Objectif et principe

Sur internet, il est très simple de se faire passer pour quelqu'un d'autre notamment avec le courrier électronique. C'est en effet à la portée de tout le monde d'envoyer un message en spécifiant un autre émetteur dans le paramétrage de son logiciel de messagerie. Par ailleurs, il peut être parfois intéressant d'envoyer des messages cryptés : envoi d'un mot de passe ou d'un code bancaire par exemple.

Pour répondre à ces deux problématiques, il existe un système permettant de signer d'une part et de crypter d'autre part ses messages. Afin d'obtenir un niveau de sécurité suffisant, ce système utilise des algorithmes mettant en place des paires de clefs.

Chaque interlocuteur possède une clef privée et une clef publique. Il est le seul à pouvoir utiliser sa clef privée (en saisissant la phrase secrète associée) alors qu'il diffuse à ses connaissances sa clef publique.

Pour signer un message et donc certifier que l'émetteur est bien la personne mentionnée dans l'entête du message, l'émetteur utilise sa clef privée et le destinataire contrôle grâce à la clef publique correspondante.

Pour crypter un message, l'émetteur utilise sa propre clef privée et la clef publique du destinataire qui pourra alors déchiffrer le message en utilisant sa clef privée.

Ce système s'appelle GnuPG. Il peut être utiliser directement dans Thunderbird grâce à Enigmail, une extension de Thunderbird.

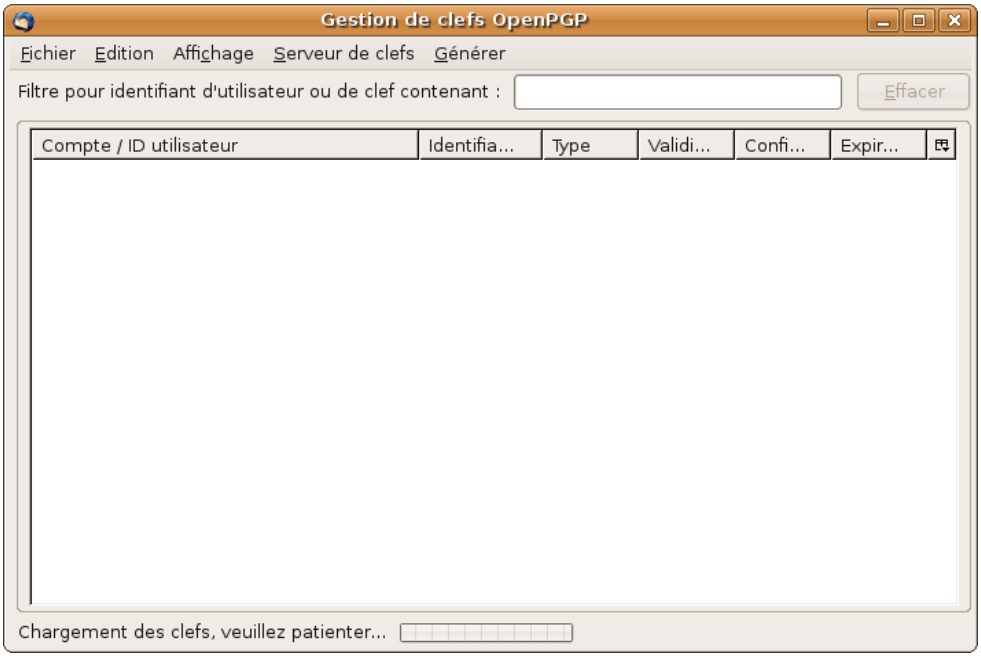
Installation

A l'aide du gestionnaire de paquet, installez les paquets suivants (sous Ubuntu) :
- gnupg
- enigmail
- enigmail-locale-fr
- seahorse

