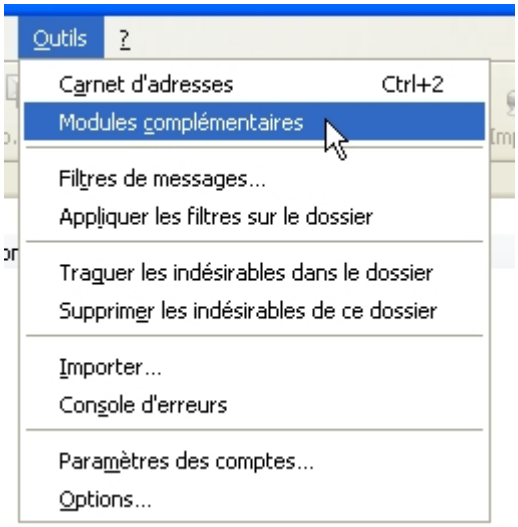
Utiliser Enigmail avec Thunderbird sous Windows

Pré-requis

Thunderbird doit être installé et votre compte courrier configuré.
GnuPG doit être installé.

Thunderbird et GnuPG, ainsi que leurs tutoriaux sont disponibles sur le CD Octopuce.

Installation d'Enigmail dans Thunderbird



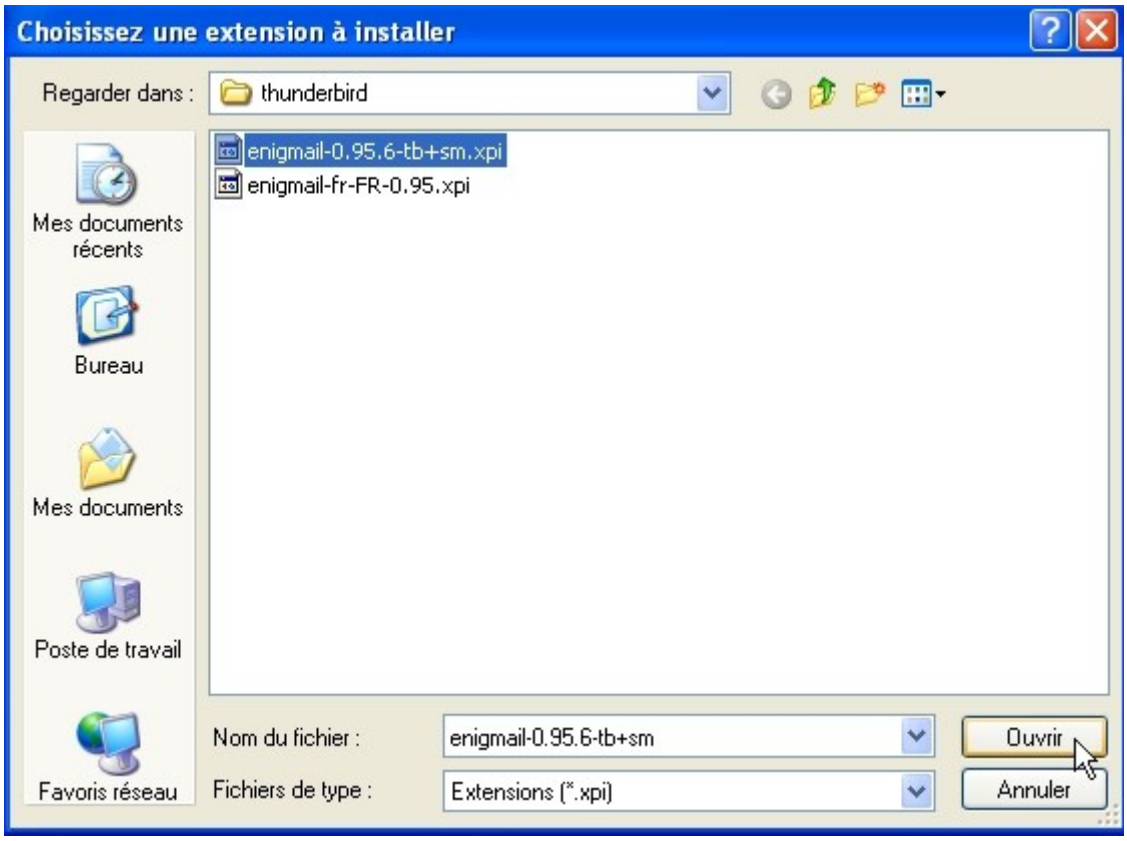
Ouvrir Thunderbird

Attention, votre adresse mail doit déjà être installée
Vous devez également avoir installé GnuPG.

Dans le menu « Outils » Cliquer sur « Modules complémentaires »

Dans la fenêtre qui s'ouvre (voir ci-dessous) cliquez sur « Installer »

