DMSI
Unité des Enquête en Ligne

Version 9.0
du 26/11/2019

MANUEL D'INSTALLATION ET D'UTILISATION FORMATION DE L'APPLICATION GPG4WIN

Sommaire

1 Installation de GPG4win

Prendre la version la plus à jour

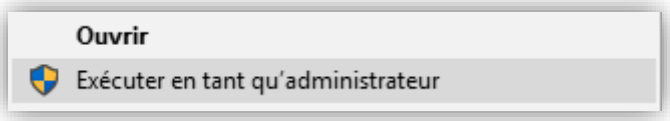
Aller sur la page https://www.gpg4win.org/download.html et cliquer sur la dernière version proposée :

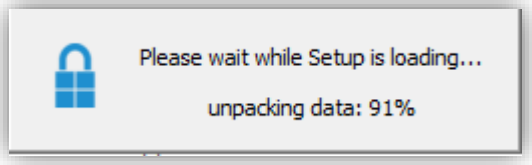
Après le téléchargement vérifier que l'empreinte de l'exécutable correspond bien au SHA256 indiqué (avec le logiciel QuickHash https://www.quickhash-gui.org/ par exemple).

Fermer toutes les applications ouvertes car l'installation pourrait nécessiter le redémarrage de votre poste

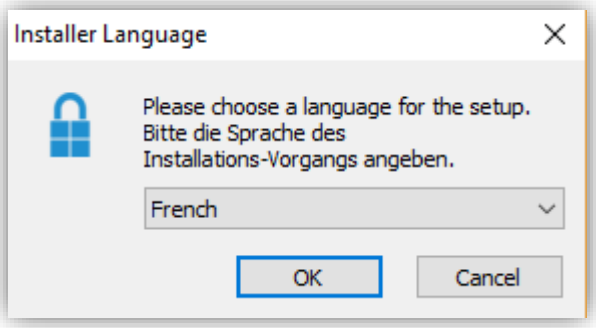
Vous devez avoir des droits d'administrateur sur votre poste pour l'installation.

Lancer l'installation en cliquant avec le bouton droit de la souris sur l'exécutable que vous venez de télécharger :

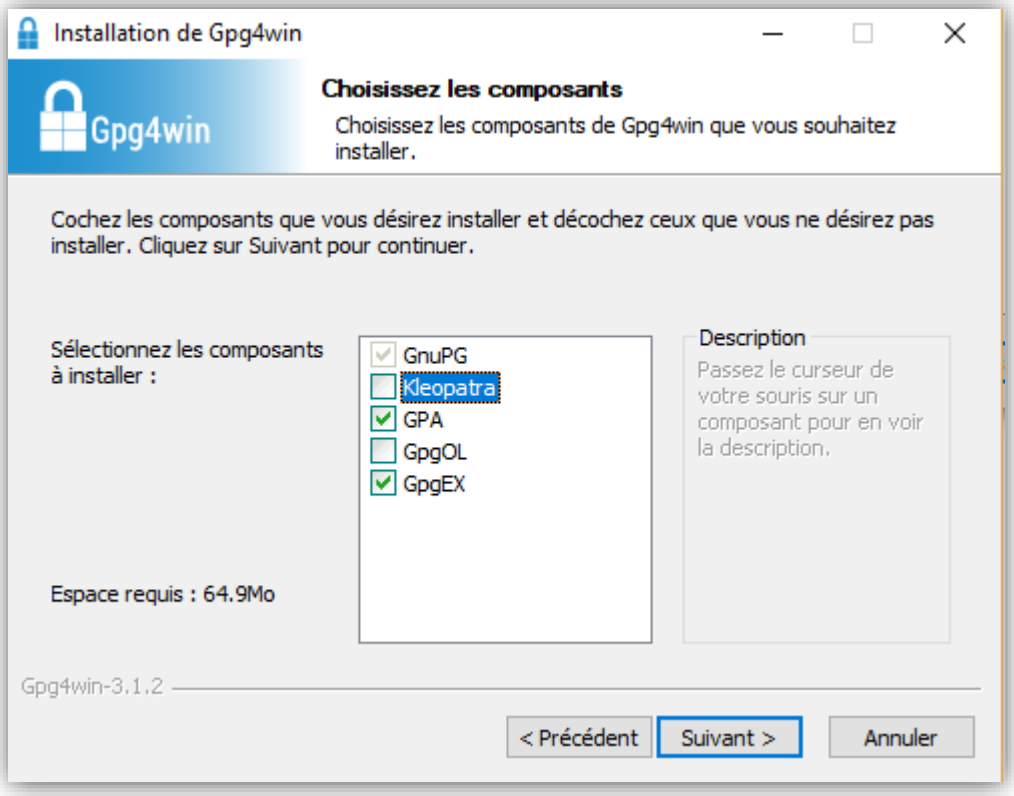




Cliquer sur le bouton OK après avoir choisi votre langue (par défaut français en fonction de votre système d'exploitation).

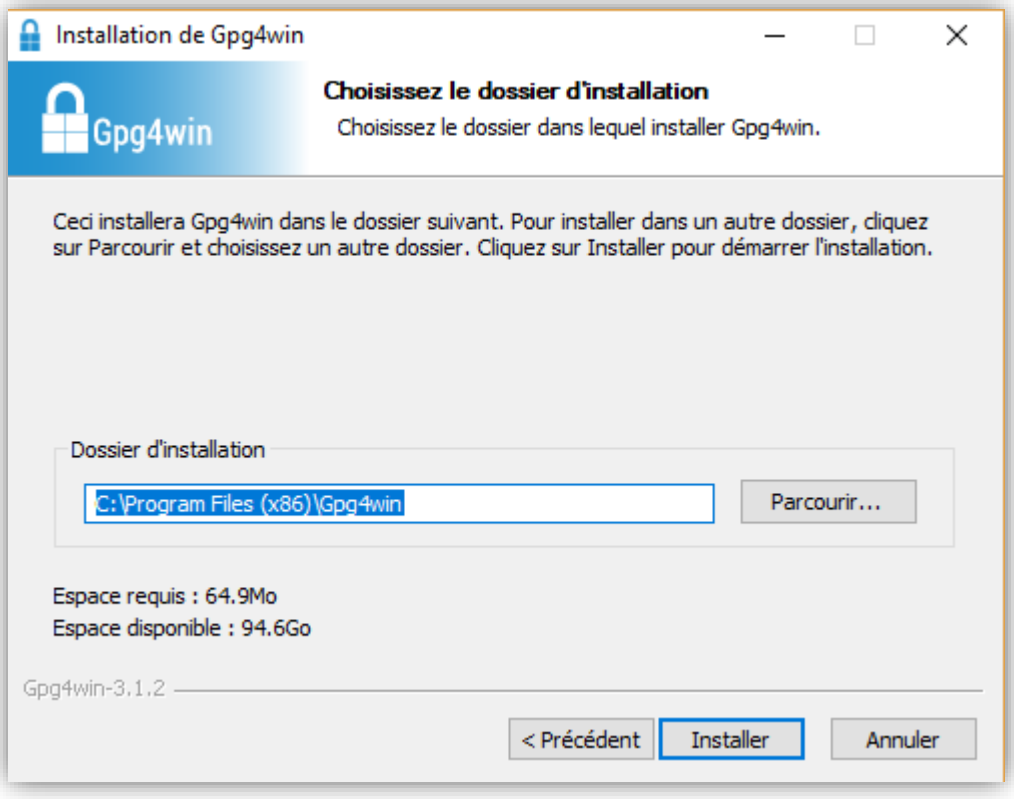


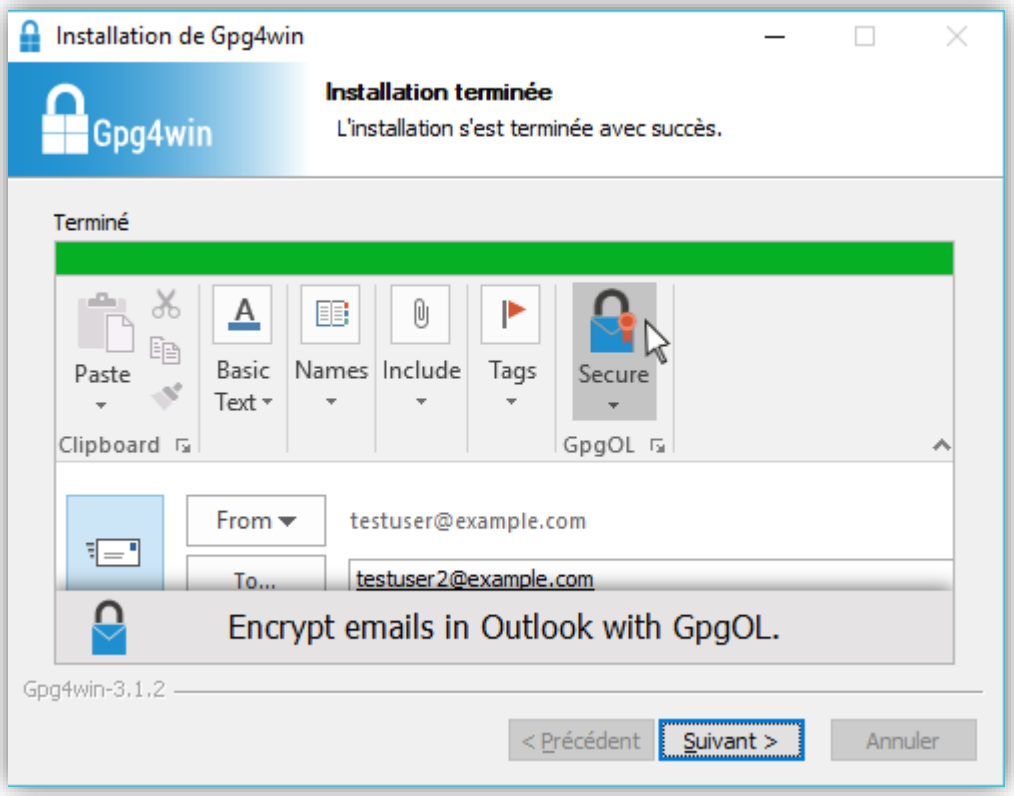
Ne cochez que les deux options (GPA et GpgEx) suivantes :

