

Le cryptage des données

Plateforme MapInMed

Table des matières

I-	Téléchargement du logiciel	3
II-	Installation du logiciel	4
III-	Utilisation du logiciel	4
1.	Importation d'une clé de cryptage	4
2.	Cryptage des données	6
3.	Décryptage des données	8
1.	Générer une clé privée.....	8
2.	Exporter sa clé publique	11
3.	Décrypter un fichier	12

I- Téléchargement du logiciel

De nombreux logiciels existent sur le marché dont le logiciel Kleopatra, logiciel libre, utilisant GnuPG.

Ce logiciel est téléchargeable à cette url:

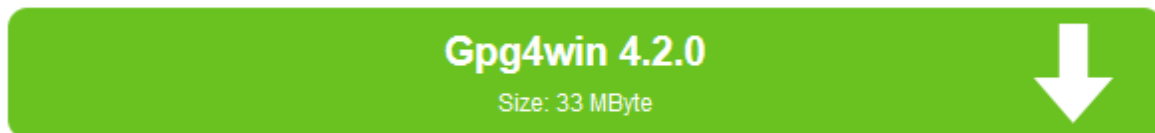
<http://www.gpg4win.org/download.html>

Télécharger Gpg4win

Download

Gpg4win 4.2.0 (Released: 2023-07-14)

You can download the full version (including the Gpg4win compendium) of Gpg4win 4.2.0 here:



[OpenPGP signature](#) (for gpg4win-4.2.0.exe)

SHA256: 829b5c8eb913fa383abdd4cf129a42e0f72d4e9924b2610134f593851f0ab119

[Changelog](#)

More Gpg4win-4.2.0 downloads

- Gpg4win source code package:
[gpg4win-4.2.0.tar.bz2](#) (Size: 214 MByte)
[OpenPGP signature](#)
SHA256 checksum:
81e0800cc090f8f387cee8e59b9f742f2e6d2d81a408414fc051a8df64e37d90
- All versions and OpenPGP signatures:
files.gpg4win.org.

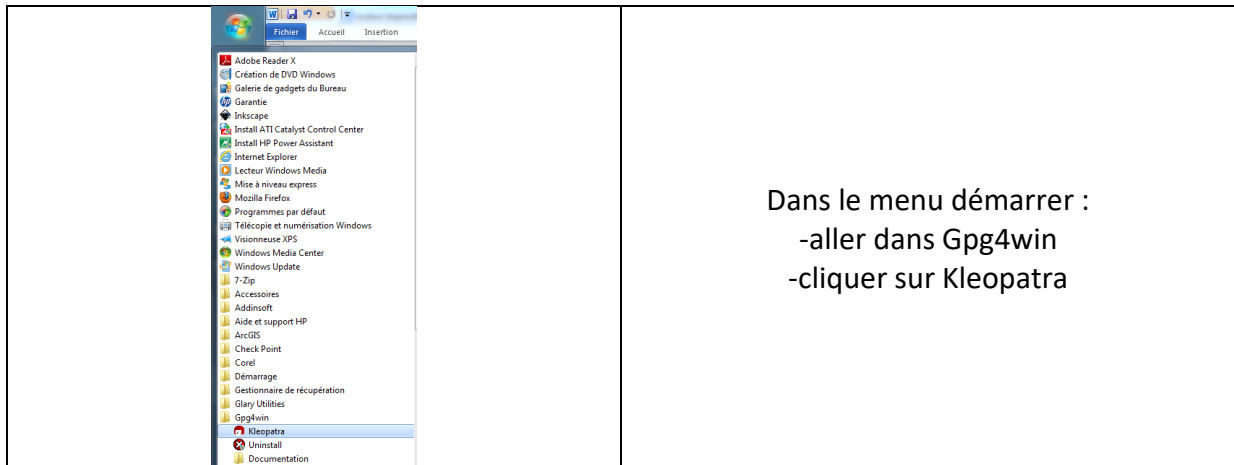
Ces derniers fonctionnent au moyen de clés permettant de crypter les données. Ces clés peuvent être **privées** ou **publics** (ce sont **les clés des personnes à qui vous envoyez les fichiers**).

II- Installation du logiciel

Lancer l'exécutable et suivre les instructions.

