SOLUTION DE CRYPTAGE DES MAILS

GPG

Dérivé de PGP, GPG est un programme de cryptage libre et gratuit qui permet à ses utilisateurs de transmettre des messages signés et/ou chiffrés par le biais d'un algorithme de chiffrement à clés asymétriques. En version de base, GPG ne comprend pas d'interface graphique et fonctionne uniquement en ligne de commande. C'est pour cela ils ont développé une interface graphique nommée « Winpt » sous Windows.

Agence Nationale de la Sécurité Informatique

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Gestion de document

Version	Date	Modification apportée
1.0	16/02/2007	Première version
2.0	06/02/2010	Deuxième version

Document Publique Document Interne

PLAN

1. Présentation

GNU Privacy Guard (GPG ou GnuPG) est un logiciel qui permet à ses utilisateurs de transmettre des messages signés et/ou chiffrés. Cela permet ainsi de garantir l'authenticité dans le premier cas et/ou, dans le second cas, la confidentialité du message.

GPG est un remplacement libre de la suite PGP de logiciels cryptographiques (plus précisément, de cryptographie asymétrique). Il est disponible selon les termes de la GNU GPL.

2. Fonctionnement de GPG

2.1. Le chiffrement asymétrique

La cryptographie asymétrique, ou cryptographie à clé publique, est une méthode de chiffrement qui repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée 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. Inversement, l'expéditeur peut utiliser sa propre clé privée pour coder un message que le destinataire peut décoder avec la clé publique ; c'est le mécanisme utilisé par la signature numérique pour authentifier l'auteur d'un message.

2.2. La signature numérique

La signature électronique n'est devenue possible qu'avec la cryptographie asymétrique. Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de nombres.

La signature numérique est un mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité. Un mécanisme de signature numérique doit présenter les propriétés suivantes :

- Il doit permettre au lecteur d'un document d'identifier la personne ou l'organisme qui a apposé sa signature.
- Il doit garantir que le document n'a pas été altéré entre l'instant où l'auteur l'a signé et le moment où le lecteur le consulte.

Pour cela, les conditions suivantes doivent être réunies :

1- **Authentique:** L'identité du signataire doit pouvoir être retrouvée de manière certaine.
2- **Infalsifiable:** La signature ne peut pas être falsifiée. Quelqu'un ne peut se faire passer pour un autre.
3- **Non réutilisable:** La signature n'est pas réutilisable. Elle fait partie du document signé et ne peut être déplacée sur un autre document.
4- **Inaltérable:** Un document signé est inaltérable. Une fois qu'il est signé, on ne peut plus le modifier.
5- **Irrévocable:** La personne qui a signé ne peut le nier.

3. WINPT pour Windows

3.1. Télécharger GPG/Winpt

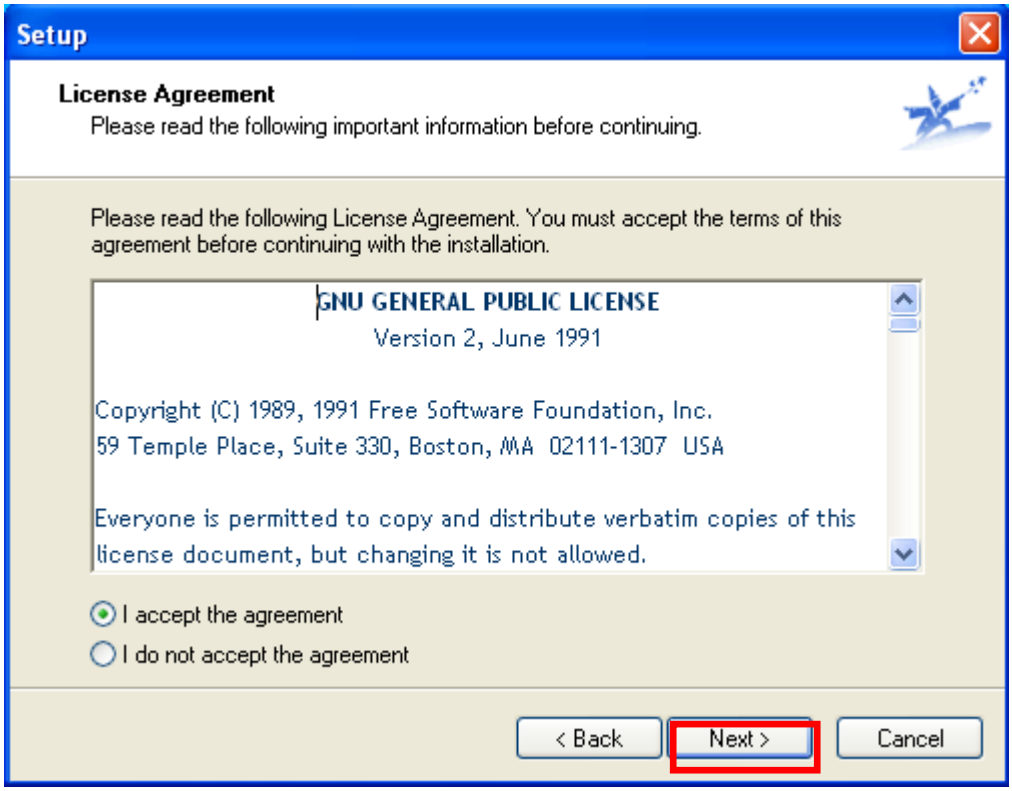
- Téléchargez la version de Winpt comme étant un paquet complet à partir de son site officiel : http://downloads.gnupt.de/gnupt.zip
- Il comprend GPG. Ce paquet va être recommandé pour tous les utilisateurs qui ne veulent pas installer l'environnement d'OpenPGP manuellement. Le forfait permet un accès pratique à vos porte-clés ainsi que la capacité de backup des clés.