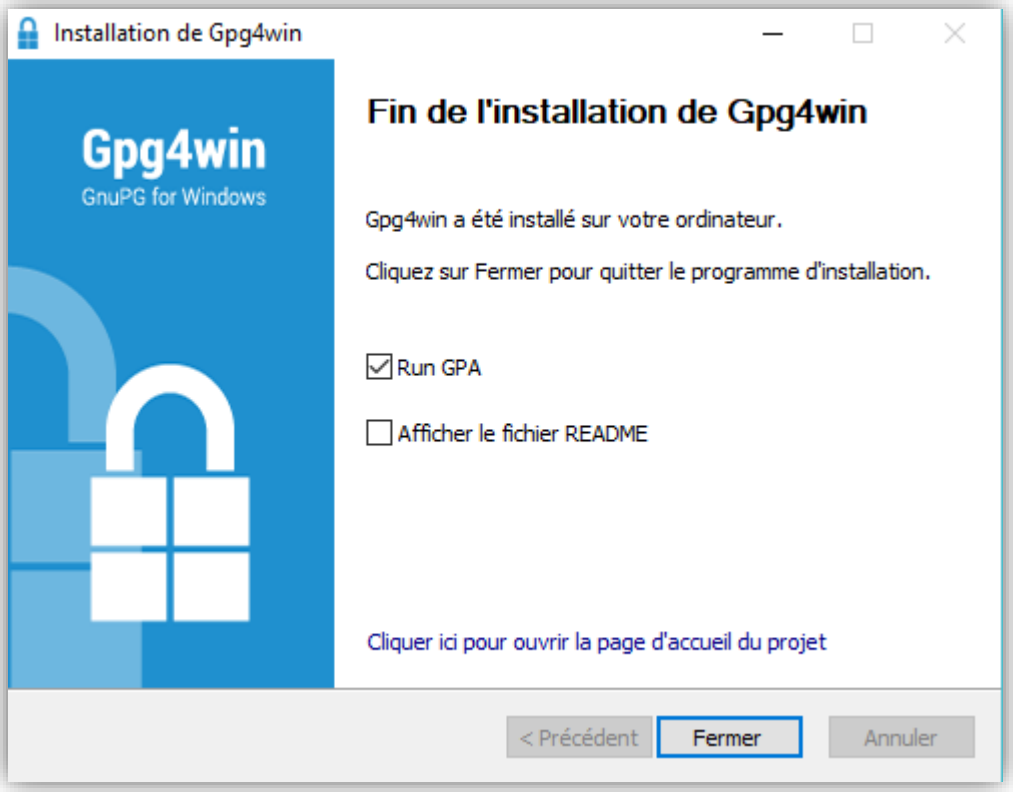


Puis cliquer sur le bouton Suivant

Cliquer ensuite sur le bouton Installer.





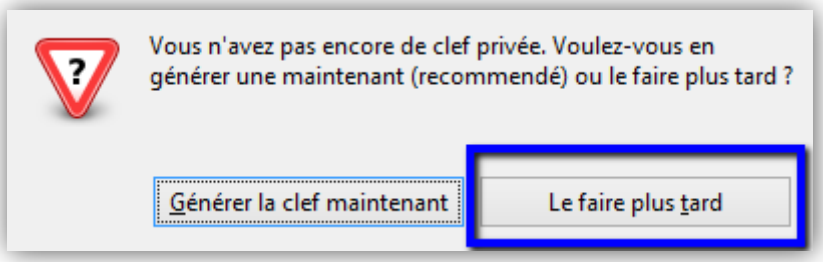


Si vous effectuez une nouvelle fois l'installation, vous serez invité(e) à redémarrer votre poste.

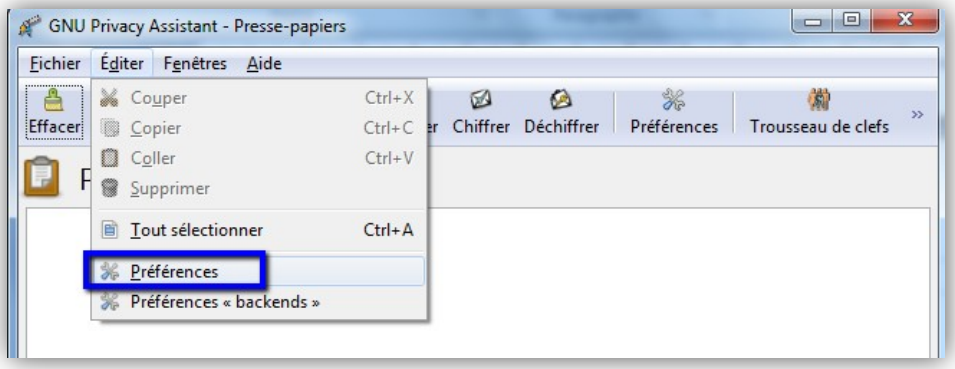
2 Paramétrage après installation

Après installation, lancer l'assistant GPA : 

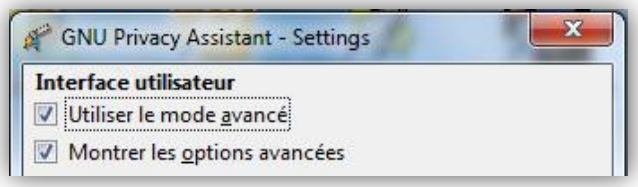
L'application va vous demander de générer une clé au démarrage :



Cliquer sur « Le faire plus tard » afin de pouvoir spécifier les caractéristiques des clés.
Aller ensuite dans le menu « Éditer » et choisir « Préférences » :

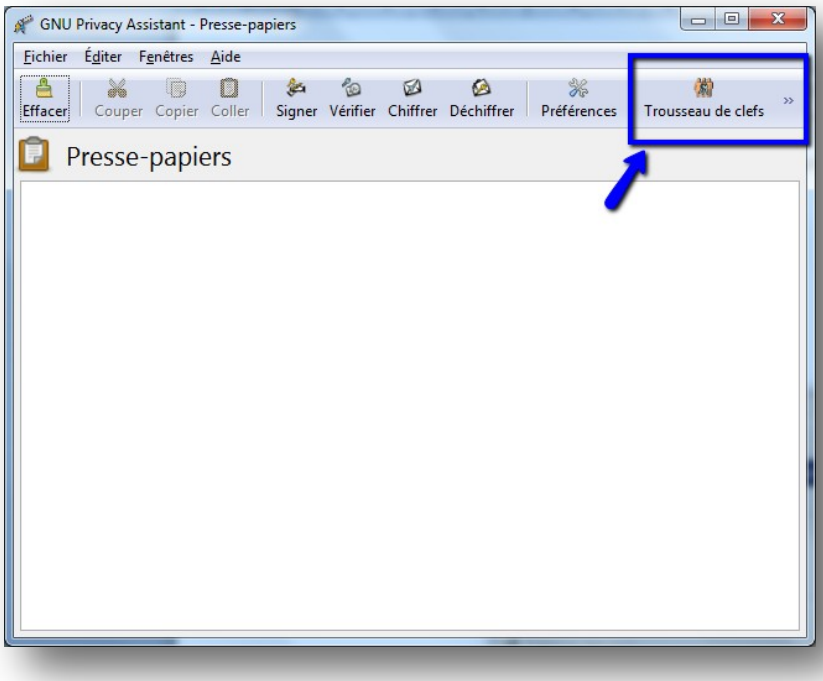


Il faut cocher les 2 cases à cocher :



Puis cliquer sur le bouton « Appliquer ».

