

Votre messagerie en toute simplicité avec Evolution

Jonathan Fussner

Alors que certains continuent à utiliser le système d'exploitation de la grande firme américaine (pour ne pas la citer!), vous décidez de venir titiller *les pinguinettes* sous le soleil du monde libre. Muni de votre distribution GNU/Linux favorite, vous voulez essayer une activité des plus banales: l'envoi/réception d'e-mails.



linux@software.com.pl

Dans la série, je veux utiliser mon ordinateur pour des applications bureautiques, il est une activité des plus banales : la messagerie électronique.

Aujourd'hui nous allons voir que l'utilisation d'un client de messagerie sur votre distribution GNU/Linux favorite ne relève pas du parcours du combattant, et une fois de plus, nous allons démontrer qu'il existe des alternatives libres et efficaces aux logiciels propriétaires. Pour cela vous allez utiliser un logiciel : *Evolution* !

Derrière ce nom plein de promesses se cache un logiciel de messagerie électronique simple et complet !

Nous allons, dans cet article, découvrir le fonctionnement de ce logiciel au travers de sa configuration et apprendre son utilisation, dans un cadre personnel uniquement (celui-ci pouvant être également utilisé dans un cadre professionnel).

Mise au point

Avant d'entrer dans le vif du sujet, revenons quelques instants sur le principe de la messagerie électronique. Le fonctionnement du courrier électronique est basé sur l'utilisation d'une boîte aux lettres électronique. Lors de l'envoi d'un e-mail, ce



Cet article explique...

Comment configurer et utiliser le client de messagerie Evolution sur une distribution GNU/Linux pour envoyer/recevoir des e-mails

dernier est acheminé de serveur en serveur jusqu'au serveur de messagerie du destinataire. Plus exactement, le message est envoyé au serveur de courrier électronique chargé du transport (appelé *Mail Transport Agent* ou *MTA*), jusqu'au MTA du destinataire à l'aide du protocole SMTP, protocole de communication qui permet d'envoyer nos e-mails.

Le serveur MTA du destinataire délivre alors le courrier au serveur de courrier électronique entrant (appelé *Mail Delivery Agent* ou *MDA*), qui stocke le courrier en attendant que l'utilisateur vienne le relever, et ceci en utilisant un des deux principaux protocoles permettant de relever le courrier sur un MDA :

- le protocole POP3 ou *Post Office Protocol (version 3)*, le plus ancien, permettant de relever les e-mails et d'en laisser une copie sur le serveur.



Ce qu'il faut savoir...

- Les bases de l'utilisation et de l'installation d'un logiciel sur une distribution GNU/Linux
- Les informations minimales de votre compte de messagerie (nom d'utilisateur, mot de passe...)

- le protocole IMAP ou *Internet Message Access Protocol*, permettant de synchroniser l'état des courriers (lu, supprimé, déplacé) entre plusieurs clients de messagerie. l'ensemble des e-mails est stocké sur le serveur, afin d'assurer cette synchronisation.

Il faut savoir que la connexion au MDA, est soumise à une authentification, à l'aide d'un login (*nom d'utilisateur*) et d'un password (*mot de passe*).

La relève du courrier se fait grâce à un logiciel appelé *Mail User Agent*.

Lorsque le MUA est un logiciel installé sur votre ordinateur, on parle de client de messagerie (par exemple notre fameux *Evolution* !).

Présentation

Evolution est un logiciel libre faisant partie du projet GNOME, un des environnements de bureau le plus employé dans le monde du libre. Il est installé par défaut avec des distributions comme Fedora ou Ubuntu. Ainsi, si vous utilisez une distribution avec l'environnement GNOME, il y a de très grandes chances qu'Evolution soit déjà installé! Vous n'aurez plus qu'à le lancer!

L'application permet en outre de gérer vos e-mails, vos contacts ainsi que vos divers agendas. De plus elle dispose d'un filtrage anti-spam paramétrable et d'une fonction de tri des messages dans des dossiers. Evolution est capable de gérer plusieurs comptes d'utilisateurs.

Bien qu'étudié pour fonctionner pleinement sous un environnement GNOME, vous pouvez installer le logiciel quel que soit l'environnement graphique que vous utilisez (KDE, Xfce, etc...).

Son interface utilisateur et son fonctionnement sont similaires à ceux de Microsoft Outlook, alors n'ayez aucune crainte, vous pourrez facilement dès la fin de cet article maîtriser la bête, sans vous sentir trop dépaycé !

Pré requis...

Évidemment la première des choses est de s'assurer qu'Evolution est installé sur votre ordinateur. Nous avons vu plus haut que pour

la plupart des distributions utilisant GNOME, c'est le cas.

Si pour une raison ou pour une autre, il s'avère que celui-ci n'est pas installé, je vous fais confiance pour le faire, en effet toute bonne distribution devrait vous fournir un outil pour l'installer simplement, Synaptic, Urpm, Yum, etc....