3.2. Installer Winpt

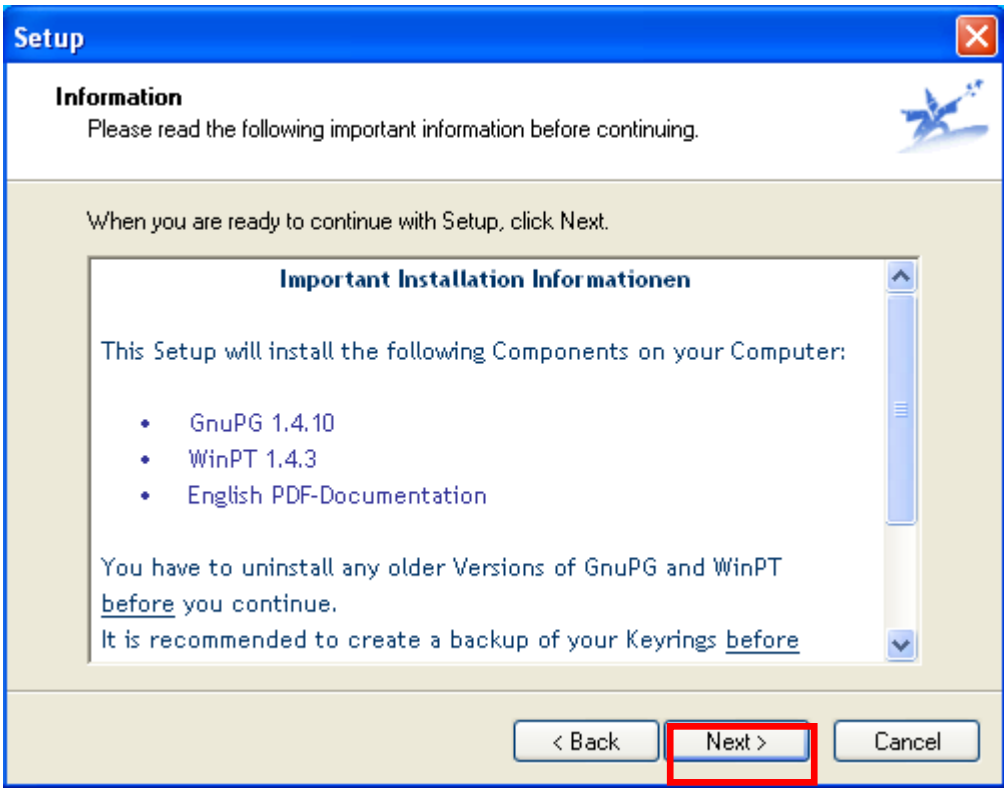
- Le processus d'installation commence, il est composé d'une suite de "fenêtres" que nous allons voir en détail.
- Cette première fenêtre permet de sélectionner la langue du processus d'installation: "**English**" doit être sélectionné. Vous cliquez sur "**OK**" ce qui vous amène à la 2ème fenêtre.

- Cliquez sur « Next »

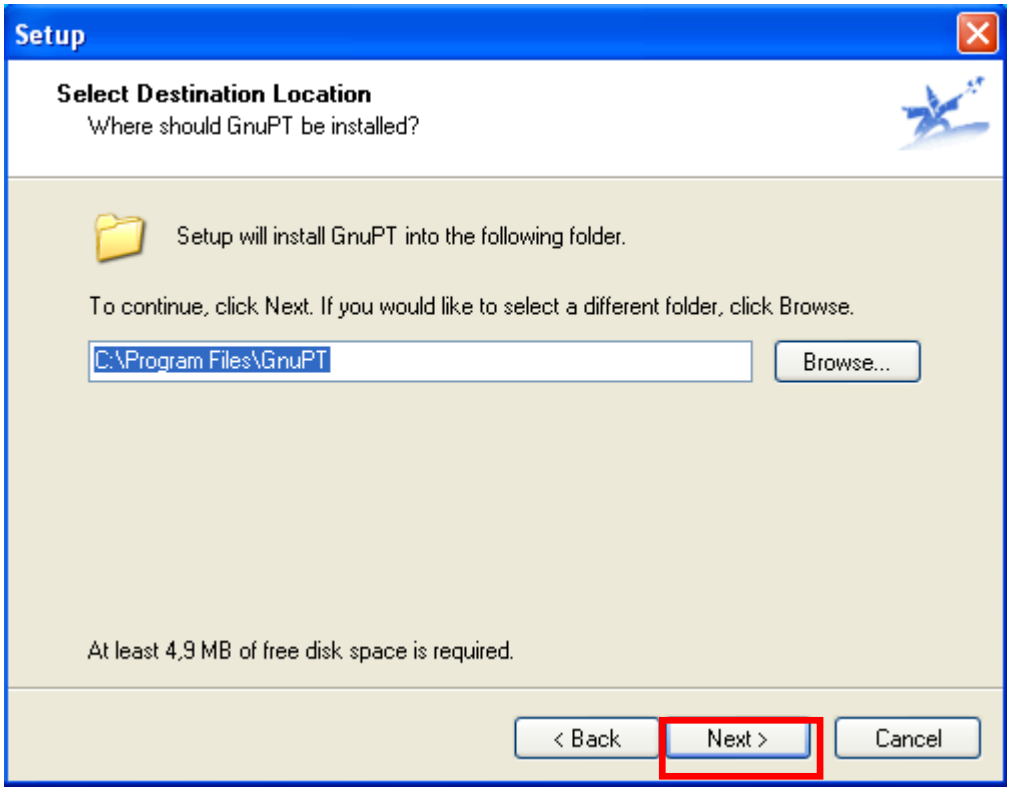
- Cette fenêtre contient les informations de licence des logiciels distribués sous “Open Source”. Acceptez la licence et cliquez sur « Next ».



- Cliquez sur « Next »

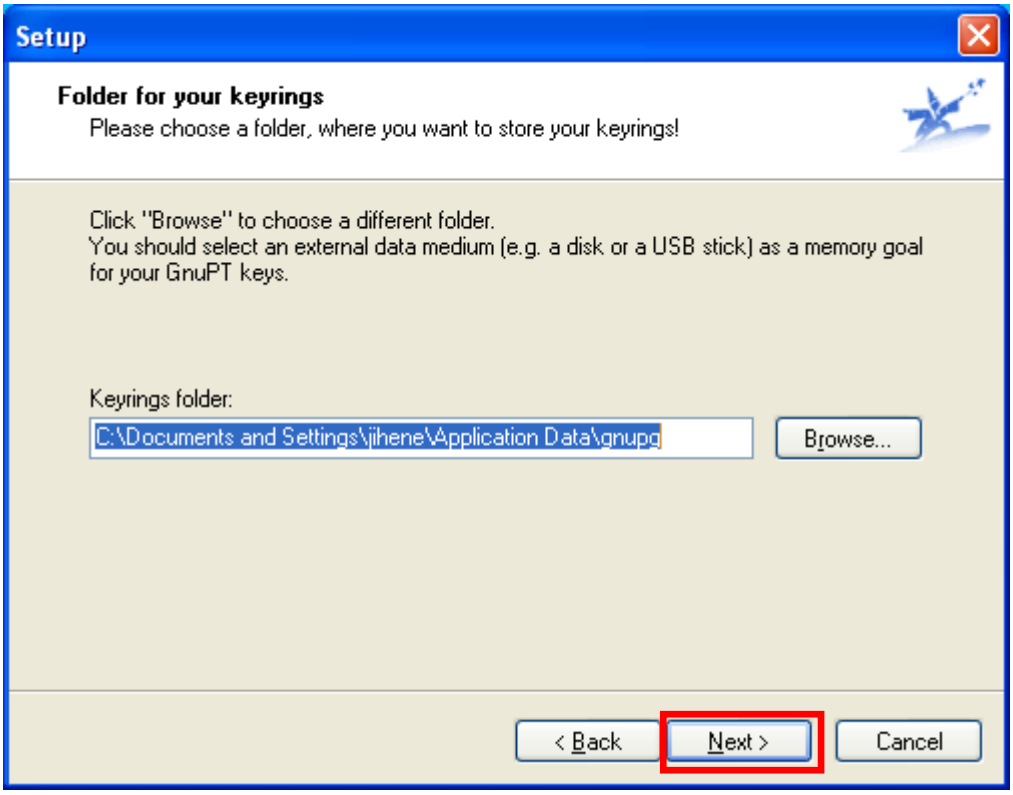


- Je vous conseille de **ne pas changer le répertoire d'installation par défaut**.

