





Le cryptage des données

U1086 INSERM "Cancers & Préventions"

Ludivine LAUNAY

Table des matières

I -	Téléc	hargement du logiciel	3
II-	Instal	lation du logiciel	4
-	Utilisa	ation du logiciel	4
1	. Imp	ortation d'une clé de cryptage	4
2	. Cry	ptage des données	6
3	. Déc	ryptage des données	8
	1.	Générer une clé privée	8
	2.	Exporter sa clé publique	11
	3.	Décrypter un fichier	12

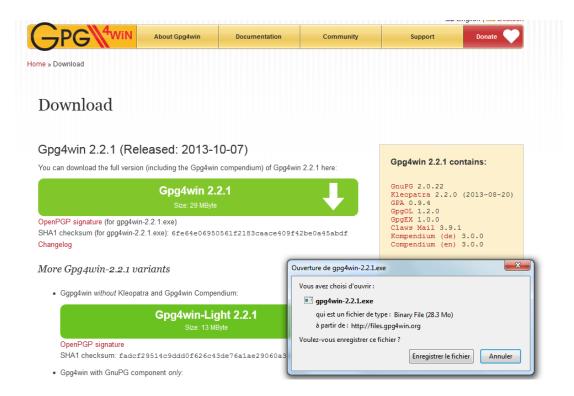
I- Téléchargement du logiciel

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



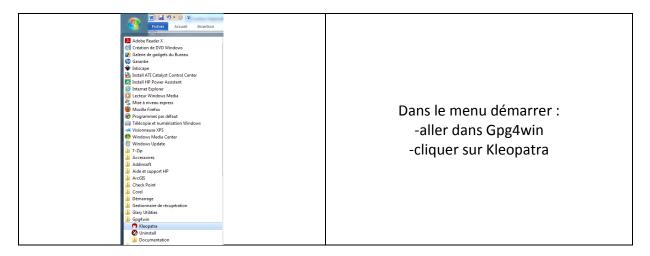
Ces derniers fonctionnent au moyen de clés permettant de crypter les données. Ces clés peuvent être **privées** ou **publics** (ce sont **les clés des <u>personnes à qui vous envoyez les fichiers</u>**).

II- Installation du logiciel

Lancer l'exécutable et suivre les instructions.

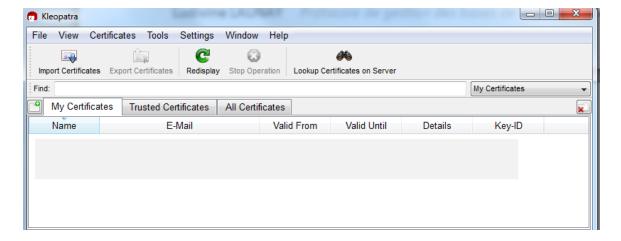
III- Utilisation du logiciel

Ouvrir le logiciel Kleopatra

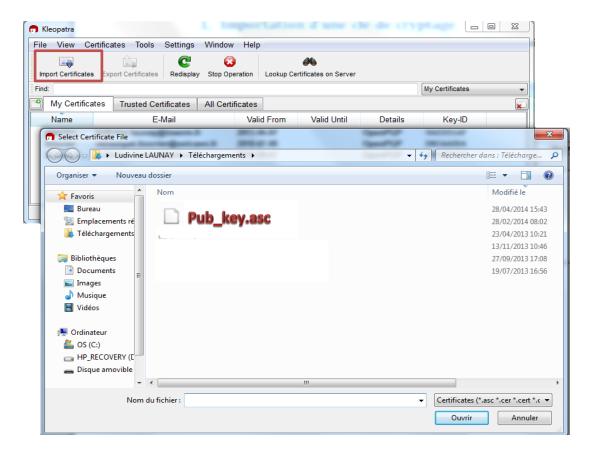


1. Importation d'une clé de cryptage

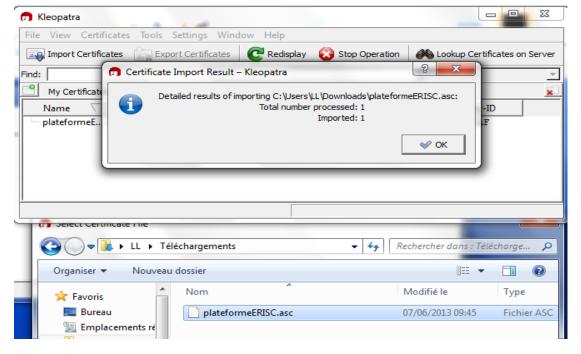
A l'ouverture du logiciel, la zone contenant les clés privées (My Certificates) est vide. Il en est de même des autres zones.