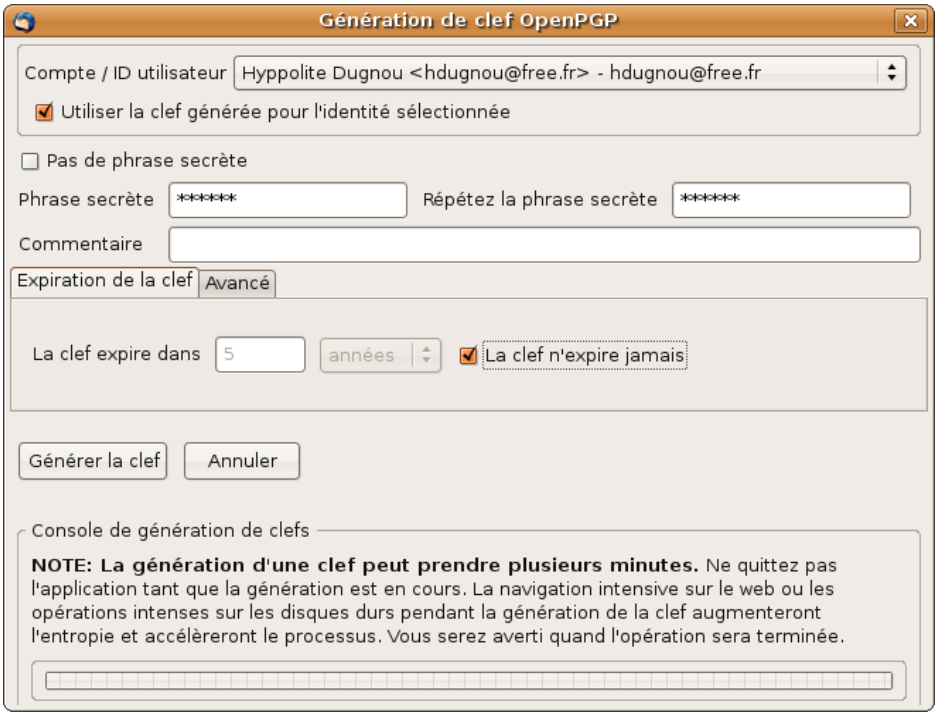
Création d'une paire de clef

Lancez Thunderbird. Vous pouvez utiliser l'assistant Enigmail qui se lance automatiquement mais je vous recommande plutôt cette méthode qui peut s'appliquer quand l'assistant ne se lance pas (c'est le cas lorsqu'on crée un compte mail plus tard) :

Menu OpenPGP > Gestion des clefs



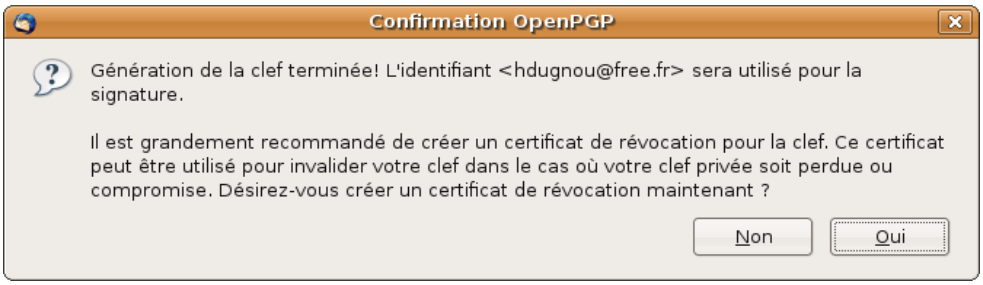
Menu Générer > Nouvelle paire de clefs



Choisissez le compte mail concerner par cette clef.
Entrez une phrase secrète dans les deux zones. Celle-ci vous sera demander par la suite à chaque utilisation de votre clef privée. Alors ne l'oubliez surtout pas !

