Enigmail : Chiffrement GPG avec Icedove

- Objet : Prise en main de l'extension Enigmail pour Icedove/Thunderbird
- Niveau requis :
  débutant, avisé
- Commentaires : *Avec icedove, créer une paire de clefs pour échanger confidentiellement des mails.*
- Version logiciel: Icedove 31.3.0 ; Enigmail 1.7.2
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !.
- Suivi :
  obsolète
  - Création par smolski 20/02/2013
  - Testé par <...> le <...>
- Commentaires sur le forum : ici[1)]

Introduction

Le couple **Enigmail** / **GnuPG** permet de chiffrer, signer nos courriels et leurs pièces jointes.
C'est une protection supplémentaire pour garantir notre vie privée.

Enigmail permet d'assurer la confidentialité, l'intégrité, l'authentification d'un message.

Enigmail

Comme *GnuPG* est un programme qui n'a pas d'interface graphique[2)], c'est le rôle d'*Enigmail* de créer l'*interface graphique* qu'on utilisera, interface qui sera elle-même adaptée à l'environnement graphique où nous l'installons.

Quoiqu'il en soit des *environnements graphiques*, les fonctions de GnuPG restent identiques car elles sont attachées directement au programme *GnuPG*.

La lecture de la documentation officielle Enigmail est fortement recommandée. La mauvaise utilisation d'Enigmail pourrait compromettre le niveau de sécurité recherché.

Notions essentielles

- **Cryptographie asymétrique**: méthode de chiffrement basée sur une paire de clé. La clé publique permet uniquement de chiffrer le message alors que la clé privée permet uniquement de déchiffrer le message.
- **Chiffrement**: le chiffrement d'un message se fait avec la clé publique du destinataire.
- **Déchiffrement**: le déchiffrement d'un message se fait avec la clé privée du destinataire.

- **Signature**: la signature permet de vérifier que le message est bien envoyé par l'expéditeur.
- **Certificat de revocation**: permet de désactiver la clé si elle est compromise ou perdue.

La **clé privée** et le **certificat de révocation** doivent rester confidentiels. Il convient de les sotcker dans un endroit en sécurité et à l'abri des regards indiscrets.

Pré-requis

1. Messagerie Icedove installée et configurée.
2. Un compte de messagerie fonctionnel.

Pour plus d'informations, voir sur le wiki Icedove: Client de courriel

L'utilisation de KeePassX est recommandé pour enregistrer vos clés, certificat et passphrase de manière centralisé et sécurisé. Voir le wiki KeePassX

Installation

Installation du paquet directement depuis les dépots Debian

```
apt-get update && apt-get install enigmail
```

Par précaution et pour ne pas modifier la/les messagerie(s) que vous utilisée(s), il est possible de créer un nouveau profil dédié à la messagerie sécurisée:

```
icedove -ProfileManager
```

pour lancer le profil:

```
icedove -P <profile>
```

Assistant de configuration

L'assistant permet de configurer Enigmail étape par étape et facilite l'utilisation pour les débutants.

Qu'est ce qu'on va faire :

- Choisir un compte de messagerie qui utilisera Enigmail
- Paramétrer Enigmail
- Générer une paire de clé

- Générer un certificat de révocation
- Vérifier la configuration d'Enigmail

On commence :

On lance l'**Assistant de configuration** depuis le menu: `Enigmail > Assistant de configuration`

On se laisse guider dans la configuration d'Enigmail:

On choisit de configurer Enigmail pour tous les comptes ou seulement certains comptes.

Pour les débutants il est recommandé de configurer toutes les identités pour éviter toute confusion.

On utilise le mode **Chiffrement automatique pratique**. L'utilisation généralisée est recommandée uniquement si tous vos correspondants utilisent le chiffrement et sont capables de lire vos courriels.

On choisit de signer automatiquement tous les courriels sortants. Il sera toujours possible de désactiver la signature lors de la rédaction des courriels.

L'assistant demande la permission de modifier certains paramètres pour une utilisation transparente. Les modifications sont d'ordre technique hormis l'utilisation du texte brut à la place de HTML. L'utilisation d'HTML peut poser problème lors de la signature ou chiffrement. Il est très fortement recommandé d'effectuer les modifications.

Si vous avez précédemment utilisé Enigmail et créé une clé, vous pouvez la sélectionner pour cette identité. Sinon, on va générer une nouvelle paire de clé.

On crée une paire de clé pour un compte. L'utilisation d'une Phrase secrète permet d'ajouter un niveau de sécurité supplémentaire. La signature et le chiffrement avec cette clé ne pourra se faire qu'en tapant cette phrase secrète.

La dernière fenêtre affiche un récapitulatif des modifications qui seront effectuées.

On patiente le temps de générer une nouvelle clé (l'utilisation intensive de l'ordinateur permet d'accélérer le processus).

On choisit de générer le certificat **immédiatement**.

On enregistre le certificat dans un dossier en sécurité.

L'assistant a terminé la configuration.

Il nous reste à sauvegarder la paire de clé. Dans le menu Icedove: `Enigmail > Gestion de clé`

Sélectionner la clé à exporter (une des clés avec le texte en gras) puis ouvrir le menu avec un clic-droit:

Dans le menu `Exporter des clés vers un fichier`, exporter la clé privée puis réitérer l'opération pour exporter la clé publique.