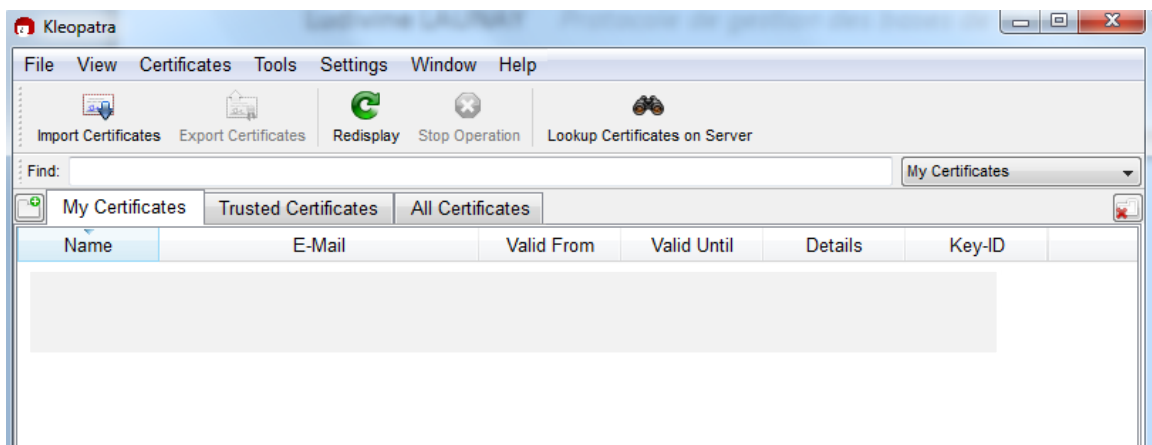
III- Utilisation du logiciel

Ouvrir le logiciel Kleopatra

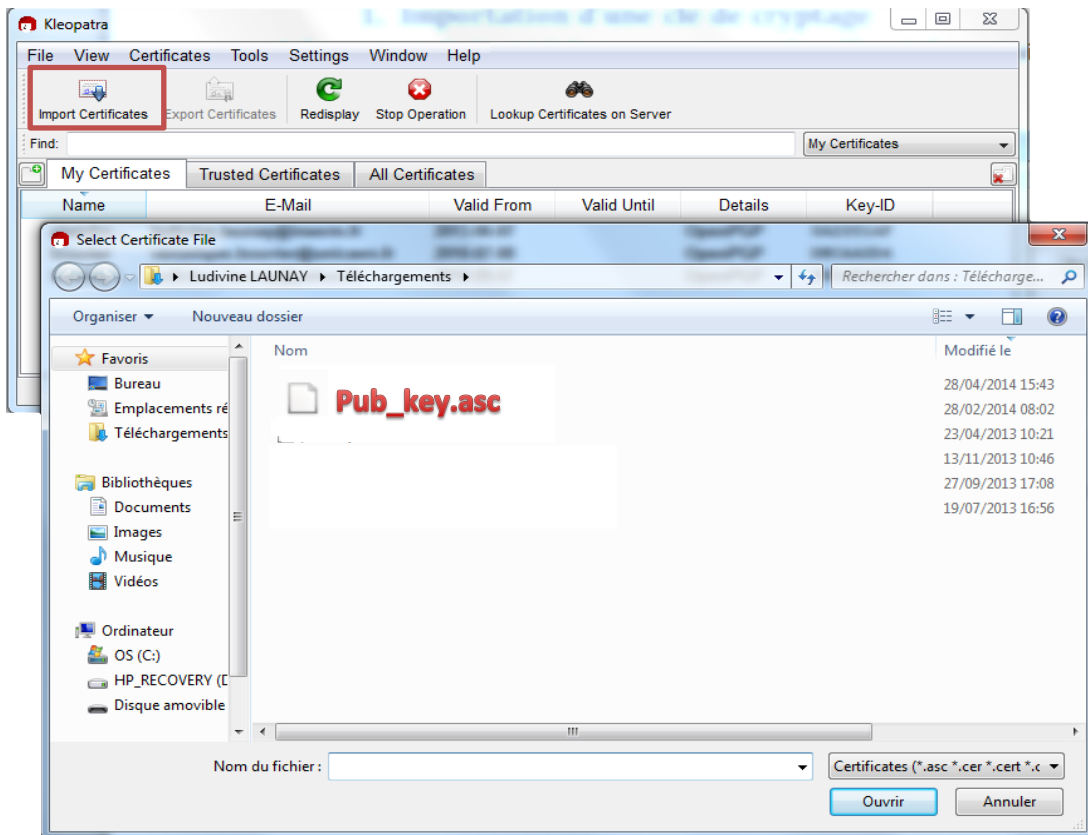


1. Importation d'une clé de cryptage

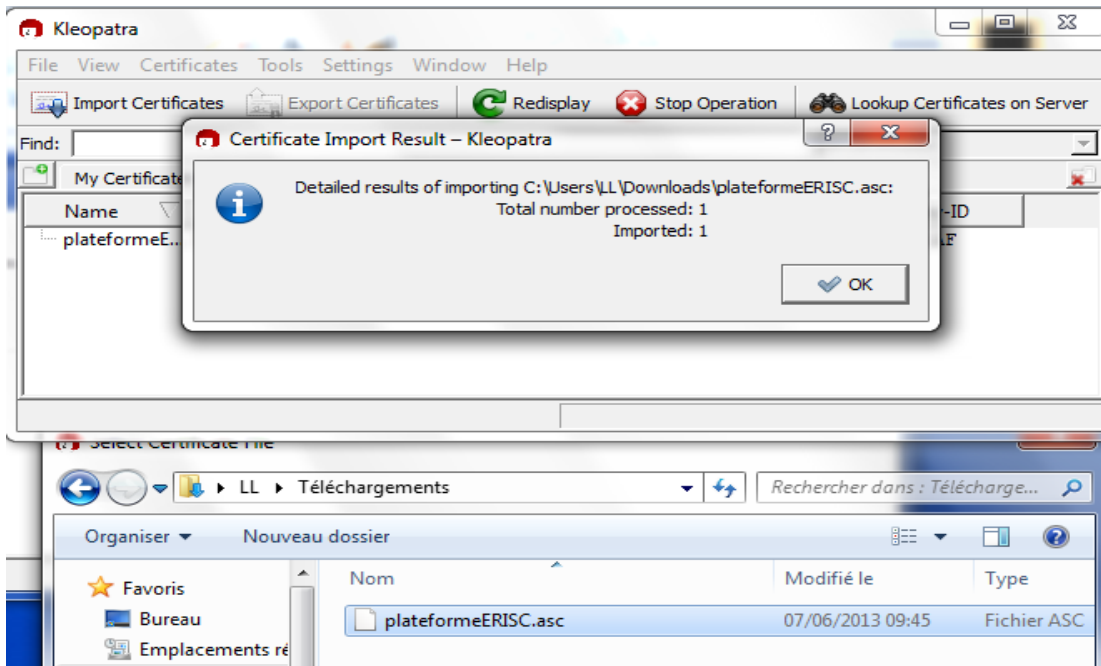
A l'ouverture du logiciel, la zone contenant les clés privées (My Certificates) est vide. Il en est de même des autres zones.



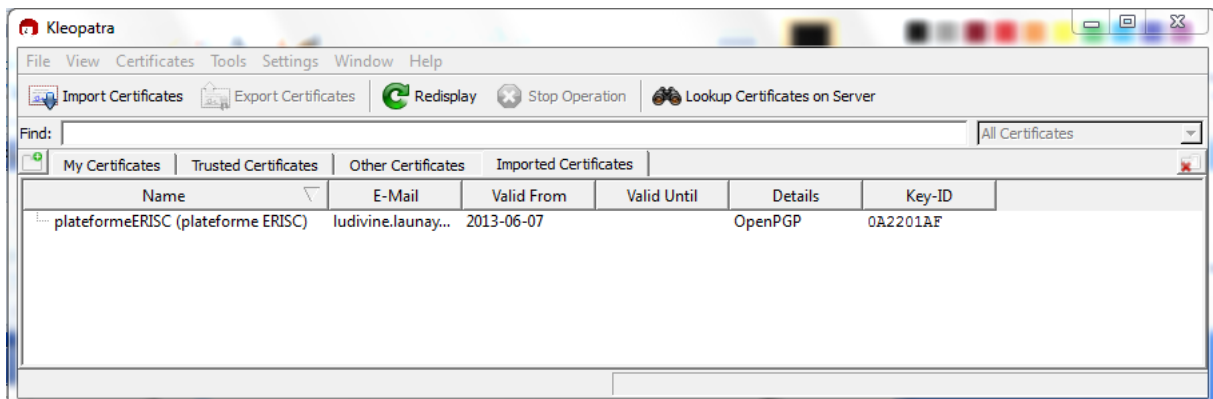
Vous allez devoir importer la clé publique du destinataire du fichier.