Dans le vif du sujet: la configuration

Maintenant que vous êtes briffés sur Evolution, passons aux choses sérieuses: sa configuration ! Nous nous baserons sur la version 2.24.2 qui est, à ce jour, la dernière version stable du logiciel. Dans notre cas, le client de messagerie est installé sur une distribution GNU/Linux Ubuntu 8.10. Pour commencer, il faut évidemment lancer le logiciel ! A cet instant une fenêtre similaire à celle de la Figure 1 apparaît.

Configuration des comptes utilisateurs

Cette partie a pour but de créer les comptes nécessaires pour recevoir et envoyer des e-mails.

Nous partons du principe que vous possédez déjà un compte de messagerie, chez votre fournisseur d'accès favoris ou n'importe quel autre fournisseur de service de messagerie, et allons utiliser les informations qu'il vous a communiqué.

Pour ce faire nous aurons besoin des informations suivantes : nom d'utilisateur, mot de passe de messagerie, coordonnées des serveurs (ex : *pop.xxx.fr* et *smtp.xxx.fr*).

Pour créer un compte, allez dans le menu *Edition*, puis *Préférences*. Une fenêtre s'ouvre, et pointe sur le sous-menu *Comptes de Mes-*

sagerie, c'est ici que nous allons cliquer sur bouton *Ajouter*.

Un assistant de création de compte apparaît. En suivant les instructions, cliquez sur *suivant* !

I – Votre Identité :

- La première partie de la configuration consiste à saisir vos nom et prénom (voir Figure 2) afin de les faire apparaître lors de l'envoi d'un mail (ex : *Jonathan FUS-SNER*), puis l'adresse de messagerie que vous possédez et souhaitez utiliser (ex : *jonathan@exemple.com*).
- Cliquez sur *suivant* !

II – La réception des messages

- Il faut maintenant sélectionner le type de serveur utilisé par votre fournisseur de service pour pouvoir réceptionner les messages, en règle générale il vous est indiqué.
- Les protocoles de communication utilisés pour la réception sont Post Office Protocol (POP) ou IMAP. Dans notre exemple Figure 3, nous sélectionnerons POP (en effet c'est le protocole le plus utilisé), si vous devez en utiliser un autre, sélectionnez le dans la liste.
- Toujours à l'aide des informations que vous avez en votre possession, indiquez l'adresse du serveur utilisé (ex : *pop.exemple.com*), ainsi que votre nom d'utilisateur (ex : *jonathan@exemple.com*). L'utilisation d'une connexion sécurisée est conseillée.

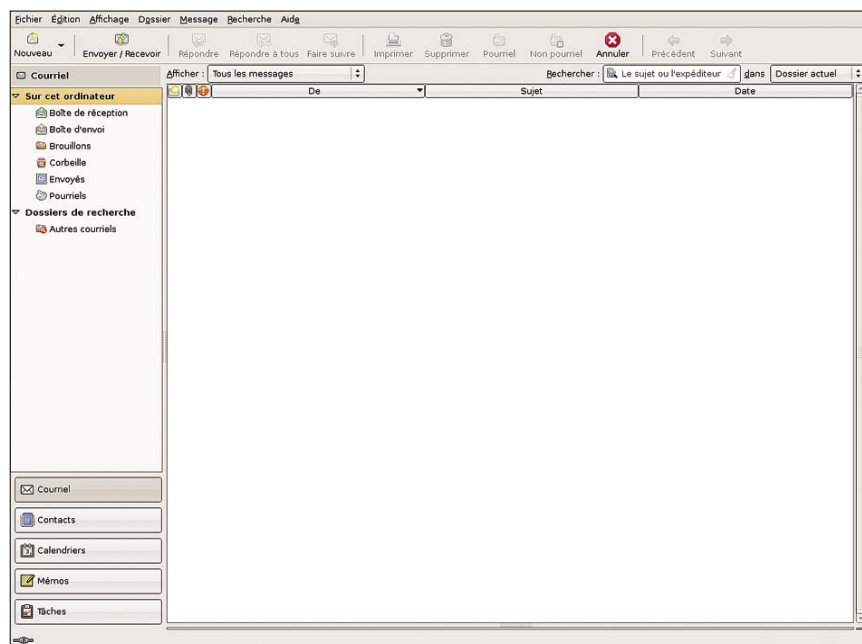


Figure 1. Fenêtre principale d'Evolution

Identité

Saisissez vos nom et adresse électronique ci-dessous. Les champs « optionnels » ci-dessous n'ont pas besoin d'être remplis, à moins que vous ne désiriez inclure ces informations dans les messages que vous envoyez.

Informations requises

Nom complet :

Adresse électronique :

Informations optionnelles

En faire mon compte par défaut

Répondre à :

Organisation :

Figure 2. Assistant de création d'un compte de messagerie – Vos informations personnelles

Réception du courriel

Sélectionnez une option parmi les suivantes

Type de serveur :

Description : Pour la connexion et le téléchargement du courriel depuis des serveurs POP.

