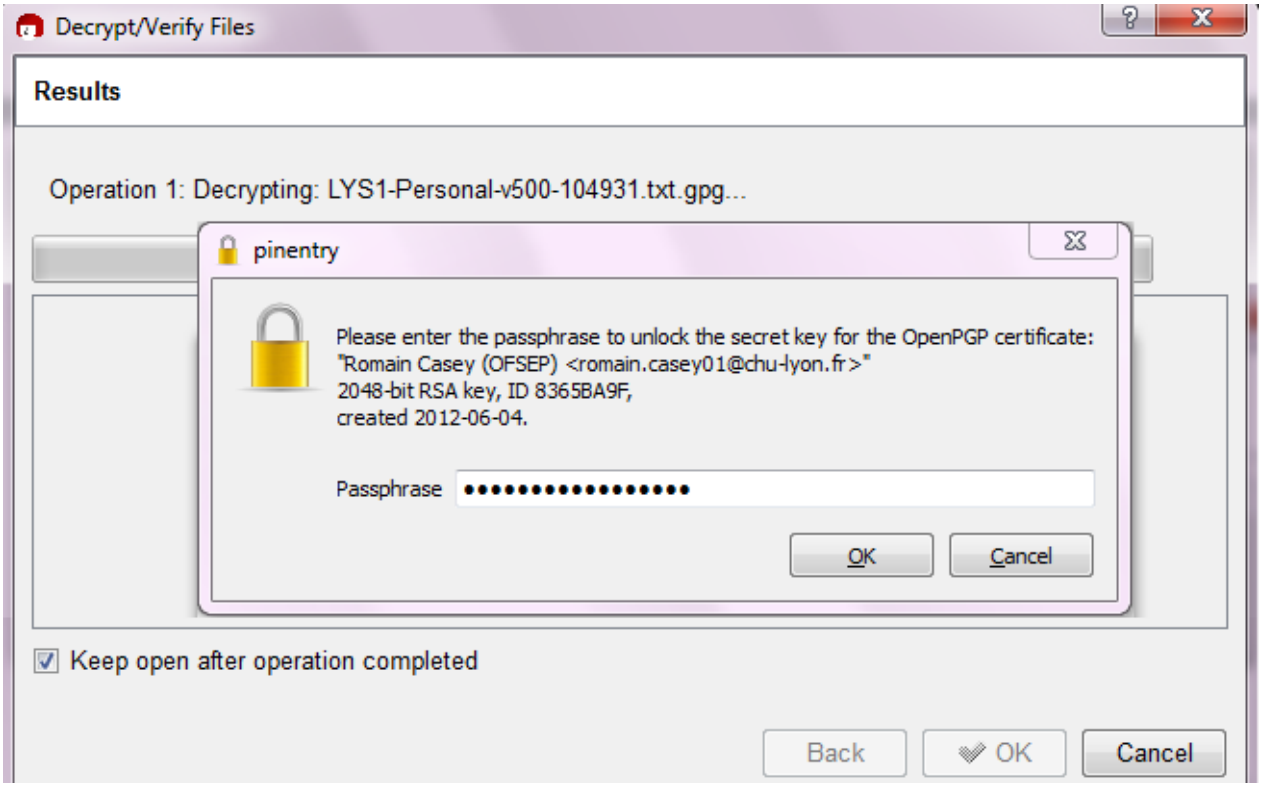


Sélectionnez alors les fichiers que vous avez enregistrés sur votre disque dur.

