Chiffrer son courriel avec Enigmail

Guide d'installation et d'utilisation
pour Mozilla Thunderbird, Enigmail et WinPT

Présenté par Fabián Rodríguez
www.FabianRodriguez.com

28 septembre 2004

Remerciements et crédits

Ce guide n'aurait été possible sans la rédaction originale de l'article “Email Encryption with Thunderbird and Enigmail” par Jay Seth et la traduction française effectuée par l'équipe de GeckoZone. Le guide est inspiré de ces textes avec l'autorisation des auteurs respectifs, mais comporte des images actualisées et du matériel adapté.

- Auteur original : Jay Sheth - www.moztips.com
- Traduction originale : Nucleos, Bouiaw, Frédéric Chateaux - www.geckozone.org
- Adaptation et révision: Fabián Rodríguez – FabianRodriguez.com

Licence

Précisions

Ce guide a été créé avec OpenOffice.org 1.1.2 sous Mandrake Linux 10. Il traite des versions de logiciels libres suivants:

- Thunderbird 0.8
- Enigmail 0.86.1
- WinPT 1.0rc2

Introduction

Ce guide est une introduction rapide au fonctionnement de base de la cryptographie et à l'installation d'outils de base sous Windows pour la protection d'envois par courriel. **Il n'est en aucun cas un ouvrage complet expliquant les détails et les possibilités des logiciels mentionnés** et **présuppose une connaissance des enjeux et complexités du chiffrement**. Son auteur a privilégié l'utilisation de logiciels libres et l'interface graphique (plutôt que la ligne de commande), ce qui explique certains choix et omissions. Pour signaler toute amélioration ou commentaire, adressez-vous à Fabián Rodríguez sur son site Internet: www.FabianRodriguez.com

Il est important de tenir compte d'autres paramètres (comme la sécurité physique de l'environnement informatique) lorsque de tels outils sont employés, avant de leur confier la protection des données critiques ou hautement confidentielles.

Mozilla Thunderbird, Enigmail et WinPT

La fondation Mozilla offre des pré-versions de son logicielde messagerie Mozilla Thunderbird (ci-après *Thunderbird*). Bien que Thunderbird n'en soit qu'à la version 0.8, ses fonctionnalités et sa qualité dépassent de loin ce qu'on peut espérer retrouver dans un logiciel avec ce numéro de version. Cela s'explique en partie par le fait que Thunderbird soit basé sur le logiciel de messagerie de la Suite Mozilla, qui est développée depuis 1998, dérivée des produits de Netscape Corporation.

Enigmail est une extension disponible pour Thunderbird qui permet le chiffrement asymétrique basé sur la norme OpenPGP. Enigmail utilise le logiciel libre GnuPG, (prononcer *Gnou-Pé-Gé*) pour arriver à ses fins. Vous avez peut-être déjà entendu parler d'un logiciel qui s'appelle PGP. GnuPG est l'équivalent en logiciel libre. La norme OpenPGP est basée sur des outils employés dans les domaines militaire, financier et autres depuis le début des années 90.

Windows Privacy Tools (WinPT) est un ensemble d'applications pour la signature numérique et le chiffrement de contenus. WinPT inclût WinPT Tray, qui permet de gérer les clés et signatures, ainsi que de chiffrer fichiers et textes (utile pour les envois sur un service comme Hotmail)

Principes de base du chiffrement

Pourquoi chiffrer ses messages ?

Le courriel est un moyen efficace de communiquer avec ses amis, ses collègues, ou encore sa famille, mais il ne permet pas d'authentifier l'identité de l'expéditeur, ou de s'assurer qu'il n'est déchiffrable que par le destinataire. Une solution courante à ce problème est le chiffrement des messages, qui encode un courrier électronique, ce qui le rend lisible uniquement par la personne possédant la clé permettant de le déchiffrer.

Le chiffrement symétrique[1]

Afin d'expliquer le chiffrement symétrique, prenons l'exemple de Bob et Alice. Bob veut envoyer un

1 Cryptographie symétrique sur Wikipedia: http://fr.wikipedia.org/wiki/Cryptographie_sym%E9trique

message secret à Alice. Il peut saisir son message dans un traitement de texte, le chiffrer, l'attacher en pièce jointe et enfin l'envoyer à Alice. Cela a l'air assez simple, non ? Où donc est le problème ?