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



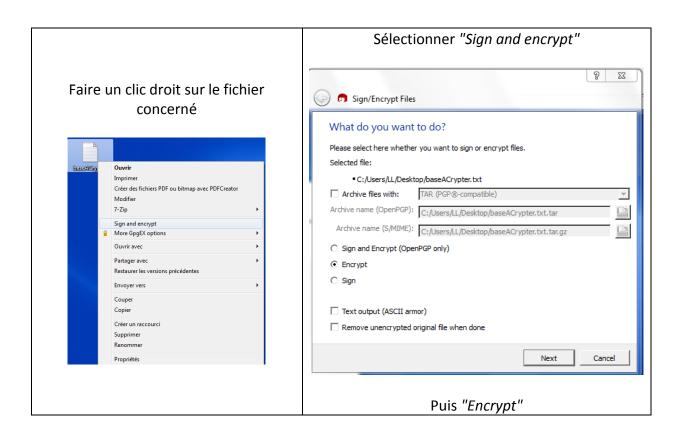
Les fichiers liés aux clés de cryptage ont l'extension .asc. Sélectionnez le fichier puis faites "ouvrir".

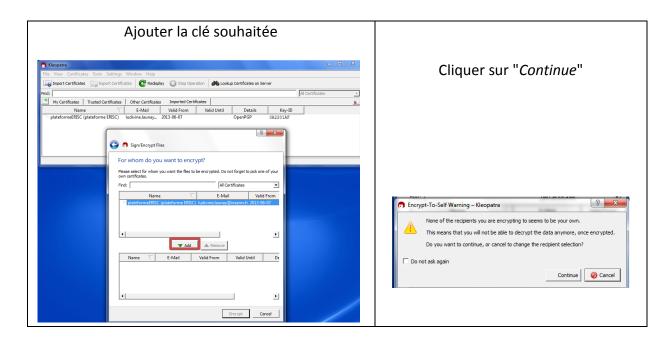


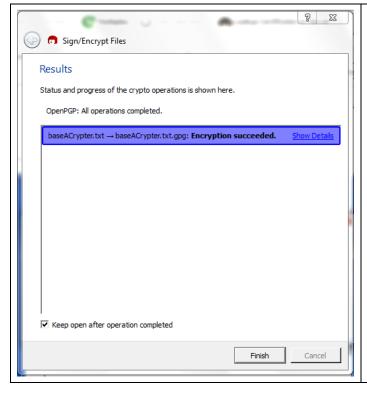
La clé apparait désormais dans la zone "Imported Certificates"



2. Cryptage des données





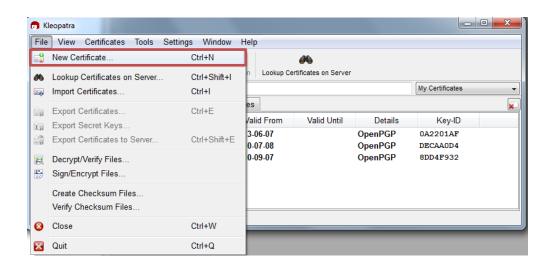


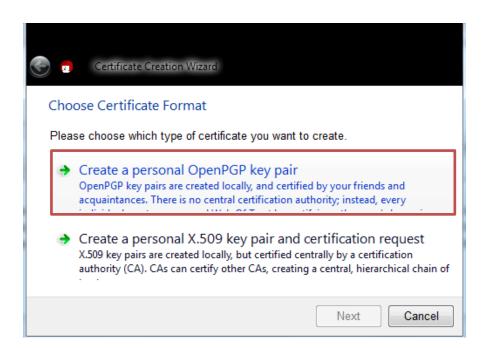


3. Décryptage des données

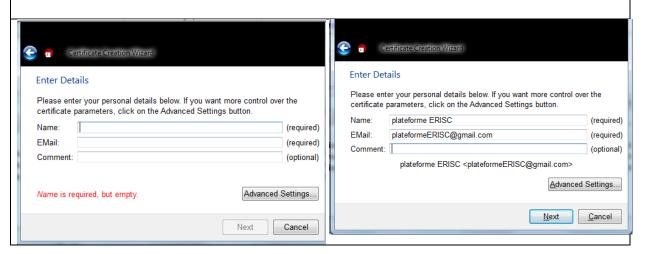
Vous ne pouvez décrypter des fichiers que s'ils sont cryptés au moyen de la clé publique de votre propre clé (vous devez posséder la clé privée de la clé utilisée et le mot de passe associé). Cela suppose par conséquent que vous ayiez envoyé celle-ci à vos correspondants.

