

CHIFFRER
ET
SIGNER
SES EMAILS AVEC
ENIGMAIL
POUR THUNDERBIRD

Par **Maisse Sébastien**



Document en date du 02 mai 2006

Sommaire

Concernant ce document :	3
Préambule :	3
Qu'est-ce que Enigmail ?.....	4
Téléchargement de GNUPG :.....	4
Installation de GNUPG :.....	5
Téléchargement de ENIGMAIL :.....	9
Installation de ENIGMAIL :.....	9
Configuration de ENIGMAIL :.....	11
Ressources :.....	24
Quelques url's :.....	24
Conclusion :.....	24
Merci !.....	24

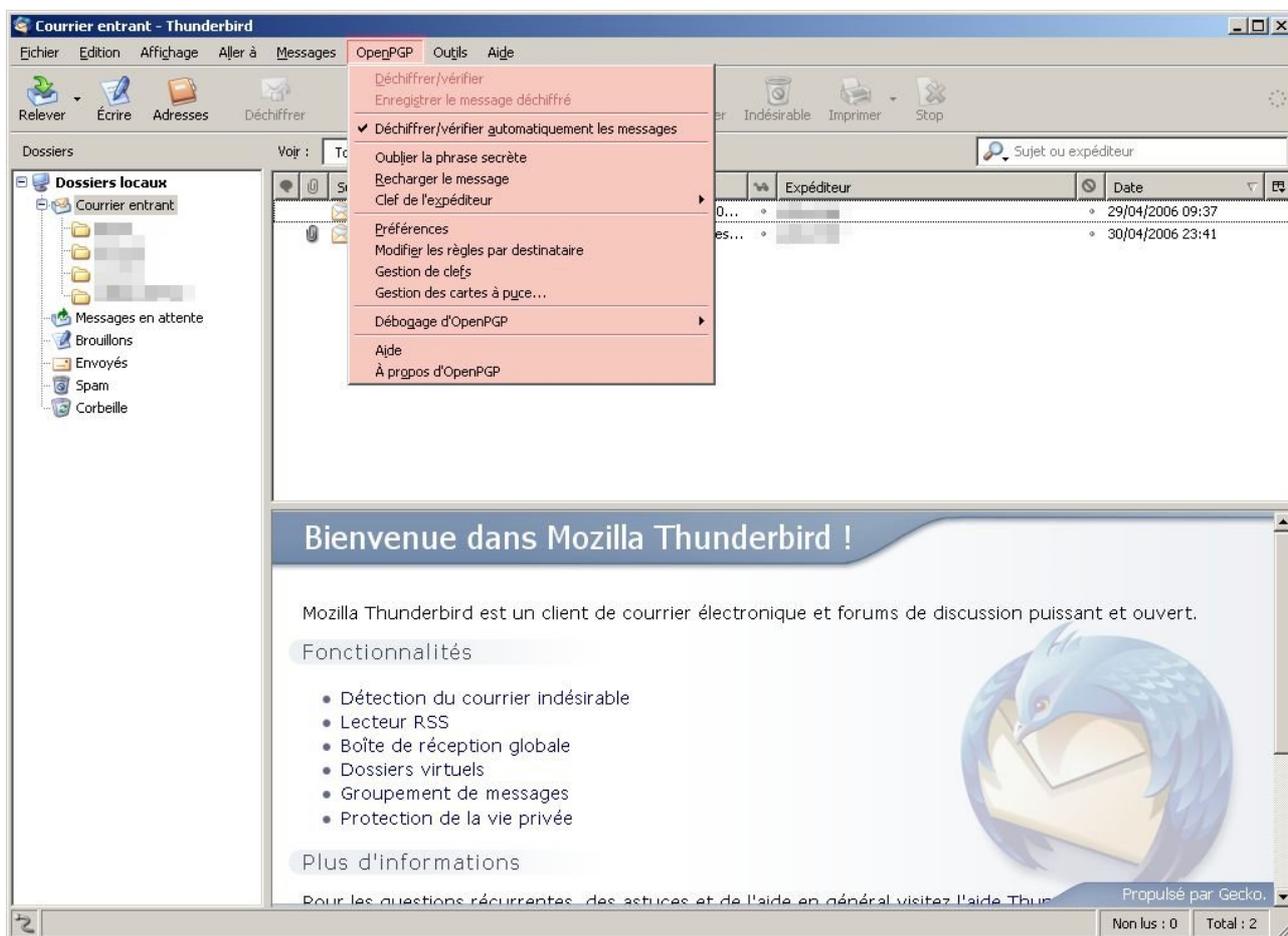
Concernant ce document :

Ce document a pour vocation de vous aider dans la mise en application de l'extension **Enigmail** pour le client de messagerie **Thunderbird** développé par l'équipe Mozilla.

L'extension en question vous permettra de signer et/ou chiffrer vos prochains e-mails.

Préambule :

Bienvenue dans ce document qui a pour but de vous faire découvrir l'installation ainsi que la configuration de l'extension Enigmail (utilisant GNUPG) dans Thunderbird.



OpenPGP (enigmail) installé dans Thunderbird

Qu'est-ce que Enigmail ?

Enigmail est une extension qui permet d'utiliser au sein de Thunderbird, un logiciel de type GNUPG (qui permet de chiffrer/déchiffrer et signer des e-mails).

Voici une petite définition disponible sur Wikipédia.org

Enigmail est un plugin de signature numérique et de chiffrement pour les clients email Mozilla et Mozilla Thunderbird, sous Microsoft Windows, Linux, Mac OS X et d'autres systèmes d'exploitation comme Solaris et FreeBSD, ou même AIX.

Il utilise GnuPG pour assurer la partie cryptographie de ses opérations, mais en se greffant à un client graphique de courrier électronique il évite d'avoir recours à la ligne de commande pour signer et chiffrer messages et fichiers.

Téléchargement de GNUPG :

Avant toute chose, nous devons tout d'abord procéder à l'installation du logiciel GNUPG (GNU Privacy Guard), c'est un équivalent de PGP en version Open source.

Ce logiciel est disponible gratuitement sur le site officiel :

<http://www.gnupg.org/>

Si vous souhaitez télécharger directement le programme d'installation pour l'environnement windows :

<ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.3.exe>

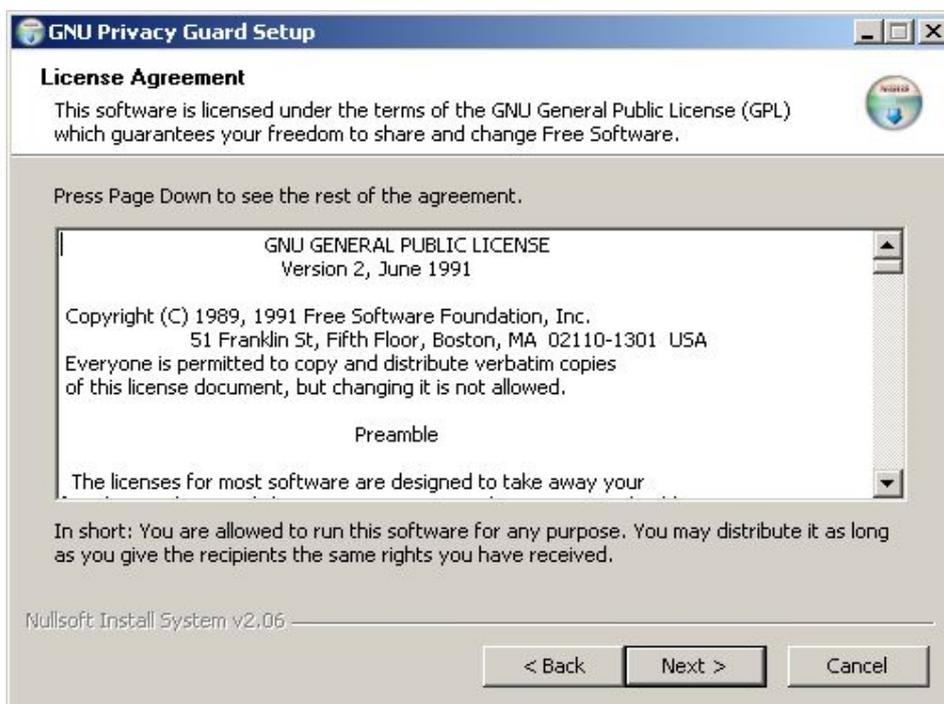
Note : à la date de rédaction de ce document, la version disponible était la **1.4.3**

Installation de GNUPG :

