par Iznogood
<iznogood/at/iznogood−factory.org>

L´auteur:

Je suis sous GNU/Linux depuis un bon moment et actuellement sur une Debian. Malgré des études électronique, je fais surtout du travail de traduction pour la communauté GNU/Linux, disponible sur Iznogood−Factory.

Contrôler des signatures gpg des courriels avec Sylpheed−Claws

Résumé:

Je vais tenter de montrer comment installer un greffon gpg et contrôler une signature de courriel avec Sylpheed−Claws en utilisant quelques commandes de bash par tubes.

Traduit en Français par:
Iznogood
<iznogood/at/iznogood−factory.org>

Pourquoi contrôler les signatures?

J'ai un jour reçu un courriel d'un ami qui m'a demandé: "Pourquoi m'as−tu envoyé un courriel avec un virus en pièce jointe?" Houlà! Quelqu'un avait pris mon adresse et s'en était servi pour lui envoyer un courriel... Nous avons eu de la chance car le virus a été détecté. Mais que serait−il passé s'il n'y avait eu qu'une date de rendez−vous pour nous rencontrer dans une ville à 150 kms de sa maison, comme nous en avons pris l'habitude... ou un patch pour un programme en développement. Ce serait une mauvaise journée!

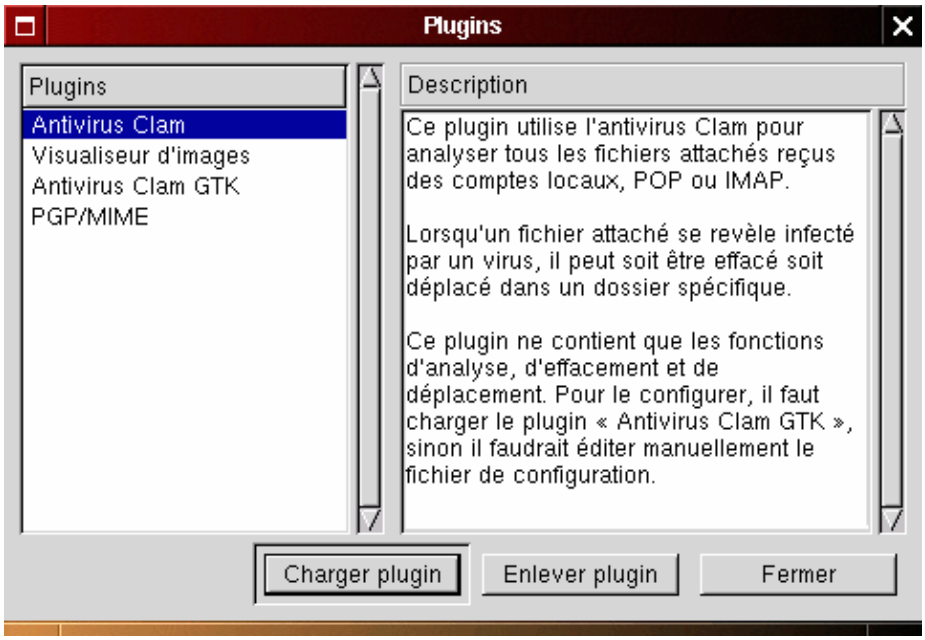
Depuis ce jour, je signe toujours mes courriels. Et je vérifie celles des courriels que je reçois lorsqu'ils en ont. C'est une sécurité supplémentaire contre les intrus. Mais quelque fois, je reçois un courriel d'une nouvelle personne avec une signature gpg que je n'ai pas encore contrôlée. Comme je suis très fainéant, je ne veux pas à chaque fois ouvrir un xterm, écrire la commande gpg pour avoir la clé publique dans mon trousseau et vérifier alors la signature pour chaque nouvelle adresse de courriel. C'est pourquoi je l'ai fait réaliser comme une action depuis Sylpheed−Claws.