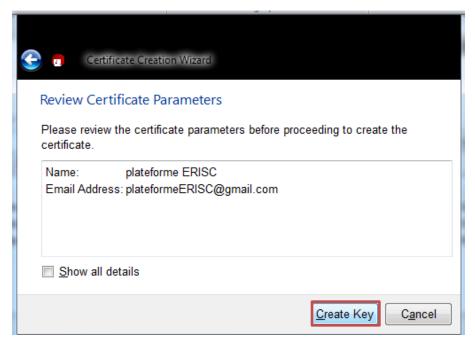
1. Générer une clé privée



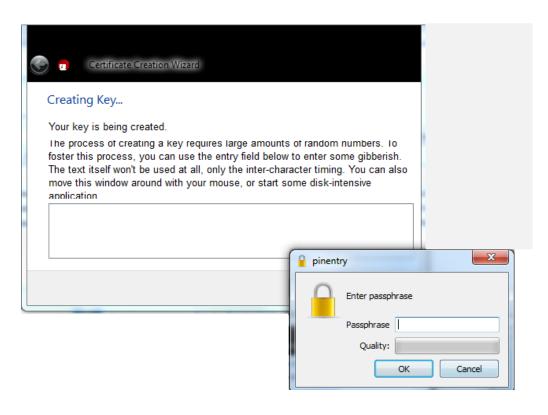


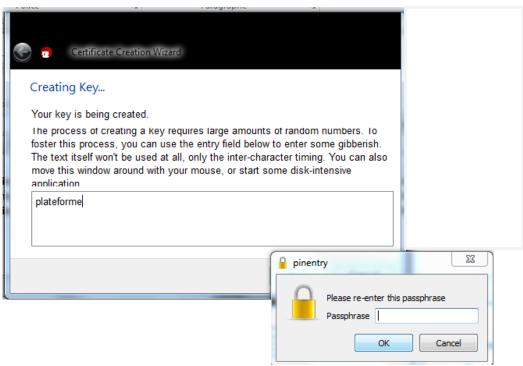
Choississez un nom pour votre clé et renseignez l'adresse email associée (celle-ci ne sera utilisée que si vous postez votre clé publique sur le serveur dédié à cet effet)

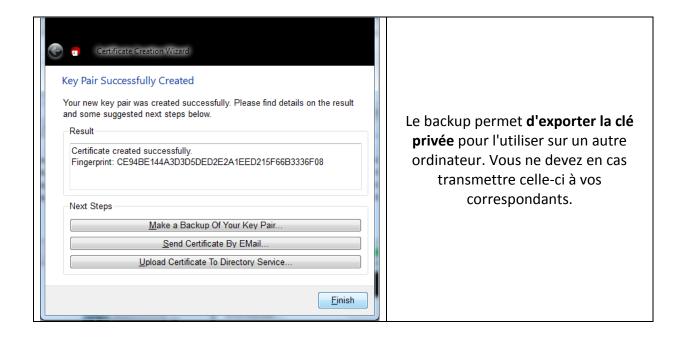




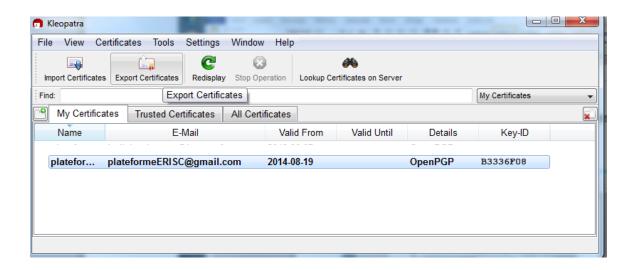
Choisissez un mot de passe suffisamment sécurisé pour le décryptage des données

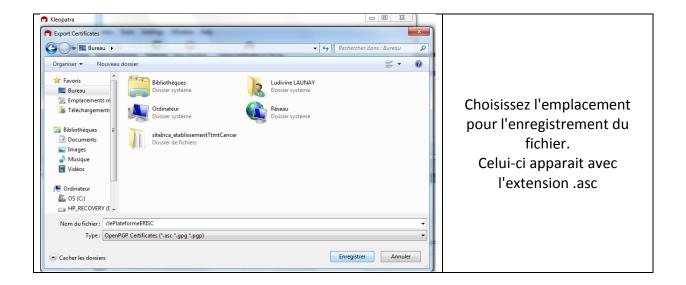






2. Exporter sa clé publique





3. Décrypter un fichier

Faites un clic droit sur le fichier à décrypter

