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

Über den Autor:

Schon seit einiger Zeit in GNU/Linux involviert, betreibe ich nun ein Debian−System. Neben elektronischen Studien habe ich überwiegend französiche Übersetzungen für die GNU/Linux−Gemeinschaft gemacht, die unter Iznogood−Factory verfügbar sind.

Überprüfung von gpg−Mailsignaturen mit Sylpheed−Claws

Zusammenfassung:

Ich werde versuchen zu zeigen, wie man eine GPG−Erweiterung innerhalb von Sylpheed−Claws installiert und eine Mailsignatur mittels einiger bash−Pipe−Befehle überprüft.

Übersetzt ins Deutsche von:
Hermann J. Beckers
<hj.beckers(at)onlinehome.de>

Warum Signaturen überprüfen?

Ich erhielt eine Email von einem Freund, der mich fragte: "Warum schickst Du mir eine Email mit einem angehängten Virusprogramm?" Huuu! Jemand hatte meine Email−Adresse abgefangen und ihm eine Email mit meiner Adresse geschickt. ... Er hatte Glück, weil der Virus entdeckt wurde. Aber was wäre geschehen, wenn es nur um einen Termin für ein Treffen in einer Stadt gewesen wäre, 150 km von seinem Haus, was für uns nicht ungewöhnlich ist ... oder ein Patch für ein in Entwicklung befindliches Programm. Das wäre ein schlechter Tag!

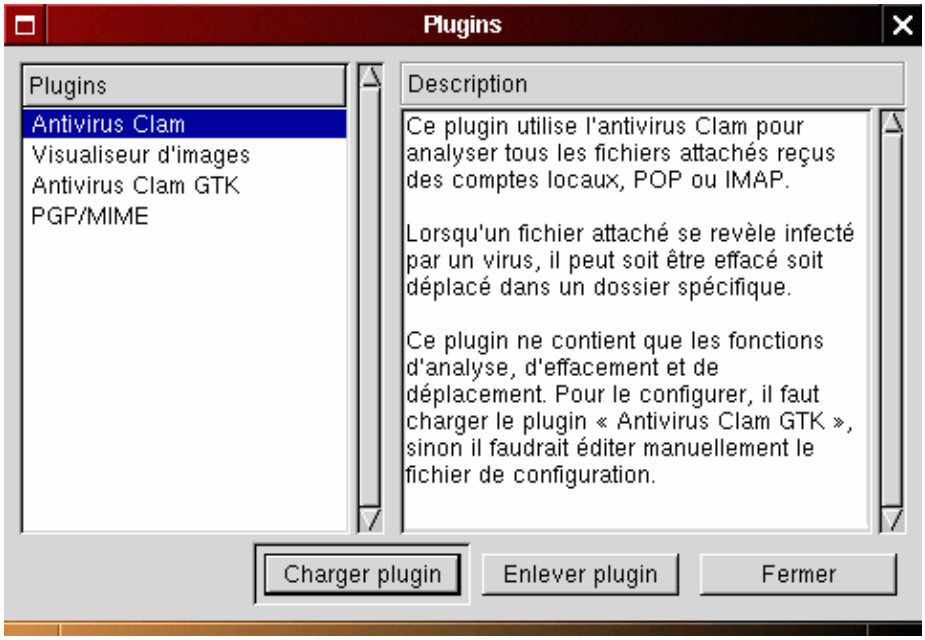
Seit dieser Zeit signiere ich meine Emails immer. Und ich überprüfe die Email−Signatur, wenn die Email eine enthält. Eine weitere Sicherung gegen Eindringlinge. Aber manchmal erhalte ich eine Email von einer unbekannten Person mit einer GPG−Signatur, die ich noch nicht überprüft habe. Da ich ein sehr träger Typ bin, möchte ich kein Xterm öffnen, um den gpg−Befehl einzugeben, damit der öffentliche Schlüssel auf meinen Computer landet und die Signatur für jede neue Email−Adresse überprüft wird. Darum habe ich das als eine Aktion in Sylpheed−Claws geschrieben.