Les fichiers liés aux clés de cryptage ont l'extension **.asc**. Sélectionnez le fichier puis faites "ouvrir".

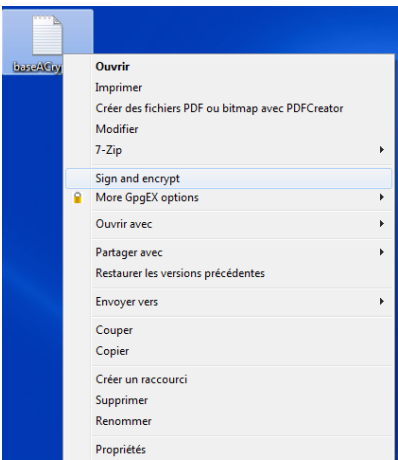


La clé apparaît désormais dans la zone "Imported Certificates"



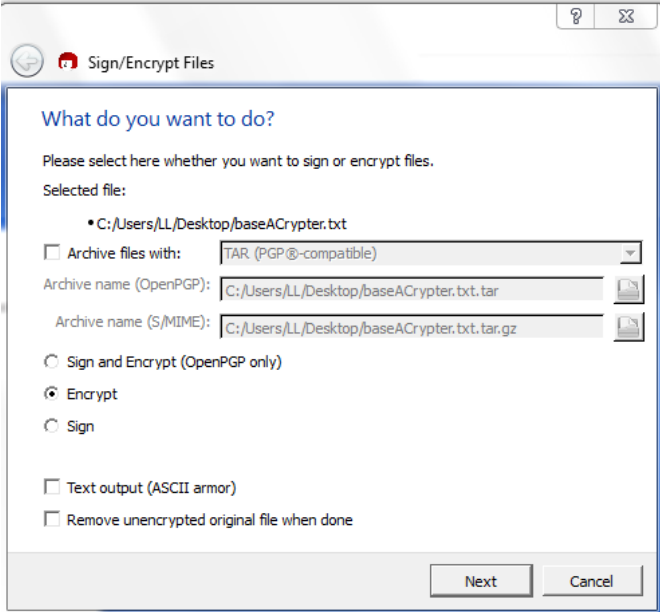
2. Cryptage des données

Faire un clic droit sur le fichier concerné



The screenshot shows a context menu for a file named 'baseACryt'. The 'Sign and encrypt' option is highlighted.