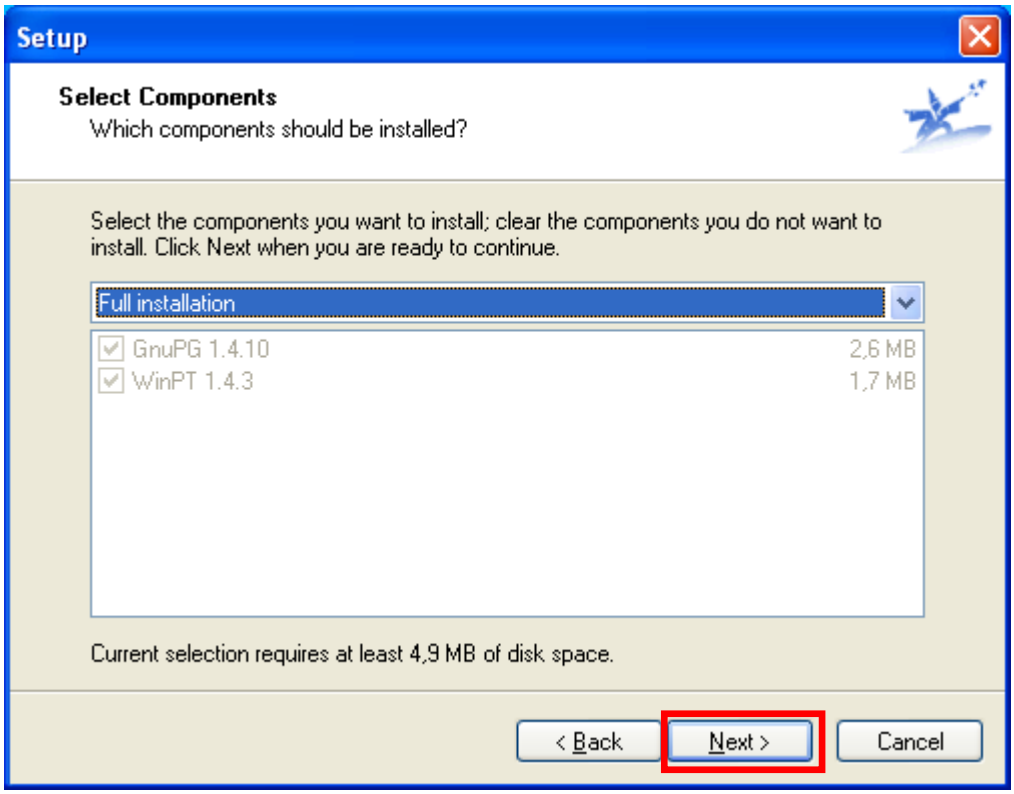


- Cliquez sur « oui » afin de créer le répertoire de Gnupt.

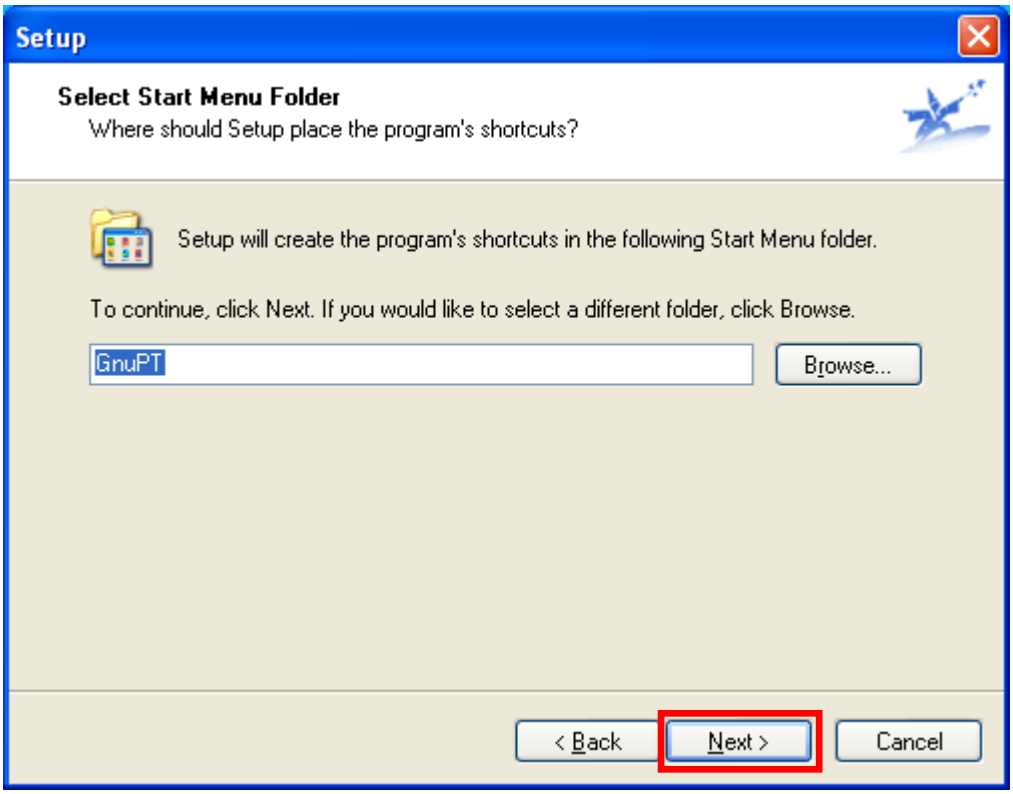
- Choisissez le répertoire où vous allez sauvegarder vos clés.



