21 août 2008

# GnuPG : pour plus de confidentialité

Catégorie : Sécurité Tags : LP

~~Retrouvez cet article dans : Linux Pratique 32~~

Les échanges d'informations sur le réseau soulèvent parfois des problèmes de confidentialité. En effet, certains courriers électroniques peuvent facilement être lus par des personnes malveillantes... En outre, comment être sûr de la provenance d'un e-mail ? Afin de prévenir les problèmes de sécurité, il est, de nos jours, possible d'utiliser des procédés cryptographiques. En particulier, il existe des méthodes à clés asymétriques, permettant soit de signer un e-mail, soit de le chiffrer. GnuPG est l'un des outils (libre de surcroît) utilisant un système à clés asymétriques.

## Créer ses clefs

Tout d'abord, il faut vérifier que l'application ~~gnupg~~ est installée sur votre machine. Si ce n'est pas le cas, rendez-vous sur le site officiel (http://www.gnupg.org/).
Attention ! La création des clefs est une étape importante et une faute de frappe est vite arrivée ! Remarquez tout d'abord que vous disposez d'un répertoire ~~.gnupg/~~ dans votre répertoire personnel. Il contient, entre autres, un fichier nommé ~~gpg.conf~~. Ce fichier contient notamment des adresses de serveurs de clefs (par exemple, hkp://subkeys.pgp.net). Ainsi, si vous entrez la commande :

```
$ gpg --search-keys dupont
```

Cette commande interroge le serveur de clefs (par défaut celui mentionné dans ~~gpg.conf~~). Toutes les clés publiques au nom de Dupont s'affichent à l'écran. Elles peuvent être en cours d'utilisation ou supprimées (mention revoked)
Pour créer votre clef, il faut entrer la commande :

```
$ gpg --gen-key
```

Diverses questions vous sont posées, choisissez les propositions par défaut (c'est-à-dire, « 1-DSA et ElGamal », « 1024 bits » et « 0 = la clé n'expire pas »). Renseignez ensuite votre nom réel (ex. : Jean Dupont), votre adresse e-mail (ex. : jean.dupont@societe.net) et un commentaire (pourquoi pas le nom de votre société par exemple).
Ce sont les informations que tout le monde pourra voir, une fois que vous aurez envoyé votre clef publique sur un serveur. Enfin, un mot de passe vous est demandé. Il sera utile lorsque vous souhaiterez signer et/ou chiffrer vos e-mails (ne l'oubliez pas !).
Ensuite, le programme génère automatiquement vos clefs (publique et privée).
Pour vérifier :

```
$ gpg –list-key
/home/jean/.gnupg/pubring.gpg
-----------------------------
pub  XXXXX/XXXXXXXX 2005-10-04 Jean Dupont (Société) <jean.dupont@societe.net >
sub  XXXXX/XXXXXXXX 2005-10-04
```

(La série de X représente une série de nombre quelconque. Le deuxième nombre de la ligne pub, composé de 8

chiffres et caractères, constitue les derniers termes de votre fingerprint (l'empreinte de votre clef) et constitue l'identifiant (ou ID) de votre clef.

# Création du Certificat de révocation

Si un jour votre clef est compromise (par exemple, si quelqu'un vous vole votre clef privée), il sera utile de pouvoir supprimer cette clef. Il faut donc créer ce que l'on appelle un « certificat de révocation ». Pour cela, entrez la commande suivante :

```
$ gpg --gen-revoke XXXXXXXX > revoke_XXXXXXXX (remplacez XXXXXXXX par la série de 8 chiffres et caractères de la ligne pub, voir précédemment).
```

Cette commande génère un fichier, nommé ~~revoke_XXXXXXXX~~, contenant la signature pour la révocation de votre clef (si besoin). À nouveau, acceptez les propositions par défaut à chaque question posée et choisissez bien « votre clé a été compromise ». Enfin, vérifiez que le fichier n'est pas vide.

# Ajouter des clefs à son trousseau

Peut-être avez-vous déjà reçu un e-mail se terminant par « Signature Non Valide ». Cela ne signifie pas que votre correspondant a fait une mauvaise manipulation, mais simplement qu'il ne fait pas partie de votre « trousseau de clefs ». Qu'est-ce que cela signifie ?
Vous avez à présent votre trousseau et vous souhaitez ajouter des personnes clairement identifiées à votre trousseau. Dans la pratique, cela devrait se passer comme cela : vous vous rencontrez à une réunion et vous échangez vos cartes de visite. Vous aurez pris soin d'inscrire sur votre carte de visite le fingerprint de votre clef publique. Vous avez en plus pris le soin de vérifier de vos propres yeux que la personne est bien celle qu'elle prétend être (!)
La réunion est terminée et vous rentrez chez vous. Vos allez à présent mettre à jour votre trousseau de clefs et de contacts certifiés. Notez que les 8 derniers caractères du fingerprint de votre ami correspondent à l'ID de sa clef (comme précisé plus haut).
Maintenant, il vous faut télécharger sa Clef Publique :

```
$ gpg --recv-key XXXXXXXX
```

Puis, vous vérifiez le fingerprint :

```
$ gpg --fingerprint XXXXXXXX
```

Si ces nombres sont identiques, vous pouvez signer la clef, c'est-à-dire approuver avec certitude que cette clef est bien celle de votre ami :

```
$ gpg --sign-key XXXXXXXX
```

(répondez que « oui, vous avez vérifié très soigneusement »)
Enfin, vous pouvez renvoyer cette clef publique (celle de votre ami) sur le serveur, avec votre garantie sur son identité, ce qui accorde encore un peu plus de crédit sur l'authenticité de la clef (dans la pratique, peu de gens pensent à cette étape).

```
$ gpg --send-key XXXXXXXX
```