À propos de Sylpheed

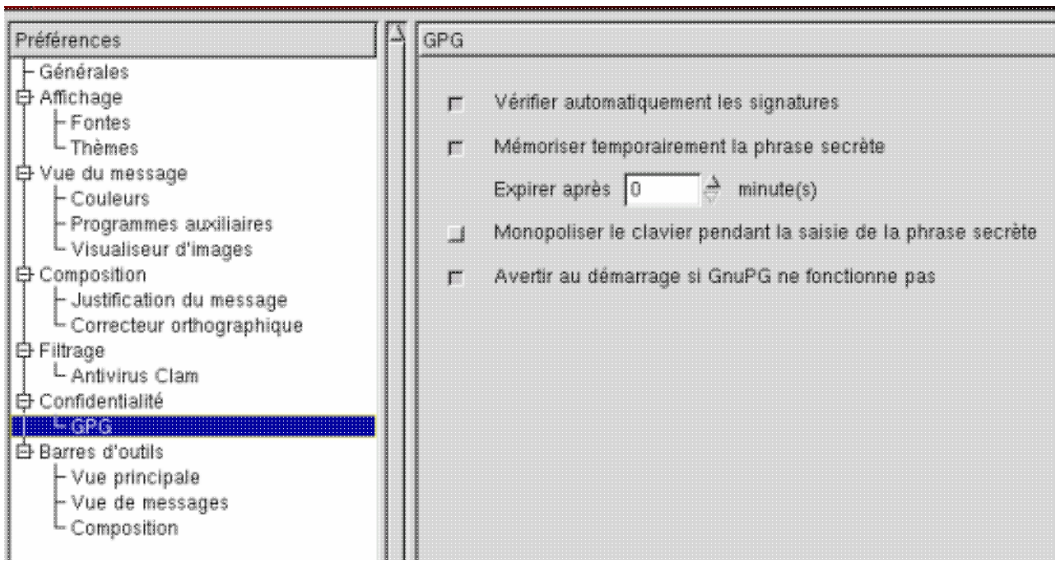
Sylpheed est un gestionnaire de nouvelles et de courriels graphique, avec GTK, léger et rapide. Il est disponible en deux versions: Sylpheed, la branche principale et Sylpheed−Claws, la version plus avancée. Sylpheed−Claws supporte GPG avec un greffon appelé PGP/MIME.
Vous avez besoin de sylpheed−claws, sylpheed−claws−plugins, sylpheed−claws−pgpmime et gpg de compilés sur votre machine. Pour les utilisateurs de Debian Sarge, c'est plus facile avec aptitude, vous avez simplement besoin de télecharger les paquets ci−dessus (parmi d'autres mais vous pouvez faire une recherche) ou vous pouvez faire un

```
apt-get install sylpheed-claws sylpheed-claws-plugins sylpheed-claws-pgpmime gpg
```

Pour le rendre fonctionnel, vous avez besoin d'aller dans Configuration −> Plugins puis Chager le greffon appelé pgpmime.so comme montré sur les images (vous pouvez, bien sûr, choisir d'autres greffons pour vous aider à utiliser Sylpheed−Claws).

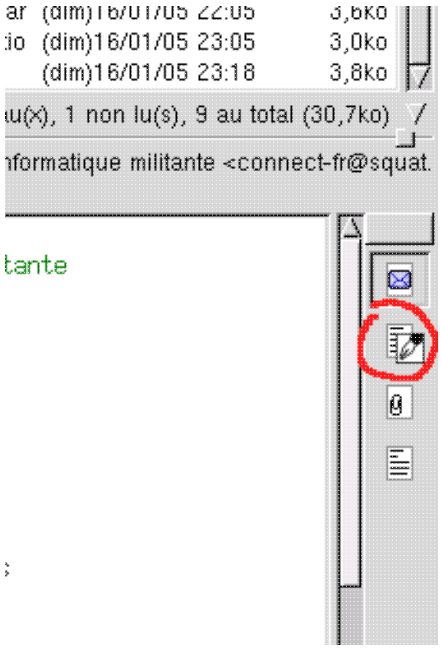


Cela vous montrera PGP/MIME sur la gauche. Vous pouvez maintenant fermer la fenêtre. Allez ensuite dans Preferences dans le menu de Configuration.