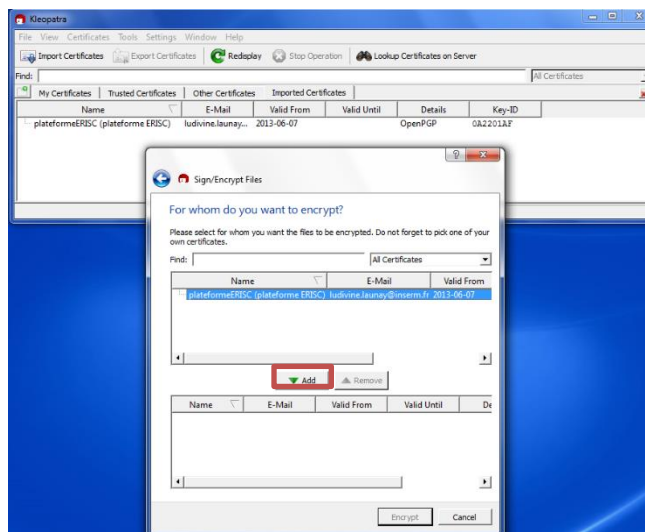
Sélectionner "Sign and encrypt"



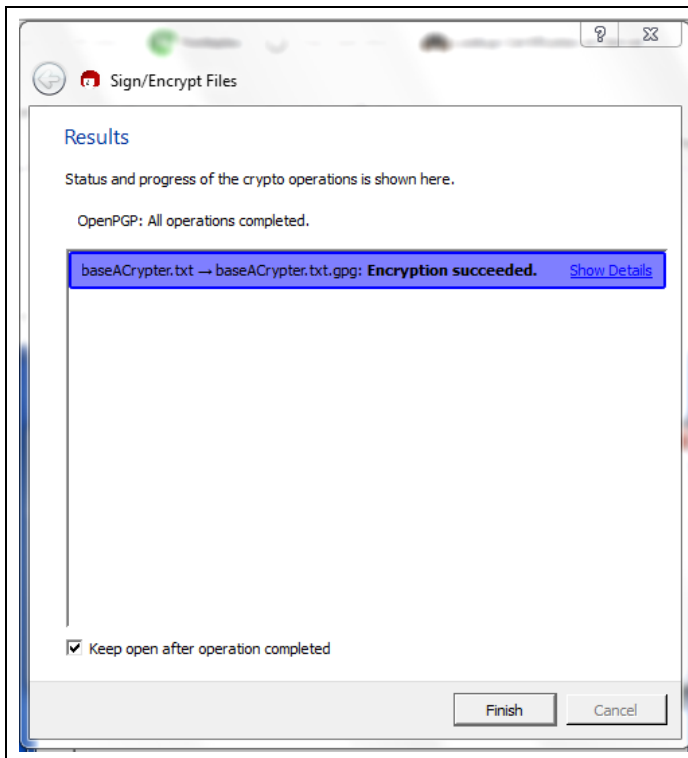
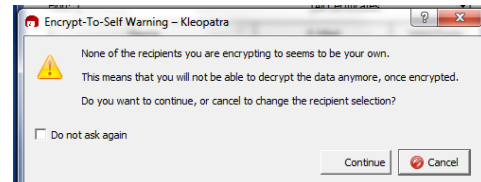
The screenshot shows the 'Sign/Encrypt Files' dialog box. The 'What do you want to do?' section has 'Encrypt' selected. The 'Selected file' is 'C:/Users/LL/Desktop/baseACrytper.txt'. The 'Archive files with' dropdown is set to 'TAR (PGP@-compatible)'. The 'Archive name (OpenPGP)' is 'C:/Users/LL/Desktop/baseACrytper.txt.tar' and the 'Archive name (S/MIME)' is 'C:/Users/LL/Desktop/baseACrytper.txt.tar.gz'. The 'Text output (ASCII armor)' and 'Remove unencrypted original file when done' options are unchecked. The 'Next' button is visible.

Puis "Encrypt"

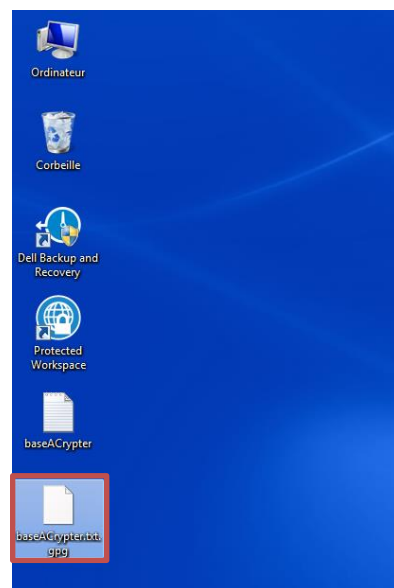
Ajouter la clé souhaitée



Cliquer sur "Continue"