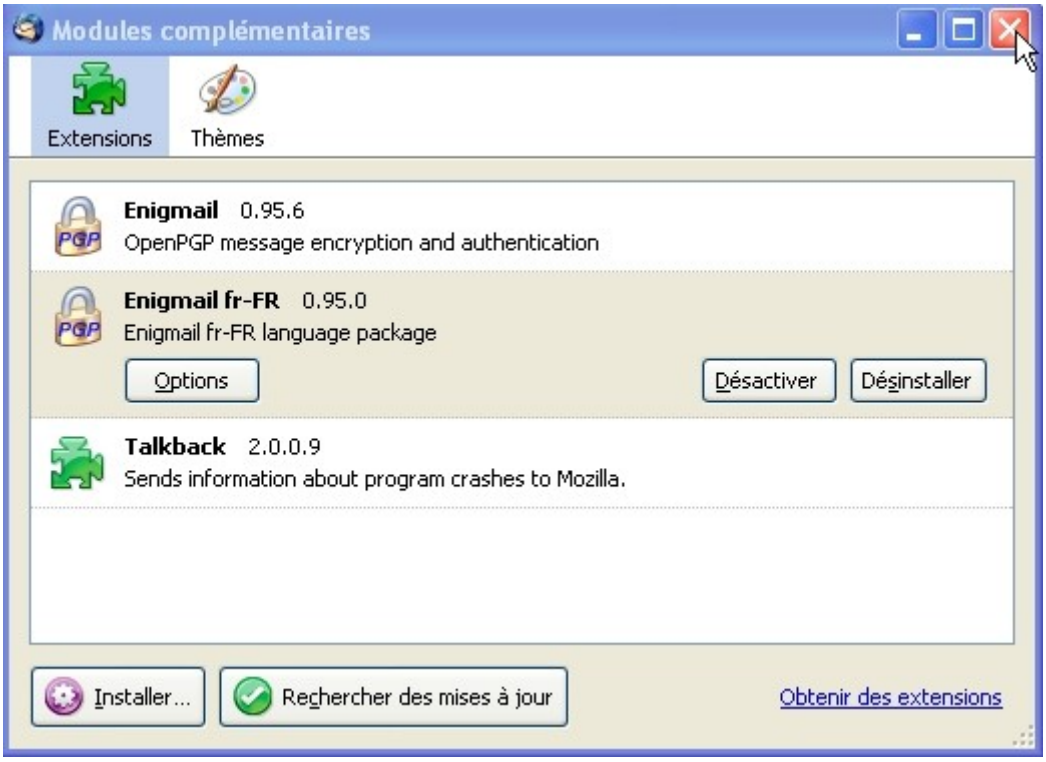
Naviguez dans vos répertoire jusqu'au CD puis, jusqu'au répertoire logiciels et enfin thunderbird. Choisissez le fichier : enigmail-0.95.6-tb+sm.xpi, comme indiqué dans la fenêtre ci-dessous.



Cliquez sur « Ouvrir »

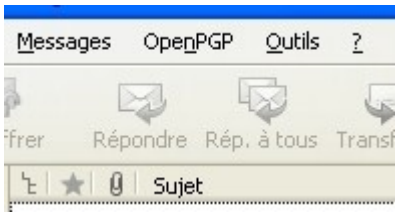
Attendez que le bouton « Installer maintenant » soit net et cliquez dessus.

Faites de même avec le second fichier : enigmail-fr-FR-0,9x,xpi (il s'agit de la traduction française de enigmail).



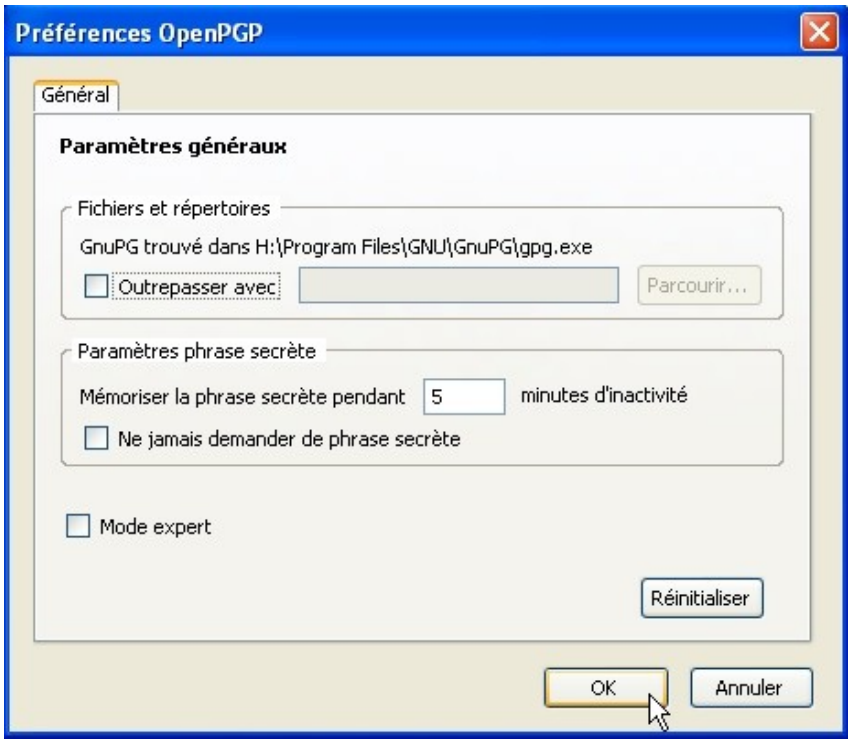
Voici les deux extensions affichées dans la fenêtre Extensions.
Il faut maintenant quitter et redémarrer Thunderbird pour que ces changements soient pris en compte.

Configuration d' Enigmail



Lorsque vous redémarrez Thunderbird, un nouvel onglet apparaît dans le menu « OpenPGP »

Choisissez cet onglet et cliquez sur « Préférences »



Dans la fenêtre qui s'ouvre vérifiez l'existence d'un chemin vers l'exécutable GPG.

Ici
\Program Files\GNU\GnuPG\gpg.exe

Cliquez sur « OK » pour refermer la fenêtre.

Génération d'une paire de clefs

L'utilité de Enigmail est subordonnée à l'existence d'une paire de clefs liées a votre adresse mail déjà configurée dans Thunderbird.