Afin qu'Alice puisse lire le message secret que lui a envoyé Bob, elle doit connaître la clé qu'il a utilisé pour le chiffrer. Si la clé avait été envoyée par courriel et si quelqu'un avait accès à ce message, cette personne aurait alors la possibilité de déchiffrer et de lire tous les courriels provenant de Bob qui utilisent la même clé. Ainsi, *la principale difficulté dans les systèmes de chiffrement symétrique est la communication sécurisée de la clé*.

OpenPGP: Le chiffrement asymétrique[2]

Pour pallier au problème d'échange de clés lors de l'établissement de communications sécuritaires, des logiciels utilisant le chiffrement *asymétrique* ont été conçus. Une des normes basées sur ce concept est la norme OpenPGP. Ce type de chiffrement utilise deux clés liées mathématiquement :

- Une clé privée : Elle est utilisée pour déchiffrer un message que vous avez reçu. La vôtre ne devra jamais être révélée, même si elle est elle-même chiffrée par un mot de passe que vous détenez.

- Une clé publique : n'importe qui peut utiliser votre clé publique pour chiffrer un message avant de vous l'envoyer. Elle peut être communiquée à n'importe qui.

Reprenons l'exemple de Bob et Alice pour illustrer l'utilisation du chiffrement asymétrique:

Bob et Alice veulent s'échanger des messages chiffrés. Si Bob veut envoyer un message chiffré à Alice, il doit connaître la clé publique de cette dernière. Étant donné qu'elle est autorisée à communiquer sa clé publique à d'autres personnes, Alice l'envoie par courriel à Bob. Ce dernier peut maintenant l'utiliser pour chiffrer son message avant de l'envoyer à Alice.

Maintenant, imaginons qu'une troisième personne, Robert, veuille intercepter et lire les messages de Bob et d'Alice. Bob a donc chiffré son courriel avec la clé publique d'Alice. Robert ouvre le logiciel de messagerie d'Alice alors qu'elle n'est pas à son ordinateur, et découvre que Bob lui a envoyé un message chiffré. En regardant dans le répertoire « Courriels envoyés » d'Alice Robert voit que celle-ci avait transmis à Bob sa clé publique.

Il tentera sans succès d'utiliser la clé publique d'Alice pour déchiffrer le message de Bob. C'est normal car seule la clé privée d'Alice combinée au mot de passe qui y est associé permettent de déchiffrer le message que Bob a envoyé.

La signature numérique

Qu'est-ce que « signer » un message ? C'est le fait d'utiliser la clé privée pour assurer l'authenticité, l'origine et la date de création de contenus. Si vous signez vos courriels, votre destinataire saura que c'est obligatoirement le possesseur de la paire de clés qui a signé ce message.

Des fonctionnalités plus avancées de OpenPGP permettent de signer la clé publique de vos interlocuteurs afin de signaler une vérification d'identité à un degré plus ou moins élevé de confiance. Ce processus ressemble au travail des notaires et constitue, dans son ensemble, ce qu'on appelle la « Web of Trust »

2 Cryptographie asymétrique sur Wikipedia : http://fr.wikipedia.org/wiki/Cryptographie_asym%E9trique

(toile de confiance). Ainsi, il est suggéré de faire signer sa clé publique par autant de vos interlocuteurs qu'il sera possible, afin que son authenticité soit plus facile à déterminer.

Installation de logiciels de courriel et chiffrement

Logiciels requis

Comme mentionné dans la section précédente, l'extension Enigmail pour Thunderbird fonctionne avec GnuPG pour permettre l'envoi de messages chiffrés. GnuPG effectue le chiffrement en arrière-plan, tandis que Thunderbird (grâce à l'extension Enigmail) permet de lire et d'envoyer des courriels chiffrés.

Voici une liste des fichiers que vous devrez télécharger :

1. **Thunderbird**, le client de messagerie (version 0.8 ou supérieure) en version française:
   http://www.mozilla-europe.org/fr/products/thunderbird/

2. Windows Privacy Tools (WinPT) version 1.0rc2, incluant GnuPG, le logiciel de cryptographie et WinPT Tray pour la gestion des clés et le chiffrement de contenus et fichiers:
   http://winpt.sourceforge.net/fr/download.php

3. **Enigmail** et **EnigMIME**, les deux extensions nécessaires au chiffrement de courriels avec Thunderbird:
   http://enigmail.mozdev.org/download.html
   (attention, vous devrez utilisez le bouton droit de la souris et sauvegarder les fichiers .XPI au lieu de les installer à partir du navigateur)