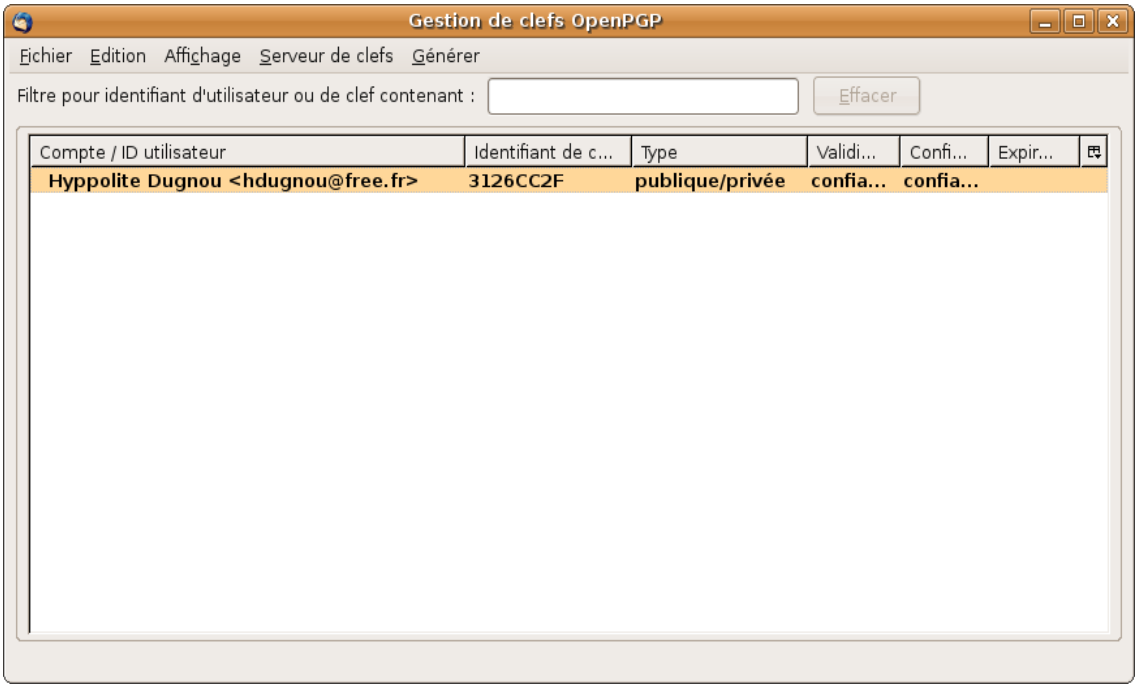
> Bouton Générer la clef

Utilisez votre ordinateur afin de générer des codes aléatoires.



Créez aussi un certificat de révocation en cas de perte de votre clef privée.
> Bouton Oui
Et stockez le en lieu sûr.

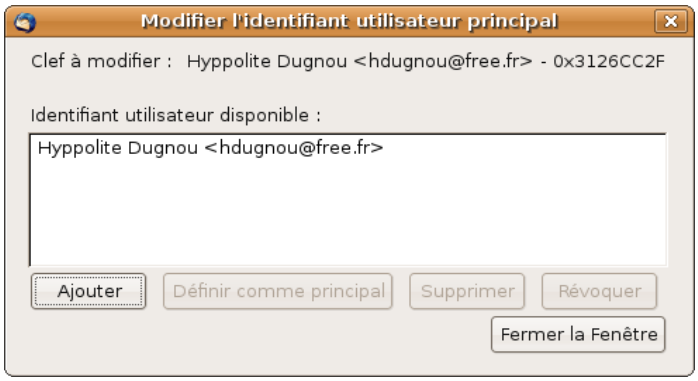
Voilà votre paire de clef est créée.



Signez votre paire de clefs : clic droit et "Signer la clef". Cette opération est nécessaire pour certains serveurs de clefs.

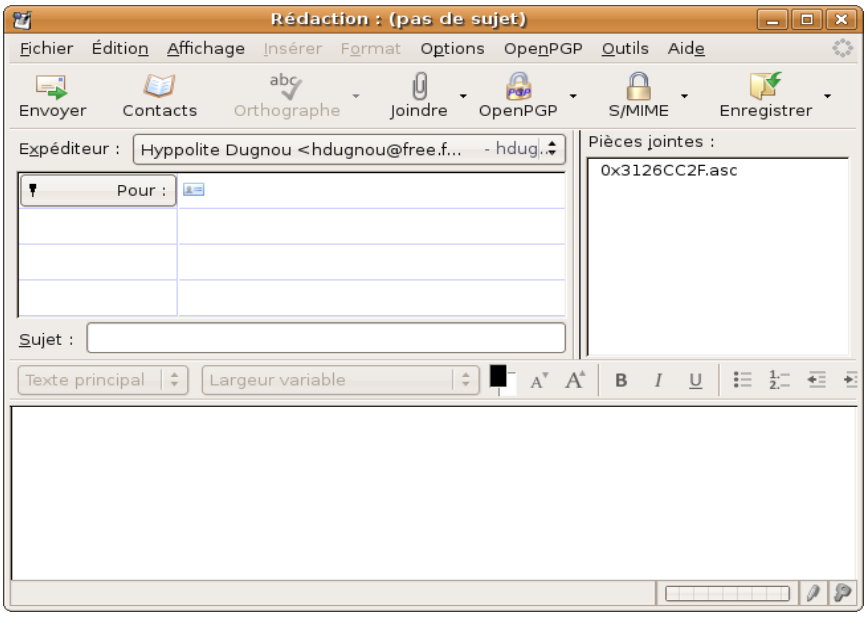
Vous pouvez répéter ces opérations pour chacun de vos comptes de messagerie.