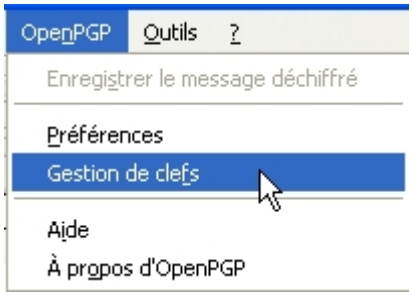
Si votre adresse mail n'est pas configurée dans Thunderbird, prenez le temps de la configurer en suivant l'aide du tutorial qui se trouve sur le CD, puis revenez à ce chapitre.

Nous allons maintenant créer cette paire de clés :

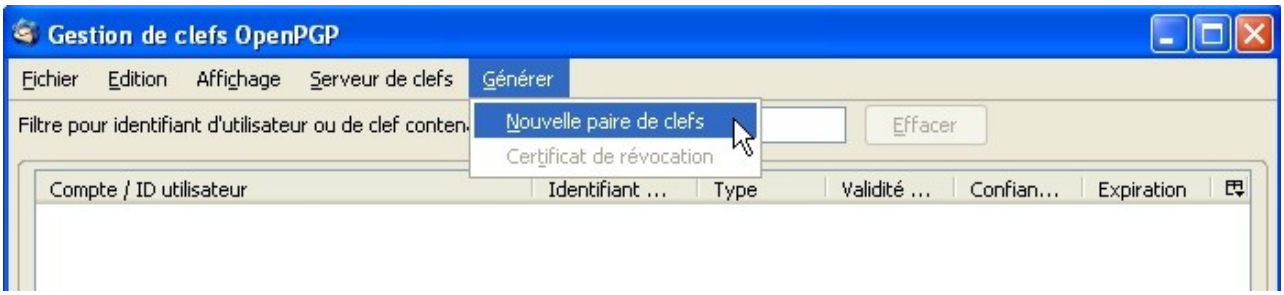
- Une clef privée qui vous servira a authentifier vos messages (signature) et à lire les mails chiffrés adressés par vos correspondants
- Une clef publique que vous transmettrez à vos correspondants et qui leur servira à vérifier que votre signature est authentique (vous êtes bien l'expéditeur du message).

Une fois installé enigmail vous a proposé de générer cette parie de clé. Si vous avez refermé cette fenêtre rien n'est perdu.

Cliquez sur « Open GPG » puis « Gestion de cléfs » comme indiqué dans la figure ci-dessous.



Dans la fenêtre qui s'ouvre choisissez « Générer » et « Nouvelle paire de clefs »



A partir de maintenant, vous devez pouvoir consacrer une dizaine de minutes pour la création et la configuration de la paire de clés.

Vérifiez que votre adresse est correcte et que la case « Utiliser la clef générée pour l'identité sélectionnée » est bien cochée.

Choisissez une phrase secrète.
ici il n'est pas question d'un mot de passe mais d'une phrase... Cette phrase doit être difficile à pirater !
Pour ne pas l'oublier (normalement elle ne doit être inscrite dans aucun document susceptible d'être confié à d'autres personnes que vous seul, ou perdu...) il existe des moyens mnémotechniques.

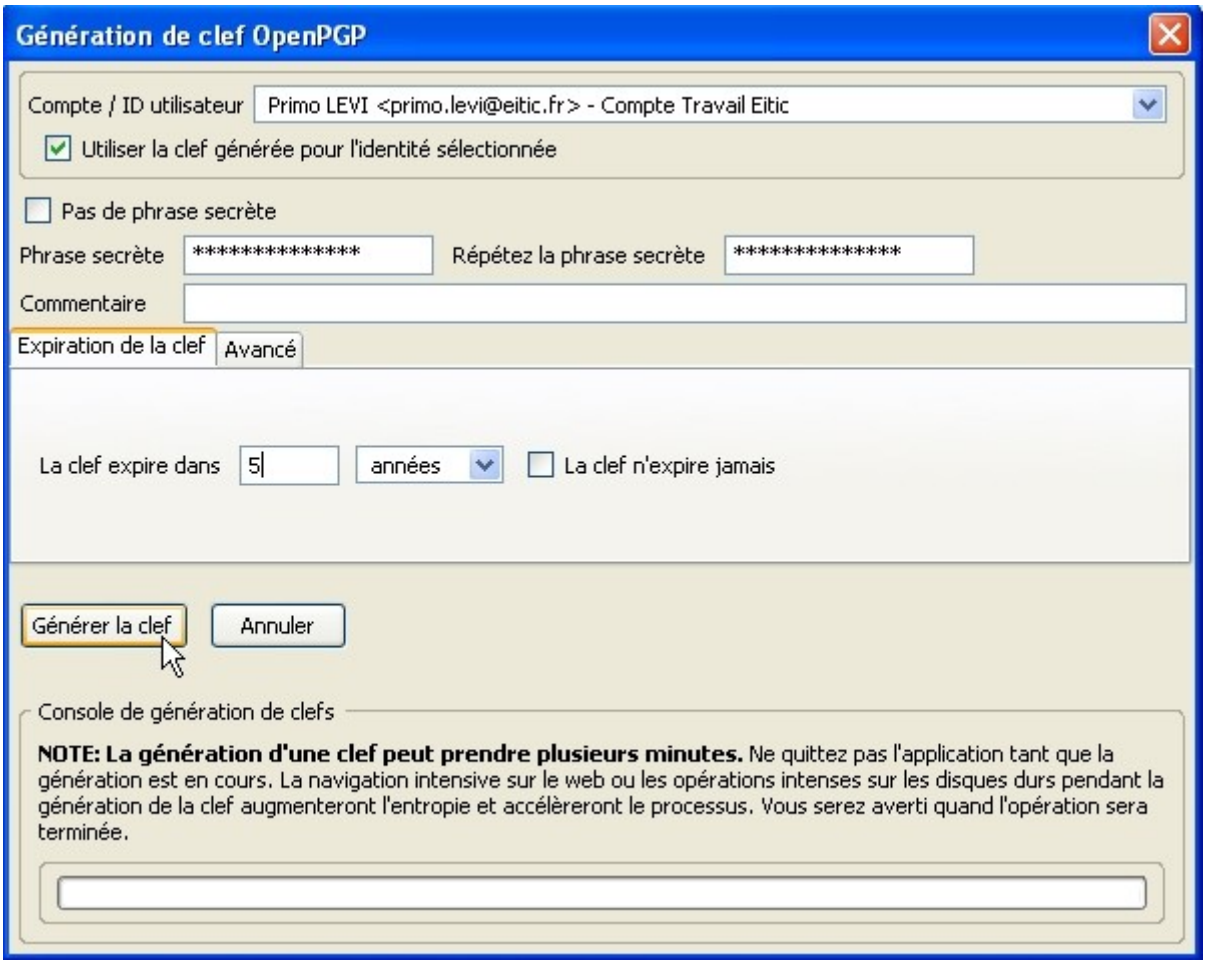
Voici un exemple :