Sur la gauche, vous avez Confidentialité –> GPG. Cliquer dessus vous montrera 4 cases à cocher. Vous devez au moins valider la première (Contrôle automatique de signature). Vous pouvez maintenant contrôler vos mesages. Les autres sont intéressantes si vous signez vos messages: la seconde garde votre mot de passe pendant la session, la troisième vous donne la main lors de la saisie au clavier et la dernière vous prévient si gpg ne fonctionne pas.

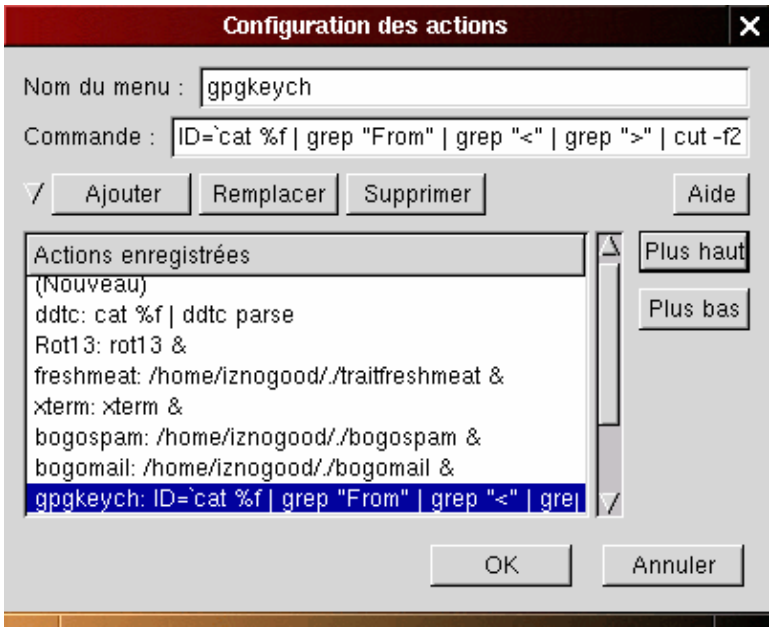
S'il y a un message avec une signature, vous verrez ce logo sur la droite du corps du message:



Cette icône avec une plume montre que le contrôle avec gpg est actif mais que l'auteur n'est pas dans votre trousseau ou que la signature st mauvaise.

Comment faire un contrôle de signature?

Dans Sylpheed–Claws, vous pouvez réaliser des actions avec Outils –> Actions lorsque vous êtes sur le courriel que vous voulez contrôler. Mais nous devons d'abord le programmer dans Configuration –> Actions. Vous l'ouvrez:



Dans le nom de menu, vous placez le nom de la commande (vous pouvez choisir celui que vous voulez), la commande dans Commande (très difficile!) et vous l'Ajoutez. Vous avez ici la commande tubée pour faire le contrôle gpg:

```
ID=`cat %f | grep "From" | grep "" | cut -f2 -d\< | cut -f1 -d\> `;
xterm -e gpg --keyserver wwwkeys.ch.pgp.net --search-key $ID
```