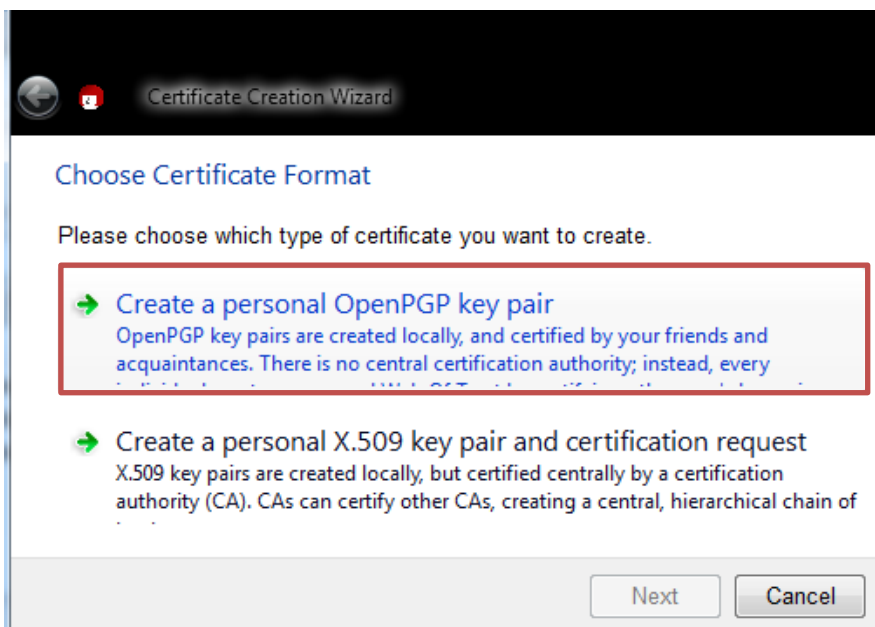
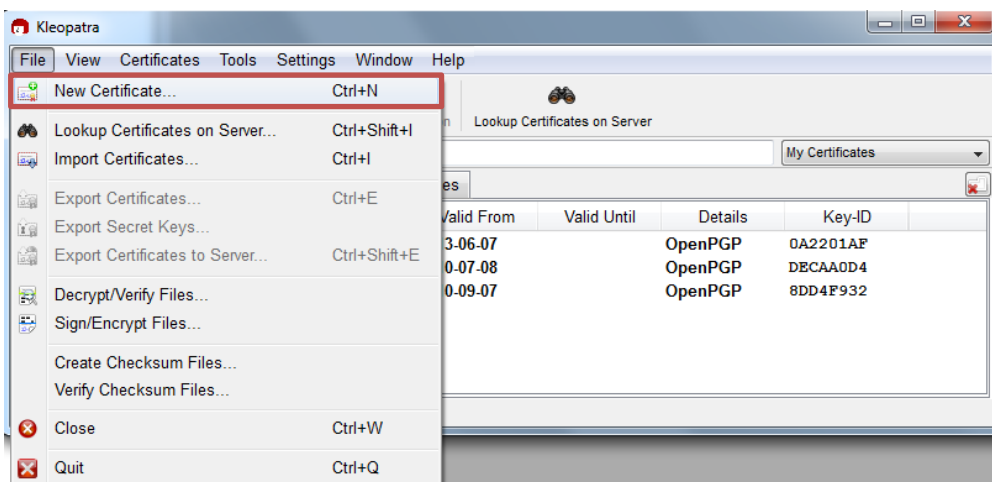
Un nouveau fichier .gpg est apparu près du fichier d'origine : il s'agit du fichier crypté



3. Décryptage des données

Vous ne pouvez décrypter des fichiers que **s'ils sont cryptés au moyen de la clé publique de votre propre clé** (vous devez posséder la clé privée de la clé utilisée et le mot de passe associé). Cela suppose par conséquent que vous ayez envoyé celle-ci à vos correspondants.

1. Générer une clé privée



Choisissez un nom pour votre clé et renseignez l'adresse email associée (celle-ci ne sera utilisée que si vous postez votre clé publique sur le serveur dédié à cet effet)

Enter Details

Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button.

Name: (required)

E-Mail: (required)

Comment: (optional)

Name is required, but empty.