- Je choisis un phrase que je n'oublierai pas, par exemple : « Les sanglots longs des violons de l'automne bercent mon cœur d'une langueur monotone ».
- Je choisis de garder la première lettre de chaque mot (en gardant le L manuscule... ou pas !) : l s l d v d l a b m c l m
- Je choisis des nombres que je n'oublierai pas non plus (et là ce peut être une date anniversaire par exemple !) 7 01 1970
- Je décide de ne pas garder les zéros (ou tous les chiffres inférieurs à x ou supérieurs à x) : 1 7 1 1 9 7
- J'intercale ces chiffres dans la suite de lettre en commençant par le début... ou la fin
- j'obtiens l 1 s 7 l d 1 v 1 d 9 l a 7 b m c l m

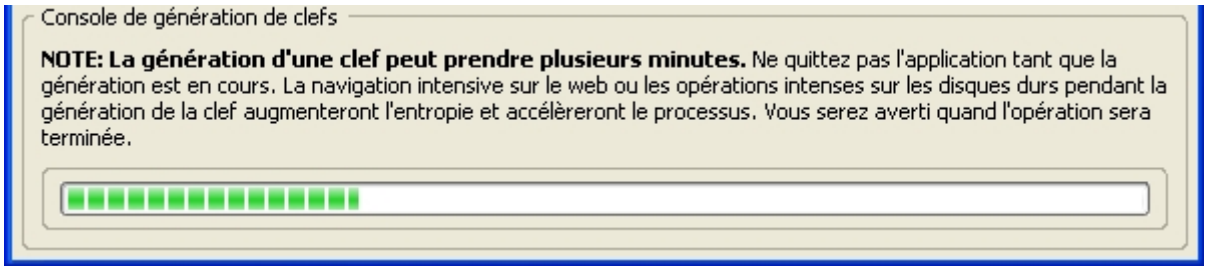
J'aurais pu aussi alterner majuscules et minuscules 1 / 2 ou 1 / 3...)

je serai donc toujours à même de reconstituer cette phrase !

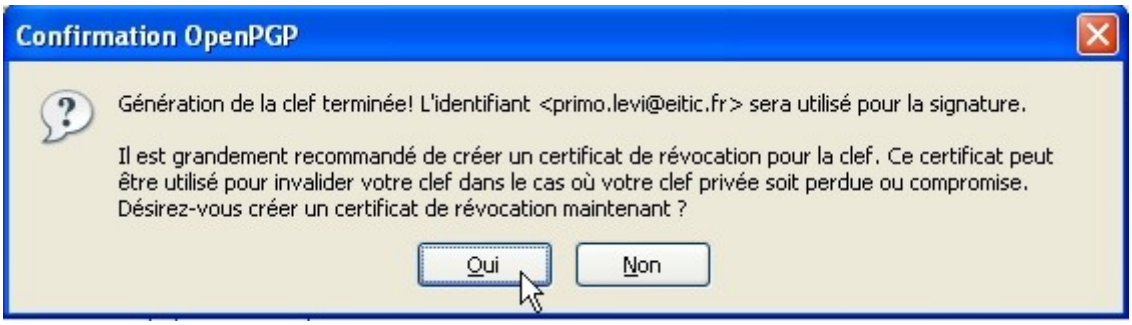
Choisissez la durée de validité de la clef et lisez attentivement la note , au bas de la fenêtre, puis cliquez sur « Générer la clef ».