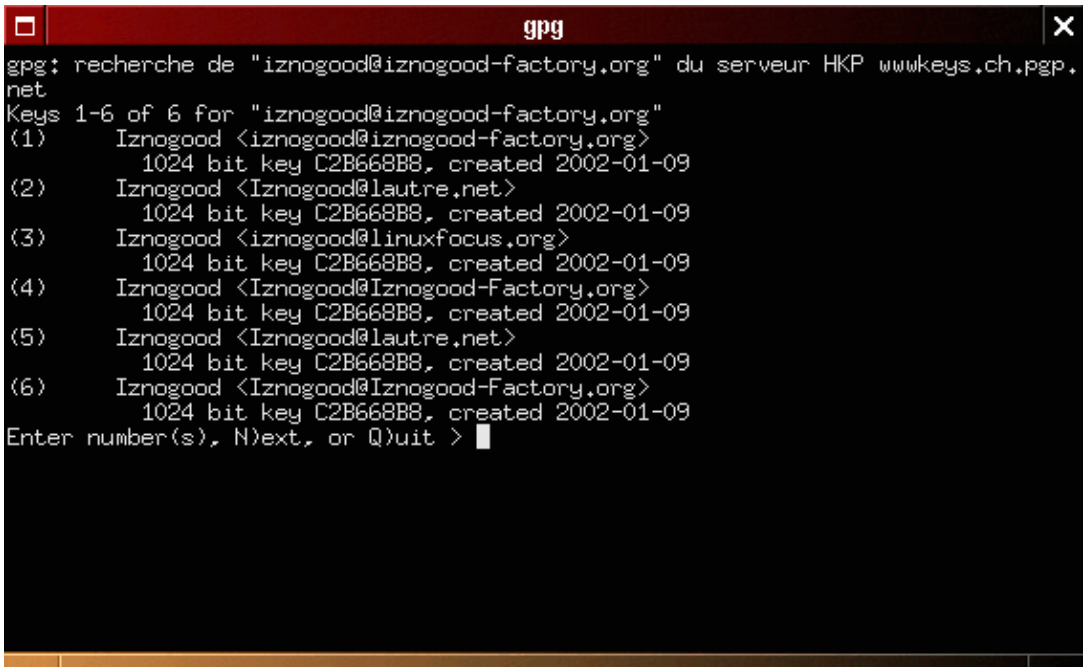
en une ligne. La commande gpg normale est:

```
gpg --keyserver servername --search-key email-address
```

avec sylpheed–claws, nous l'ouvrons dans un xterm avec "xterm –e" car nous avons toujours besoin de choisir une des options dans les noms proposés. Pour avoir l'adresse de courriel, l'$ID:

- nous lisons le message avec cat %f
- nous cherchons la ligne From avec ""
- nous gardons tout après ""

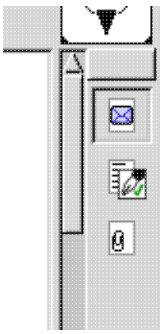
et nous avons l'adresse.
Lorsque nous contrôlons une adresse de courriel avec Actions, nous allons sur le serveur de clés wwwkeys.ch.pgp.net mais vous pouvez le remplacer par le votre ou vous pouvez avoir deux actions différentes avec deux serveurs de clés, comme moi.
Vous verrez cet xterm:



Choisissez la bonne adresse et la fenêtre se ferme. Vous avez juste à recontrôler avec l'icône sur la droite qui ouvrira un dialogue avec un bouton sur le bas pour la revérification. C'est fait! Vous devez avoir cette icône:

Si ce n'est pas le cas, cela signifie que la signature est fausse et vous pouvez mettre le courriel dans la poubelle.

Si vous avez cette icône, cela signifie que l'émetteur est un ami ou une personne en qui vous avez confiance dans votre trousseau de clés car vous devez l'avoir considéré(e) comme de confiance.



Vous n'aurez à le faire qu'une fois pour chaque nouvelle adresse de courriel et tous les courriels seront contrôlés. Votre sécurité en sera améliorée.

Conclusion

Il devrait être facile d'adapter les commandes bash en tubes vers un autre lecteur de courriel, graphique ou pas. Il est assez facile de contrôler vos courriels automatiquement. Un autre avantage: ces courriels contrôlés n'ont pas besoin de passer au contrôle anti−spam car l'adresse a été contrôlée une fois et, de ce que j'en sais, les spams n'utilisent pas de signature gpg. C'est, sans aucun doute, une manière de contrôler les courriels signés directement en entrée avec procmail pour les valider mais c'est une autre histoire que vous trouverez sur Iznogood−Factory.

Vous pouvez trouver plus d'informations sur gpg et les signatures de courriel sur:

http://www.gnupg.org/

et pour Sylpheed−Claws, c'est ici.

2005−01−21, generated by lfparser_pdf version 2.51