Über Sylpheed

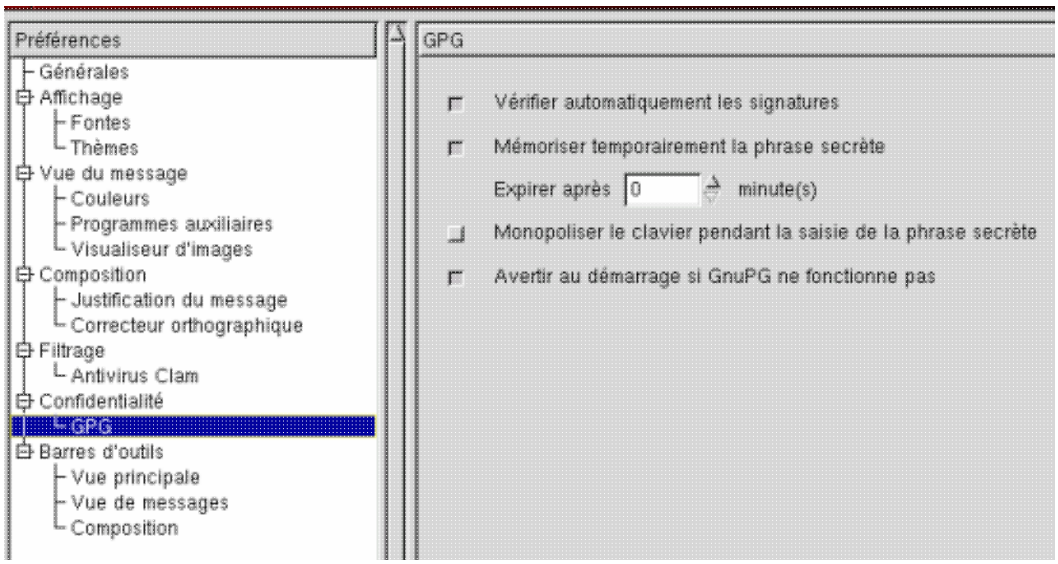
Sylpheed ist ein leichtes, schnelles grafisches GTK−Mail− und Newsprogramm. Es wird in zwei Versionen veröffentlicht: Sylpheed, der Hauptzweig und Sylpheed−Claws, die top−aktuelle Anwendung. Sylpheed−Claws unterstützt GPG mit einer Erweiterung namens PGP/MIME.
Sie müssen sylpheed−claws, sylpheed−claws−plugins, sylpheed−claws−pgpmime und gpg auf Ihrer Maschine kompiliert haben. Für Debian−Anwender ist es leicht mit aptitude; Sie müssen nur die obigen Pakete (neben anderen, aber suchen Sie danach) abrufen oder Sie führen

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

aus. Damit es funktioniert, müssen Sie, wie auf den Abbildungen gezeigt, unter Konfiguration –> Erweiterungen eine Erweiterung namens pgpmime.so laden (Sie können natürlich noch einige andere Erweiterungen wählen, die Ihnen bei der Benutzung von Sylpheed−Claws helfen).

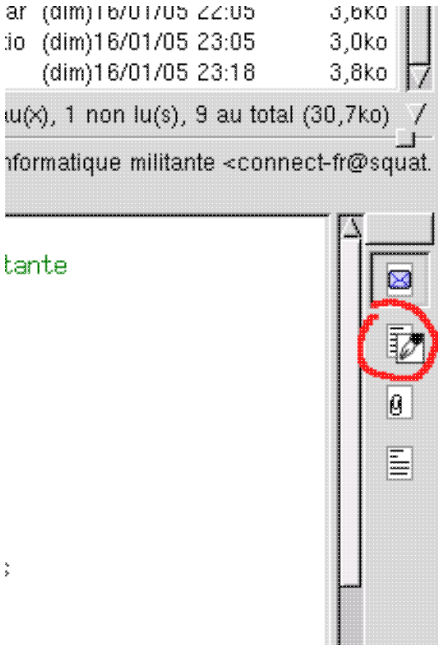


Dies zeigt Ihnen PGP/MIME auf der linken Seite. Nun können Sie das Fenster schliessen. Dann gehen Sie zu Einstellungen im Konfigurations−Menu.