Configuration

Serveur :

Nom d'utilisateur :

Sécurité

Utiliser une connexion sécurisée :

Type d'authentification

Mémoriser le mot de passe

Figure 3. Assistant de création d'un compte de messagerie – Serveur de réception des messages

- Choisissez soit SSL soit TLS (*A savoir : Transport Layer Security (TLS), est une évolution de Secure Socket Layer (SSL), un protocole de sécurisation des échanges sur Internet*) en fonction des informations de votre fournisseur. (*Attention certains serveurs ne prennent pas en charge la connexion sécurisée, dans ce cas, utilisez le mode sans chiffrement*).
- Votre authentification sur le serveur se fait par mot de passe. Lors de votre première connexion au serveur, il vous sera demandé de l'introduire. Si vous cochez la case *Mémoriser le mot de passe*, vous ne devrez pas le re-saisir à chaque connexion.
- Cliquez sur *suivant* !

III – Vos préférences : L'assistant vous propose maintenant selon vos envies de modifier l'intervalle de temps entre deux recherches de nouveaux messages ainsi que des options de conservation de vos messages sur le serveur de messagerie de votre fournisseur. Si vous avez plusieurs PC, vous pouvez lire vos e-mails sur chacun d'entre eux en activant l'option de conservation des messages sur le serveur ou tout simplement par mesure de prudence si un jour vous voulez retrouver un mail effacé par erreur. Une fois ces paramètres fixés, cliquez sur *suivant*, car nous ne sommes pas au bout de nos peines !

IV – L'envoi des messages :

- La fenêtre suivante est importante car elle concerne les paramètres qui vont être utilisés lorsque vous enverrez des messages. Sélectionnez maintenant le protocole SMTP dans la liste, puis saisissez l'adresse du serveur (*ex : smtp.exemple.com*) comme présenté en exemple Figure 4.
- Enfin dans la partie Authentification, saisissez votre nom d'utilisateur qui a priori est le même que celui saisi précédemment et cochez la case *Mémoriser le mot de passe*.
- Comme tout à l'heure, l'utilisation d'une connexion sécurisée est conseillée (voir partie III).

Pour terminer cet assistant, cliquez sur *suivant*. Il ne vous reste plus qu'à nommer la configuration que vous venez d'effectuer. Ce nom vous permettra de la distinguer des autres comptes de messagerie.

Lorsque ceci est terminé, votre nouveau compte est affiché dans la liste des comptes de messagerie.

Vous pouvez maintenant fermer cette fenêtre, la configuration minimale est opérationnelle.



Envoi du courriel

Saisissez les informations nécessaires pour envoyer le courriel. En cas de doute, adressez-vous à votre administrateur système ou à votre fournisseur d'accès Internet.

Type de serveur : SMTP

Description : Pour la distribution du courriel via un serveur de mail distant utilisant SMTP.

Configuration du serveur

Serveur : smtp.exemple.fr

Le serveur requiert une authentification

Sécurité

Utiliser une connexion sécurisée : Sans chiffrement

Authentification

Type : Connexion

Nom d'utilisateur : jonathan@exemple.fr

Mémoriser le mot de passe

situé sur la barre d'outils horizontale de la fenêtre principale. Ainsi les messages non envoyés le seront, et les messages entrants seront téléchargés et placés dans votre *Boîte de réception*. En résumé, cela va rafraîchir la liste des messages disponibles via le client de messagerie, qui va soit rapatrier les messages en local, soit au contraire les expédier vers le serveur SMTP en vue d'être transférés au serveur distant.

La première fois que vous établirez la connexion avec les serveurs de messagerie, il vous sera demandé votre mot de passe, que vous avez gardé précieusement sous la main !

Si vous recevez une erreur, vous pouvez modifier les informations sur votre compte dans : *Édition -> Préférences -> Compte de messagerie -> Cliquez sur le compte, puis Éditer.*

Supprimer ses e-mails

Les messages supprimés de votre boîte de réception, sont placés dans le dossier Corbeille. Vous devez, de manière périodique, vider cette dernière. Pour ce faire allez dans le menu *Fichier*, puis *Vider la corbeille*.

Les dossiers

Évolution organise les messages selon le principe de dossiers, affichés sur le panneau latéral gauche. Par défaut, six dossiers apparaissent (à la façon d'un système de fichiers) : *Boîte de réception*, *Boîte d'envoi*, *Brouillons*, *Corbeille*, *Envoyés*, *Pourriels*. Vous pouvez, si vous le souhaitez, créer des dossiers ou des sous-dossiers à l'intérieur de ces derniers (Figure 6), en allant dans le menu *Fichier >> Nouveau >>> Dossier de courriel*.

Figure 4. Assistant de création d'un compte de messagerie – Serveur d'envoi des messages

Vous voici de retour sur la fenêtre principale du logiciel !