Vous pouvez aussi utiliser la même paire de clefs pour plusieurs comptes mail. Dans ce cas, faites un clic droit sur la paire de clefs et choisissez "Gérer les identifiants utilisateur", ajoutez alors vos autres adresses mail



Publication de la clef publique

Vous pouvez envoyer par mail votre clé publique à vos interlocuteurs en faisant un clic droit sur vos clefs et "Envoyer des clefs publiques par courrier électronique"

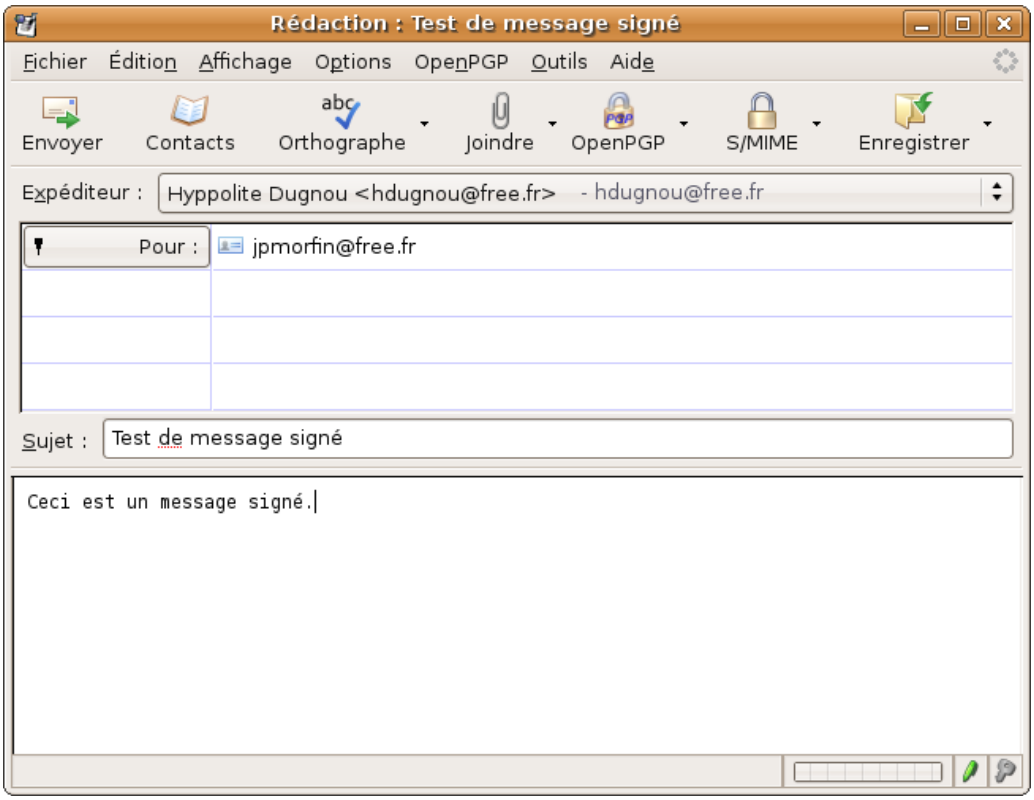


Il est aussi possible de publier ses clefs publiques par l'intermédiaire de serveurs de clefs consultables par tous. Ceci permettra à vos interlocuteurs de les retrouver automatiquement. Clic droit et "Envoyer les clefs publiques vers un serveur de clefs". Choisissez n'importe lequel des serveurs proposés.