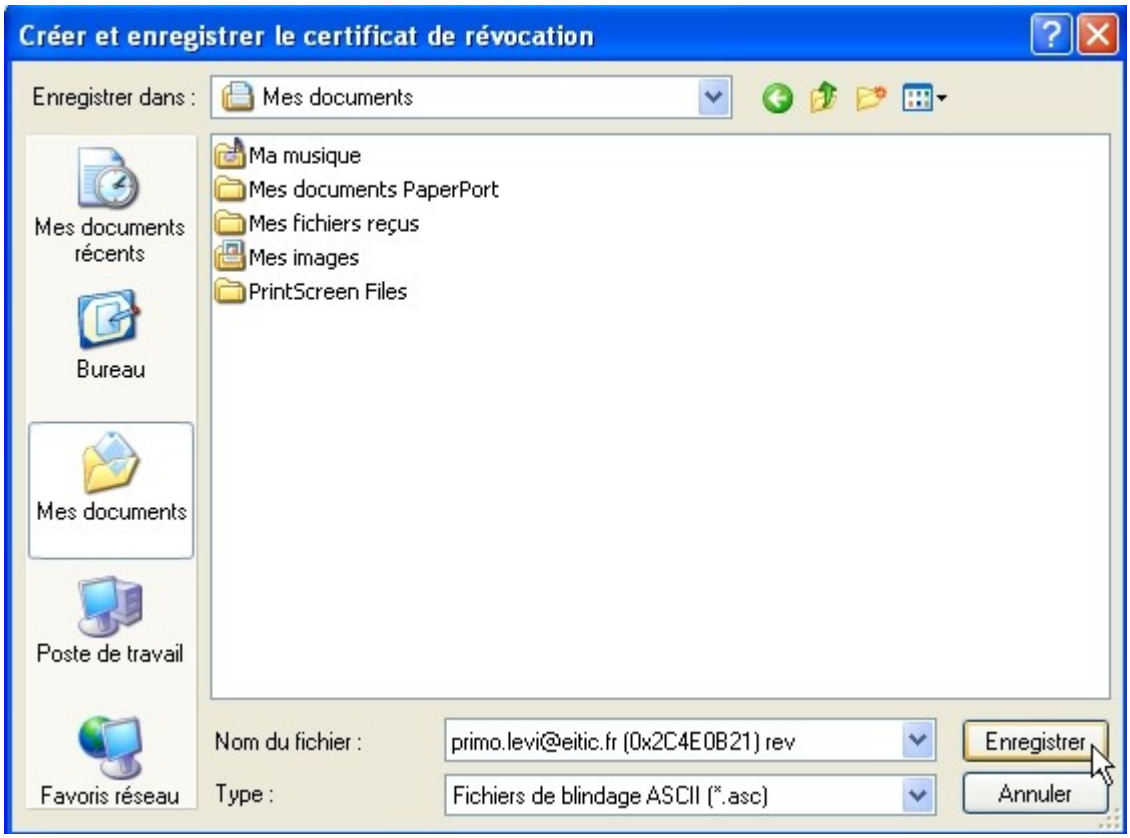
pendant la génération de la clef, travaillez normalement sur l'ordinateur, une forte activité rend votre clef plus forte !



La barre verte témoigne de l'activité de génération de la paire de clef.



Suivez scrupuleusement le conseil figurant sur la fenêtre qui vous signale la fin de la génération de la clef, enregistrez temporairement le fichier de révocation dans un répertoire de votre choix.



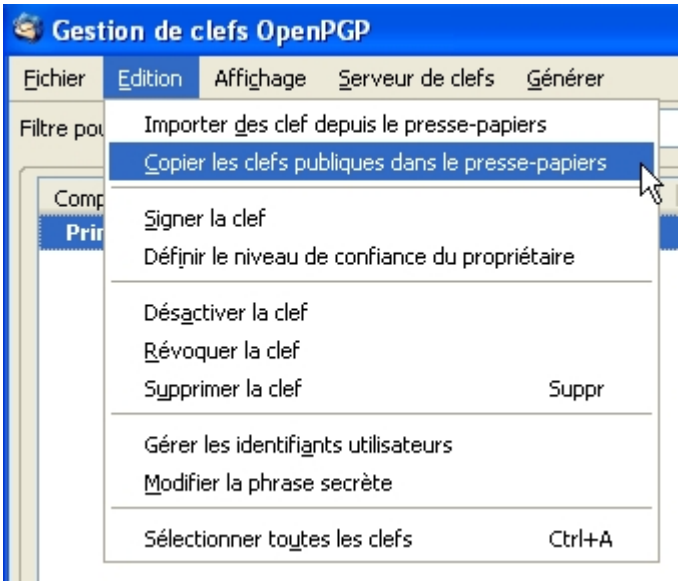
Pour cette opération, votre phrase secrète vous sera demandé pour la première fois.

Ne pas omettre de l'effacer dès qu'il sera transféré sur un autre support.

Maintenant, dans la fenêtre de gestion des clefs, votre clef apparaît.

Pour que vos correspondants puissent trouver votre clefs, vous pouvez l'envoyer sur un serveur de clefs
Sélectionnez votre clef
Dans le menu de la fenêtre « gestion des clefs » choisissez « Serveur de clefs » puis « Envoyer les clefs publiques ». Le serveur pgp.mit.edu est un bon choix car très connu. Mais sachez que tous les serveurs de clefs GPG communiquent entre eux.

Vous pouvez éditer votre clé publique et l'envoyer par mail à vos correspondants :