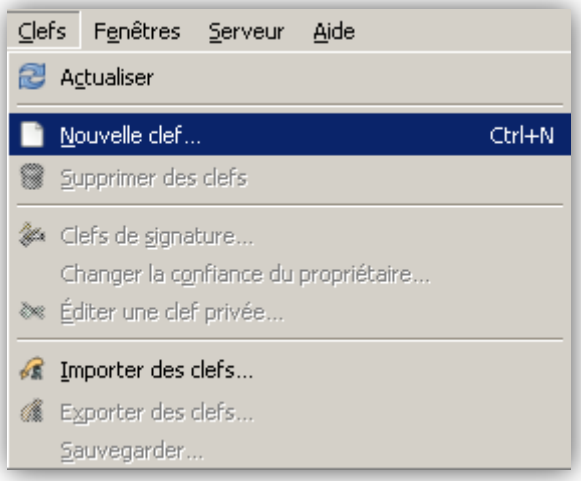
Lors des lancements ultérieurs, l'application s'ouvre sur la page par défaut suivante :



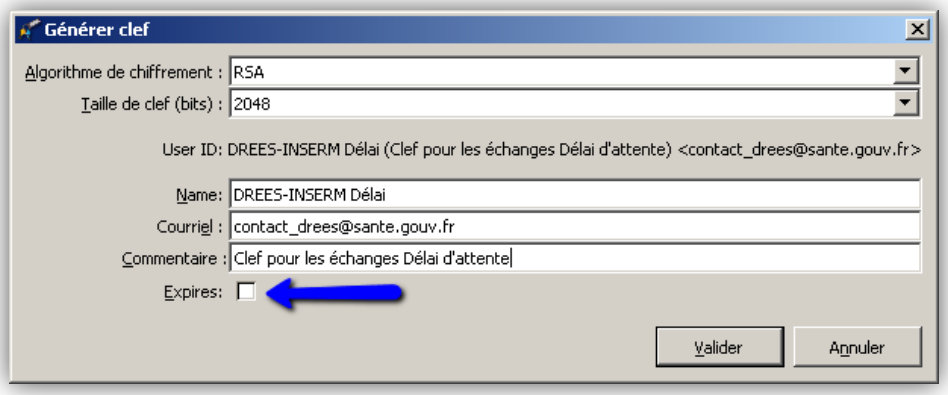
Il suffit de cliquer sur le bouton « Trousseau de clefs » pour la gestion des clés.

3 Génération d'une clé

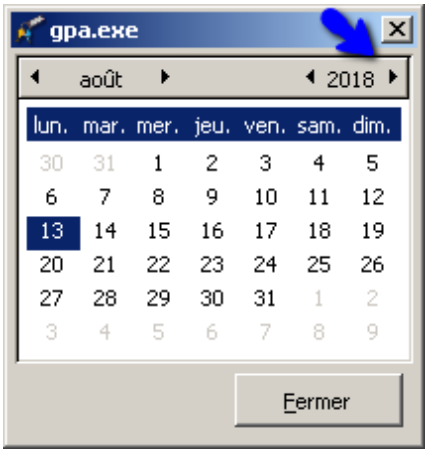
Dans le menu, cliquer sur Clefs :



Cliquer sur l'option « Nouvelle clef ».
Une nouvelle fenêtre apparaît :

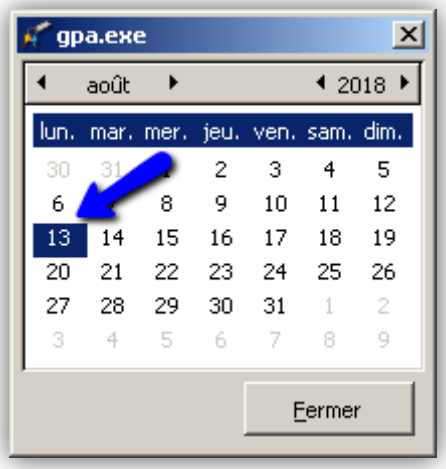


Renseigner les champs et cliquer à la fin sur la case à cocher « Expires » qui ouvrira la fenêtre de spécifications sur les clés :

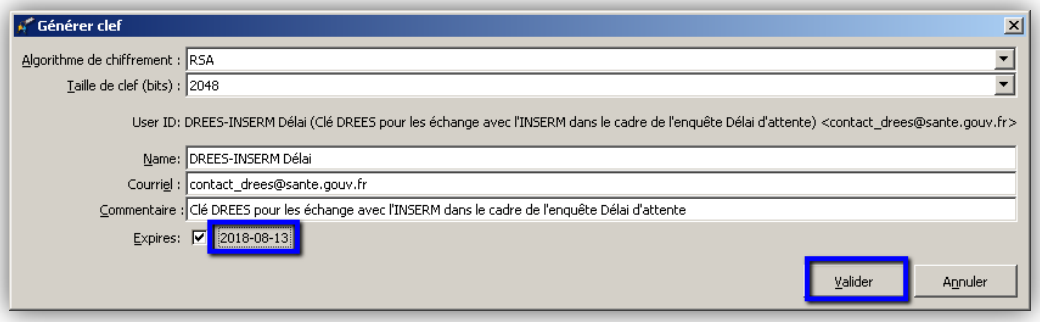


Cliquer sur la petite flèche pour faire défiler les années. Si vous générez la clé « maître » ajouter 10 années, tandis que pour **une clé de chiffrement vous devez ajouter 3 années**.

Pour valider, il faut double-cliquer sur une date :

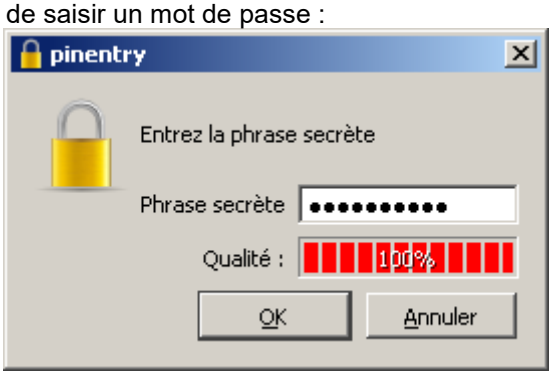


Enfin cliquer sur « Fermer ».
Pour finir il faut cliquer sur le bouton « Valider » :

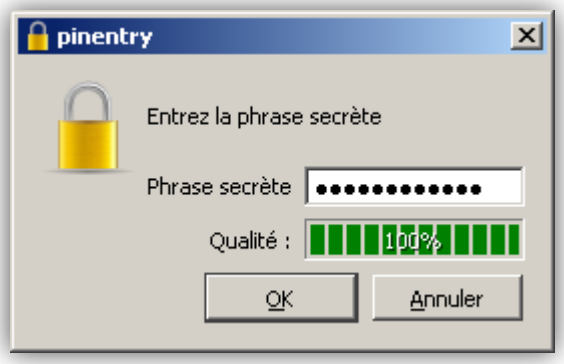


Vérifier que la date que vous avez choisie figure bien à côté de la case à cocher, puis valider.

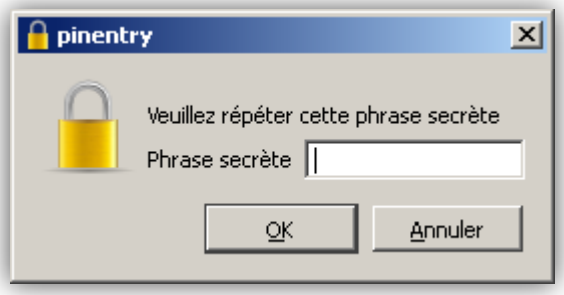
L'application va vous demander de saisir un mot de passe :



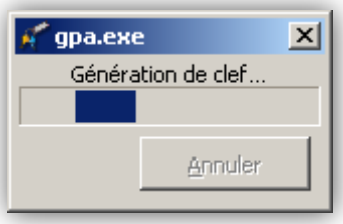
Vous devez saisir un mot de passe acceptable, c'est-à-dire que la couleur de la barre qualité doit être verte au finale :



L’application vous demande de ressaisir votre mot de passe :



Enfin l’application génère la paire de clés.