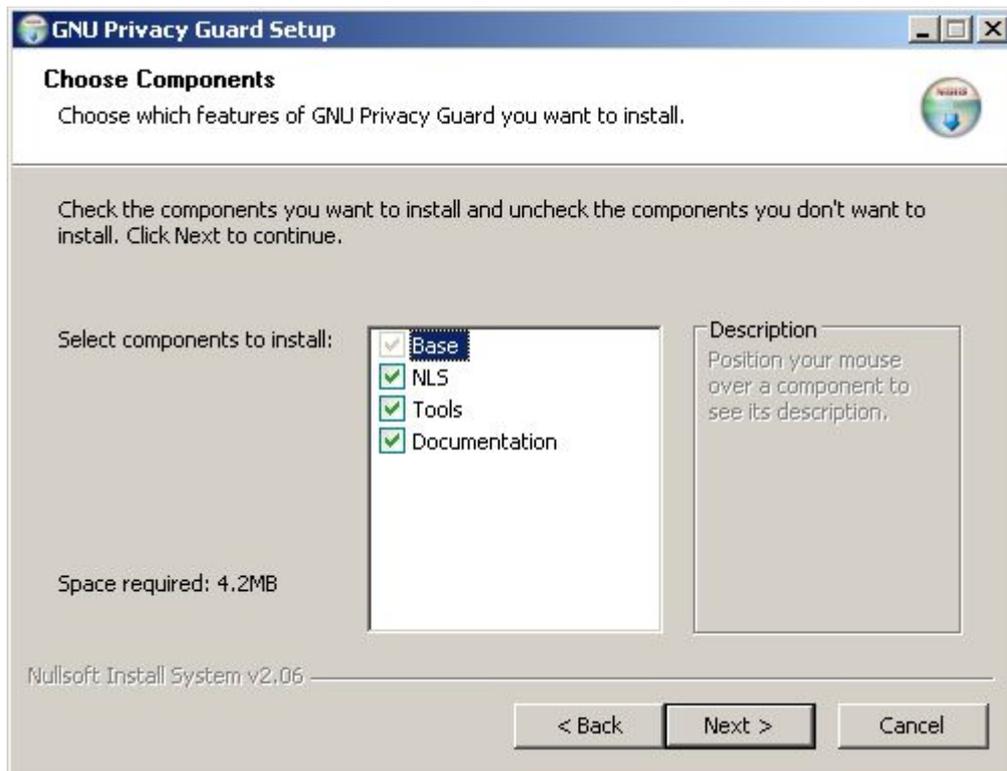
Une fois le programme d'installation téléchargé, on double clique dessus...