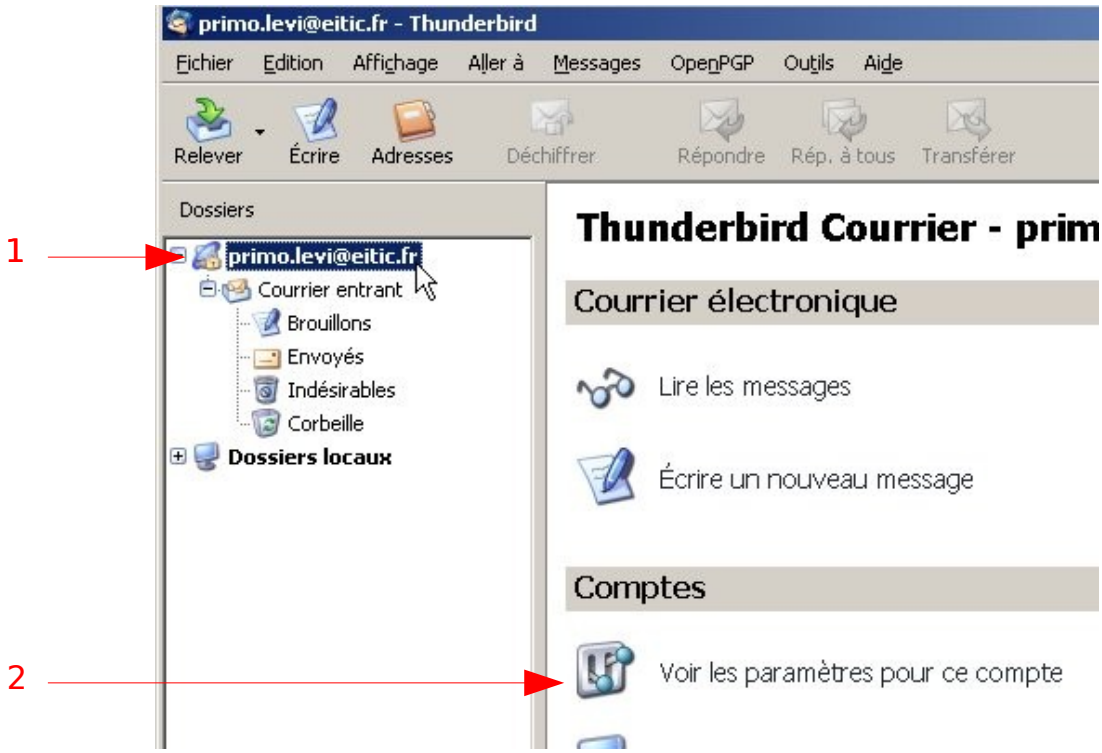
Choisissez, toujours dans la fenêtre de « Gestion des clefs » (accessible depuis le menu « Open GPG » de" Thunderbird) « Edition » puis « Copier les clefs publiques dans le presse-papiers », après avoir sélectionné votre clef.

Puis collez là (Ctrl+v) dans le bloc-notes de windows, pour l'enregistrer au format .txt et la garder en mémoire (il s'agit de votre clé publique, pas de la clé privée !).

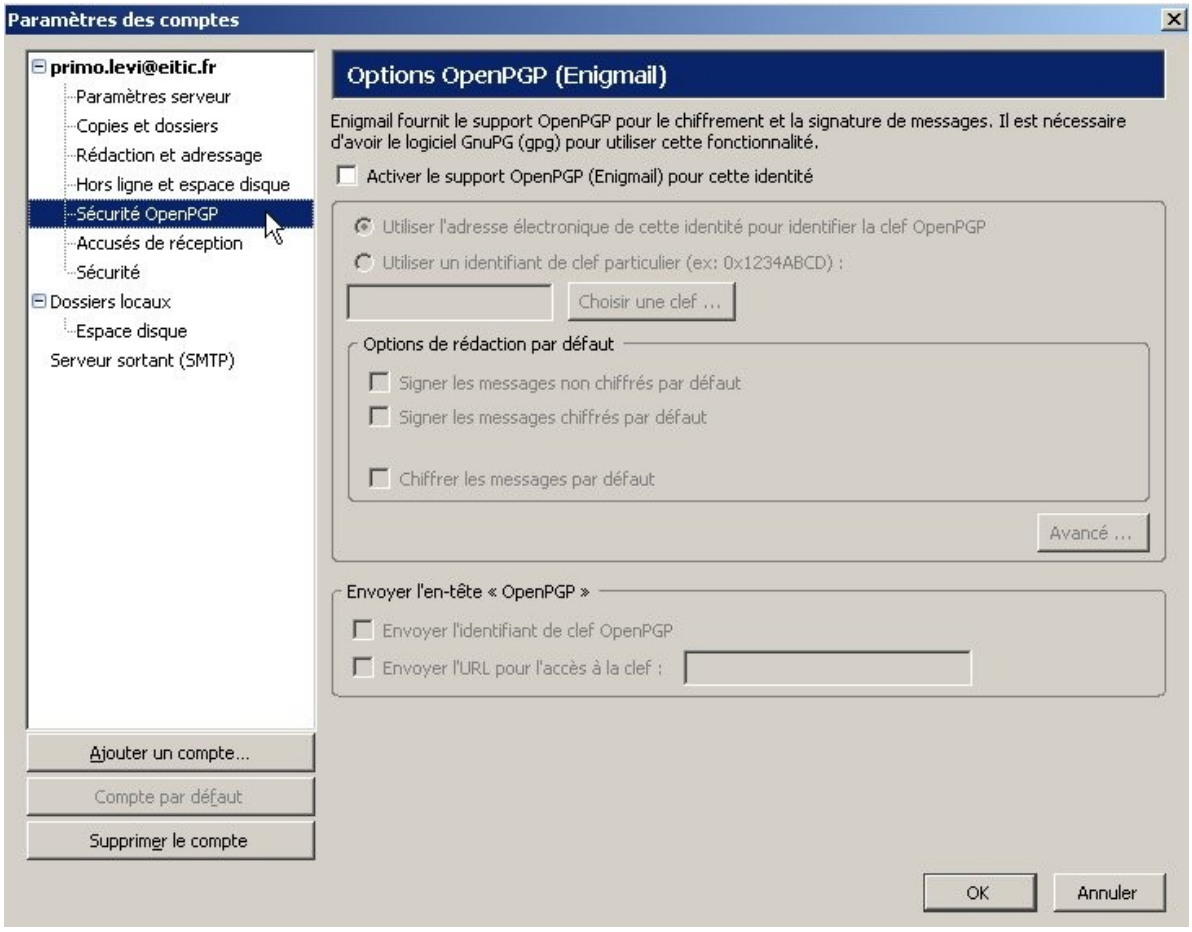
⚠ Attention, il faut copier du premier tiret au dernier, sans sauter de ligne.