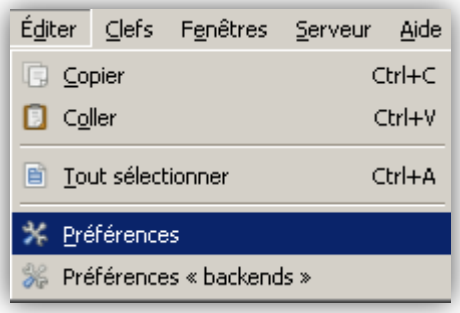


Mémoriser ou stocker le mot de passe (ailleurs que sur le poste de travail) afin de le retrouver facilement le moment venu

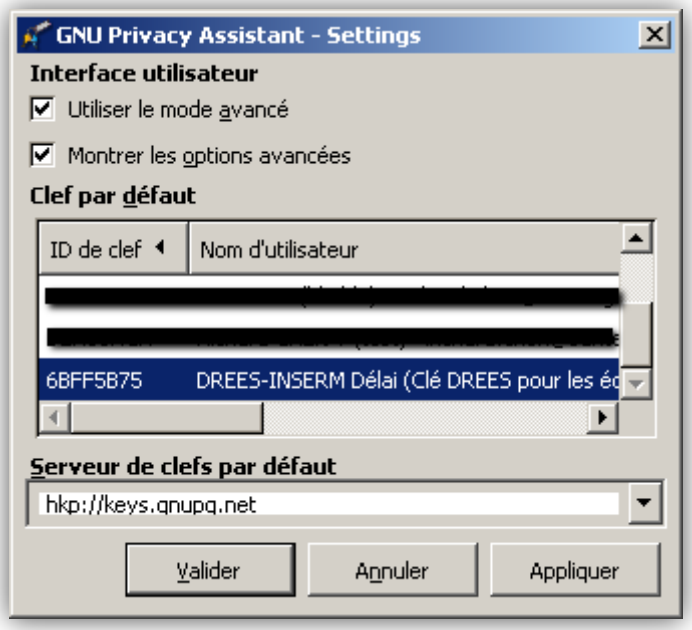
4 Signature d'une clé

4.1 Première étape : Paramétrer la clé maître comme clé par défaut

Si vous êtes administrateur des clés, une fois votre clé « maître » générée, il faut le définir comme la clé par défaut.
Pour cela il faut aller dans le menu « Éditer » et l'option « Préférences » :

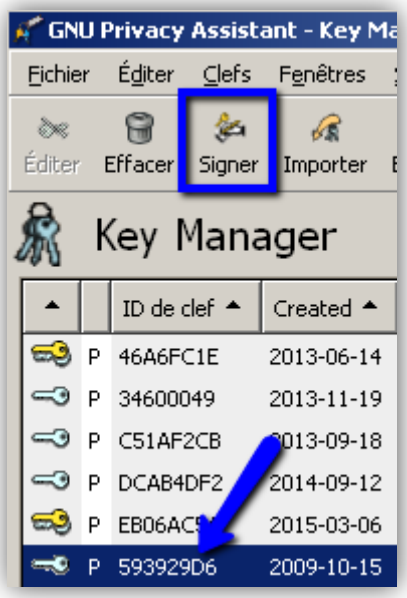


Choisir la clé « maître » puis cliquer sur le bouton « Appliquer » ou « Valider » :

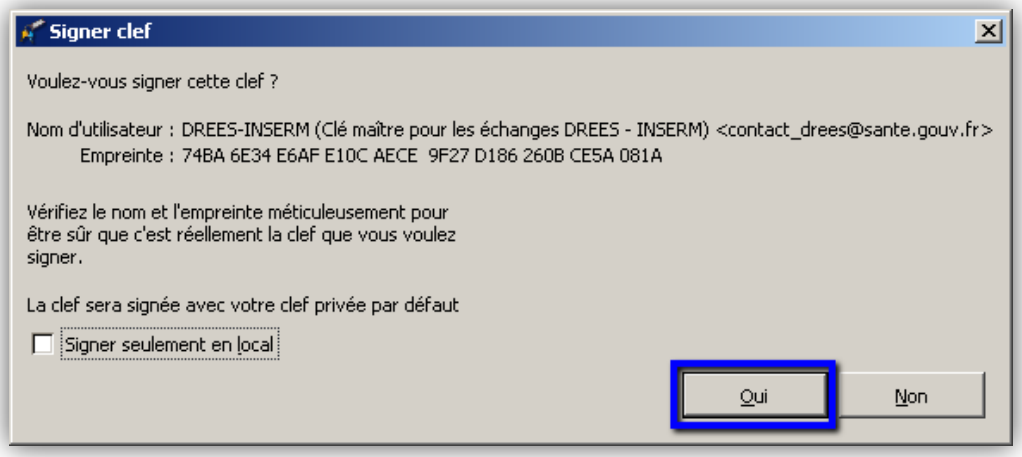


4.2 Deuxième étape : signer la clé de chiffrement

Avant de transmettre une clé publique de chiffrement, il faut la signer auparavant avec la clé « maître ». Pour cela, sélectionner la clé à signer, puis cliquer sur le bouton « Signer » :



Cliquer sur « oui » puisque vous avez paramétré votre clé « maître » comme clé par défaut :



Vous devez alors saisir votre mot de passe correspondant à votre clé « maître ».

4.3 Troisième étape

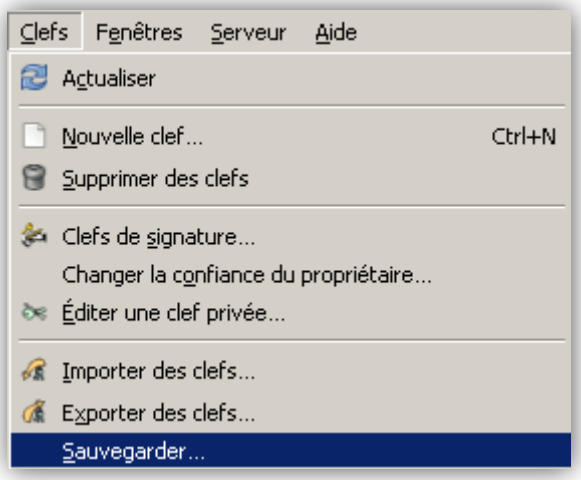
Si vous n'êtes pas l'administrateur ou si vous avez une double casquette, pensez à remettre votre clé de chiffrement par défaut en réalisant les opérations de la première étape.

5 Sauvegarde d'une paire de clé

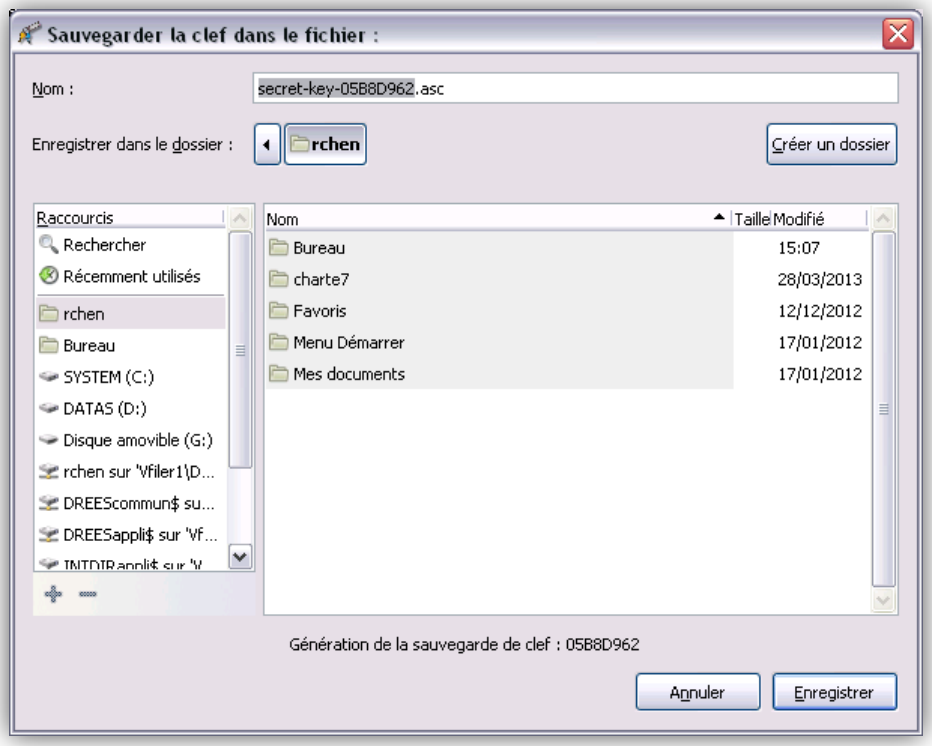
Attention ne jamais communiquer votre clé secrète !

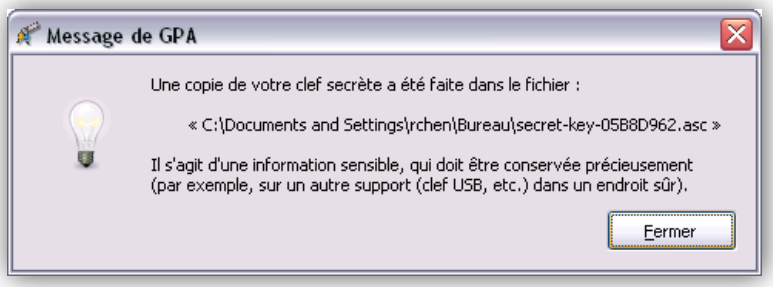
Attention : sauvegarder permet de stocker dans un support sûr votre clé publique et votre clé privée. Si vous souhaitez transmettre une clé, il faut choisir l'option « Exporter des clefs… »

Pour sauvegarder une paire clés, sélectionner une clé, puis dans le menu « Clefs » , sélectionner l'option « Sauvegarder… » :



Choisir le lieu de stockage puis cliquer sur le bouton « Enregistrer » :