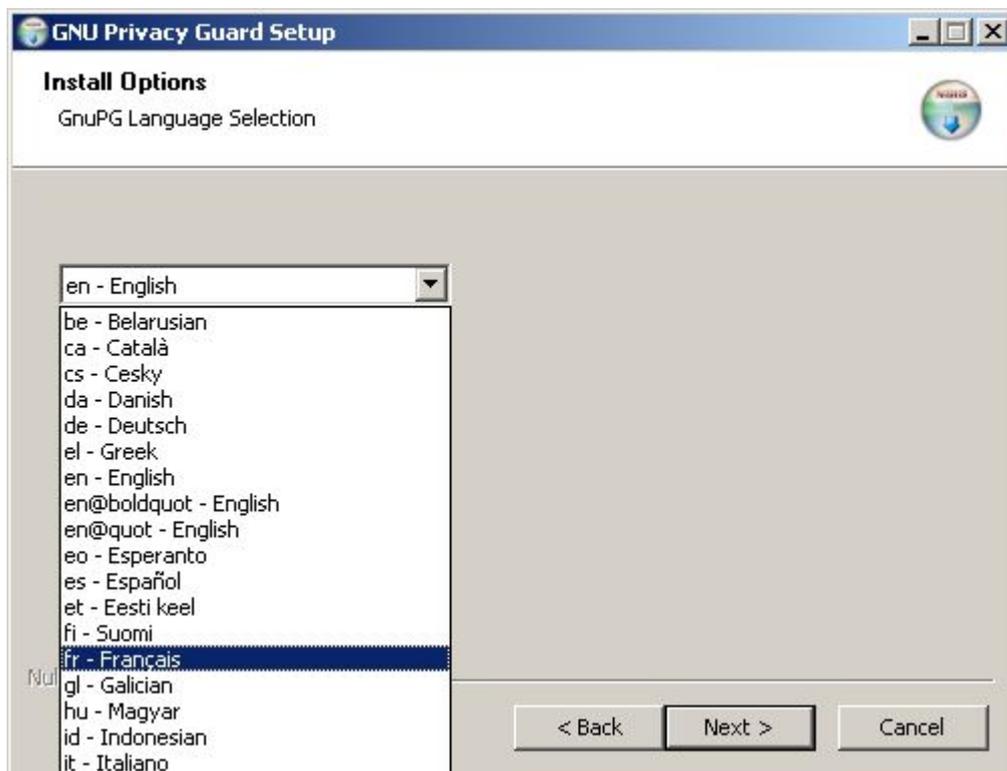
On clique sur *Next*



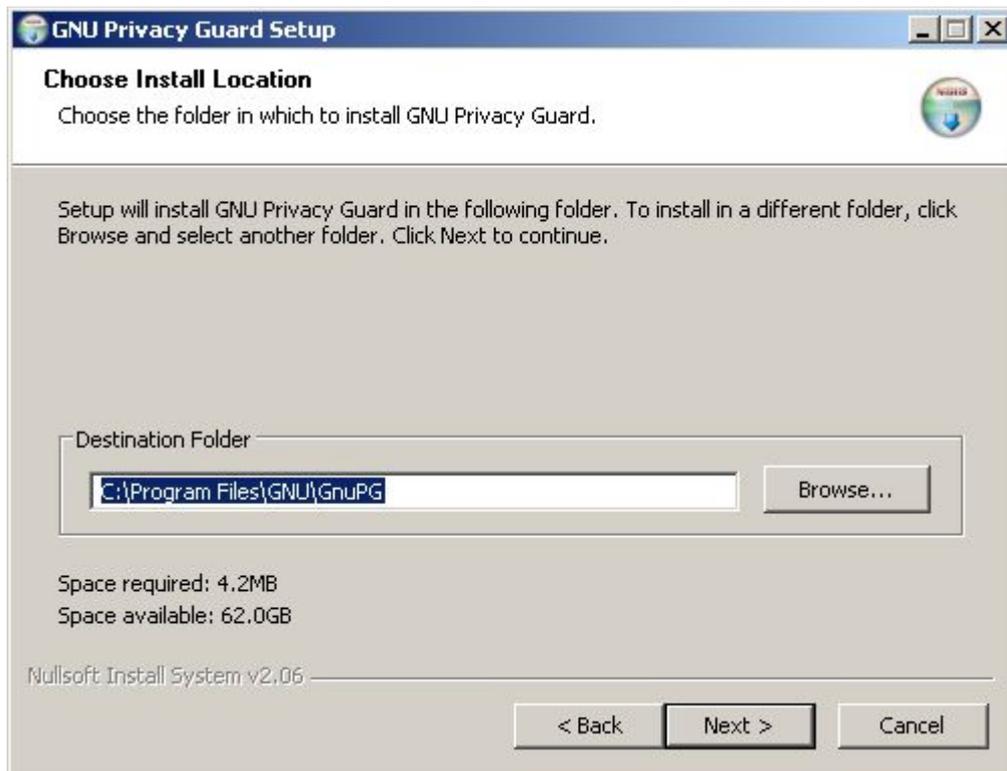
On clique sur *Next*



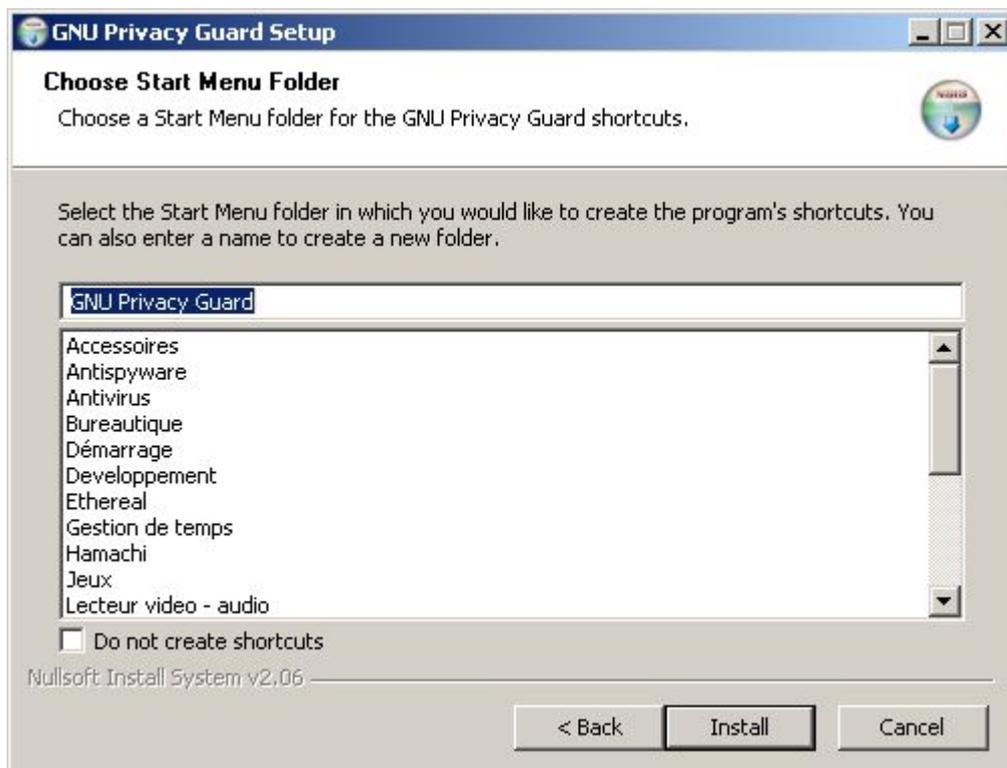
On clique sur *Next*



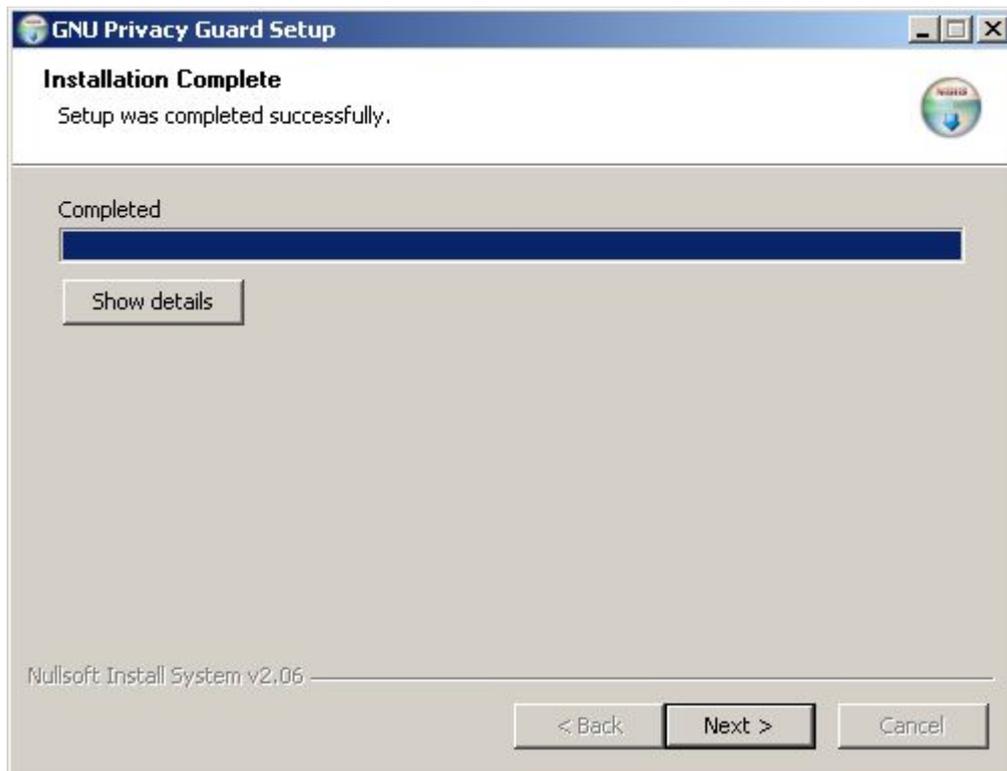
On choisi la langue (fr – Français) dans le cas présent puis on clique sur le bouton Next



On choisi le répertoire d'installation puis on clique sur *Next*



On clique sur *Next*



L'installation s'est bien déroulée...



On clique sur le bouton *Finish*

Téléchargement de ENIGMAIL :

GNUPG installé, nous pouvons à présent télécharger l'extension Enigmail. Pour ce faire, il faut aller faire un tour sur le site officiel : <http://enigmail.mozdev.org/>

L'archive est disponible en suivant lien ci-dessous :

<http://www.mozilla-enigmail.org/downloads/enigmail-0.94.0-tb15-win32.xpi>

Par ailleurs, une traduction de l'extension est disponible à l'url suivante :

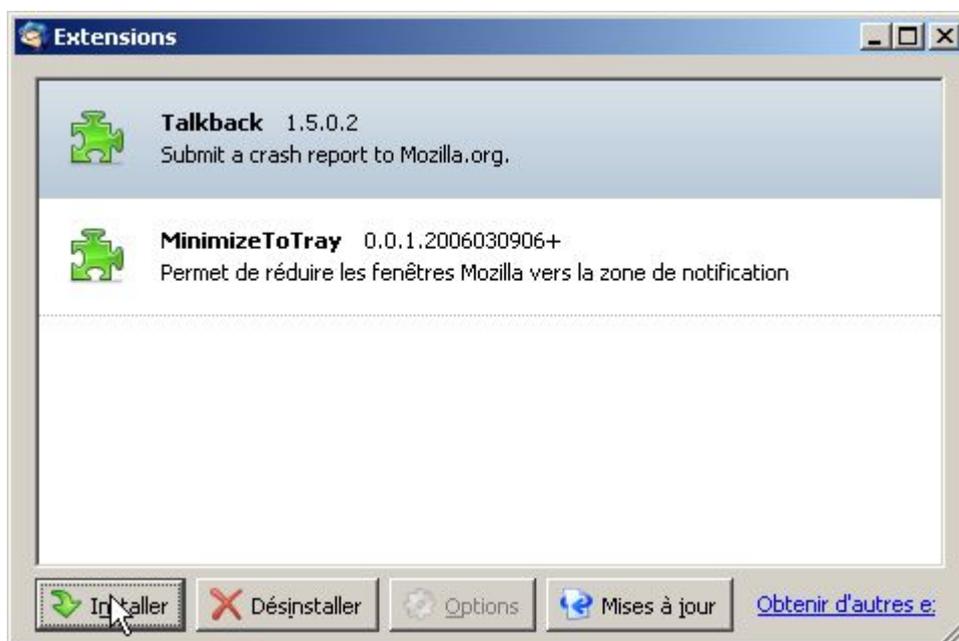
<http://www.mozilla-enigmail.org/downloads/lang/0.9x/enigmail-fr-FR-0.9x.xpi>

Note : lors de la rédaction de ce document, la version en date disponible était la **0.94.0**

Installation de ENIGMAIL :

Concernant l'installation de Enigmail, il faut lancer votre client de messagerie **Thunderbird**, une fois lancé aller dans le menu **Outils / Extensions**, là, soit vous faite un glisser-déposer du fichier de l'extension enigmail soit vous Cliquez sur le bouton **Installer**.

Procédure pour l'installation d'une extension



On clique sur le bouton *Installer*

On choisit le répertoire contenant notre extension « enigmail-0.94.0-tb15-win32.xpi »



On clique sur bouton *Installer maintenant*

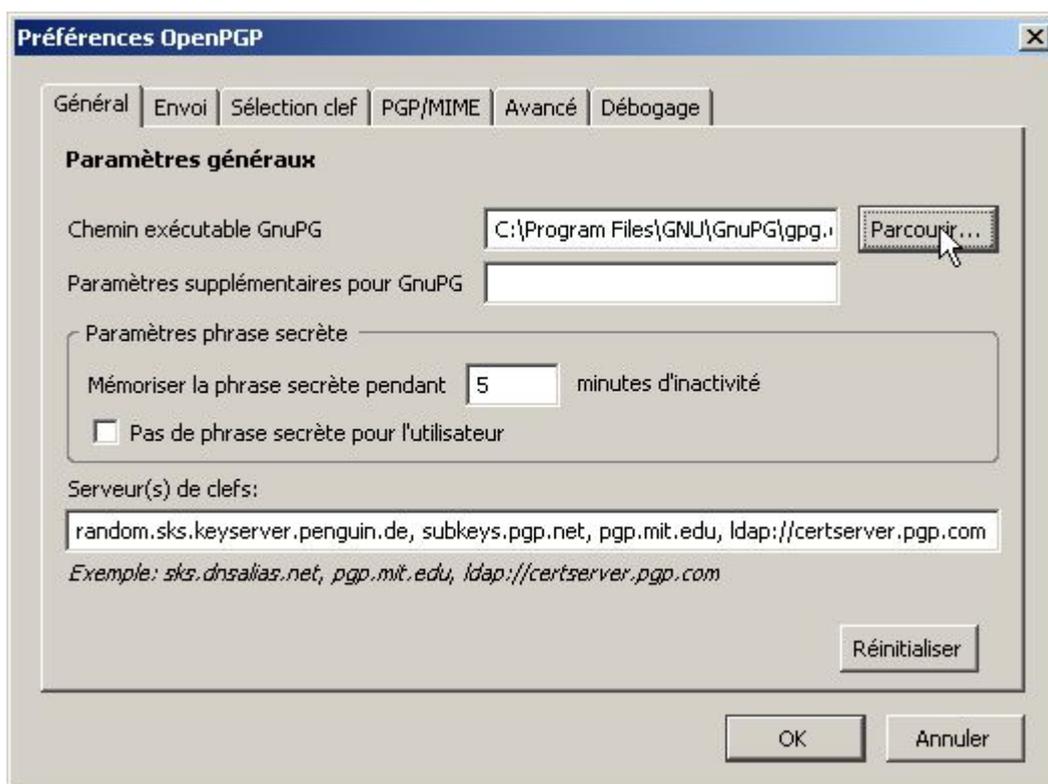


Voilà, nos deux extensions (enigmail et enigmail fr-FR) sont installées

NOTE : Il faut **redémarrer** Thunderbird pour prendre en compte l'extension nouvellement installée.