Review Certificate Parameters

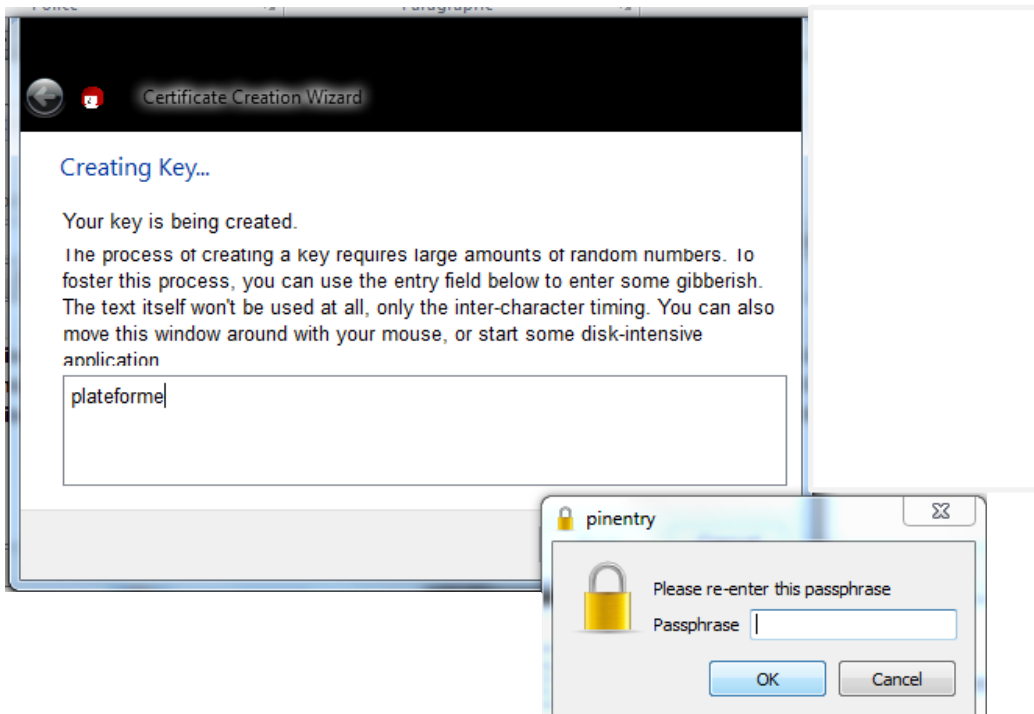
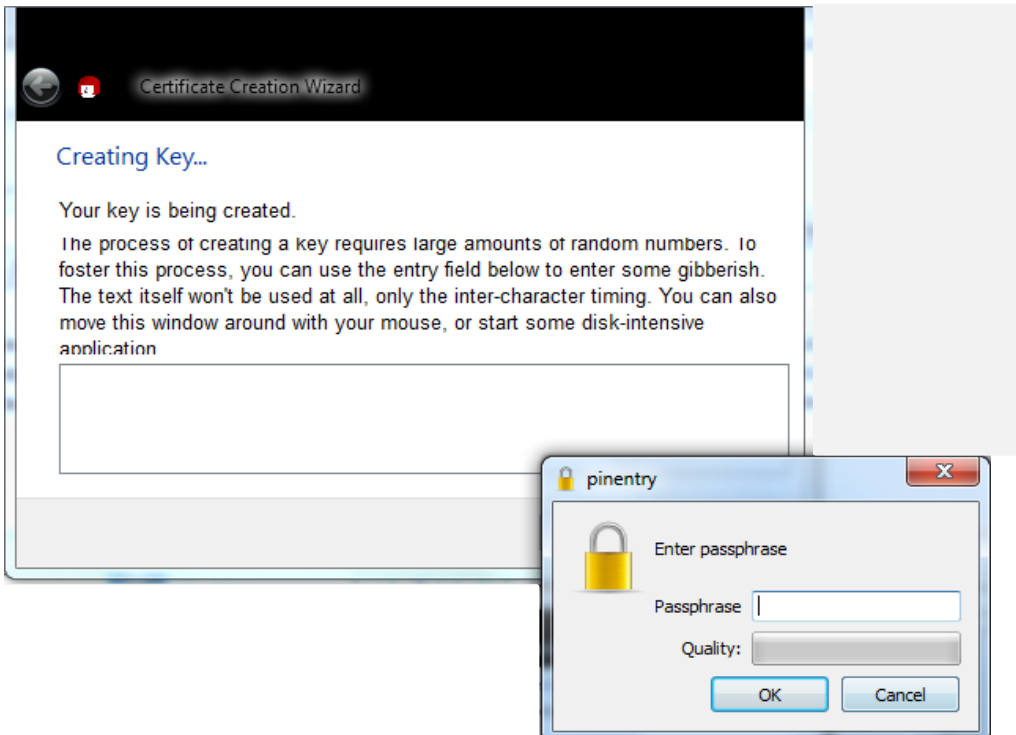
Please review the certificate parameters before proceeding to create the certificate.