Dans le vif du sujet : l'utilisation de base

Voyons maintenant un exemple concret d'utilisation du logiciel. Commençons par la boîte de réception et de traitement des messages électroniques.

La boîte de réception

La boîte de réception contient l'ensemble des e-mails (ou *mels*) que vous avez reçus et téléchargés de chez votre fournisseur via le fameux serveur POP3. Pour voir son contenu, cliquez sur *Boîte de réception* situé sur le panneau latéral gauche de la fenêtre. Si vous avez des messages ils seront affichés ici. Pour lire un e-mail sélectionnez-le en double-cliquant dessus.

Écrire un e-mail

Pour écrire un e-mail depuis la boîte de réception, cliquez sur le bouton *Nouveau*, situé en haut à gauche de la fenêtre.

Comme sur la Figure 5, entrez l'adresse e-mail du destinataire, le sujet, puis le corps du message. Vous pouvez également joindre un fichier au message, en cliquant sur *Joindre*, ou utiliser le fameux glisser-déposer.

Par la suite vous pouvez envoyer ce dernier en cliquant sur le bouton *Envoyer*.

Envoyer/Recevoir ses e-mails

Pour envoyer les messages que vous avez composés, cliquez sur le bouton *Envoyer/Recevoir*

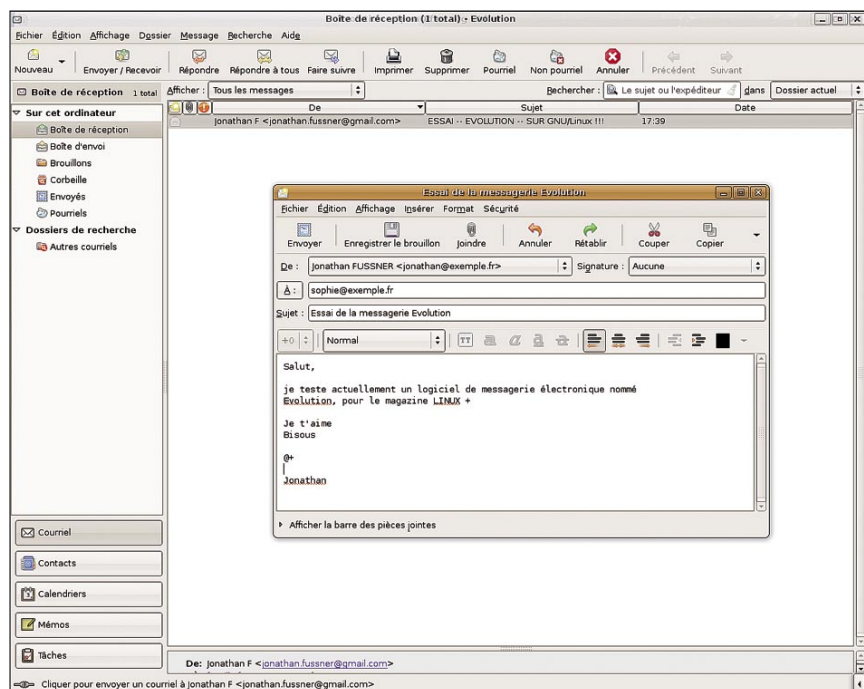


Figure 5. Rédiger votre premier message

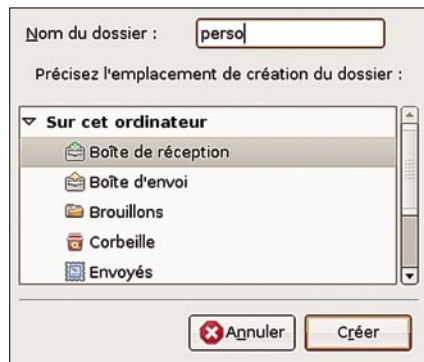


Figure 6. Créer un dossier personnel

Vous pourrez alors y déplacer vos messages, en cliquant droit sur le(s) message(s) sélectionné(s) >>> *Déplacer* ou *Copier vers le dossier*.

Lutter contre les pourriels

De nos jours, le pourriel (ou spam en anglais), cet envoi massif d'e-mails, non sollicités par les destinataires, expédiés en masse à des fins publicitaires ou malhonnêtes prend de plus en plus d'ampleur ! Pour lutter contre ce fléau, Evolution permet de gérer un module de filtrage des e-mails. Pour cela, il utilise un programme externe pour filtrer les spams, il faudra donc l'installer.

Dans notre exemple, nous allons utiliser un logiciel complémentaire, appelé *bogofilter*. Le but n'est pas ici de comprendre le fonctionnement du logiciel, mais de l'implanter à votre configuration.

Une fois n'est pas coutume, je vous fais confiance pour l'installer, si votre distribution GNU/Linux ne l'a pas intégré par défaut. Il faut savoir par exemple, qu'à partir de la version 7.10 de la distribution Ubuntu, *Bogofilter* semble être installé et activé par défaut. Il suffit donc de passer à la partie apprentissage si vous souhaitez l'utiliser.