Envoi d'un message signé

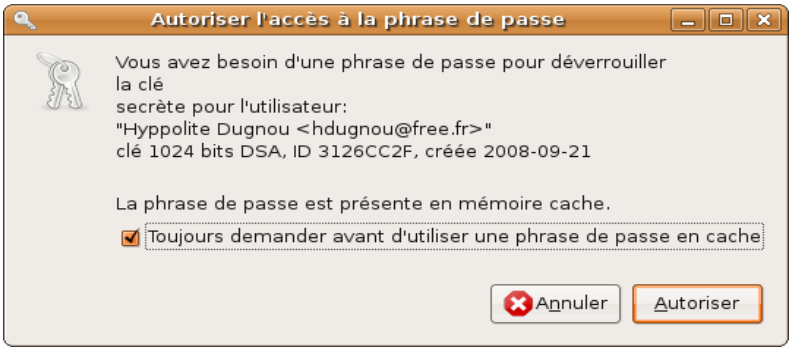
Une fois les clefs générées, la signature d'un message se fait très simplement avec Thunderbird et Enigmail. Créer un nouveau message en cliquant sur le bouton "Ecrire" (ou "Répondre") tout en maintenant la touche Maj (shift). Ceci permet de créer un nouveau message sans mise en forme (gras, italique...). Cela permet une meilleur compatibilité avec les autres logiciels de vérification de signature.

Cliquer sur le menu OpenPGP et cochez "Signer le message"



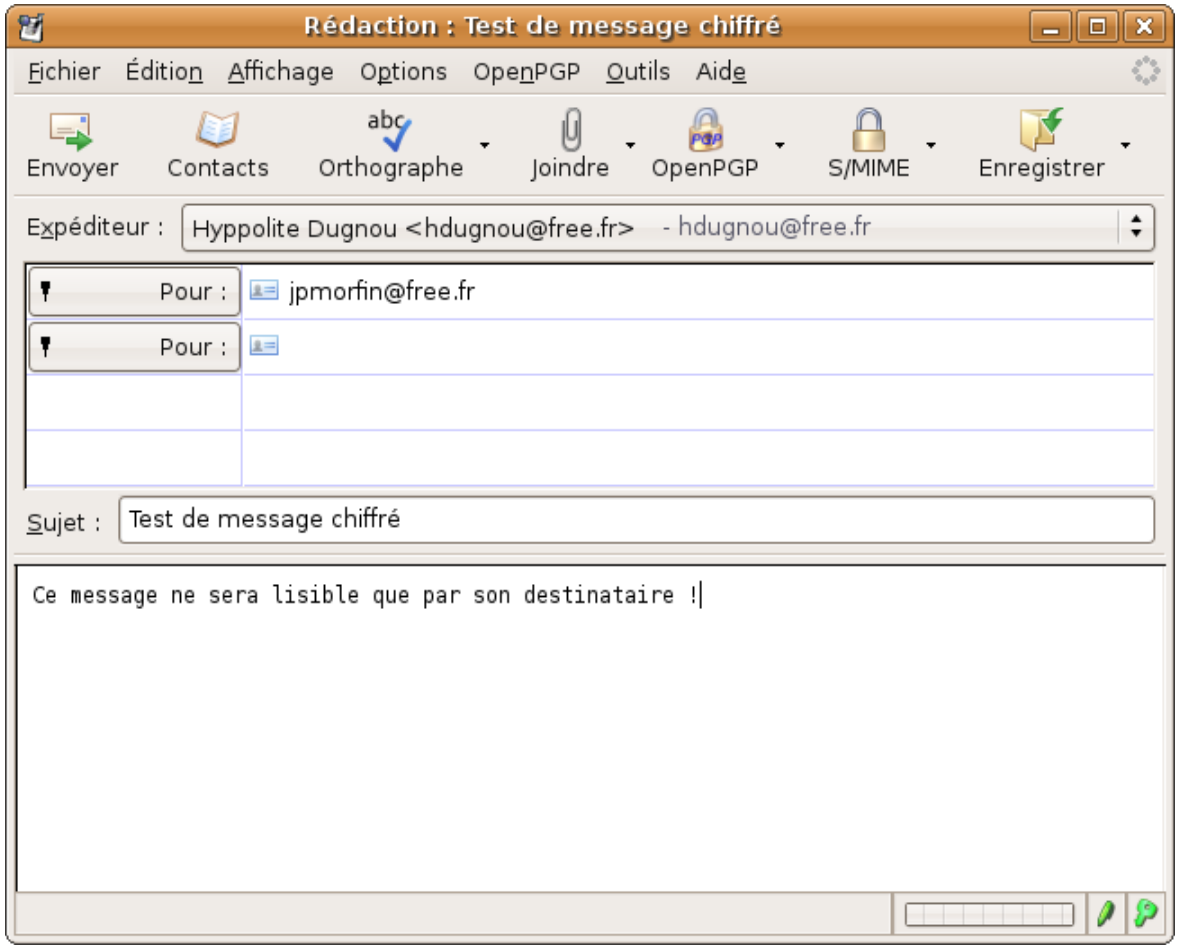
Vous remarquerez le petit crayon en vert en bas à droite de la fenêtre.