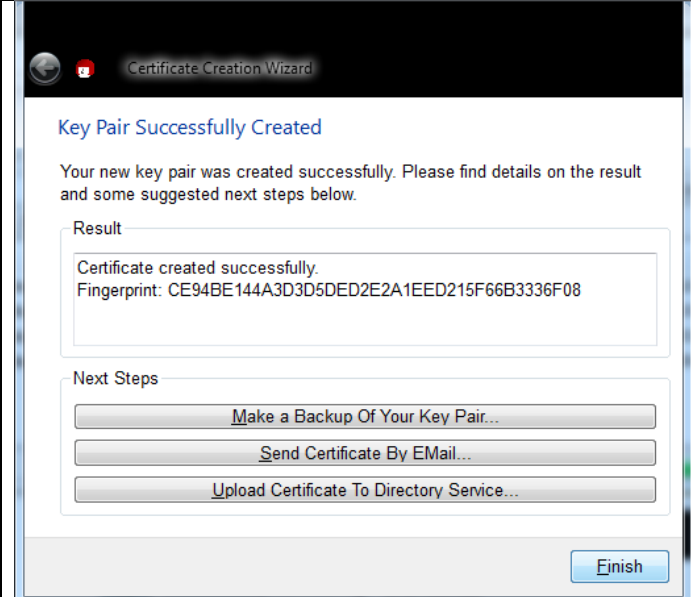
Name: plateforme ERISC

Email Address: plateformeERISC@gmail.com

Show all details

Choisissez un mot de passe suffisamment sécurisé pour le décryptage des données





Key Pair Successfully Created

Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

Result

Certificate created successfully.
Fingerprint: CE94BE144A3D3D5DED2E2A1EED215F66B3336F08

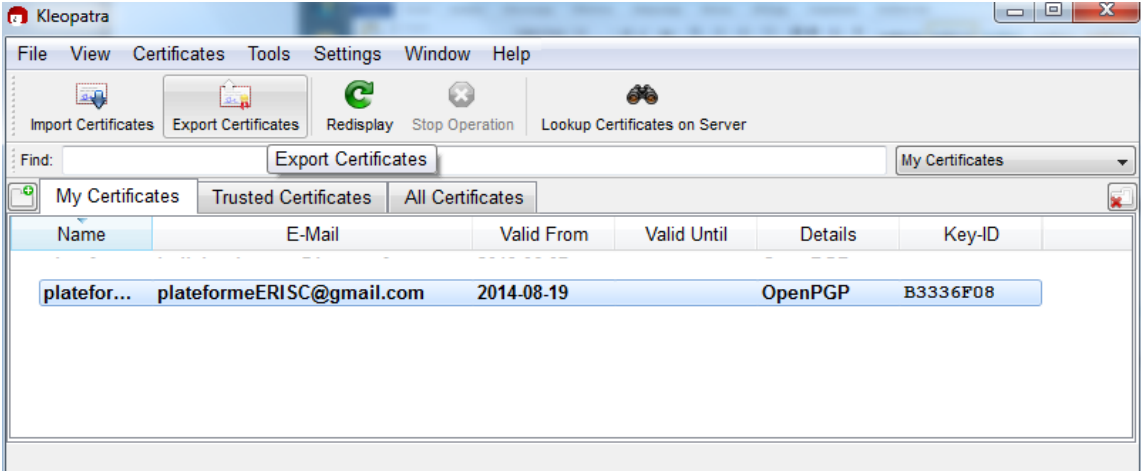
Next Steps

- Make a Backup Of Your Key Pair...
- Send Certificate By EMail...
- Upload Certificate To Directory Service...

Finish

Le backup permet **d'exporter la clé privée** pour l'utiliser sur un autre ordinateur. Vous ne devez en cas transmettre celle-ci à vos correspondants.

2. Exporter sa clé publique



Kleopatra

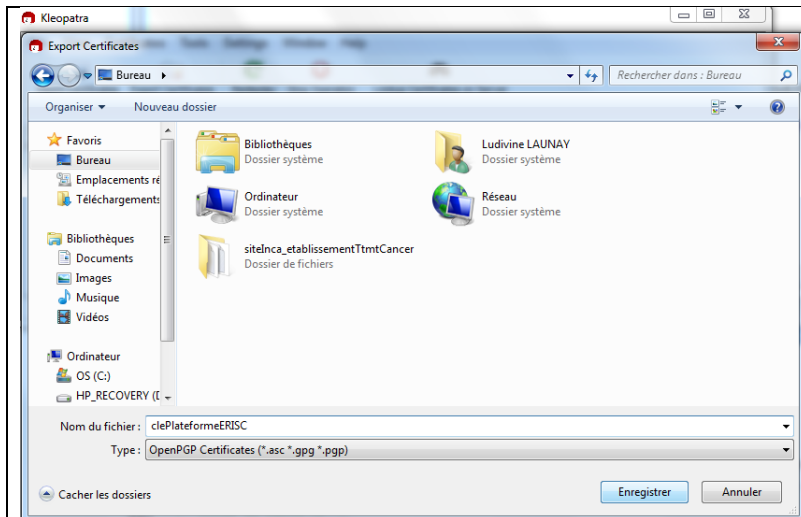
File View Certificates Tools Settings Window Help

Import Certificates Export Certificates Redisplay Stop Operation Lookup Certificates on Server