Nous allons maintenant configurer Evolution. Sur la fenêtre principale:

- Allez dans *Édition* -> *Greffons* -> dans la fenêtre recherchez *Greffon de pourriel Spamassassin* et décochez la case. En effet, Evolution permet également d'utiliser un autre logiciel de filtrage appelé SpamAssassin. Cette manipulation permet d'éviter les conflits.
- Allez ensuite dans *Édition* -> *Préférences* -> *Préférences du Courrier* -> *Pourriel*.
- Cochez la première case *Détecter les pourriels dans les messages entrants* si ce n'est déjà fait.

- Sélectionnez *Bogofilter* comme greffon pourriel par défaut et vérifiez l'affichage de l'information de disponibilité (voir Figure 7).

Il reconnaît un pourriel grâce à un modèle statistique reposant sur les mots utilisés. Il fonctionne par un mode d'apprentissage, c'est-à-dire qu'au début, vous allez devoir considérer les e-mails que vous recevez, spam ou ham (bon courriel). En effet bogofilter a besoin de savoir à quoi ressemble un e-mail normal pour pouvoir filtrer les mauvais, il faut donc cocher la grande majorité de vos Hams pour lui apprendre. Pour ce faire, lorsque vous recevez un message, sélectionnez celui-ci, et sur la barre d'outils, cliquez sur le bouton *Pourriel* ou sur le bouton *Non Pourriel* ! Si le message rentre dans la première catégorie, il est placé dans le dossier *Pourriels*.

Au fur et à mesure, le logiciel va apprendre et votre filtrage va devenir de plus en plus efficace !

Dans le vif du sujet : une petite sauvegarde !

Il est quelquefois utile de sauvegarder tous ses paramètres, ne serait-ce que par mesure de précaution !

Pour ce faire il existe une fonction dans évolution qui génère automatiquement une archive de vos paramètres (Comptes, courriels, contacts, calendriers...).

Ainsi, pour sauvegarder, allez dans le menu *Fichier*, puis *Archiver les paramètres*. A partir de là, le logiciel vous demandera de sélectionner l'endroit où sauvegarder l'archive *evolution-backup.tar.gz* et vous demandera une confirmation. Attention la fermeture d'Evolution est indispensable, c'est pourquoi vous devez cliquer sur le bouton *Oui* lors de la demande de confirmation. Voilà votre sauvegarde sera prête quelques secondes après.

Pour restaurer vos paramètres allez dans le menu *Fichier*, puis *Restaurer les paramètres*. Le logiciel vous demandera de sélectionner l'endroit où l'archive *evolution-backup.tar.gz* se situe.

Cette fonction est très pratique, notamment dans le cas d'une réinstallation de votre système.

Dans le vif du sujet : et PGP alors ?

Pour assurer à vos destinataires que vous êtes bien l'expéditeur d'un message et que ce dernier n'a pas été modifié lors de son parcours sur le réseau, vous devez *signer votre courrier électronique*. Le cryptage quant à lui *empêchera quiconque de le lire*.