Configuration de ENIGMAIL :

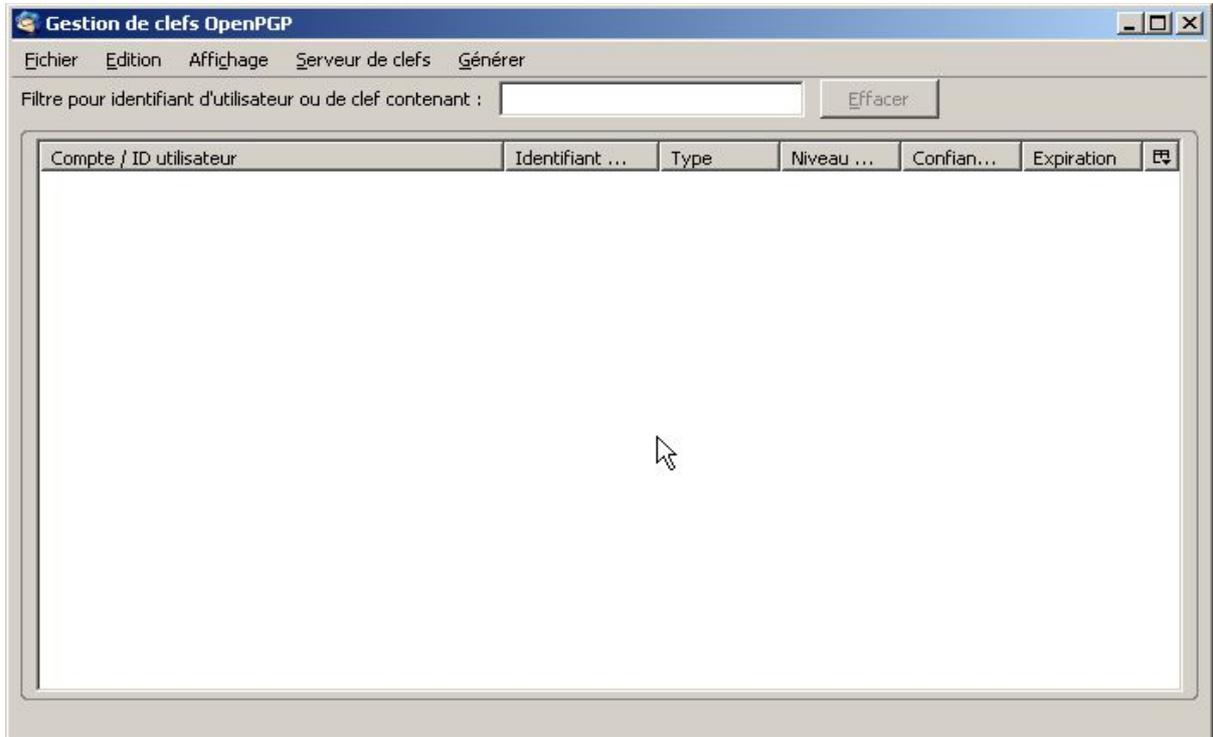
Notre extension étant installée, nous allons à présent la configurer. Pour ce faire, aller dans le menu **OpenPGP / Préférences**, nous allons tout d'abord définir le chemin d'accès de GNUPG (que nous avons installer précédemment).



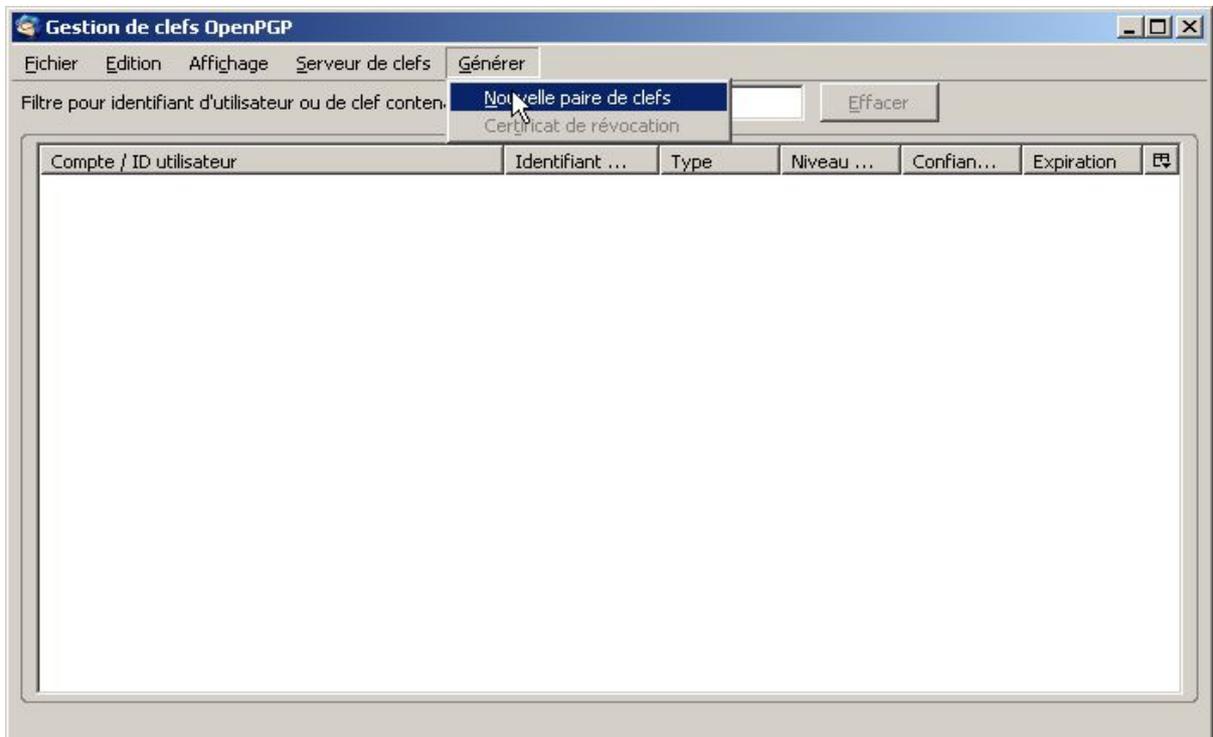
Par défaut, **GNUPG** se situe dans **c:\Program Files\GNU\GnuPG**

On clique sur le bouton *OK* pour valider notre choix.

Ceci étant fait, nous allons définir notre première clef publique / privée, pour ce faire rendez-vous dans le menu **OpenPGP / Gestion des clefs**.



Comme vous pouvez le voir, il n'y a pour le moment aucune clef.



Nous allons générer une nouvelle clef

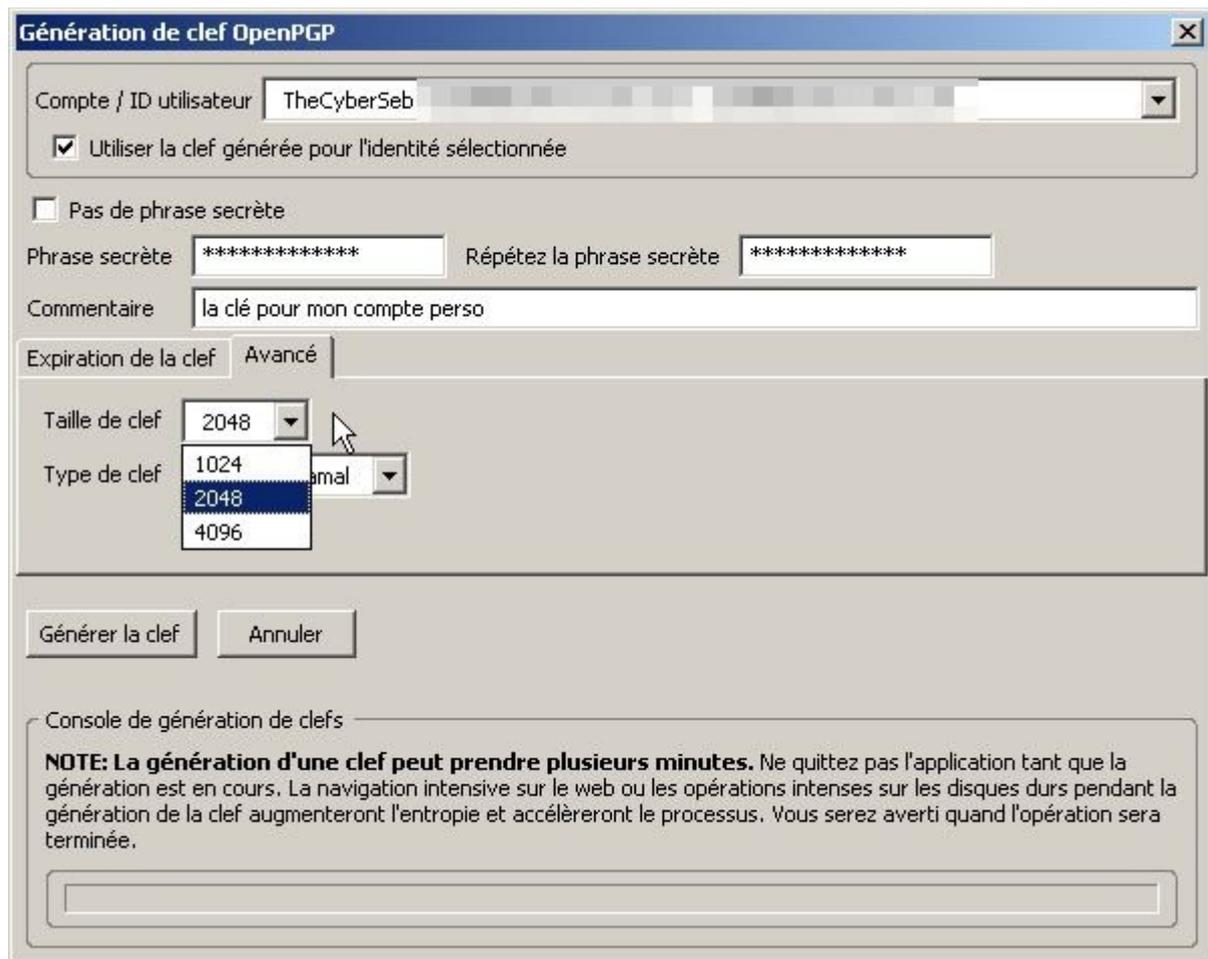
La présente clef va être définie pour le compte mail

Compte / ID Utilisateur : on choisi l'adresse e-mail pour laquelle on souhaite générer une clef

Phrase secrète : La phrase secrète doit être définie pour une meilleure sécurité.

