Tutoriel GPG

Ce qui suit est un rapide tutoriel permettant d'installer et de configurer GPG et tout ce qui va avec pour envoyer des mails chiffrés avec KMail. Bien que les opérations soient décrites pour une Mandriva LE 2005, ce tutoriel devrait également convenir aux utilisateurs d'autres distributions.

1. Installation des programmes

Il faut installer les packages **gnupg2**, **pinentry**, **cryptplug**. Le package **kgpg** peut également se révéler utile pour gérer son trousseau de clefs.
Avec mandrake, l'installation se fait facilement en tapant dans une console en root :

 # urpmi gnupg2
 # urpmi pinentry
 # urpmi cryptplug
 # urpmi kgpg (éventuellement)

2. Génération des clefs

Il faut maintenant que vous génériez une paire de clef publique/privée. Vous garderez précieusement votre clef privée, et distribuerez le plus largement possible votre clef publique (en tout cas, avec toutes les personnes avec qui vous voulez communiquer).
Il y a deux façons de faire, en ligne de commande avec gpg2, ou en utilisant l'interface graphique de kgpg.

Ligne de commande

La génération se fait simplement au moyen de la commande :

$ gpg --gen-key

Il faut spécifier le type de clef que l'on souhaite, prenez DSA + Elgamal, qui est le choix par défaut.
Il faut choisir la longueur de la clef, qui est comprise entre 1024 et 4096 bits de long. Plus la clef est longue, plus il devient dur de la casser, mais plus il faut de ressources pour les opérations de chiffrement / déchiffrement. Encore une fois, le choix par défaut (2048 bits) est très bien, et présente une **bonne** sécurité...
Il reste à rentrer quelques informations : la durée de validité de la clef, le nom d'utilisateur, l'adresse email.
Ca y est ! Votre paire de clef est générée, et rangée dans votre trousseau.
A ce stade, vous devriez également pensez à générer un certificat de révocation
(*gpg --gen-revoke*), qui vous servira à révoquer votre clef si elle est compromise.

Avec kgpg

La génération se fait en sélectionnant "Générer une clef", dans le menu clef. Une interface graphique s'ouvre, demandant les mêmes renseignements que précedemment. De même, on vous demanderat de générer également un certificat de révocation.

3. Configuration de gpg-agent

Il faut maintenant configurer gpg pour qu'il utilise gpg-agent.

Vérifiez que vous ayez bien la ligne suivante dans votre fichier gpg.conf (généralement situé dans le répertoire .gnupg) :

use agent

Dans le fichier gpg-agent.conf (situé dans le même répertoire), il vous faut :

pinentry-program /usr/bin/pinentry-qt
no-grab
default-cache-ttl 1800

4. Configuration de KMail

Nous avons fait le plus dur, la configuration de KMail est désormais simple. Il faut sélectionner la clef de cryptographie à associer à chaque compte mail (Configurer KMail, Rubrique Identité, Onglet Cryptographie), vérifier dans la rubrique Sécurité, onglet Modules externes de cryptographie que le module OpenPGP est bien sélectionné.

Ca y est !

Il est désormais possible, lors de la rédaction d'un email, de sélectionner la signature et le chiffrement. Preferrez signer et chiffrer avec OpenPGP/MIME plutôt que OpenPGP intégré, qui est à éviter. En effet, le chiffrement avec OpenPGP/MIME chiffre également les pièces jointes, au contraire de OpenPGP intégré.

5. Partager et importer des clefs publiques

Tout le système est configuré, il ne reste plus maintenant qu'à communiquer notre clef publique à nos correspondants, et récupérer leurs clefs publiques.

Un moyen pratique consiste à utiliser l'interface de kgpg.
Il suffit de sélectionner notre paire de clef, et d'exporter notre clef (Menu Clefs, Exporter la clef publique). Nous avons le choix entre divers moyens pour exporter notre clef. L'envoyer directement par email à nos correspondants, la sauver dans un fichier, que l'on peut ensuite mettre à disposition sur un site web, ou l'exporter sur un serveur de clef publique, où tous nos correspondants pourront la récupérer. Cette dernière option est la plus pratique. Le choix du serveur de clef importe peu, les serveurs se synchronisant entre eux.

L'import d'une clef peut se faire directement depuis un serveur de clef (Menu Fichier, Serveur de Clef). Comme dans un moteur de recherche, on tape le nom du correspondant dont on recherche la clef, avant de l'importer dans son trousseau de clefs.

Maintenant que vous avez communiqué votre clef à votre correspondant, et importée la sienne, il reste une dernière étape à effectuer : s'assurer de l'authenticité de la clef publique que vous venez de récupérer, pour vérifier que c'est effectivement celle de votre correspondant. Pour cela, vous devez signer la clef publique de votre correspondant avec votre clef secrête.
Pour vérifier la clef publique de votre correspondant, double-cliquez dessus pour ouvrir

ses propriétés. Il faut que l'empreinte de la clef en votre possession soit identique à l'empreinte que vous a communiqué votre destinataire. Idéalement, vous devriez rencontrer votre correspondant physiquement pour qu'il vous donne par écrit l'empreinte de sa clef. Si vous n'êtes pas paranoïaque, le fait d'avoir confirmation de l'empreinte par téléphone est suffisant. Ne faites PAS confiance à une empreinte que l'on vous a communiqué par email, sauf si ce mail est lui même signé et chiffré...

Une fois que vous vous êtes assuré que l'empreinte correspond, vous devez signer cette clef avec votre clef privée. Pour cela, dans kgpg, sélectionnez la clef publique de votre correspondant, puis dans le Menu Clef, choisissez Signer une clef. On vous demande avec quels soins vous avez vérifié l'authenticité de la clef (pas du tout, approximativement, minutieusement...).

Ouf, finit ! Vous pouvez maintenant échanger des mails avec votre correspondant en toute confidentialité (sous réserve que vos deux ordinateurs respectifs soient bien protégés, mais çà, c'est une autre histoire, et ce n'est pas le rôle de gpg...).