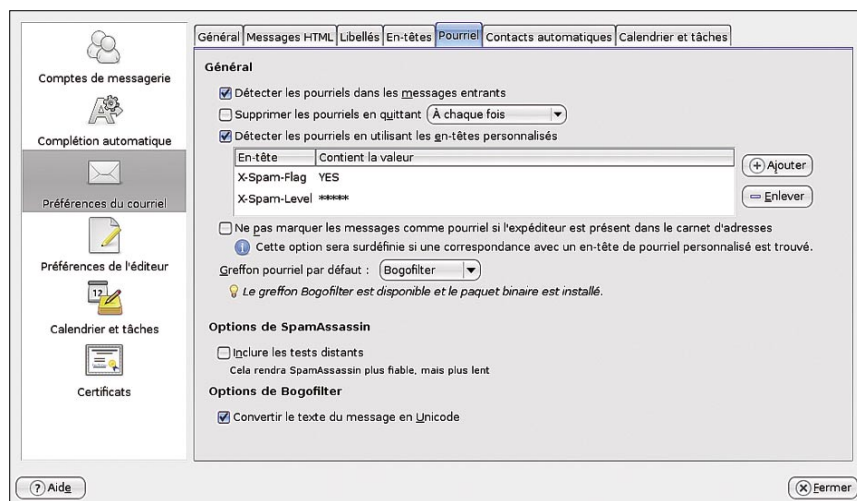


Figure 7. La gestion des Pourriels avec Bogofilter

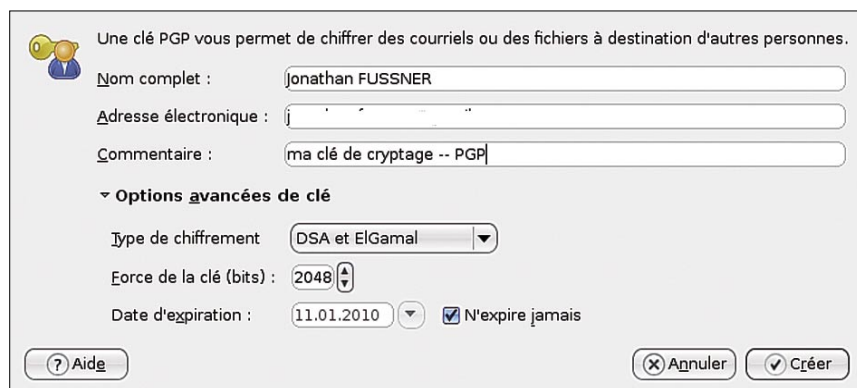


Figure 8. Créer une clé PGP

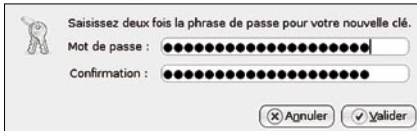


Figure 9. Phrase de passe de votre clé

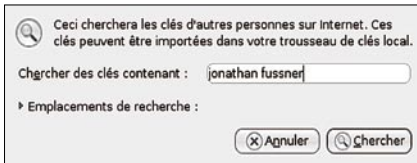


Figure 10. Rechercher des clés sur les serveurs

PGP, ou *Pretty Good Privacy*, traduites *Plutôt bonne intimité*, est un logiciel de cryptographie hybride, c'est-à-dire utilisant le système de cryptographie à clé publique et de cryptographie symétrique. Le but de cette partie, n'est pas de présenter dans le détail les techniques de cryptographie, pour cela je vous invite à lire les nombreux articles et dossiers présents sur la toile, dont vous trouverez les principales références dans l'encadré *Sur le Réseau* situé en dernière page de l'article. En effet ça serait trop long !

Néanmoins, il est nécessaire de schématiser quelque peu la cryptographie à clé publique, pour pouvoir comprendre les différentes manipulations qui nous attendent. Une clé de cryptage est une série de lettres et chiffres, utilisée pour crypter un message, c'est-à-dire le rendre illisible en appliquant une méthode qui permet de retrouver les données de départ.

Pour comprendre cette méthode, prenons un exemple avec deux personnes : Jonathan et Luc.

Dans la cryptographie à clé publique, une personne (Jonathan) qui envoie et reçoit des messages dispose de deux clés, la clé publique et la clé privée. La première est générée et publiée sur des serveurs afin de la mettre à disposition. La seconde est confidentielle et reste entre les mains de Jonathan, il ne la divulguera à personne ! Luc va exécuter la même procédure.

Si Jonathan veut envoyer un message à Luc, il crypte le message avec la clé publique de Luc qu'il aura préalablement récupérée sur un serveur dédié, et envoie le message. Lorsque Luc reçoit le message, il va le décrypter avec sa clé privée, qu'il est le seul à posséder. Si Luc veut répondre à Jonathan, il utilisera la clé publique de Jonathan !

Nous allons donc maintenant intégrer cette solution de cryptage au sein d'Evolution, ceci vous permettra à votre tour d'envoyer et de recevoir des messages cryptés avec vos contacts et ainsi d'ajouter une couche de sécurité supplémentaire. Cette solution s'appelle GnuPG et est

l'abréviation de GNU Privacy Guard. GnuPG est un clone, une implémentation libre (au sens de la GNU Public Licence) de PGP. Il respecte la norme OpenPGP définie dans la RFC 2440.

L'installation du logiciel

GnuPG est généralement inclus dans les systèmes d'exploitation libres, comme GNU/Linux ou BSD.

Pour faciliter la mise en place de GnuPG, nous allons utiliser un logiciel nommé Seahorse, si s'agit d'une implémentation graphique qui va faciliter la tâche des débutants qui ne sont pas encore très familiers avec un terminal et des lignes de commandes.

Comme tout à l'heure, je vous fais confiance pour installer Seahorse, en effet toute bonne distribution devrait vous fournir un outil pour l'installer simplement, Synaptic, Urpmi, Yum, etc....

La génération d'un trousseau de clés

Lancez le logiciel, en appuyant sur les touches ALT+F2 et en tapant Seahorse. Le logiciel apparaît, il s'agit donc du programme que vous avez installé ! Nous allons maintenant générer les clés PGP. Pour ce faire cliquez sur le menu Clé -> créer une nouvelle clé -> Sélectionnez Clé PGP et continuez. Saisissez les informations suivantes en prenant exemple sur la Figure 8 :

- Votre nom et prénom
- Votre adresse e-mail
- Un commentaire éventuel à propos de vous et de votre clé
- Cliquez sur *options avancées de clé*. Les paramètres par défaut sont très bien, je vous recommande de ne pas les changer,

néanmoins, libre à vous de affiner si besoins

- Cliquez sur *Créer !*

La dernière étape (Figure 9) est l'entrée du mot de passe de la clé. Il est recommandé d'employer une phrase avec un mélange de chiffres et lettres ; ne rendez pas ceci facile à deviner, évitez donc les phrases simples ou évidentes comme votre lieu de naissance, le prénom de votre belle-mère ou autre ! Après validation, la clé est générée, et apparaît dans la liste de vos clés personnelles. Voyez-vous la colonne nommée *Identifiant de la clé* ? Cet identifiant unique à votre clé est à noter car il vous sera demandé lors de la configuration d'Evolution.