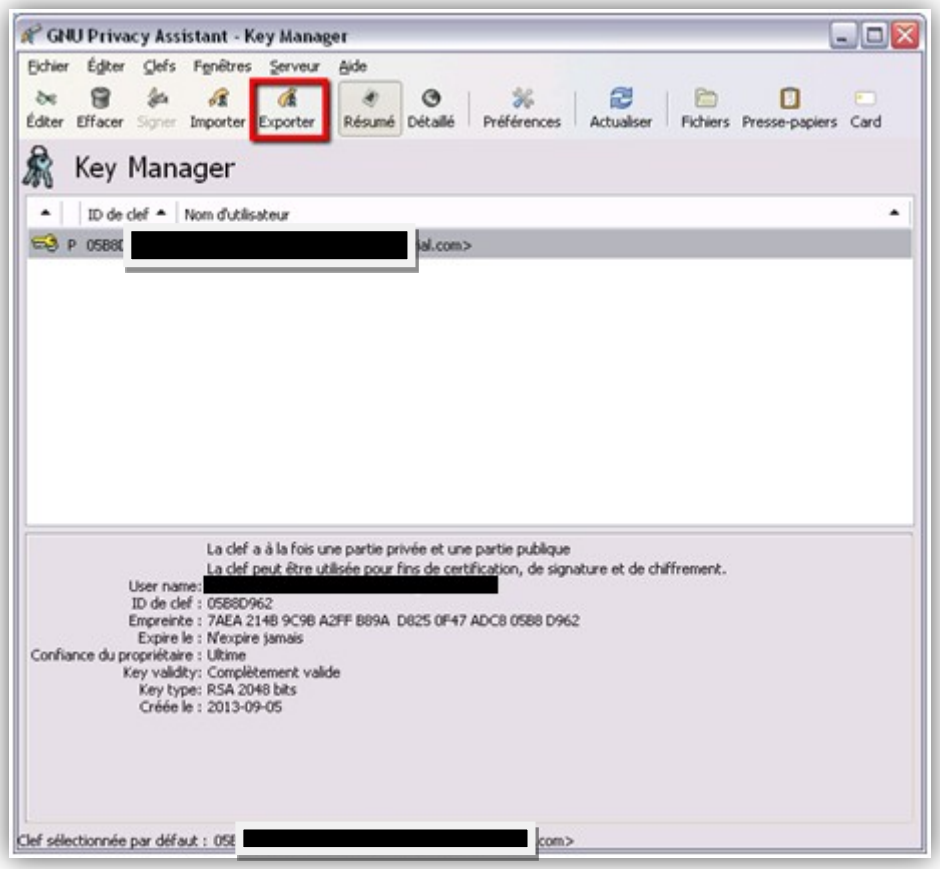




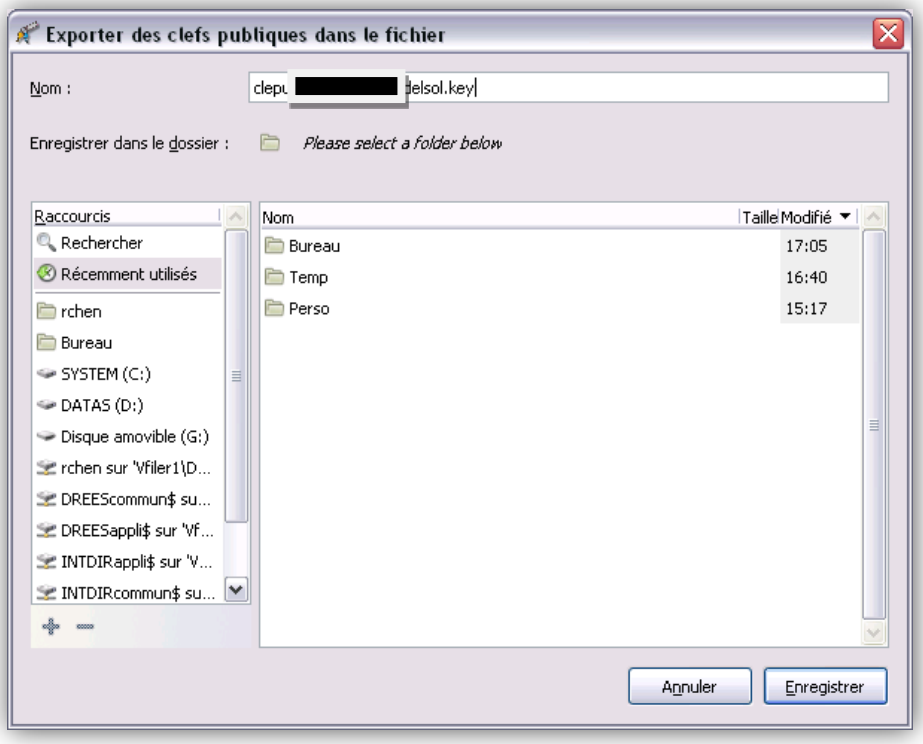
Votre clé publique et votre clé privée viennent d'être créées.

6 Exporter une clé publique pour la transmettre

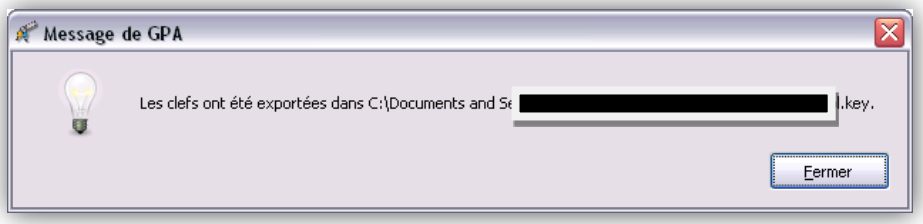
Sélectionner votre clé, puis cliquez sur « Exporter »:



Choisir le répertoire de sauvegarde et saisir un nom pour la clé :



Puis enregistrer.

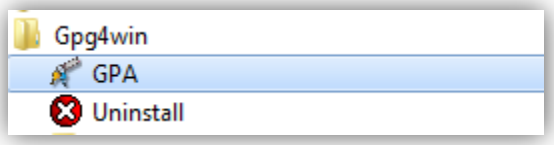


Il ne vous reste plus qu'à le communiquer la clé publique via votre messagerie (si votre clé a été signée par la clé « maître »).

Attention ne jamais communiquer votre clé secrète !

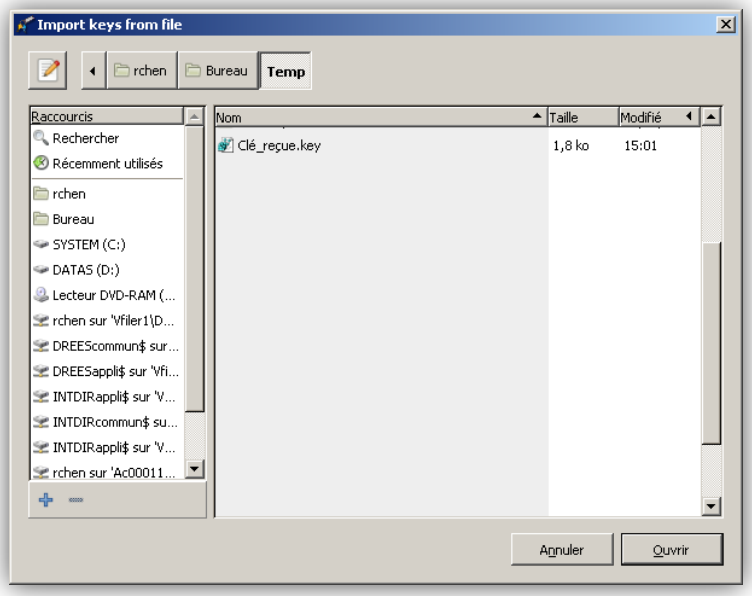
7 Importer une clé

Démarrer le gestionnaire de clé :

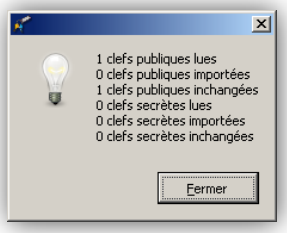


Cliquer ensuite sur l'icône « Importer » :

Chercher dans le répertoire la clé reçue, la sélectionner et cliquer sur ouvrir :