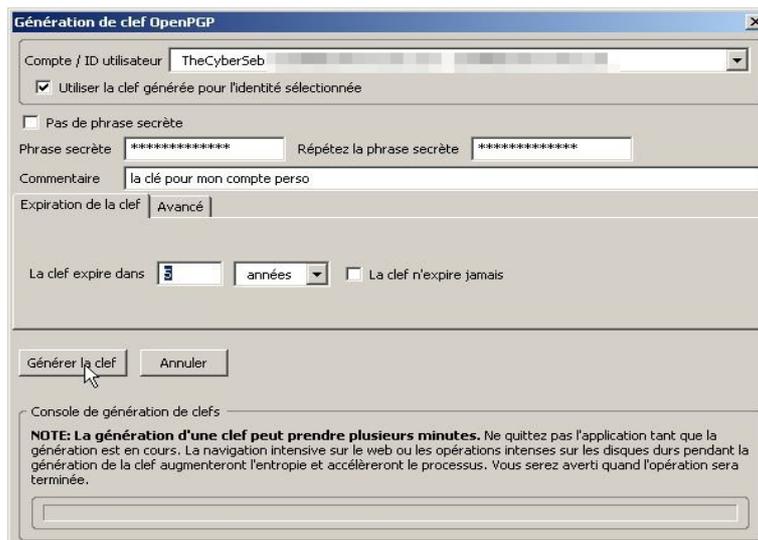
Commentaire : un petit commentaire pour la forme.

La clef expire dans : choisissez la durée de votre clef selon vos besoins.



Dans l'onglet **Avancé**, on peut définir la taille et le type de clef.

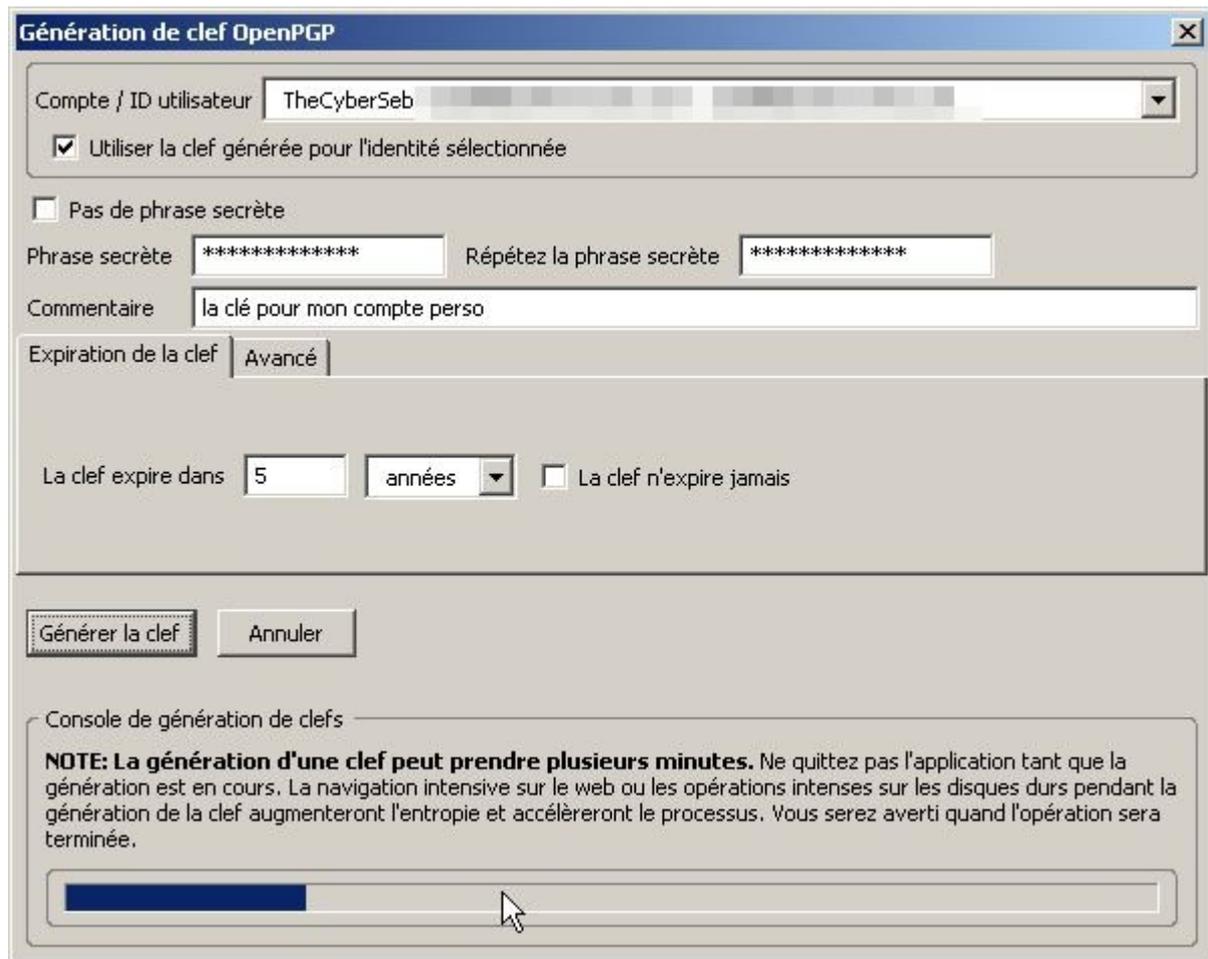
Par défaut, on aura une clef avec une taille de **2048** et utilisant le type [DSA & El Gamal](#)



On clique sur le bouton *Générer la clef*



Un message qui vous demande confirmation pour la génération de votre clef publique et privée.



Génération des clefs en cours...

Note : Selon la puissance de votre ordinateur, cela prendra plus ou moins de temps, de quelques minutes à quelques heures. *Patience...*



Une boîte de dialogue qui vous invite à la création d'un certificat de révocation, en cas de perte ou de vol de votre clé privée. On clique sur le bouton *Oui*.

Vous serez invité à indiquer un répertoire où votre certificat de révocation sera enregistré.

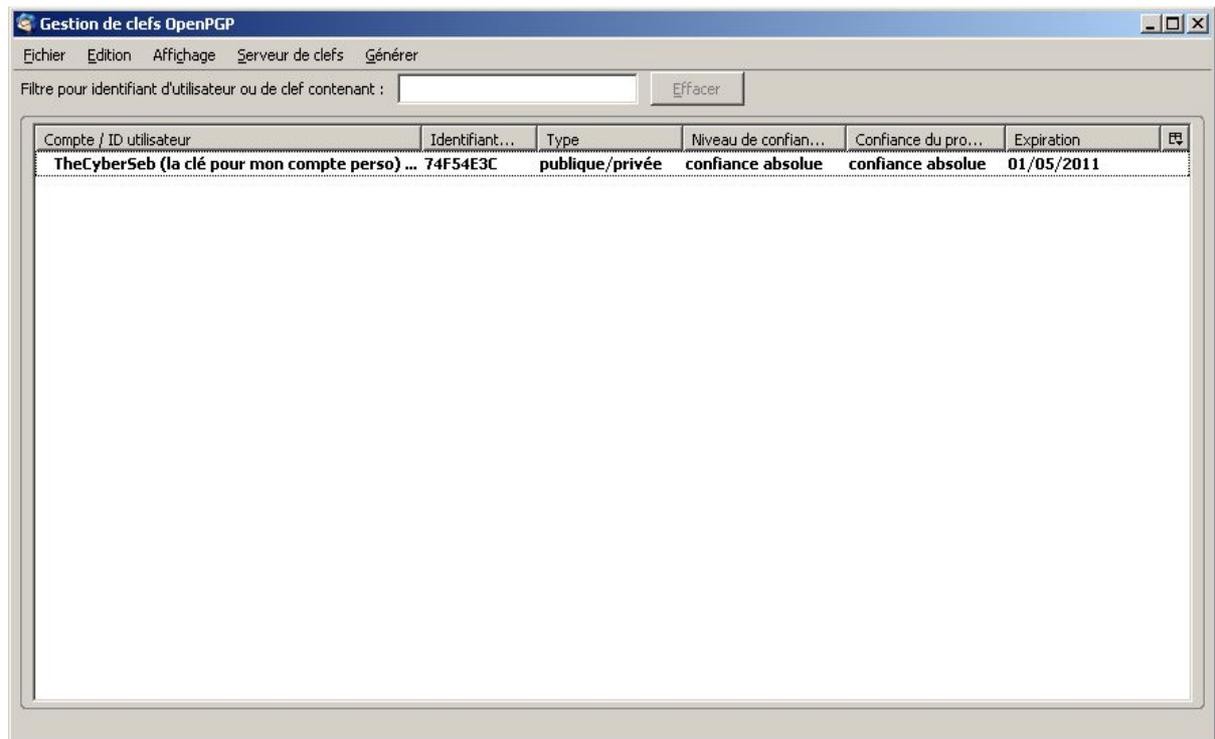
Ceci étant votre phrase secrète vous sera demander avant la génération du certificat.