N'utilisez surtout pas un traitement de texte type OpenOffice ou word pour la copie de la clef. Préservez le format texte simple.

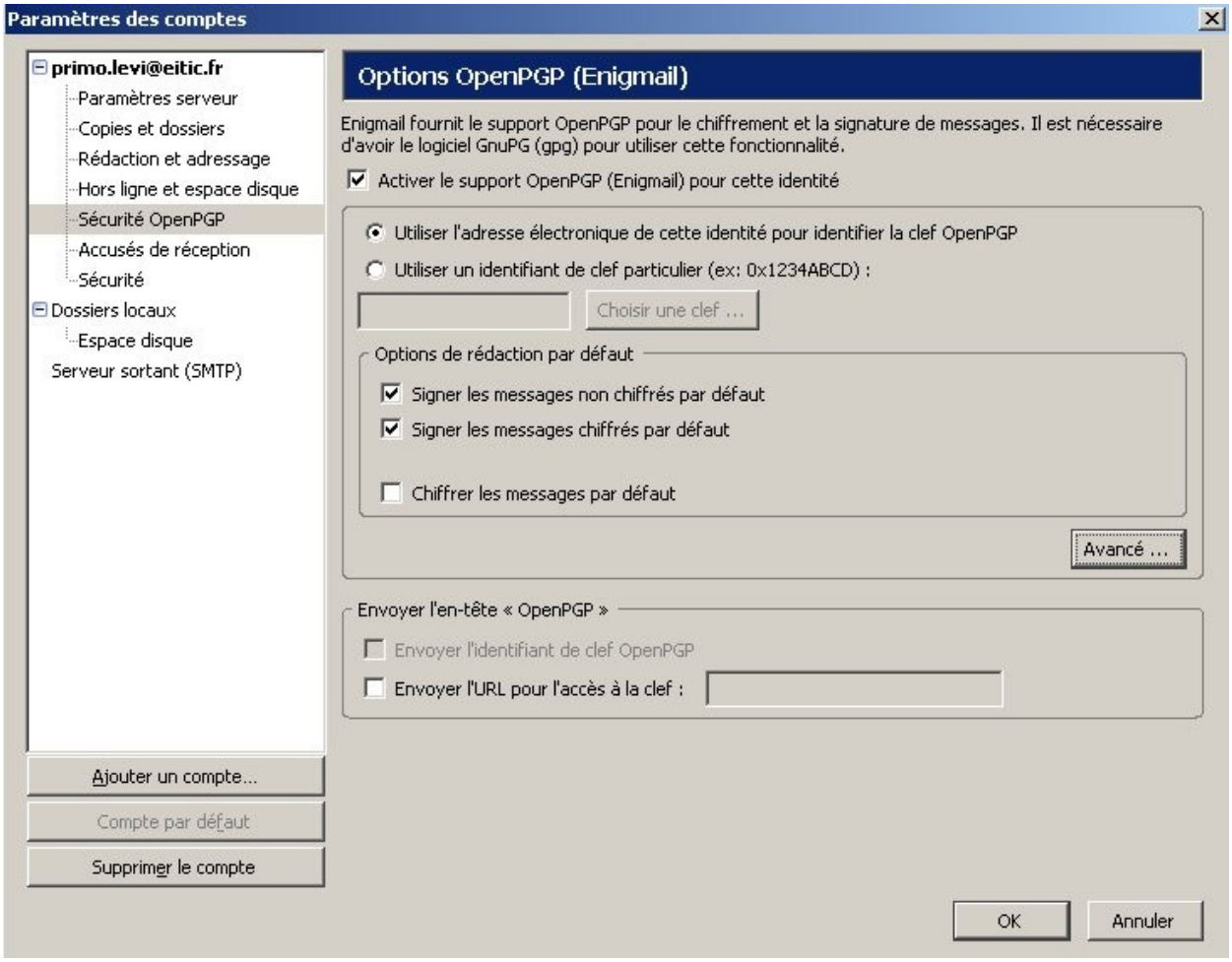
Configuration de Thunderbird



Cliquer sur l'adresse elle même (1) puis sur « Voir les paramètres pour ce compte » (2)



Dans le menu de gauche choisir « Sécurité OpenGPG »



Cochez les cases

- « Activer le support OpenGPG (Enigmail) pour cette identité »
- « Utiliser l'adresse électronique de cette identité pour identifier la clef OpenGPG »

Puis choisissez les options de rédaction par défaut qui vous conviennent, ici signer les messages chiffrés et non chiffrés automatiquement.

Validez en cliquant sur « OK ».

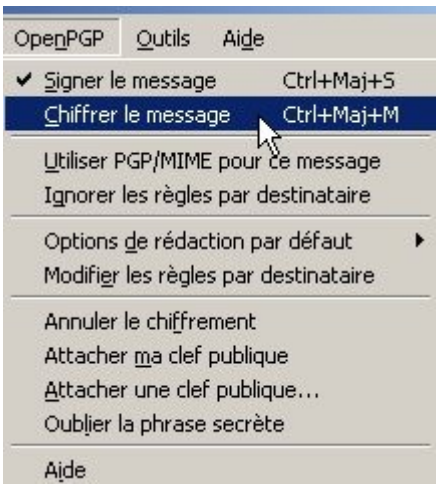
Envoi d'un message authentifié par signature GPG, et éventuellement chiffré