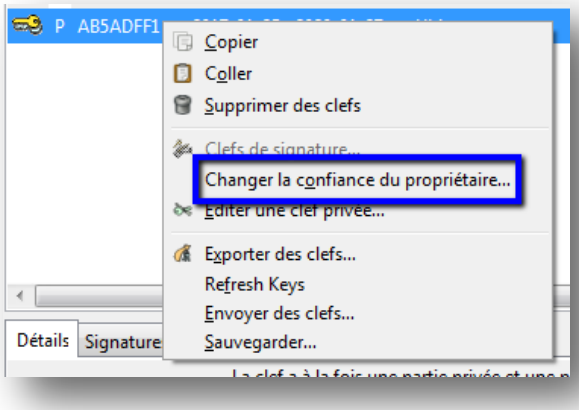
La clé a été importée



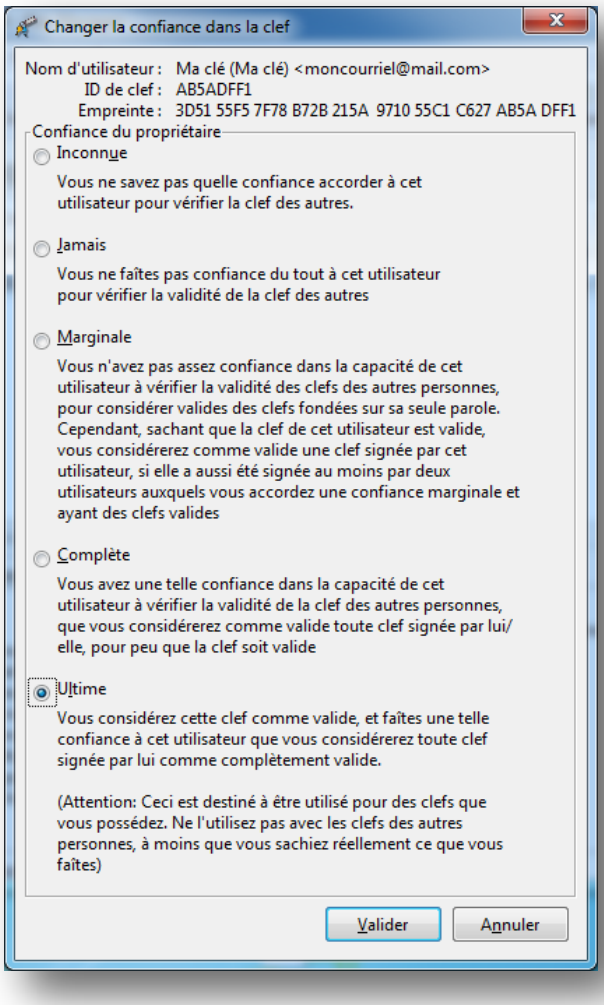
8 Modifier le niveau de confiance d'une clé

Vous devez modifier la confiance d'une clé qui vient d'être importée.

Dans le trousseau de clés, cliquer droit sur la clé concernée :



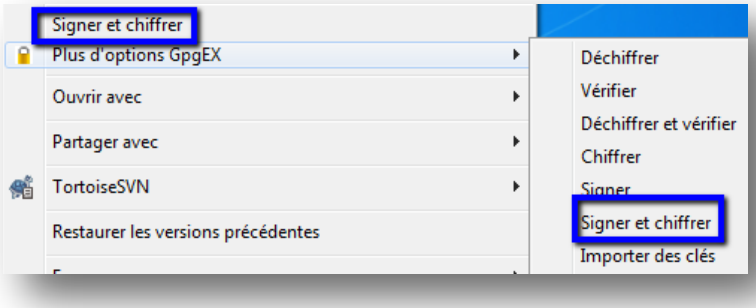
Choisissez le niveau de confiance :



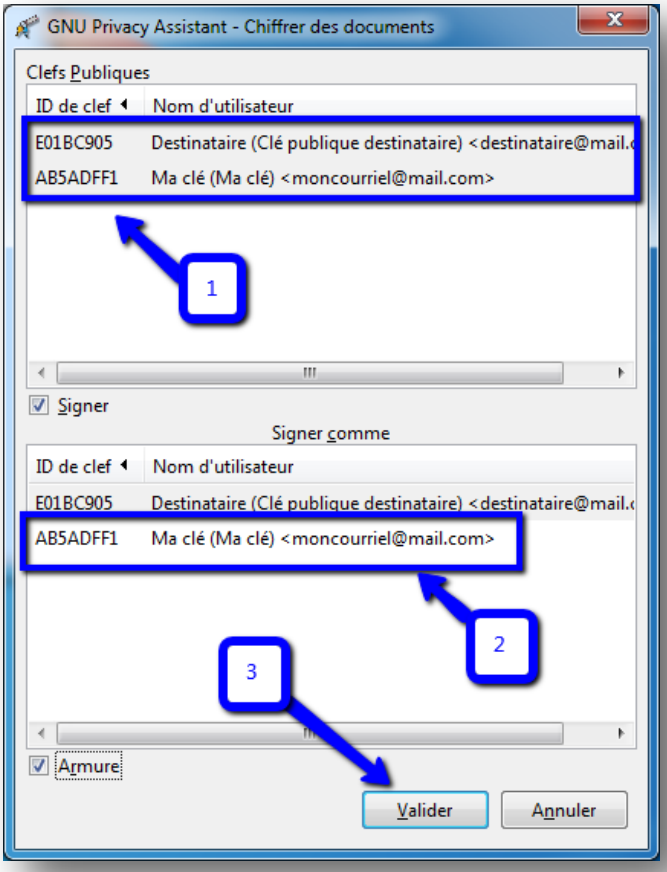
Choisissez complète (ou ultime lorsque l'échange est en main propre)

9 Chiffrer

Pour chiffrer un fichier, il suffit de faire un clique-droit sur le fichier à chiffrer :



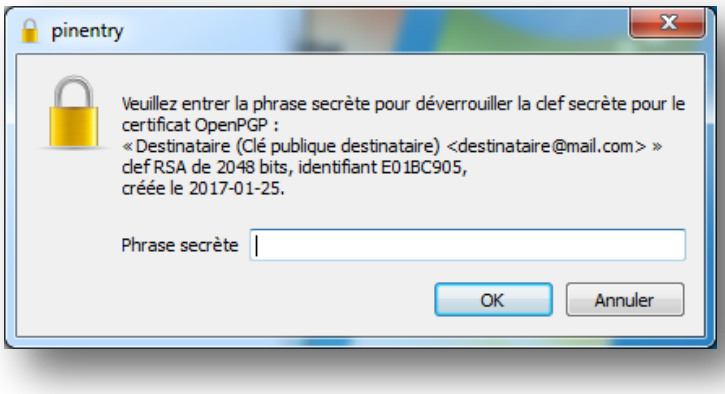
Cliquer sur Signer et chiffrer



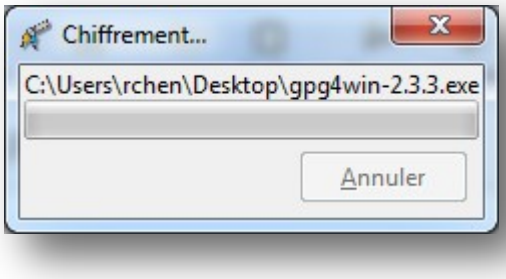
1 Sélectionner sa propre clé et celle du/des destinataire(s)

2 Sélectionner sa clé pour signer

3 Valider



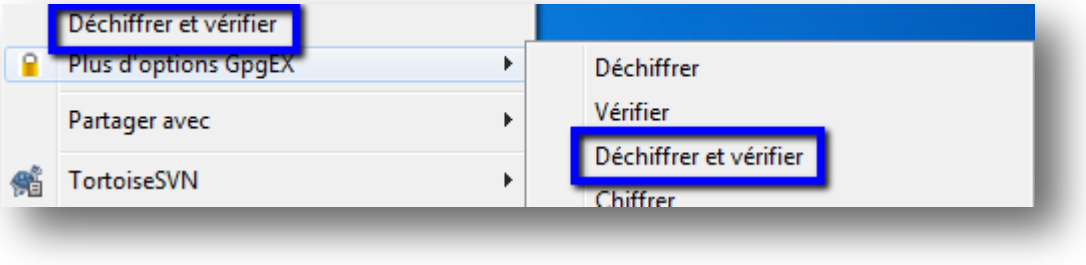
Entrer votre mot de passe



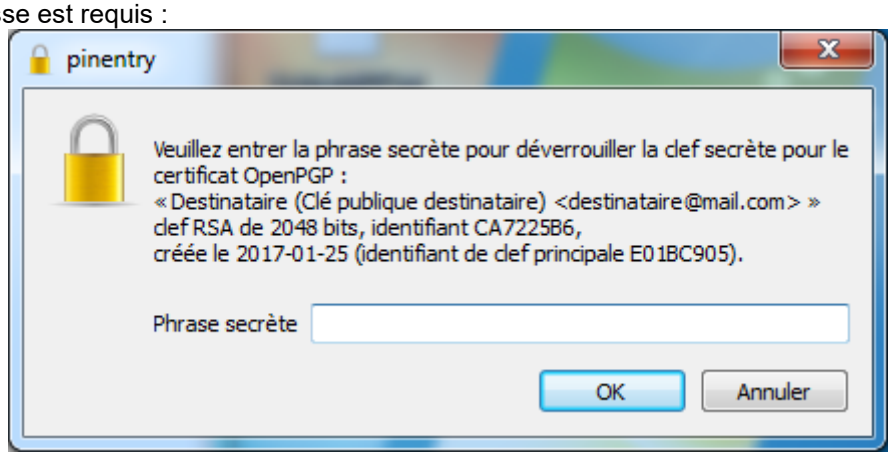
Le fichier est alors chifré

10 Déchiffrer

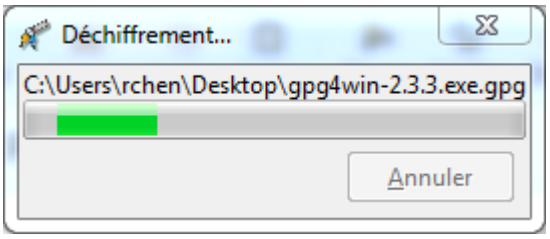
Cliquer droit sur le fichier crypté pour faire apparaître le menu contextuel. Choisir « Déchiffrer et vérifier » :