Voilà le certificat a bien été créé...



On clique sur le bouton *OK*

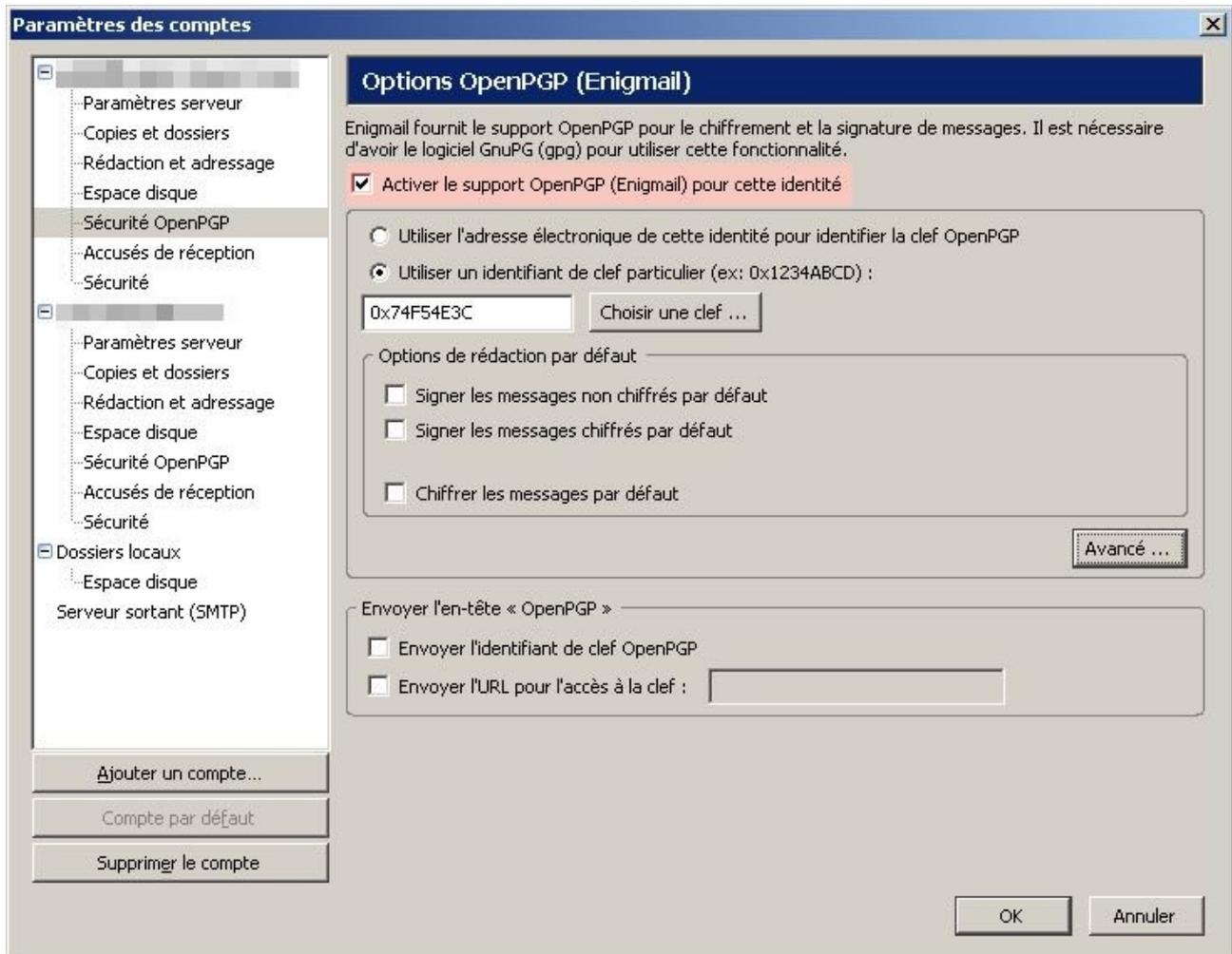


La clé publique / privée a bien été générée comme on peut le voir dans l'écran ci-dessus.

Ceci fait, nous allons vérifier que Thunderbird a bien pris en compte notre configuration.

Pour ce faire, aller dans le menu **Outils / Paramètres des comptes**

Choisissez votre compte e-mail pour lequel vous avez générer une clef.

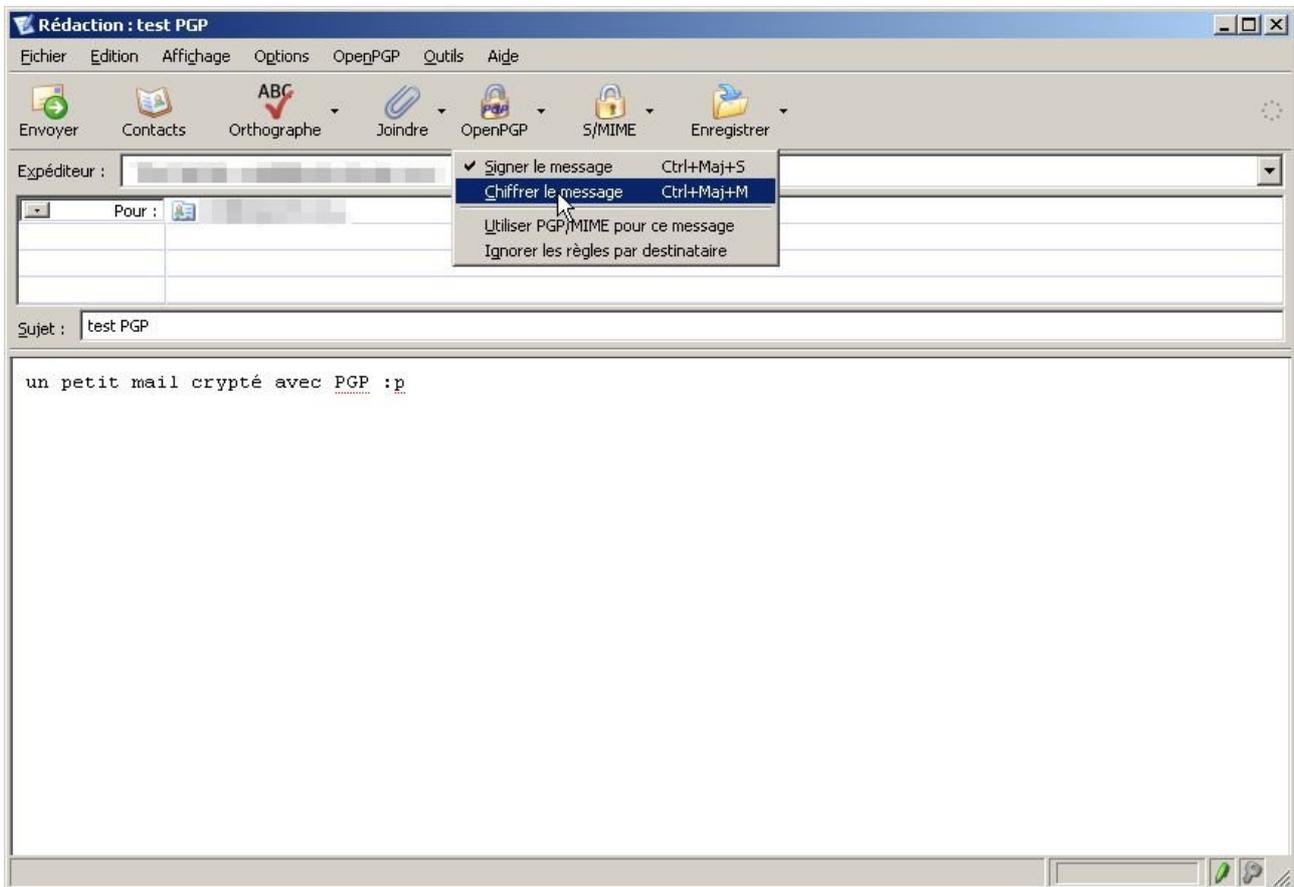


Vérifier que le support Enigmail est bien activé. Si ce n'est pas le cas cochez la case **Activer le support OpenPGP (Enigmail) pour cette identité**

Ceci étant, nous allons pouvoir rédiger notre premier e-mail signé...