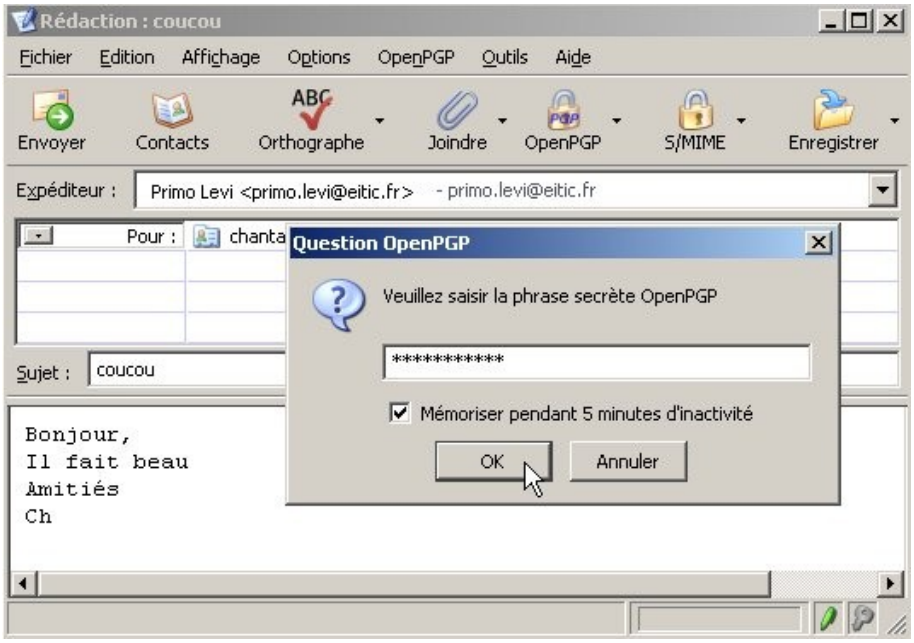
L'envoi de ce type de message est maintenant très aisé.

Rédigez votre message normalement.

Dans l'exemple nous avons choisi de signer automatiquement les messages envoyés.

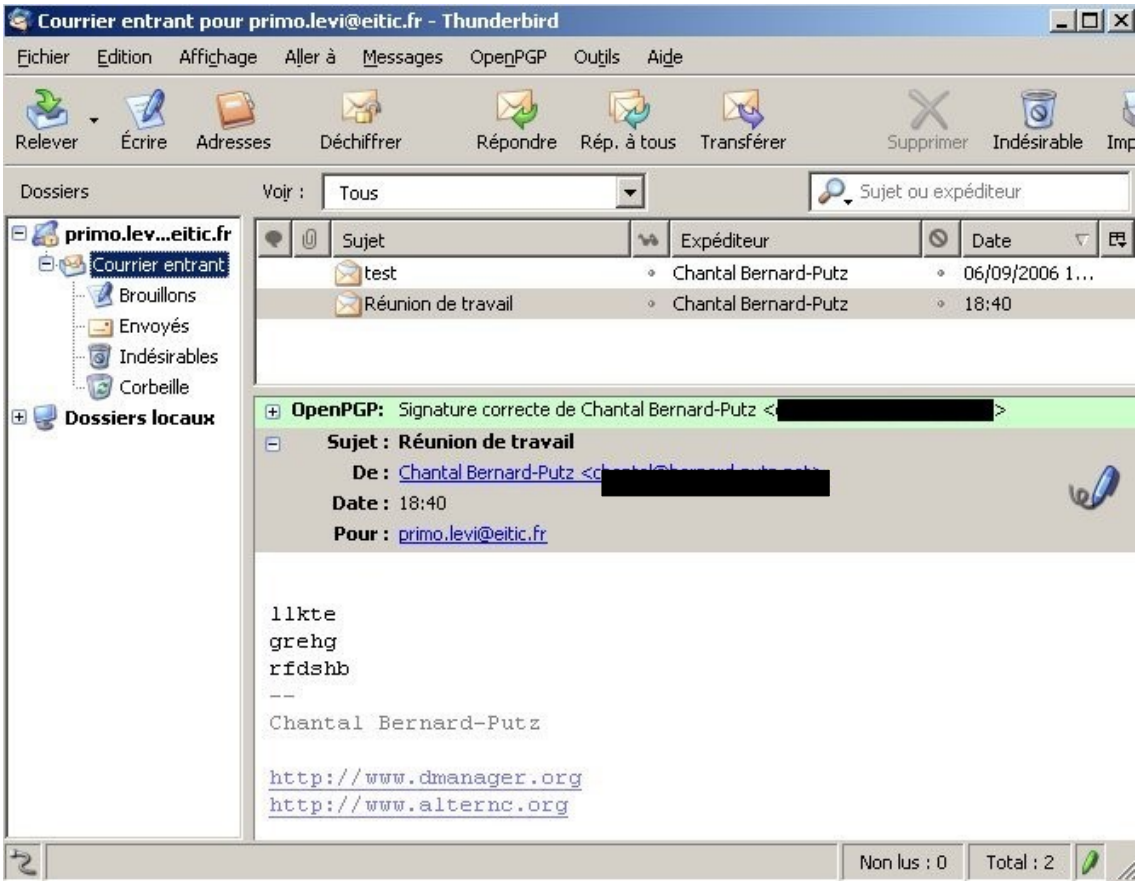
Il est toujours possible de chiffrer un message (dans la fenêtre de rédaction du message, depuis l'onglet « OpenGPG » cliquer sur « Chiffrer le message ») ou de ne pas signer (un clic sur « Signer le message » décochera cette fonction).





Au moment de l'envoi une fenêtre « Question OpenGPG » demandera la phrase secrète (mot de passe) de votre clé.

Réception d'un message signé (ou signé et chiffré)



Si vous avez la clé publique de votre correspondant un message surligné de vert vous confirmera que la signature est correcte.