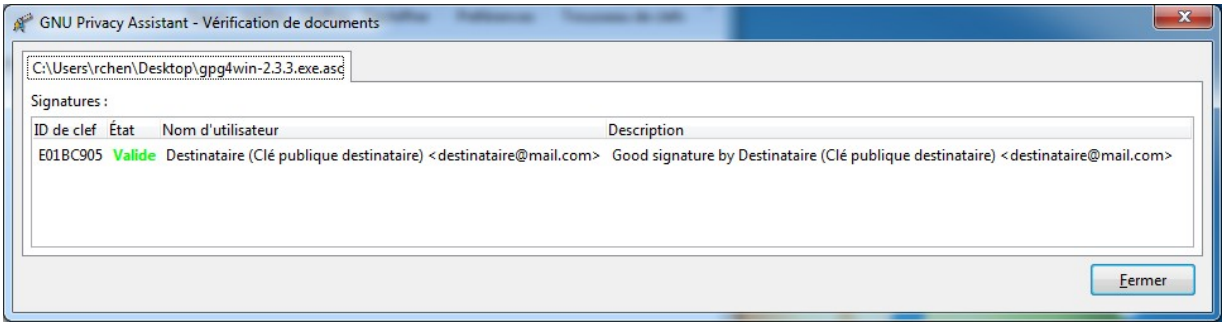
Votre mot de passe est requis :



L'application déchiffre :



Le fichier déchiffré se trouve dans le répertoire avec le fichier initial (crypté).



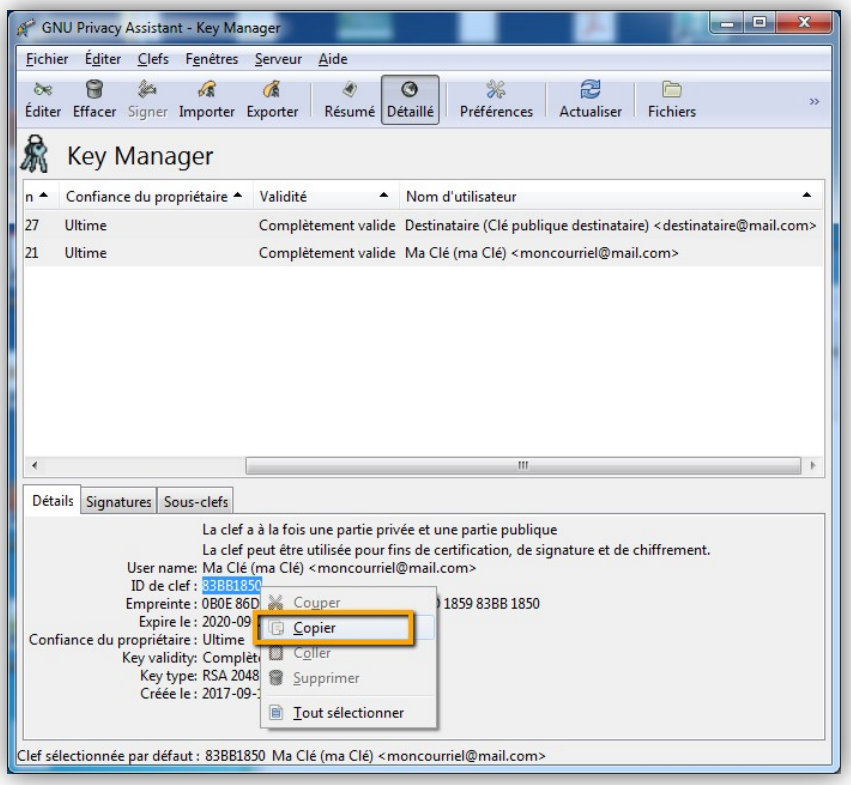
La signature est valide.

Si la signature est invalide, il est très probable que la personne qui vous a envoyé le fichier n'est pas votre interlocuteur ou vous n'avez pas encore importé sa clé publique.

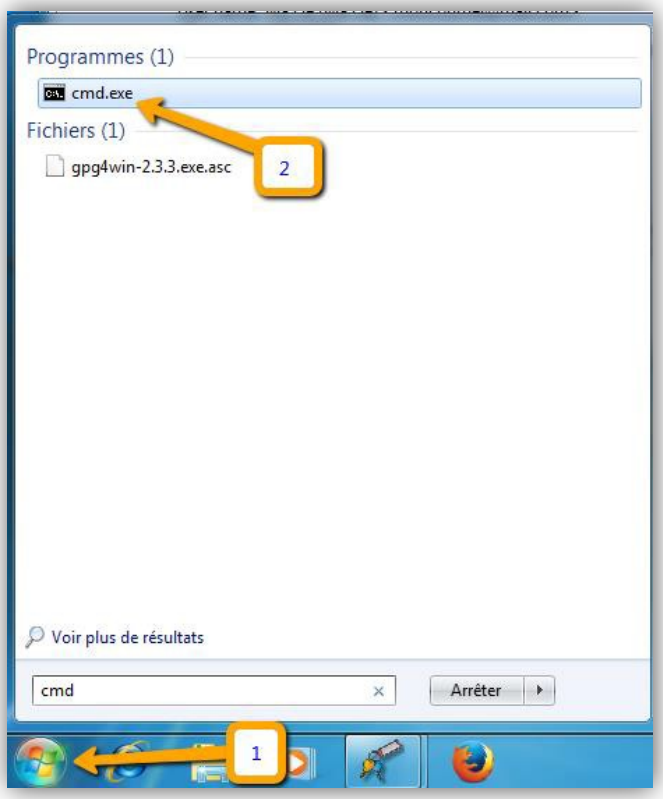
11 Révocation d'une clé

Prévoir dans quel répertoire vous voulez créer le certificat de révocation. Dans l'exemple, le certificat est créé dans le répertoire Documents de l'utilisateur.

Récupérer l'identifiant de la clé compromise en sélectionnant la clé, puis en cliquant droit avec la souris sur le champ en face de « ID de clef » et enfin copier :



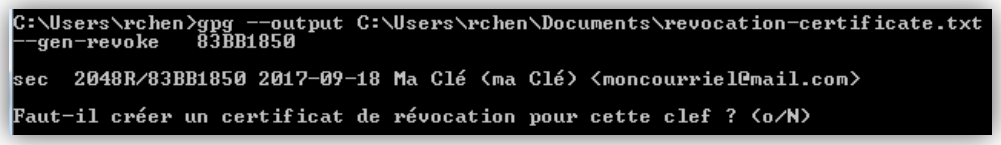
Dans le menu démarrer, procéder à la recherche comme suit en tapant « cmd » :



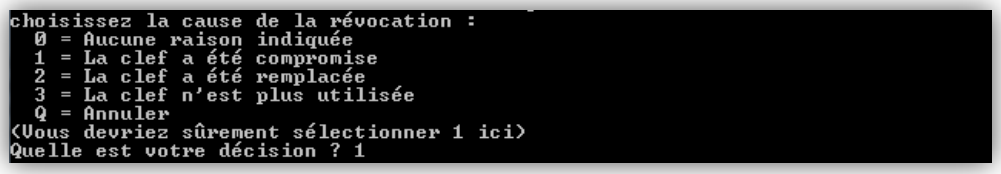
Puis entrer la commande suivante **en l'adaptant pour indiquer votre chemin complet et le nom du fichier** :

- gpg –output c:\votre chemin]\nom-fichier.txt --gen-revoke 83BB1850
  - ⇨ « c:\[votre chemin]\nom-fichier.txt » est à adapter en fonction de l'emplacement de votre répertoire.
  - ⇨ «83BB1850» est à remplacer par l'identifiant de votre clé

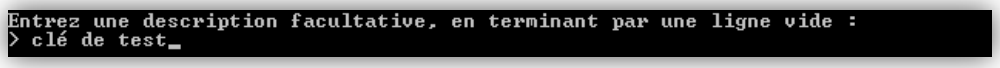
Une fois la commande saisie, taper sur la touche « Entrée » : il vous faudra alors confirmer que vous voulez bien révoquer la clé en tapant sur la touche « o » du clavier alphabétique et non le zéro :



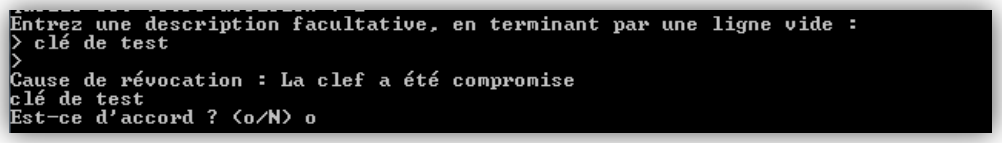
Puis indiquer le motif en choisissant dans la liste des motifs (entrer cette fois-ci un chiffre ou taper sur la touche « q » pour annuler) puis « Entrée » :



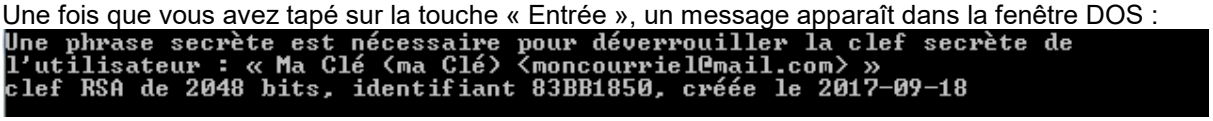
Puis enfin une description qui est facultative, puis la touche « Entrée » et **à nouveau la touche « Entrée »**.