Je vous conseille maintenant de faire une sauvegarde. Pour ce faire, clic droit sur votre clé puis -> *Exportez votre clé, enregistrez -la en lieu sûr !*

La synchronisation de votre clé publique

Pour que votre correspondant puisse vous envoyer des e-mails cryptés ou signés il faut qu'il possède votre clé publique, nous l'avons dit précédemment. Pour ce faire vous pouvez naturellement lui envoyer par mail la copie que vous venez de sauvegarder, ou choisir de la synchroniser sur un serveur dédié aux clés sur lequel il pourra aisément de son côté la récupérer en interrogeant ce dernier !

Pour ce faire :

- Clic droit sur votre clé -> Synchroniser et publier des clés.
- Cliquez sur le bouton Serveurs de clés.
- Dans la liste Publier les clés sur : Sélectionnez un des serveurs dans la liste, je vous

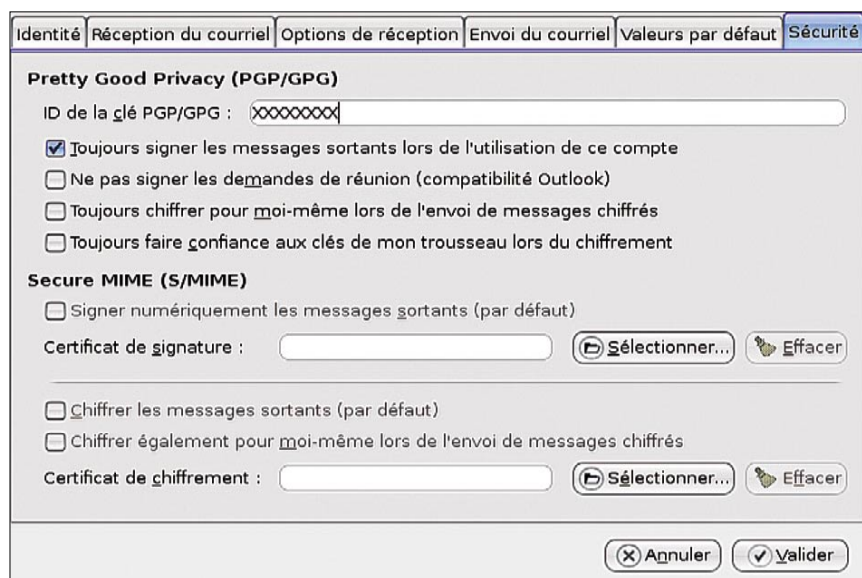


Figure 11. Configurer Evolution pour GPG/PGP



Auteur

Jonathan Fussner est étudiant en informatique dans le domaine de l'administration de systèmes et réseaux. Passionné et utilisateur de systèmes GNU/Linux, vous pouvez le contacter sur son site internet : <http://www.fussner.net>

conseille `ldap://keyservers.pgp.com` puis cliquez sur le bouton fermer.

- Vous pouvez maintenant synchroniser votre clé sur le serveur à l'aide du bouton *Synchroniser*.
- Patientez quelques instants, votre clé est maintenant publiée.

Récupérer la clé publique de votre correspondant

Avant de rentrer dans le vif du sujet avec Evolution, il y a encore une manipulation importante à réaliser. En effet pour que vous puissiez envoyer un mail crypté à un de vos contacts, il faut récupérer bien évidemment sa clé publique. Comme précédemment soit il vous l'a envoyée par mail ou autres, soit vous devez la récupérer sur un serveur de clé dédié :

Dans le premier cas, sur la fenêtre principale de Seahorse, allez dans le menu *Clé* et importez la clé en spécifiant le chemin d'accès à la clé publique de votre contact (logiquement un fichier en .asc).

Dans le second cas, nous allons rechercher la clé de votre contact sur un des serveurs dédiés.

Pour ce faire, allez dans le menu *Distant -> Chercher des clés distantes*.

Puis saisissez le nom de la clé, ou le nom de votre contact, afin de rechercher sa clé et de l'importer. La figure 10 illustre cette manipulation.

Après l'importation de la clé de votre contact, celle-ci s'affiche sous l'onglet *Autres clés obtenues*.

Nous allons maintenant signer les clés publiques que nous avons obtenues d'autres personnes.