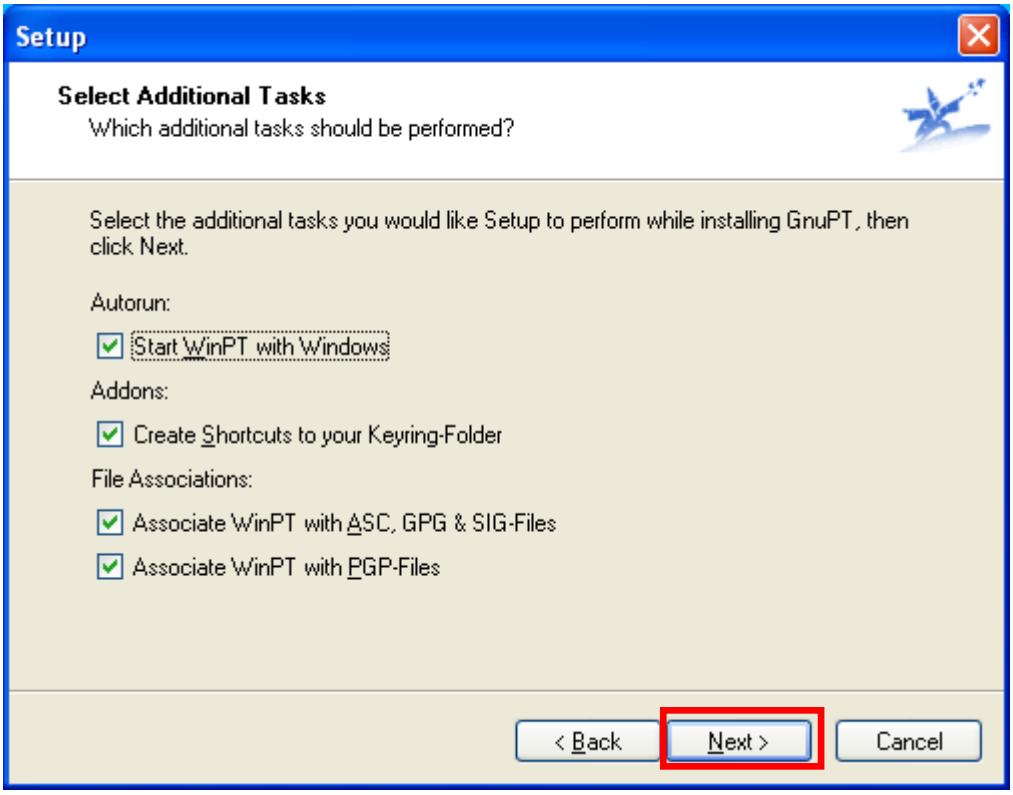
- Cette fenêtre vous permet de personnaliser les composants du programme que vous souhaitez installer. Normalement, pour une installation sous Windows (98, 2000, XP) et avec Outlook Express comme lecteur de courrier électronique, vous choisissez « Full installation ». puis cliquez sur « Next ».



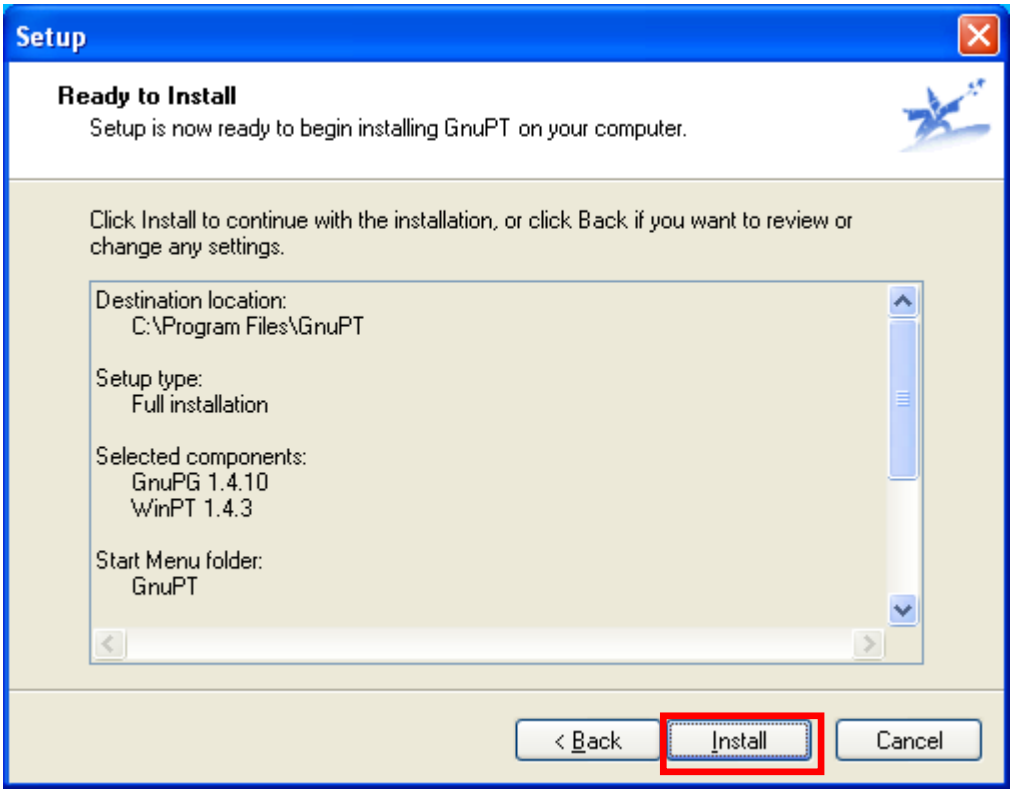
- Le programme d'installation va créer des raccourcis du programme dans le dossier suivant dans le menu démarrer. puis cliquez sur « Next ».



- Sélectionnez les tâches additionnelles que vous voulez mettre lors de l'installation GnuPT. Puis cliquez sur « Next ».



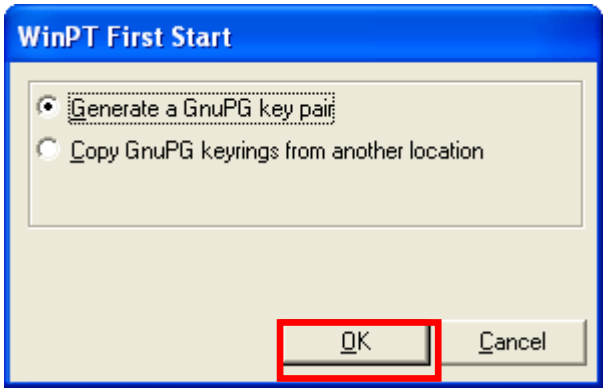
- L'installation est maintenant prête à être installer sur votre ordinateur GnuPT. Cliquez sur « Install ».



- L'installation est terminée, cliquez sur « Finish » pour quiter.

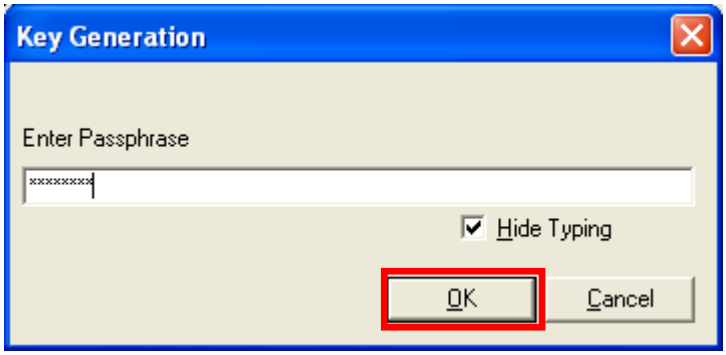
3.3. Générer une paire de clé

- Une fois l'installation est terminée, cette fenêtre apparait automatiquement pour générer une paire de clé.