Find: Export Certificates My Certificates

My Certificates Trusted Certificates All Certificates

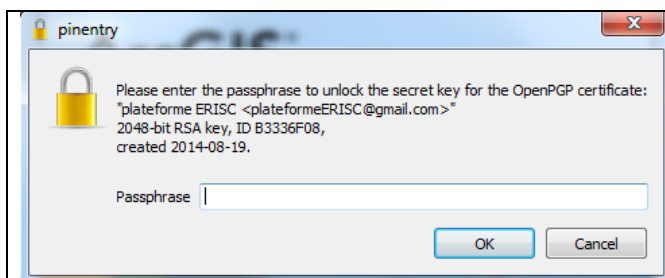
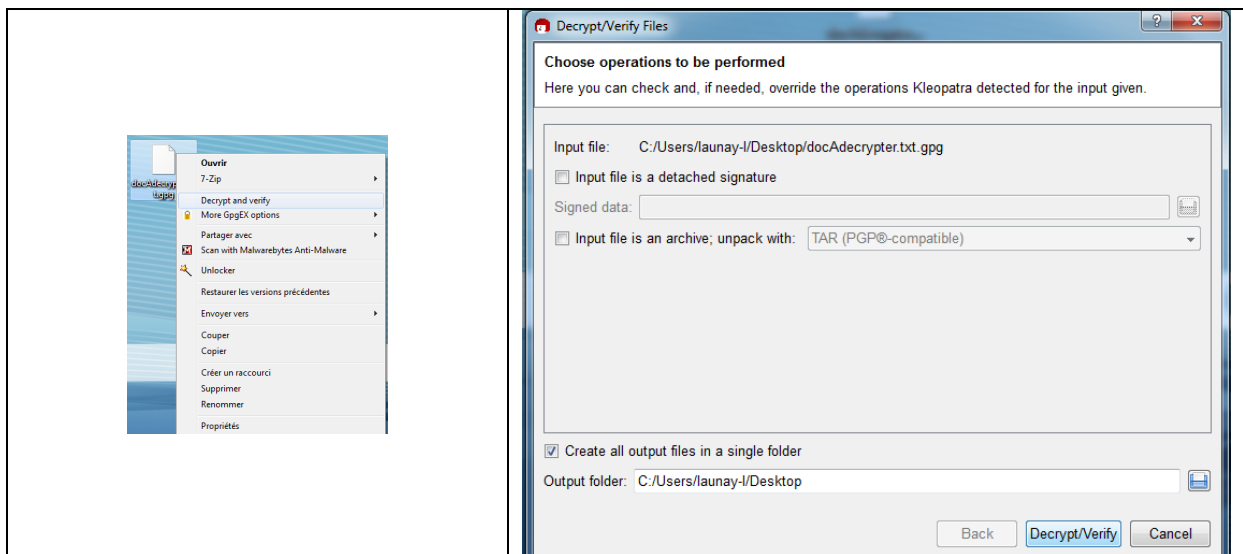
Name	E-Mail	Valid From	Valid Until	Details	Key-ID
platefor...	plateformeERISC@gmail.com	2014-08-19		OpenPGP	B3336F08



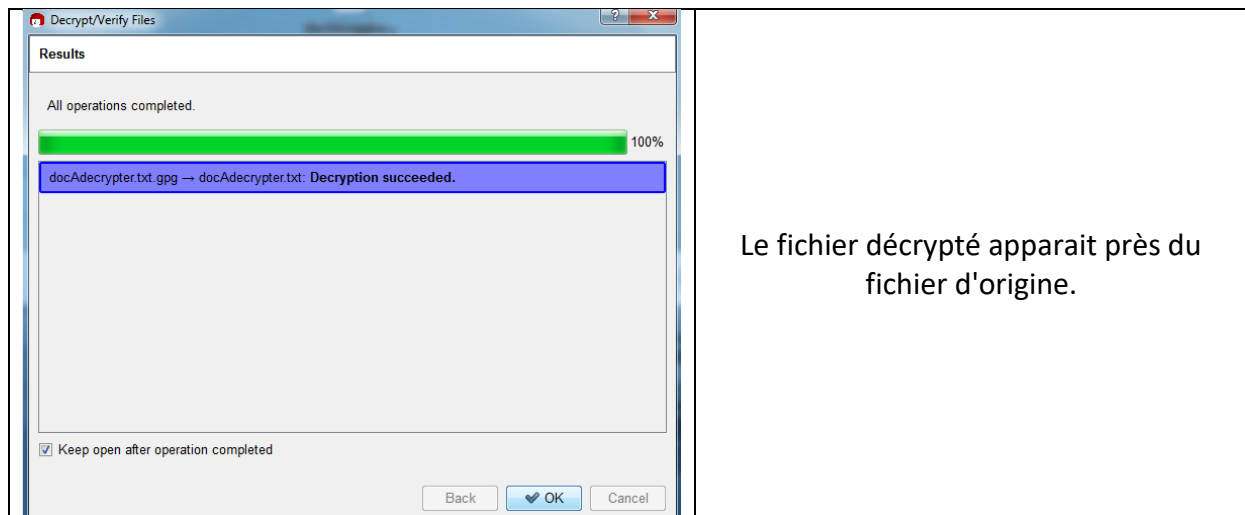
Choisissez l'emplacement pour l'enregistrement du fichier.
Celui-ci apparait avec l'extension .asc

3. Décrypter un fichier

Faites un clic droit sur le fichier à décrypter



Saisissez le mot de passe associé à votre clé de cryptage



Le fichier décrypté apparaît près du fichier d'origine.