Une confirmation ou une demande de votre phrase secrète apparaît afin de pouvoir utiliser votre clef privée pour la signature.



Envoi d'un message chiffré

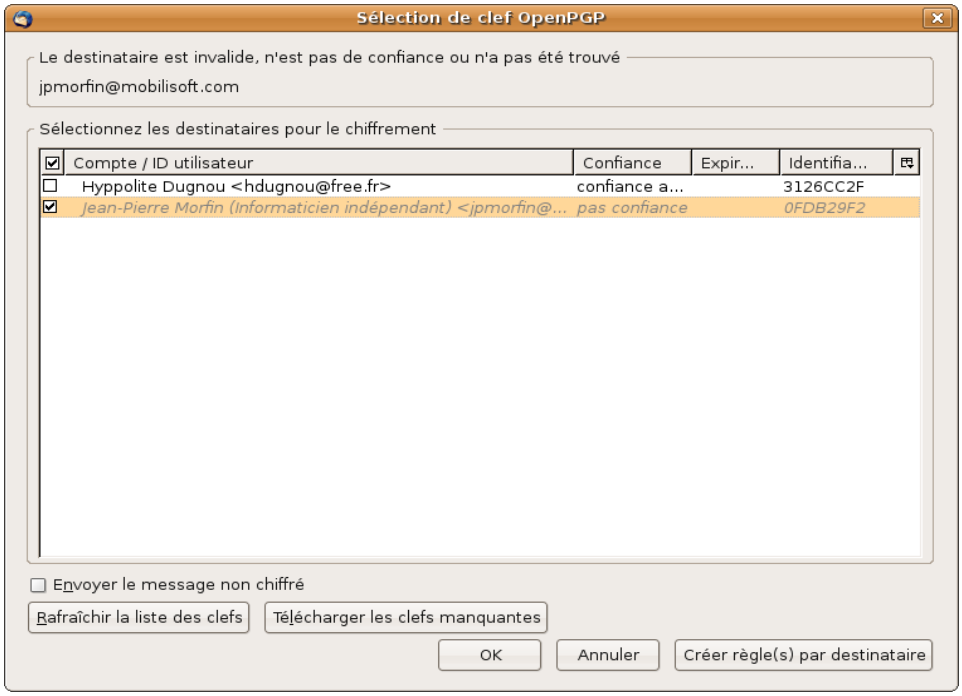
De même que pour la signature, il est préférable de créer un message en maintenant la touche Maj (shift). Tapez votre message et dans le menu OpenPGP, cochez "Signer le message" et "Chiffrer le message".



Cette fois-ci, le crayon et la clef sont en vert en bas à droite de la fenêtre de message.

Envoyez votre message.

Il est alors nécessaire de rechercher la clef publique du destinataire. Les serveurs de clefs sont là pour ça. Cliquez sur le bouton "Télécharger les clefs manquantes" si votre destinataire n'est pas dans la liste. Puis cochez-le dans la liste des clefs. Puis OK.

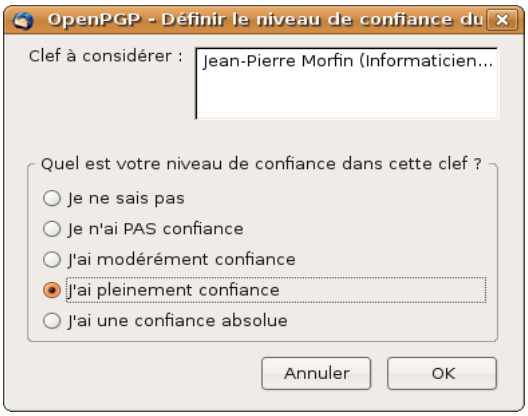


Réception d'un message chiffré

Si vous recevez un message qui a été chiffré par votre interlocuteur, votre phrase secrète vous sera automatiquement demandée pour le déchiffrer. Une petite enveloppe apparaît dans l'entête du message afin de connaître le niveau de confiance attribuée à la clef ayant signé et chiffrée le message.