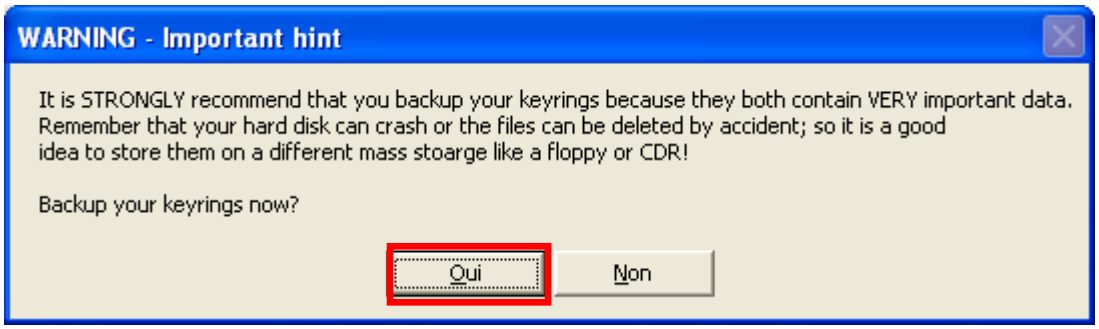
- Vous êtes inviter à saisir votre nom et votre adresse mail.

- Saisissez une passphrase forte



- Et voilà, la génération de la clé est terminé.

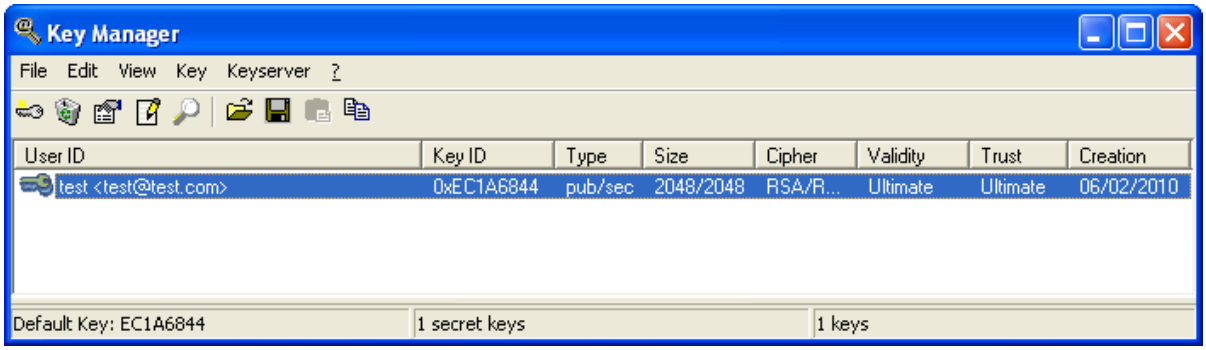
- Il est conseillé de créer un backup de vos clés sur une autre masse de stockage tel que : disquette ou un CD.. donc cliquez sur « oui ». puis sélectionnez l'emplacement de sauvegarde du backup.



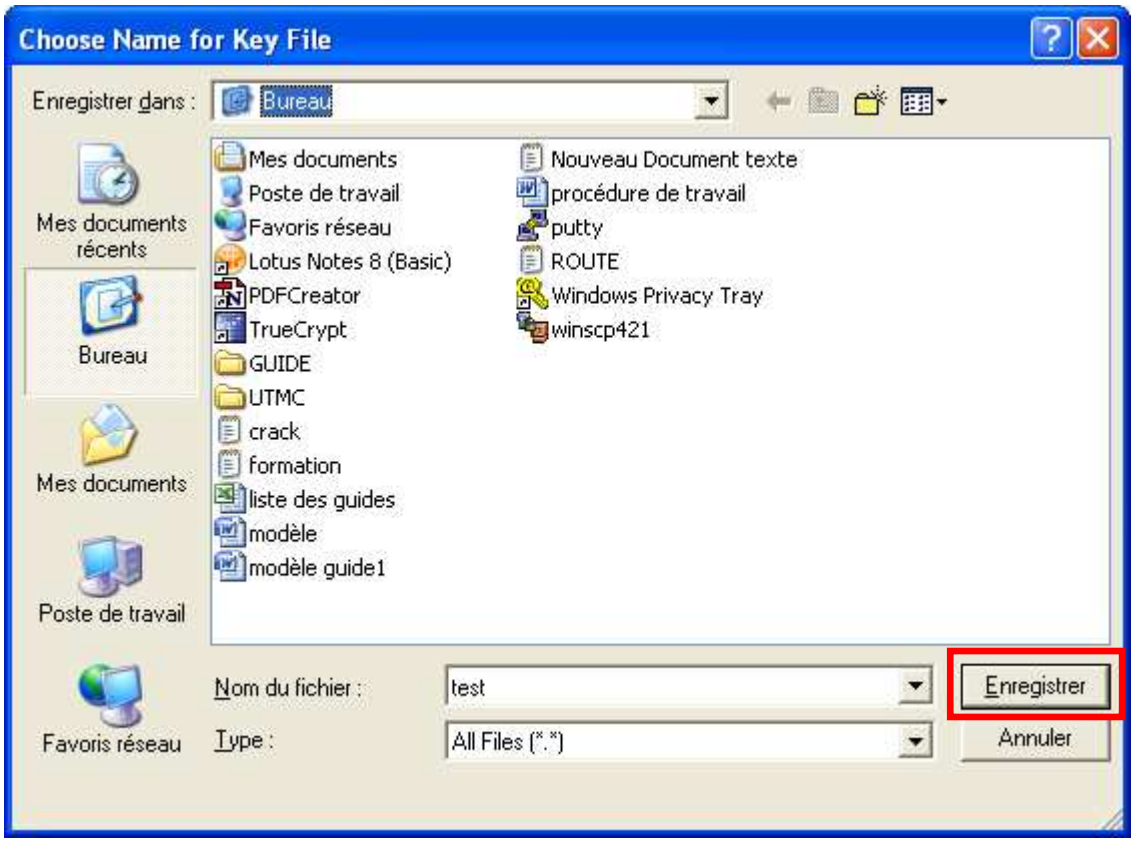
3.4. Exporter et Importer des clés publiques

a. Exporter la clé publique

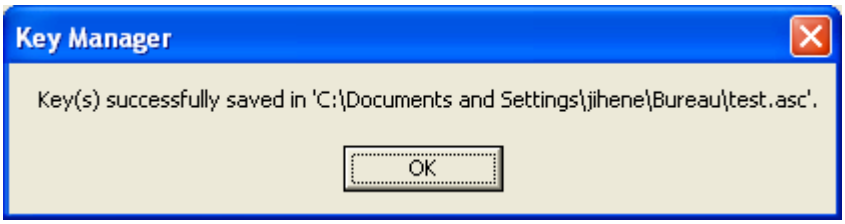
- Cliquez avec le bouton droit sur l'icône «  » dans la barre de tâche.
- Cliquez sur « ***Key manager*** ». une fenêtre s'apparaît comme suit, cliquez sur votre clé afin de l'exporter :