On sauvegarde dans un endroit sécurisé le certificat (rev.asc), la clé publique/privée (pub-priv.asc) et la clé privée (pub.asc). Les certificats et la clé publique/privée ne doivent jamais être publiés. Sinon, il convient de révoquer cette clé le plus rapidement possible.

On s'assure que le compte est correctement paramétré et prêt à être utilisé par Enigmail. On vérifie dans le menu `Paramètres des comptes > Sécurité OpenPGP`et pour chacun des comptes que la case **Activer le support OpenPGP pour cette identité** est coché. 

La configuration d'Enigmail est terminée et prête à être utilisé.

Utilisation

Pour tester le bon fonctionnement d'Enigmail, on va envoyer un message à Adele (The friendly OpenPGP email robot).

Publier sa clé publique

On va commencer par envoyer notre clé publique. On écrit un message à Adele et on attache la clé publique depuis le menu: `Enigmail > Attacher ma clé publique`.

Adele: adele-en@gnupp.de

Déchiffrer un courriel

Adele répond en chiffrant son message en utilisant notre clé publique. Adele ajoute à son message sa propre clé publique. On peut lire: *Enigmail message déchiffré*.

Il est possible de vérifier si le message est bien chiffré en affichant le code source du message (Ctrl+U)

Importer une clé publique

On profite du message d'Adele pour importer la clé publique. Dans le menu Icedove: `Enigmail > Clef de l'expéditeur > Importer la clé publique`.

Chiffrer et signer un courriel

Une fois la clé importée, on va répondre à Adele en chiffrant le message. Puisqu'on dispose de la clé publique d'Adele, le chiffrement et la signature pour ce destinataire se fera automatiquement.

En bas à droite, la clé et le stylo doivent changer de couleur. On peut vérifier dans le menu Enigmail, on doit lire **Le message sera chiffré** et **Le message sera signé**.

Adele répond au message. Le message est chiffré et contient le message d'origine. Le chiffrement de message vers le correspondant Adele est donc opérationnel.

Vous savez maintenant utiliser Enigmail. Il ne reste plus qu'à partager votre clé publique.

Utilisation avancée

Partager sa clé publique

Pour recevoir des courriels chiffrés, il est nécessaire de partager sa clé publique.

Il existe différents moyen de partager sa clé publique:

1. copier sur une clé USB
2. stocker sur votre site web personnel
3. envoyer en pièce jointe
4. publier sur un serveur de clé

La clé publique correspond au fichier `Firstname Lastname you@domain.com (0x89ABCDEF) pub.asc`.

Publier sa clé publique sur un serveur

La publication de la clé sur un serveur publique présente un risque de spam.

Il faut s'assurer qu'un serveur de clé est défini. Depuis le menu: `Enigmail > Préférences`.
Dans les préférences Enigmail, spécifier le serveur de clé:

Adresse de serveur de clé:

- pool.sks-keyservers.net

Depuis le **Gestionnaire de clés**, sélectionner la clé à publier puis ouvrir le menu avec `clic-droit > Envoyer les clefs publiques vers un serveur de clefs`.

Sélectionner le serveur de clé sur lequel on veut publier.

Révoquer sa clé

Si la clé est compromise, il convient de la révoquer immédiatement. Il suffit d'utiliser le certificat de révocation.

Dans le gestionnaire de clés, dans le menu: Fichier > Importer des clefs depuis un fichier. Puis sélectionner le fichier correspondant `Firstname Lastname you@domain.com (0x89ABCDEF) pub.asc`. Un message d'avertissement permet de vérifier que la clé est bien révoquée.

Si la clé est disponible sur un serveur de clé, penser à l'actualiser depuis le menu: `Serveur de clefs > Rafraichir les clefs publiques sélectionnées`.

Importer une clé

L'import de clé s'effectue dans le **Gestionnaire de clés Enigmail**: `Menu > Enigmail > Gestion de clefs`.

Depuis le menu du gestionnaire de clés : `Menu > Fichier > Importer des clefs depuis un fichier`, puis on sélectionne le fichier [ex: *Debian Facile spam@bla.fr (0x2G88AB5C) pub-priv.asc*].

Configuration avancée

Générer une paire de clé

A partir du **Gestionnaire de clés**, générer les clés depuis le menu: `Générer > Nouvelle paire de clefs`.

1. Choisir le compte à utiliser
2. Définir la phrase secrète
3. (Ajouter un commentaire)
4. Définir le délai d'expiration
5. (Définir la taille et le type de clé dans l'onglet Avancé)
6. Générer la clé

Pour bien faire, on génère tout de suite le certificat de révocation.

Gestionnaire de clé

Le gestionnaire de clé affiche toutes les clés (les clés de vos correspondants et les vôtres). Il est disponible depuis le menu Icedove: `Enigmail > Gestion de clefs`.

- **Les paires de clé sont affichées en gras**
- *Les paires de clé invalides / révoquées sont affichées en italique*

Le gestionnaire permet de générer, importer, exporter des clés. Générer des certificats et révoquer des clés. Il permet également de publier les clés publiques sur un serveur de clés.

Problèmes connus

Liens

- Documentation officielle Enigmail (en anglais) Site officiel Enigmail
- Tutoriel Tutoriel Security in-a-box
- Le guide autodéfense courriel de la FSF qui explique pas-à-pas l'installation et l'utilisation d'Enigmail.

1)

N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !

2)

il ne s'utilise qu'en ligne de commande