À présent, si votre ami vous envoie un message signé, la mention « Signature valide » apparaîtra en bas de son e-mail. Vous aurez donc l'assurance que c'est bel et bien lui qui vous a envoyé cet e-mail.
Si jamais au moment de la vérification du fingerprint celui-ci s'avère ne pas correspondre, il vous faut alors supprimer la clef publique de votre trousseau via la commande : ~~gpg --delete-keys XXXXXXXX~~

# Chiffrement du message

Votre client de messagerie vous permet d'envoyer un message signé et/ou chiffré (sous Evolution : menu Sécurité dans Nouveau Message).
Si vous envoyez un message signé et/ou chiffré, vous aurez à entrer votre mot de passe pour valider l'envoi. Puis, votre message va parcourir le réseau jusqu'à l'ordinateur du destinataire sous forme chiffrée à partir de votre clef publique. Seul le détenteur de la clef privée associée sera en mesure de déchiffrer votre message.
En outre, vous avez certainement remarqué qu'une fois que vous avez envoyé un message chiffré, vous ne pouvez plus lire le message ! (à moins d'avoir effectué une sauvegarde en clair). En effet, celui-ci est chiffré et vous n'avez pas la clef pour le déchiffrer, puisque c'est votre destinataire qui l'a !

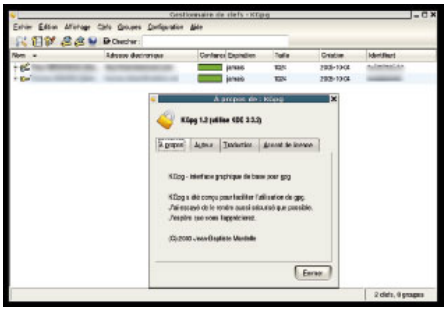
Lorsque vous recevez un message chiffré, si tous les éléments sont réunis, Evolution (ou tout autre client de courriels) traite le message afin de le présenter en clair, mais le message reste stocké chiffré sur votre système. Il vous faudra d'ailleurs ressaisir le mot de passe à chaque fois que vous souhaiterez lire le message en question. Plutôt que de préciser à chaque envoi que vous signez et chiffrez le message, il est possible de régler ces options par défaut via les préférences de votre client de courriel.
Dans Evolution, menu Outils > Paramètres, sélectionnez votre compte e-mail, puis cliquez sur Éditer. Choisissez ensuite l'onglet Sécurité. Dans la partie « Pretty Goog Privacy », renseignez d'abord l'ID de votre clef, puis cochez parmi les options proposées celles qui vous conviennent. Enfin, confirmez vos réglages en cliquant sur Valider.

# Interfaces graphiques disponibles

Nous venons de voir comment utiliser gnupg en ligne de commande, mais il existe plusieurs interfaces graphiques pour vous permettre de créer et de gérer vos clefs simplement.

- Tout d'abord, Seahorse, interface graphique de l'environnement Gnome (Fig. 1)


- Puis, Kgpg, interface graphique de l'environnement KDE (Fig. 2)



- Enfin, certains clients de mail disposent d'un outil intégré pour gérer les clefs de cryptage. Thunderbird, par exemple, dispose du plugin Enigmail, dont l'utilisation est détaillée dans l'article suivant.

### Liens

- Site officiel GnuPG : http://www.gnupg.org/
- Un document très complet sur le sujet : http://matrix.samizdat.net/crypto/gpg_intro/index.html
- Site officiel de Seahorse : http://seahorse.sourceforge.net/
- Site officiel de Kgpg : http://developer.kde.org/~kgpg/french.html

~~Retrouvez cet article dans : Linux Pratique 32~~

Posté par Fleur Brosseau (Fleur) | Signature : Fleur Brosseau | Article paru dans

### Laissez une réponse

Vous devez avoir ouvert une session pour écrire un commentaire.

« Précédent Aller au contenu »

Identifiez-vous
Inscription

- Programmation
- Réfléchir
- Sécurité
- Utilitaires
- Web

## Archives

- septembre 2008
- août 2008
- juillet 2008
- juin 2008
- mai 2008
- avril 2008
- mars 2008
- février 2008
- janvier 2008
- décembre 2007
- novembre 2007
- février 2007

## GNU/Linux Magazine

- GNU/Linux Magazine 108 - Septembre 2008 - Chez votre marchand de journaux
- Edito : GNU/Linux Magazine 108
- GNU/Linux Magazine HS 38 - Septembre/Octobre 2008 - Chez votre marchand de journaux
- Edito : GNU/Linux Magazine HS 38
- GNU/Linux Magazine 107 - Juillet/Août 2008 - Chez votre marchand de journaux

## GNU/Linux Pratique

- Linux Pratique N°49 -Septembre/Octobre 2008 - Chez votre marchand de journaux
- Edito : Linux Pratique N°49
- À télécharger : Les fichiers du Cahier Web de Linux Pratique n°49
- Linux Pratique Essentiel N°3 - Août/Septembre 2008 - Chez votre marchand de journaux
- Edito : Linux Pratique Essentiel N°3

## MISC Magazine

- Misc 39 : Fuzzing - Injectez des données et trouvez les failles cachées - Septembre/Octobre 2008 - Chez votre marchand de journaux
- Edito : Misc 39
- MISC 39 - Communiqué de presse
- Salon Infosecurity & Storage expo - 19 et 20 novembre 2008.
- Misc 38 : Codes Malicieux, quoi de neuf ? - Juillet/Août 2008 - Chez votre marchand de journaux