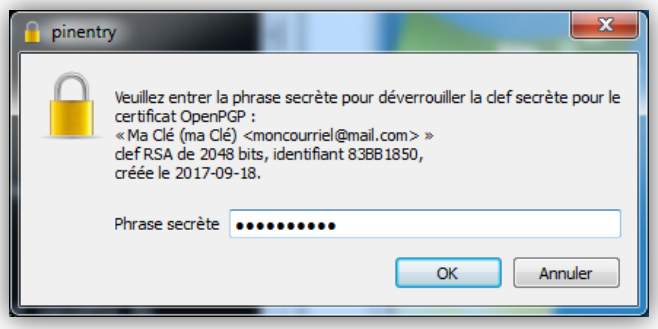
Confirmer en tapant la touche « o » du clavier alphabétique et non le zéro.



Une fois que vous avez tapé sur la touche « Entrée », un message apparaît dans la fenêtre DOS :



Qui ouvre une fenêtre applicative qui vous invite à entrer le mot de passe pour cette clé :



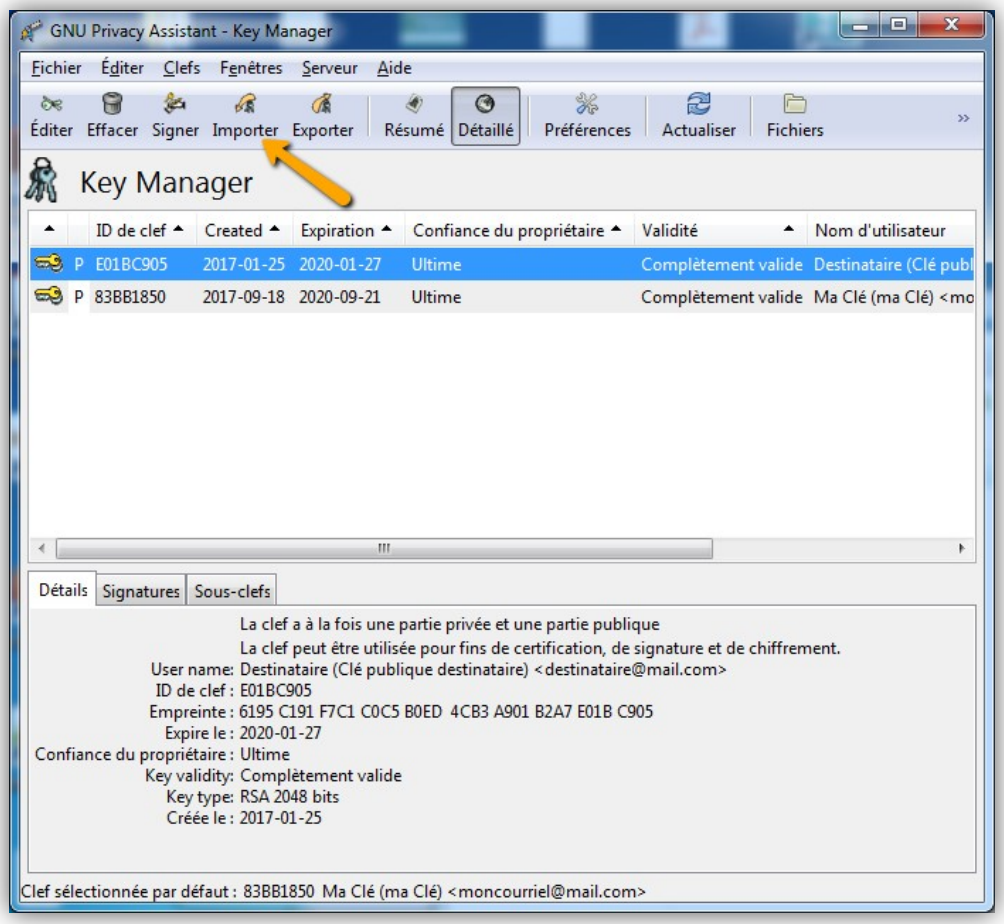
Votre certificat de révocation a été créé :

```
Une phrase secrète est nécessaire pour déverrouiller la clef secrète de
l'utilisateur : « Ma Clé (ma Clé) <moncourriel@mail.com> »
clef RSA de 2048 bits, identifiant 83BB1850, créée le 2017-09-18

sortie forcée avec armure ASCII.
Certificat de révocation créé.

Veuillez le déplacer sur un support que vous pouvez cacher ; toute personne
accédant à ce certificat peut l'utiliser pour rendre votre clef inutilisable.
Imprimer ce certificat et le stocker ailleurs est une bonne idée, au cas où le
support devienne illisible. Attention quand même : le système d'impression
utilisé pourrait stocker ces données et les rendre accessibles à d'autres.
```

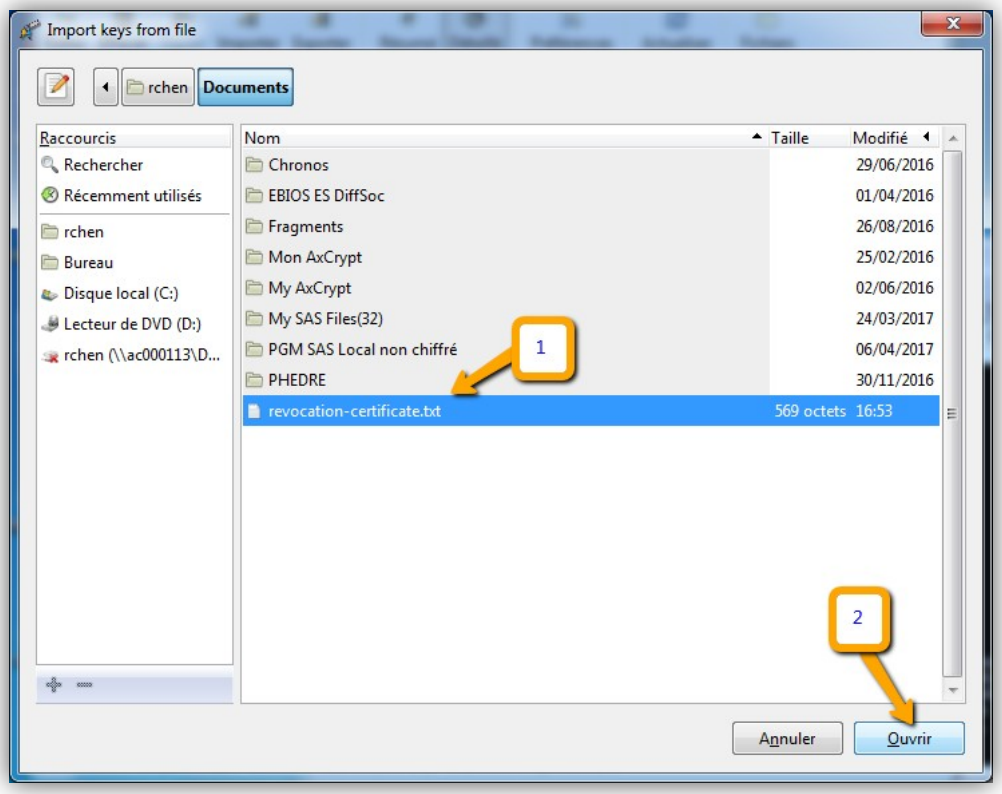
Il faut alors le transmettre à vos interlocuteurs.

12 Importer un certificat de révocation

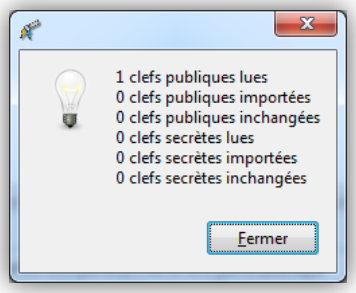
Dans l'écran du trousseau de clé, cliquer sur le bouton « Importer » :



Une fenêtre Explorateur apparaît qui vous invite à aller chercher le fichier de révocation dans le répertoire où elle a été stockée :



Le certificat a été importé :



La clé a été révoquée et cela est indiqué dans l'onglet suivant :