Pour ce faire cliquer sur l'icône **Ecrire** ou menu **Fichier / Nouveau / Message**

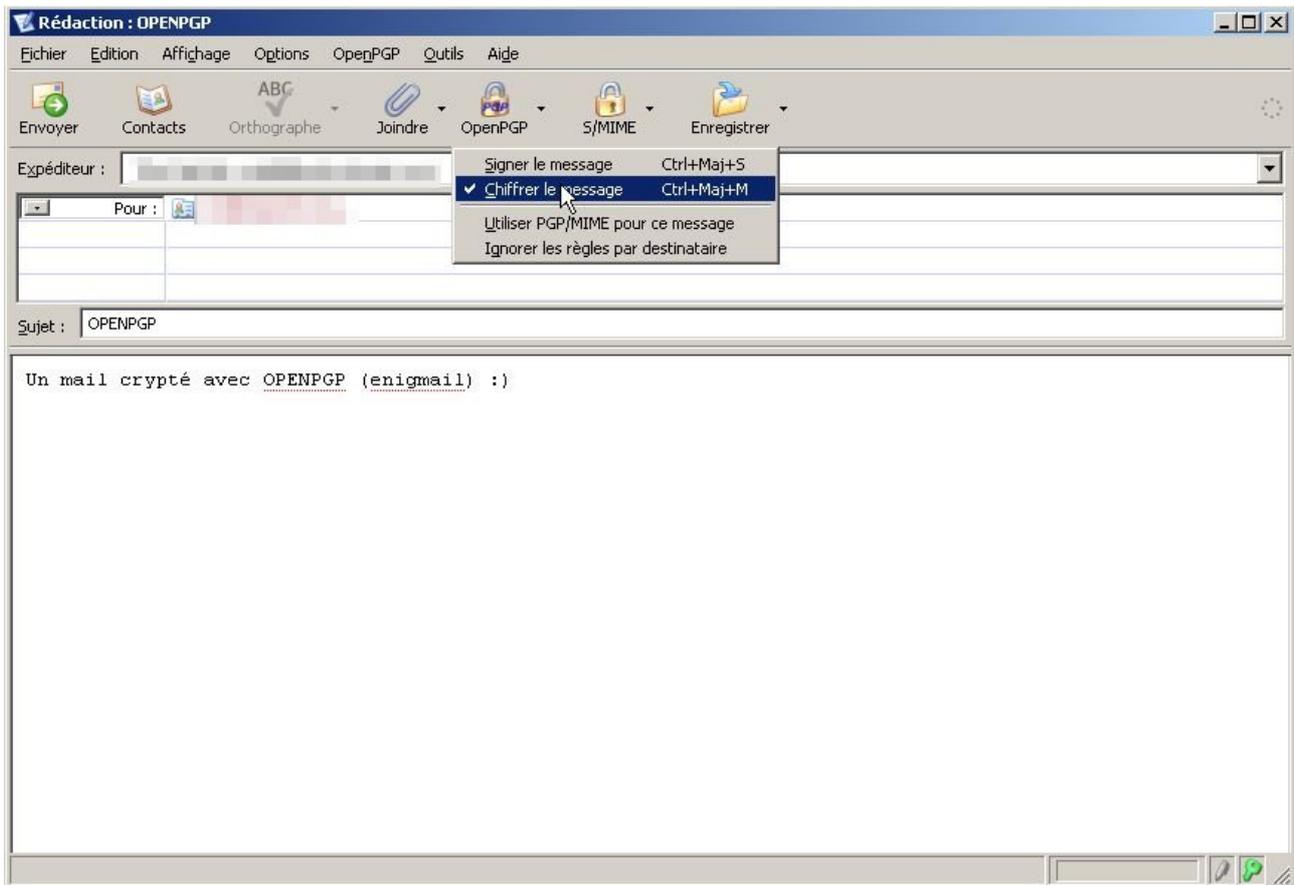
Comme vous pouvez le voir, il y a une icône supplémentaire (OpenPGP) :



Taper votre e-mail comme à l'habitude... Puis cliquez sur le bouton **OpenPGP**.

Comme vous pouvez le voir par défaut, l'e-mail votre être signé.

Si je souhaite chiffrer l'e-mail ... je choisi l'option **Chiffrer le message**.

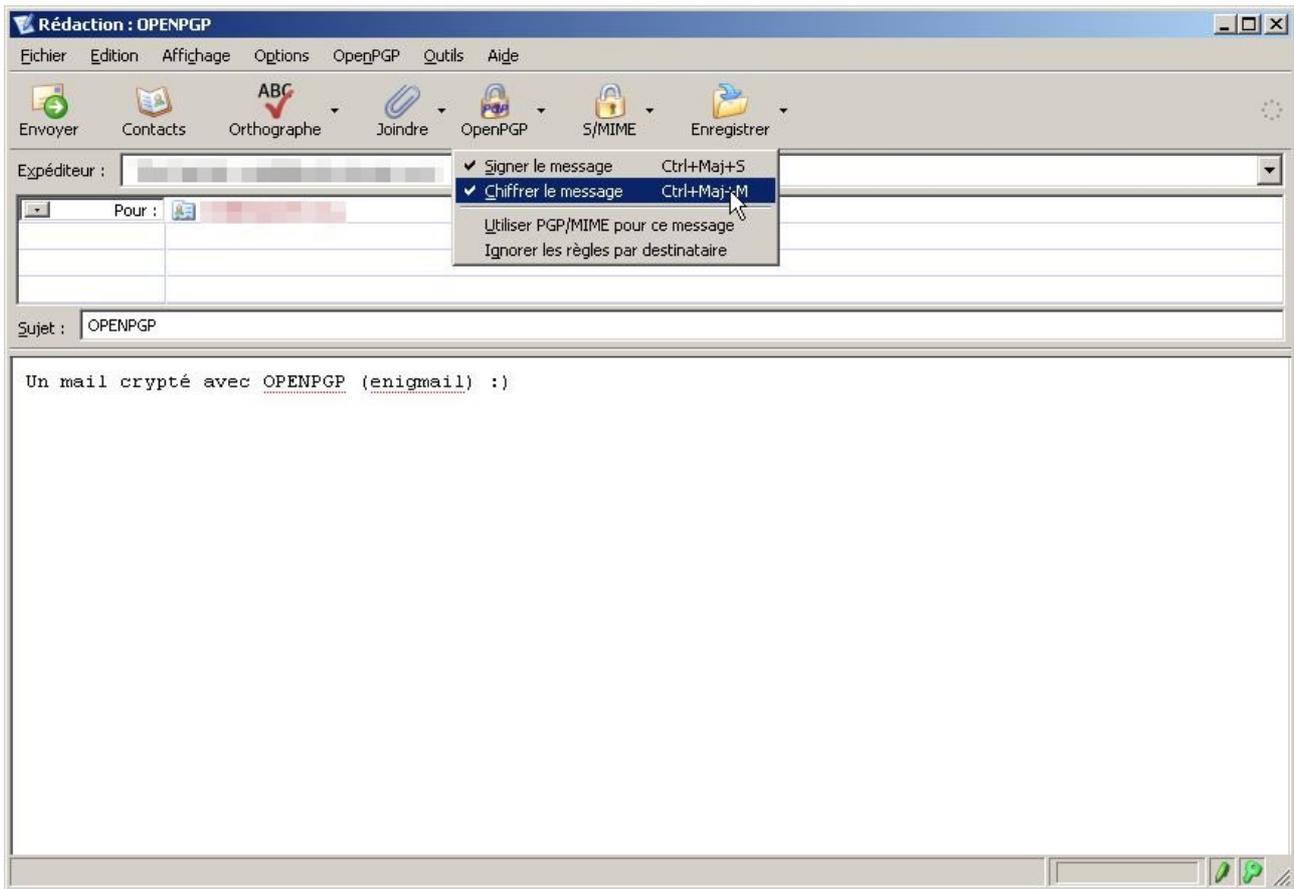


Si je souhaite choisir à nouveau **Signer le message**, vous aurez un message d'avertissement



On clique sur le bouton *OK*

Dans le cas suivant par exemple, l'e-mail sera signé et chiffré...