- Dans la barre de menu, ouvrez le menu ***« Key »***, puis choisissez ***« export »***.
- Vous devez choisir le nom et l'emplacement de votre clé comme suit, puis enregistrez :



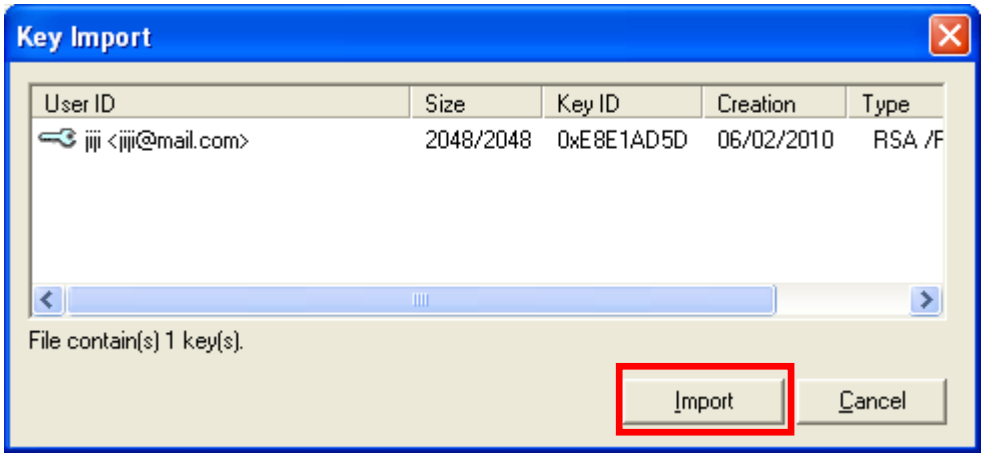
- La clé est enregistrée avec succès. Maintenant vous pouvez l'envoyer à vos correspondants qui vous allez partager avec eux des mails cryptés. Soit vous les envoyé par mail, soit de les données sur flash disc ou autre.



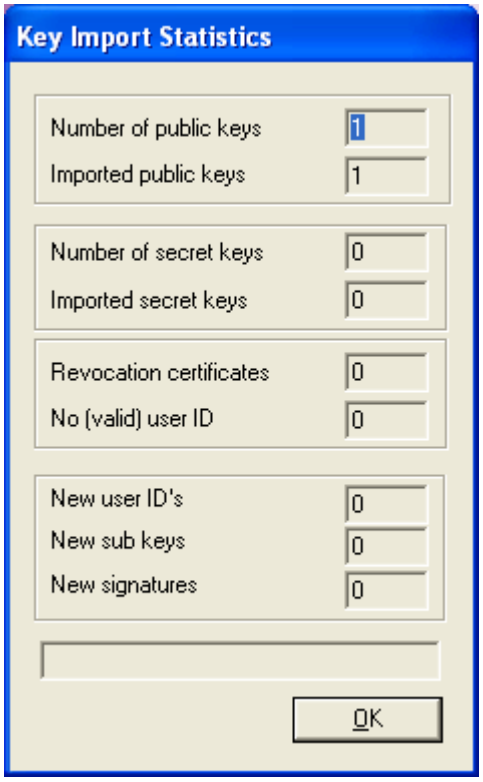
b. Importer une clé publique

Pour pouvoir encrypter des messages et les envoyer à vos correspondants, vous avez besoin de leur clé publique pour pouvoir déchiffrer les messages. Ces clés publiques doivent être importées dans le gestionnaire des clés. De la même façon que l'exportation, vos correspondants vous envoient leur clé publique via un courrier électronique. Ensuite, à l'aide du gestionnaire des clés, importez la clé publique de votre correspondant. Comme suit :

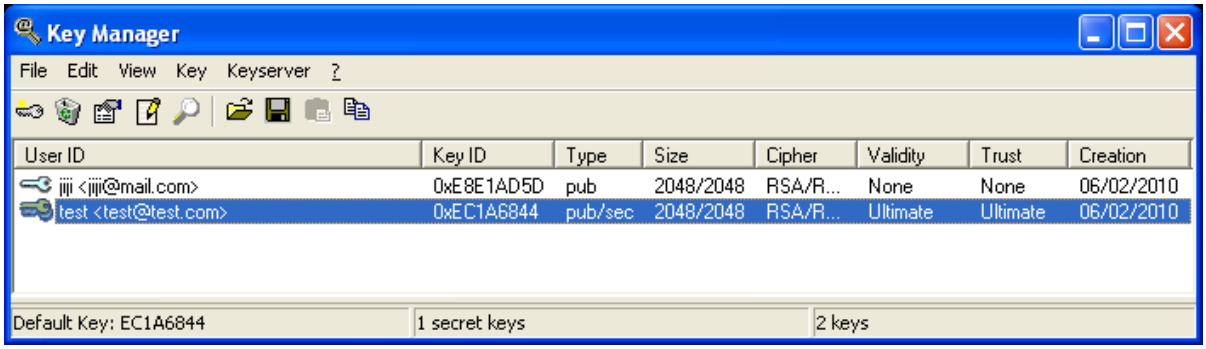
- Cliquez avec le bouton droit sur l'icône «  » dans la barre de tâche.
- Cliquez sur « ***Key manager*** ».
- Dans la barre de menu, ouvrez le menu ***« Key »***, puis choisissez ***« import »***.
- Cliquez sur le nom de la clé à importer, puis sur ouvrir
- Cliquez sur « ***import*** »



- Puis sur « ***OK*** »



- Et voilà la clé est ajoutée à votre liste.