Il est très important de bien vérifier l'identité des personnes dont vous signez les clés, cela nous sera nécessaire pour les utiliser et envoyer des messages aux détenteurs de ces dernières.

Pour avoir confiance en cette clé, faites un clic droit, allez dans *Propriétés* puis dans l'onglet *Confiance*, puis cochez les deux cases. Lorsque vous aurez coché la première case, la clé appartenant à votre destinataire se déplace dans l'onglet *Clés de confiance*. Vous n'aurez plus qu'à faire un clic droit sur la clé, puis de la *Signer*, en choisissant la précaution que vous avez prise pour signer cette clé (c'est à dire la rendre non obsolète).

Ces informations sont alors partagées lors de votre prochain envoi des clefs publiques vers 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*.

Je vous conseille de vous référer au *manuel Gnu Privacy Guard* qui détaille l'ensemble des concepts de signature et de révocation de clés, utiles au quotidien.

Intégration dans Evolution

Voyons enfin comment GPG s'intègre dans un client de messagerie comme Evolution.

La première des choses à faire est de paramétrer votre compte afin d'utiliser votre clé PGP (Figure 11). Pour cela, éditez votre compte de messagerie : *Edition -> Préférences -> Sélectionnez votre compte* puis faites *Edition*. Positionnez-vous dans l'onglet *Sécurité*. Dans le champs ID de la Clé PGP/GPG, entrez l'ID de votre clé, celui que nous avons vu il y quelques instants. Puis validez et fermez la fenêtre !

Voilà la configuration minimale au niveau d'Evolution est terminée! Tout ça... pour ça ! me direz-vous ! Oui mais ces efforts permettent maintenant de signer et de crypter des messages en toute sécurité.

Envoi d'un message crypté

Si vous voulez utiliser votre clé PGP pour envoyer un message, créez-en un nouveau, et dans le menu *Sécurité*, lorsque vous composez, sélectionnez à la manière de la Figure 12, *Signer avec PGP* ou *Crypter avec PGP*.

Le tour est joué !

Réception d'un message crypté

Lorsque vous recevez un message crypté, et que vous possédez comme nous l'avons vu la clé publique de votre expéditeur, double cliquez sur le message pour l'ouvrir. Il vous est alors demandé votre mot de passe (celui de votre clé privée que vous avez généré). Une fois saisi, le message est décrypté et affiché !

Conclusion

Voilà, nous avons vu au cours de cet article, les notions de base pour utiliser Evolution ! Rassurez-vous, ceci n'est que le minimum de ce que l'on peu faire avec ce logiciel ! Mais plus tard, lorsque vous serez plus familier avec ces concepts, vous pourrez vous aventurer plus aisément dans la multitude de fonctions qu'offre Evolution tels que la gestion des contacts, d'agendas, de tâches, de mémos et bien d'autres.

Décidément, il fait beau sous le soleil du monde libre ! ☺



Sur le réseau

- Le site du projet Evolution (en Anglais) : <http://projects.gnome.org/evolution/>,
- Jouons avec Bogofilter: <http://www.coagul.org/spip.php?article482>,
- How to work PGP (en Anglais) : <http://www.pgpi.org/doc/pgpintr/>,
- Le manuel Gnu Privacy Guard : <http://www.gnupg.org/gph/fr/manual.html>.

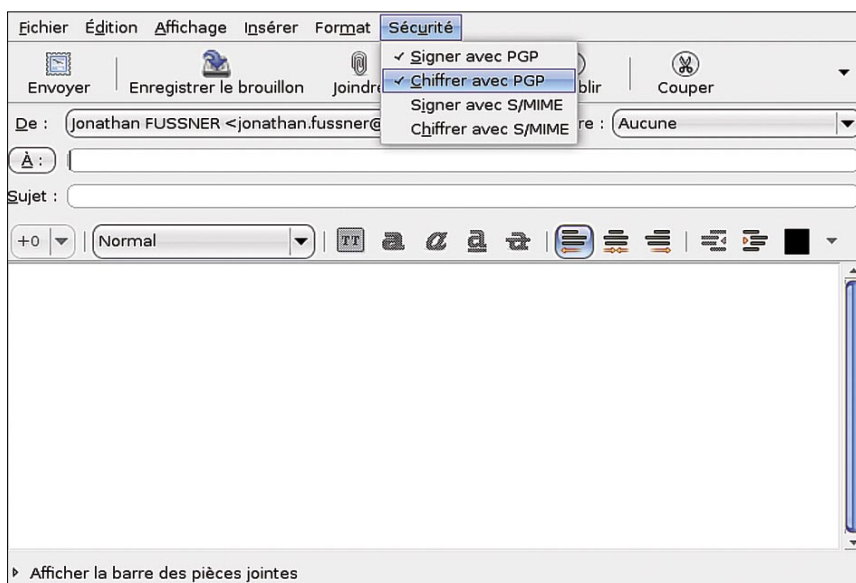


Figure 12. Envoyer un mail crypté