Dann wählen Sie Einstellungen im Konfigurations−Menu. Links sehen Sie Vertraulichkeit −> GPG. Ein Klick darauf zeigt 4 Check−Boxen. Sie müssen zumindet die erste markieren (Automatische Signaturprüfung). Prüfen Sie Ihre Nachrichten. Die anderen sind interessant, wenn Sie Ihre Nachrichten signieren: die zweite Box hält Ihre Passphrase während der Sitzung im Speicher, die dritte aktiviert die Tastatur und die letzte warnt, wenn gpg nicht funktioniert.

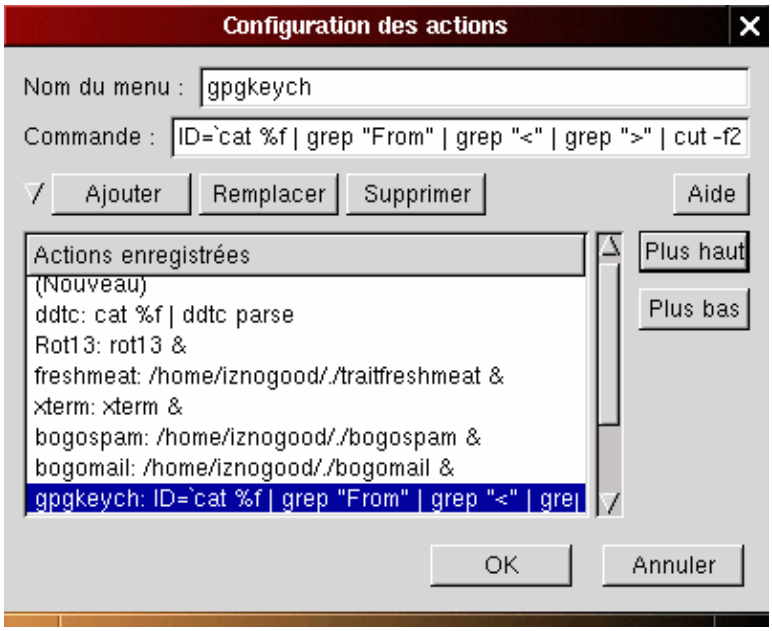
Wenn es eine Email mit einer Signatur gibt, sehen Sie ein Logo rechts vom Nachrichten−Inhalt:



Dieses Bild mit einem Stift zeigt an, das die gpg−Steuerung aktiv ist, aber der Autor findet sich nicht in Ihrer Datenbank oder die Signatur ist falsch.

Wie erstelle ich einen Signatur–Tester?

In Sylpheed–Claws können Sie Aktionen über Hilfsmittel –> Aktionen ausführen, wenn Sie sich in einer Email befinden, die Sie prüfen wollen. Aber zuerst müssen Sie es unter Konfiguration –> Aktionen programmieren. Sie öffnen es:



Unter Menu–Name geben Sie den Befehlsnamen an (Sie können einen Ihnen genehmen wählen), den Befehl unter Befehl (sehr schwierig!) und dann Hinzufügen. Hier ist die Befehls–Pipe, die die GPG–Überprüfung vornimmt:

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

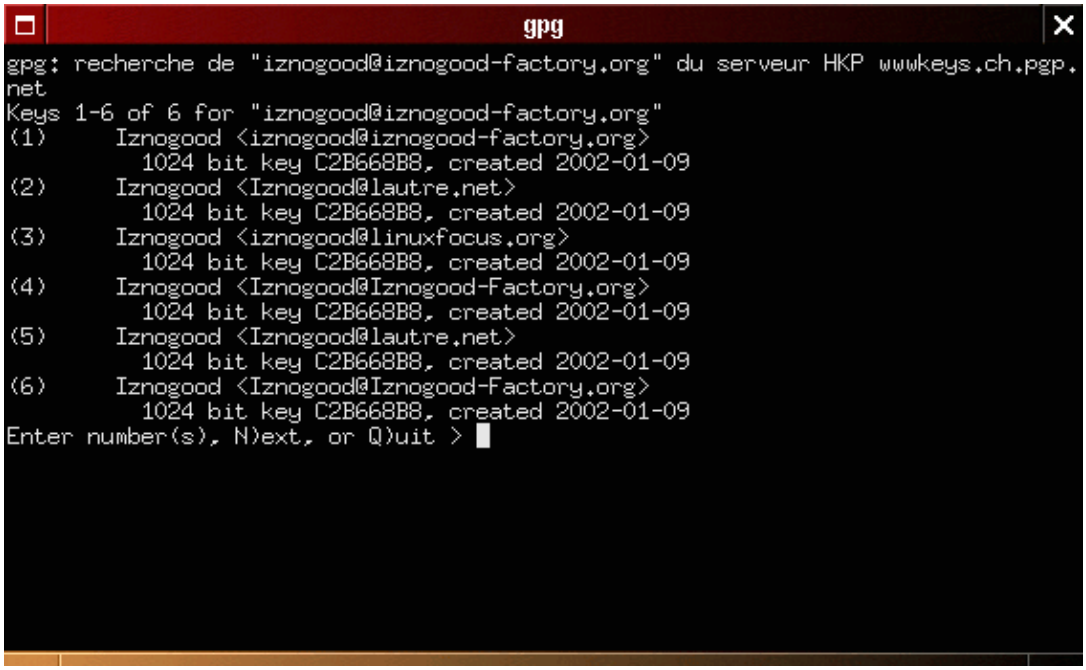
in einer Zeile. Der normale gpg–Befehl lautet:

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

Mit sylpheed–claws öffnen wir dafür ein xterm mittels "xterm –e", da wir immer eine Namens–Option wählen müssen. Um die Email–Adresse, das $ID, zu erhalten:

- lesen wir die Nachricht mit cat %f
- wir suchen die From–Zeile mit "<" und ">"
- wir behalten alles vor "<" und nach ">"

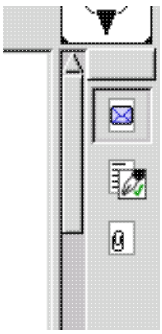
.... und wir haben die Adresse.
Wenn wir die Email–Adresse über Aktionen prüfen, geht die Anfrage an den Schlüssel–Server wwwkeys.ch.pgp.net, aber Sie können dies mit Ihrem Server ersetzen oder zwei verschiedene Aktionen mit zwei verschiedenen Schlüsselserversn benutzen, wie ich es tue.
Sie werden dieses xterm sehen:



Wählen Sie die richtige Adresse und das xterm–Fenster schliesst sich. Sie müssen nur erneut das Bild auf der rechten Seite prüfen, das eine Schaltfläche am unteren Rand zur erneuten Verifizierung öffnet. Fertig! Sie sehen dieses Bildfenster:

Falls nicht, bedeutet es, dass die Signatur falsch ist und Sie sie in den Mülleimer stecken können.

Wenn Sie dieses Bild sehen, bedeutet es, das der Absender ein Freund oder eine vertrauenswürdige Person in Ihrer GPG–Datenbank ist, da sie ihm/ihr bereits vertraut haben.



Sie müssen dies nur einmal für eine neue Email–Identität durchführen, denn alle Emails werden automatisch geprüft und Ihre Sicherheit wird verbessert.

Schlussfolgerung

Es ist recht einfach, die bash−Pipe−Befehle an andere (grafische oder nicht−grafische) Email−Programme anzupassen. Es ist recht einfach, Ihre Emails automatisch zu prüfen. Ein weiterer Vorteil: diese kontrollierten Emails müssen nicht den Spam−Prüfprozess durchlaufen, da Sie einmal die Adresse geprüft haben und, soweit ich weiss, benutzen Spams keine GPG−Signaturen. Es gibt zweifellos einen Weg, um die Kontrolle über signierte Emails mittels procmail direkt in die Eingabe zu verlagern, um sie direkt zu überprüfen, aber das ist eine andere Geschichte, die Sie auf Iznogood−Factory finden werden.

Sie finden mehr Informationen über gpg und Email−Signaturen unter:
http://www.gnupg.org/
und für Sylpheed−Claws unter
http://sylpheed−claws.sourceforge.net/.

2005−07−22, generated by lfparser_pdf version 2.51