4. Installation et configuration et utilisation d'Enigmail pour Mozilla Thunderbird

4.1. Installation

Voici une liste des fichiers que vous devrez télécharger:

- Thunderbird, le client de messagerie en version française: http://www.mozilla-europe.org/fr/products/thunderbird/
- Enigmail l'extension nécessaire au chiffrement de courriels avec Thunderbird: http://enigmail.mozdev.org/download.html

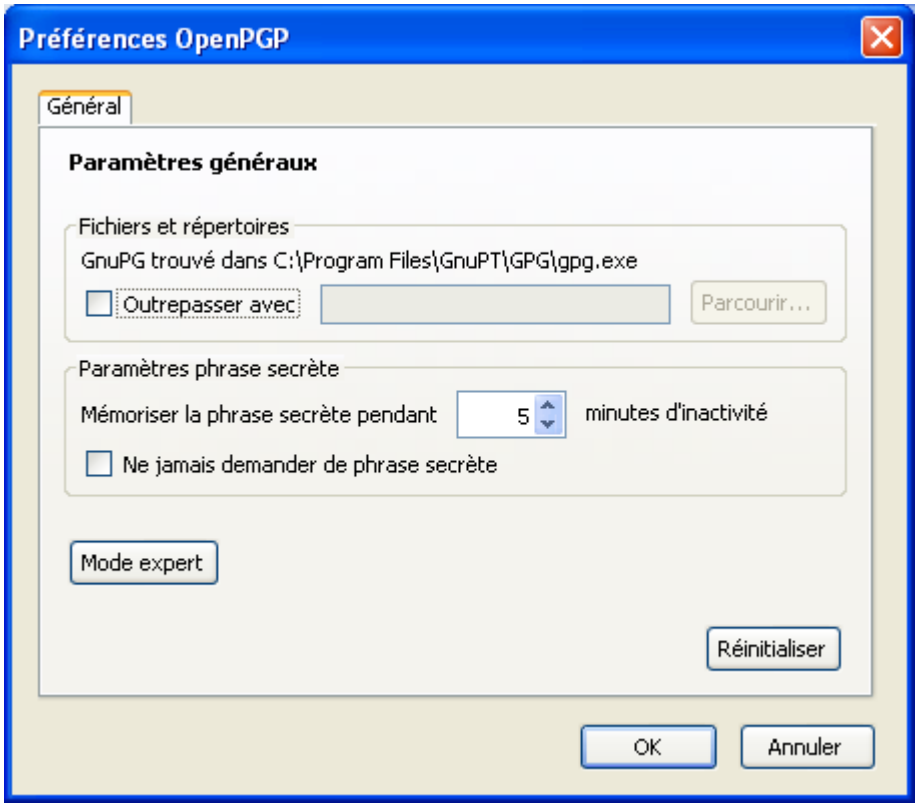
(Attention, vous devrez utilisez le bouton droit de la souris et sauvegarder les fichiers .XPI au lieu de les installer à partir du navigateur).

- Lancez Thunderbird en utilisant le raccourci créé par le programme d'installation.
- Configurez un compte de façon à pouvoir envoyer et recevoir des courriels.

4.2. Configuration

- Pour le fichier Enigmail (extension **.xpi)** suivez les étapes suivantes:

1- Ouvrez « Modules complémentaires » dans le menu « Outils » de Thunderbird, puis sélectionnez « Extensions ».
2- Cliquez sur « Installer »
3- Installez le fichier XPI correspondant, en ignorant l'avertissement concernant les signatures numériques.
4- Une fois l'extension est installée, redémarrez Thunderbird une autre fois. Le menu Enigmail devrait être visible parmi les menus disponibles
5- Ouvrez le menu « OpenPGP », puis sélectionnez « Préférences »
6- Dans l'onglet « Général », assurez-vous que le « chemin d'accès au fichier exécutable GPG » est bien ***C:\Program Files\GnuPT\GPG\ gpg.exe.***



7- Ouvrez le menu « Outils » puis sélectionnez « Paramètres des comptes » et trouvez la section correspondante au compte de messagerie électronique que vous avez configuré. Cliquez sur l'onglet catégorie « Rédaction et adressage » et décochez « Rédiger les messages en HTML ».
8- Allez dans l'onglet « Sécurité OpenPGP » et choisissez « Activer le support OpenPGP.
9- À l'aide du bouton « Choisir une clé », choisissez la clé que vous avez générée pour cette installation.

4.3. Utilisation d'OpenPGP

a. Exportation de la clé publique

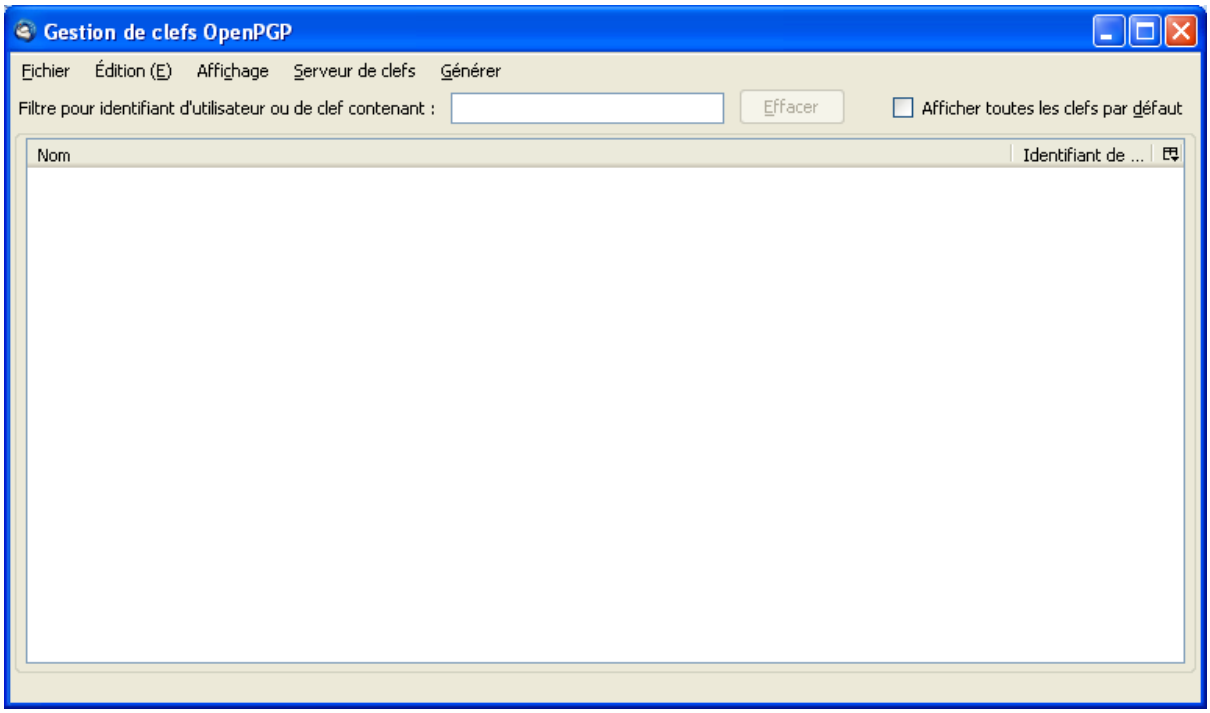
Il est maintenant temps d'envoyer votre clé publique à vos correspondants, de façon à ce qu'ils puissent vous envoyer des fichiers chiffrés et vérifier votre signature. N'importe quelle personne qui a votre clé publique peut chiffrer et vous envoyer du courrier que vous pourrez, seul, le lire en utilisant votre clé privée.