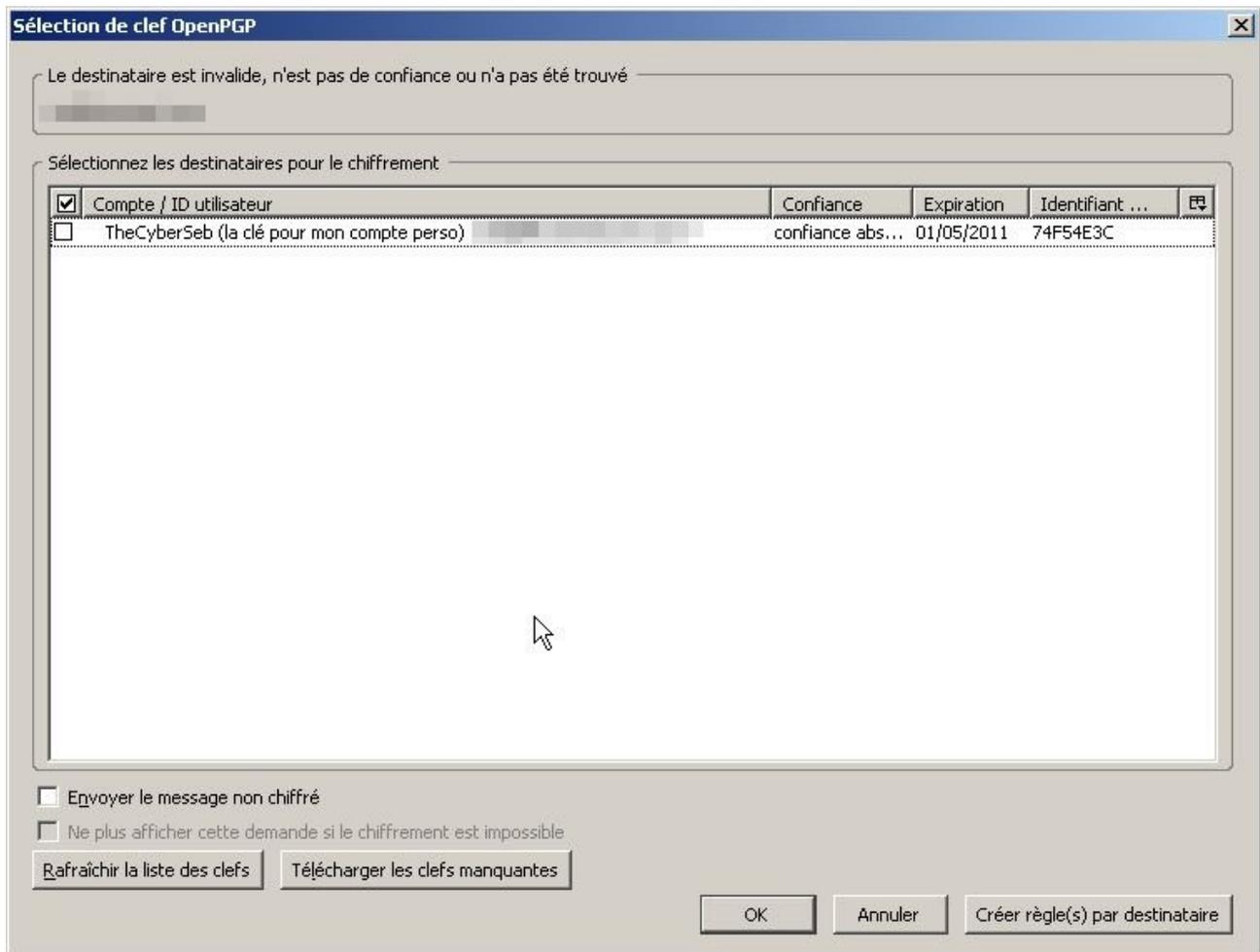
Ceci étant, je vais juste signer l'e-mail que je veux envoyer...



Votre phrase secrète vous sera demandé

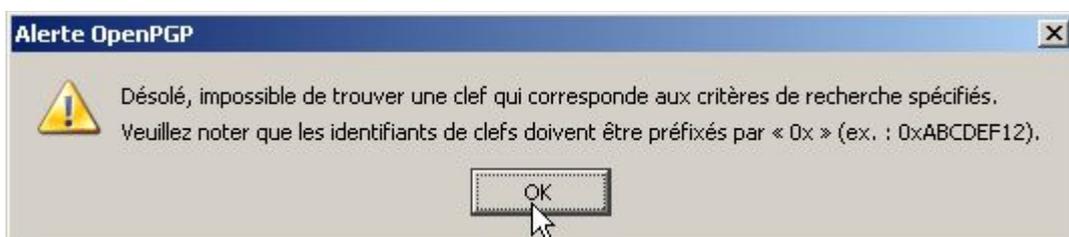
A cet instant l'e-mail signé est parti...

Dans le cas où vous souhaitez envoyer un e-mail chiffré, il vous faudra disposer de la clef publique de votre destinataire.

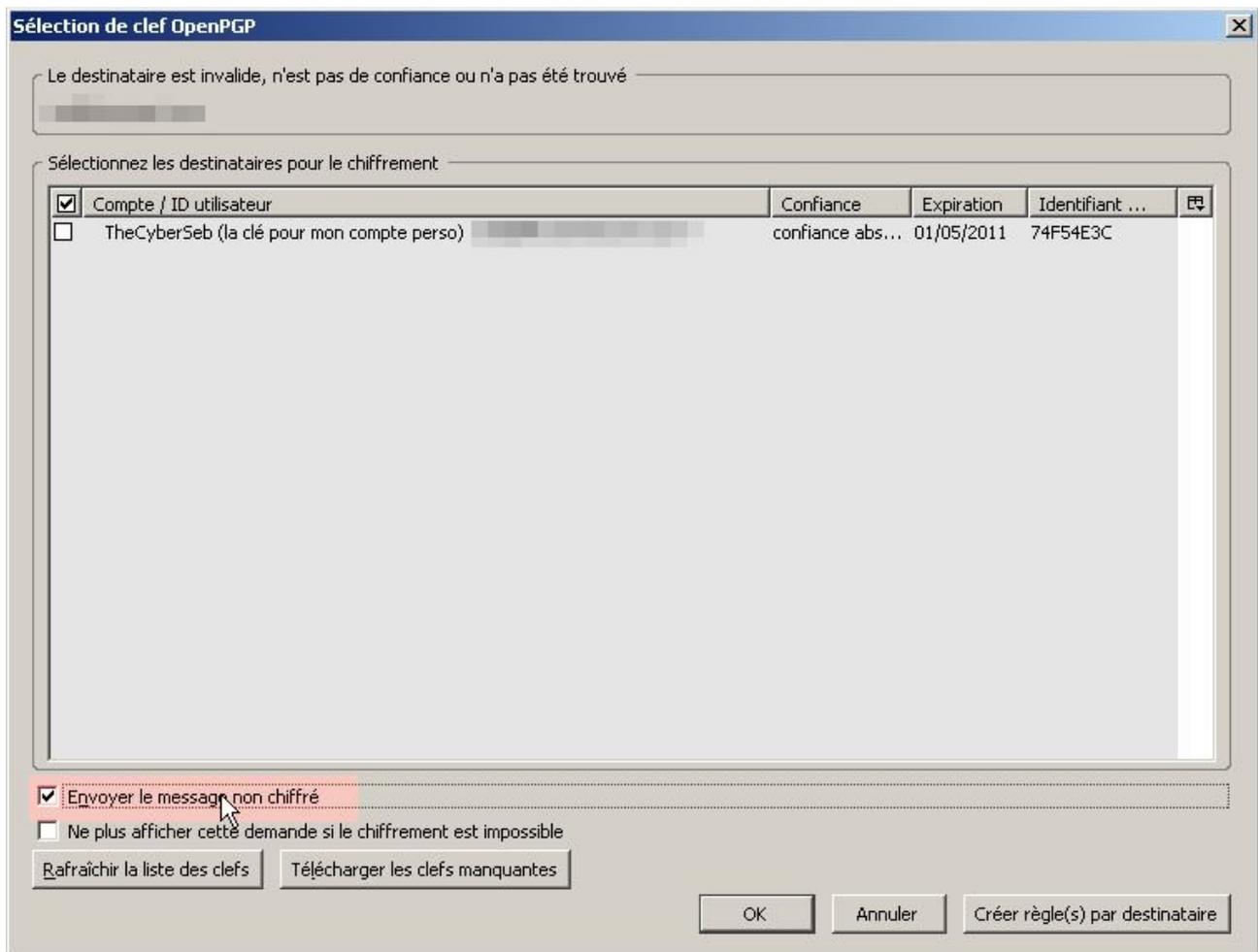


Visiblement, il n'est pas dans la liste des destinataires susceptibles de pouvoir recevoir du courriel chiffré. Ceci ayant pour action de faire une recherche sur un des serveurs de clef.

On clique sur le bouton **Télécharger les clefs manquantes**



Dans le cas présent, la personne destinataire ne dispose pas de clef.



Ici, pas trop de choix, l'e-mail sera envoyé non chiffré.

L'e-mail que j'ai envoyé tout-à-l'heure est bien arrivé...

Date: Tue, 02 May 2006 15:25:24 +0200
De: TheCyberSeb
À:
Objet: OPENPGP

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Un mail crypté avec OPENPGP (enigmail) :)

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.3 (MingW32)

Comment: Using GnuPG with Mozilla - <http://enigmail.mozdev.org>

iD8DBQFEV13EoenRP3T1TjwRAjICAKCrk7RerPAv9WXbPGptleQ31zIzpaCgt5FG
0W4txL435SKJ2H1/WWHTg7s=
=2QOa

-----END PGP SIGNATURE-----

Ressources :

Quelques url's :

Enigmail : <http://enigmail.mozdev.org/>

Thunderbird : <http://www.mozilla-europe.org/fr/products/thunderbird/>

GNUPG : <http://www.gnupg.org/>

Portail de la cryptologie (wikipedia) : <http://fr.wikipedia.org/wiki/Portail:Cryptologie>

Conclusion :

Vous avez à présent une base pour utiliser le chiffrement ainsi que la signature pour vos prochains e-mails.

Si vous avez des questions / suggestions concernant ce document, je vous encourage à me contacter soit par e-mail à thecyberseb@hotmail.com, soit en laissant un message sur le forum qui se trouve à l'url suivante :

<http://forum.monserveurperso.com>

Pour de plus amples documents sur divers sujets, faites un tour à l'url ci-dessous...

<http://tutorial.monserveurperso.com>

Merci !

Au **site internet** qui publie avec ou sans ma bénédiction mon document.

Merci à **Monsieur Pat** pour la relecture ainsi que la correction orthographique.

MERCI d'avoir pris le temps de lire ce document :-)