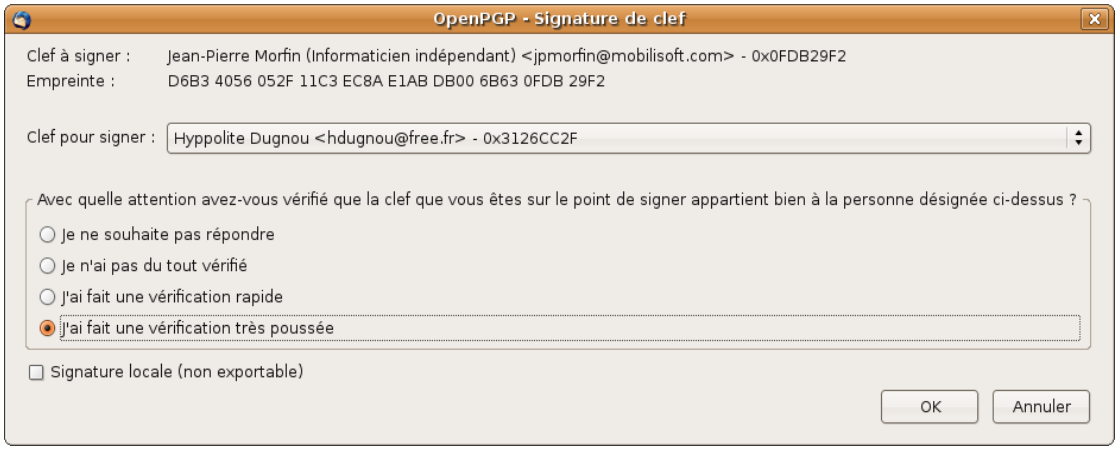
Niveau de confiance des clefs

Dans le gestionnaire de clefs, il est possible d'attribuer un niveau de confiance à chacune des clefs qui y sont stockées. Ceci en fonction de leur origine. Si vous avez obtenu une clef directement depuis votre interlocuteur (sur un support physique : CD, clef USB...) vous pouvez lui attribuer une confiance élevée. Alors que si vous l'avez simplement trouver sur un serveur de clefs, votre niveau de confiance sera plus modéré.
Clic droit sur la clef et "Définir le niveau de confiance du propriétaire"



Ces informations de niveau de confiance vous seront indiquées par la suite lors de la réception d'un nouveau message signé en cliquant sur l'enveloppe de l'entête du mail.

Une bonne pratique est de aussi de signer les clefs dans lesquels vous avez confiance. Clic droit sur la clef et "Signer la clef"



Ces informations sont alors partagées via les serveurs de clefs permettant ainsi la mise en commun du niveau de confiance des clefs sur le réseau. Pour connaître les personnes ayant signé une clef : clic droit sur une clef publique et "Voir les signatures".

Aller plus loin avec Seahorse

Seahorse est un outils de gestion de clefs plus pointu. Avec lui, vous pourrez par exemple inclure votre photo à votre clef, ajouter des sous clefs à vos clefs et faire tout un tas d'opérations les concernant.

Enigmail et Seahorse s'appuient tous les deux sur gnupg et partage donc la même base de clefs. gnupg peut d'ailleurs être utilisé directement en ligne de commande.
Pour plus d'informations, tapez dans un terminal : man gnupg

Sauvegarder ses clefs

Il est très important de ne pas perdre ses propres clefs (paires privées et publiques). Pour les sauvegarder, vous pouvez les exporter avec un clic droit sur la clef et "Exporter les clefs vers un fichier" que vous mettrez en lieu sûr. Si vous utilisez un utilitaire de sauvegarde, il suffit de sauvegarder le dossier /home/votreLogin/.gnupg

Dernier conseil : ne diffusez jamais vos clefs privées. Même s'il faut une phrase secrète pour l'utiliser, il existe des outils pour les "cracker".

Jean-Pierre Morfin
cours sous licence
Creative Commons By
http://www.g3l.org/