- Créez un nouveau message en appuyant sur le bouton « Écrire » ou sur les touches raccourci CTRL-M.

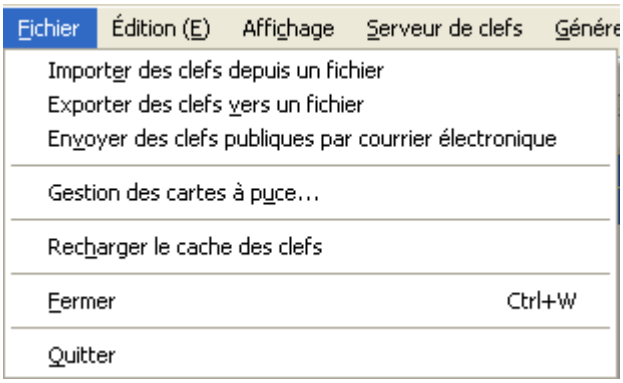
- Ouvrez le menu «OpenPGP » et choisissez « Attacher ma clé publique ».
- Lorsque votre interlocuteur recevra votre clé publique, il pourra l'importer dans son trousseau de clé.

b. Importation de la clé publique

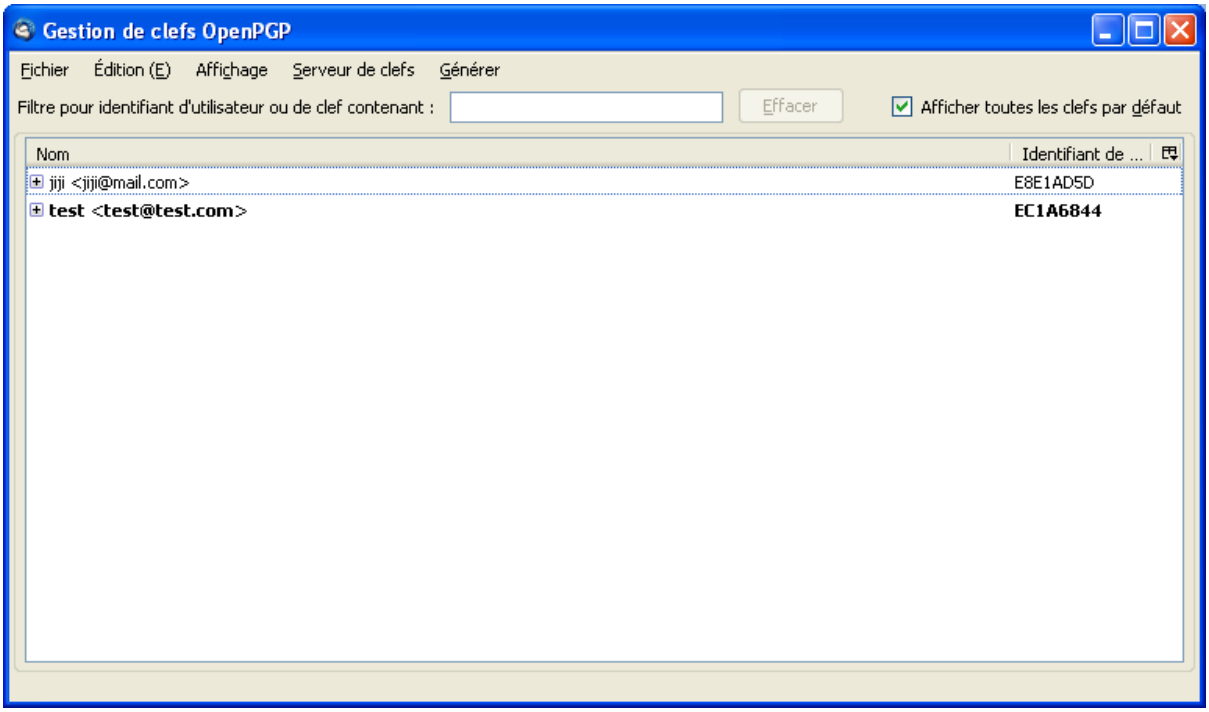
- Vous pouvez importer votre liste de clé à partir de Winpt vers thunderbird comme suit :
- Ouvrez le menu « OpenPGP » de thunderbird
- Cliquez sur « gestion de clefs ».



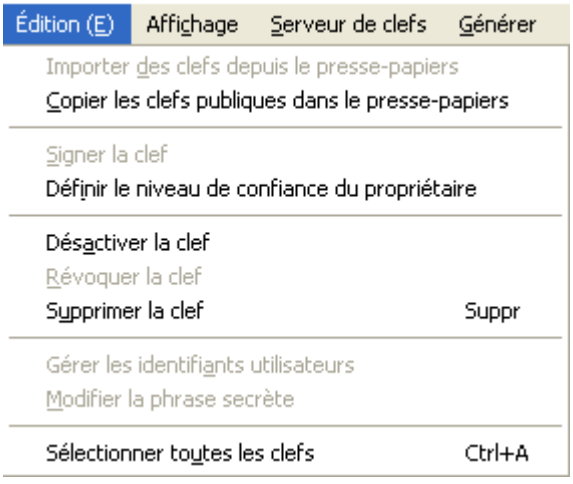
- Dans le menu “fichier”, vous pouvez importer/exporter une clé depuis un fichier, envoyer la clé publique via mail…



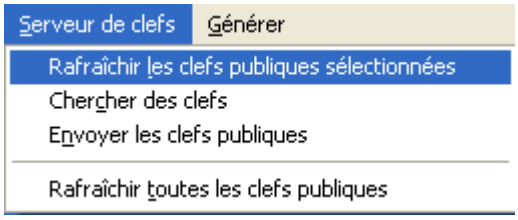
- Et voilà, les clés sont importées:



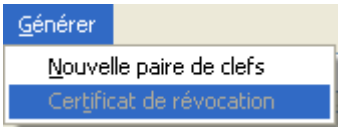
- Dans le menu " edition", vous pouvez sélectionner un ou plusieurs clés afin de les copier vers le presse papier, supprimer, désactiver et définir le niveau de confiance du propriétaire de la clé.



- Le menu "serveur de clefs", vous permet de chercher et/ou d'envoyer des clés vers un serveur.



- ET enfin pour le menu “Générer”, il permet de générer un nouvelle clé.



c. Envoi des messages chiffrés avec Thunderbird

Vous pouvez également envoyer un message chiffré avec Thunderbird, comme suit :

- Rédigez normalement votre message dans Thunderbird.
- Une fois que c’est fait, cliquez sur le bouton OpenPGP de la barre d’outils et cochez les cases « Signer le message » et « Chiffrer le message ». Cochez aussi l'option « Utiliser PGP/MIME pour ce message ».
- Si votre interlocuteur utilise aussi OpenPGP. Cela facilitera l'encodage des fichiers attachés.
- Si le destinataire utilise un webmail, il pourra déchiffrer le message à l’aide Winpt Tray par exemple.