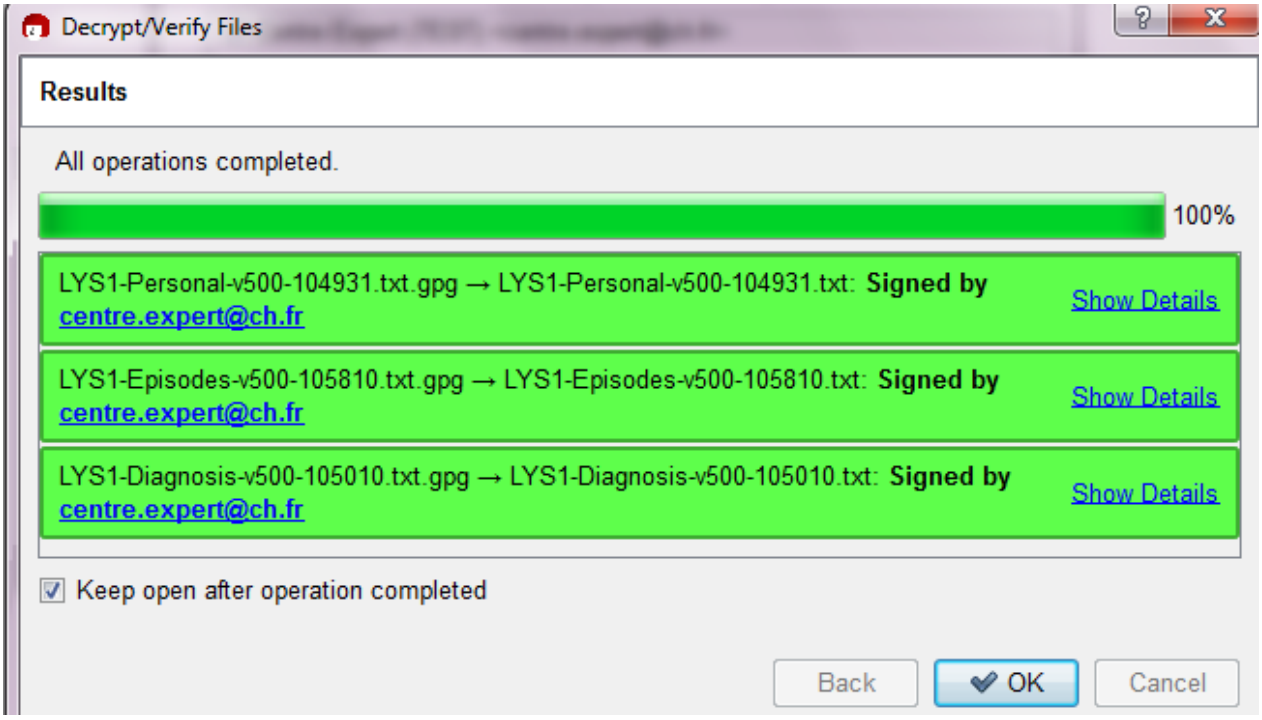


Appuyez sur le bouton « Decrypt/Verify » puis saisissez votre phrase de passe.

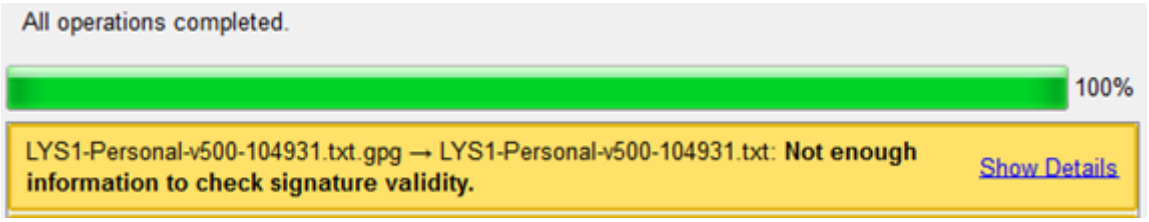

Decrypt/Verify Files
Choose operations to be performed
Here you can check and, if needed, override the operations Kleopatra detected for the input given.
Input file: C:/Users/caseyro01/Desktop/Import_EDMUS/LYS1-Diagnosis-v500-105010.txt.gpg
Input file is a detached signature
Signed data:
Input file is an archive; unpack with: TAR (PGP®-compatible)
Input file: C:/Users/caseyro01/Desktop/Import_EDMUS/LYS1-Episodes-v500-105810.txt.gpg
Input file is a detached signature
Signed data:
Input file is an archive; unpack with: TAR (PGP®-compatible)
Input file: C:/Users/caseyro01/Desktop/Import_EDMUS/LYS1-Personal-v500-104931.txt.gpg
Create all output files in a single folder
Output folder: C:/Users/caseyro01/Desktop/Import_EDMUS
Back
Decrypt/Verify
Cancel



Si l'opération se termine convenablement et que vous avez précédemment certifié la clé de votre correspondant, vous devez voir s'afficher la fenêtre suivante.



Si vous avez omis de certifier la clé de votre correspondant, vous avez le message suivant.



Dans les deux cas, les fichiers déchiffrés se trouvent dans le même répertoire que les fichiers chiffrés et ils sont maintenant prêts à être lus !

Références et documentation

- GnuPG : http://www.gnupg.org/ et http://www.gnupg.org/howtos/fr/.
- GPG4Win : http://www.gpg4win.org et http://www.gpg4win.org/doc/en/gpg4win-compendium.html.
- GPGTools (Mac OS) : http://www.gpgtools.org/.