4. Le **« Language Pack » français** pour Enigmail:
   http://downloads.mozdev.org/enigmail/lang/enigmail-fr-FR-0.8x.xpi
   (attention, vous devrez utilisez le bouton droit de la souris et sauvegarder ce fichier au lieu de l'installer à partir du navigateur)

Installation

Les procédures décrites dans cet article ne concernent que les versions Windows des différents logiciels. Téléchargez tous les fichiers indiqués ci-dessus dans un répertoire de votre ordinateur, par exemple : `c:\temp\thunderbird` puis suivez les instructions pour l'installation dans cet ordre:

1. WinPT (incluant GnuPG)
2. Mozilla Thunderbird
3. Extensions Enigmail, EnigMIME et language pack

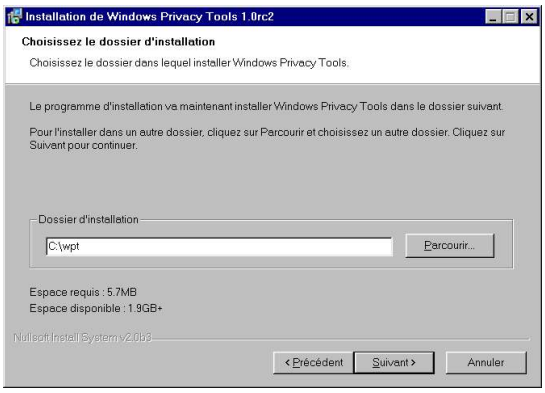
Installation et configuration de GnuPG à l'aide de WinPT

WinPT permet d'installer facilement GnuPG et d'y avoir accès par des outils graphiques ou par la ligne de commande. Nous privilégions ici la création de clés avec WinPT car Enigmail ne permet pas encore directement la création de cles de plus de 1024 octets[3]. Lors de la conception du logiciel il était encore courant de penser qu'une longueur de clé de 1024 octets était suffisante.

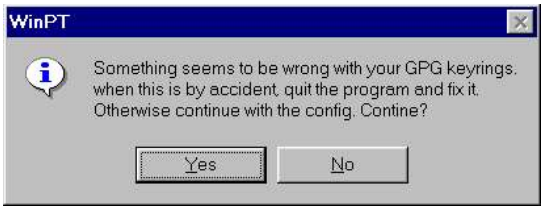
3 Bug #6900: « RFE: Improve key generation », http://bugzilla.mozdev.org/show_bug.cgi?id=6900

Consultez la documentation de WinPT (le WinPT handbook, disponible séparément) **avant** de continuer, afin de bien comprendre les implications de la génération de votre paire de clés.

1. Installez WinPT en suivant ses instructions, toutefois choisissez le répertoire **`c:\wpt`** comme cible de l'installation et **`Français`** pour la langue des applications. Cela en facilitera l'accès éventuel.



2. Éventuellement, lors de l'installation, un message d'erreur s'affichera:



   Choisissez **`YES`**. Comme il s'agît d'une nouvelle installation, il est normal que le logiciel s'étonne de ne pas trouver les informations nécessaires.

3. La prochaine étape consiste à spécifier si vous allez utiliser des clés d'une autre installation ou créer de nouvelles clés.

   Si vous n'avez jamais utilisé de chiffrement, choisissez la première option, puis dans le dialogue suivant une grosseur de clé de 4096 octets pour une sécurité accrue (malgré les avertissements).

   Suivez les instructions pour compléter l'installation. Dans tous les autres cas, choisissez l'option appropriée et continuez.

Installation et configuration d'Enigmail pour Thunderbird

1. Exécutez le programme d'installation ThunderbirdSetup-0.7.2-fr.exe

2. Lancez Thunderbird en utilisant le raccourci créé par le programme d'installation et dans le menu **`Tools > Langue de l'application`** choisissez **`Français`**.

3. Lancez de nouveau Thunderbird en utilisant le raccourci créé par le programme d'installation.

4. Configurez un compte de façon à pouvoir envoyer et recevoir des courriels.

5. Pour les trois fichiers **`.xpi`** (extensions Enigmail et Enigmime, puis Language Pack français) répétez les étapes suivantes:

    1. Ouvrez le menu « Outils » de Thunderbird, puis sélectionnez « Extensions » :

    2. Cliquez sur « Installer »

    3. Installez le fichier XPI correspondant, en ignorant l'avertissement concernant les signatures numériques[4]

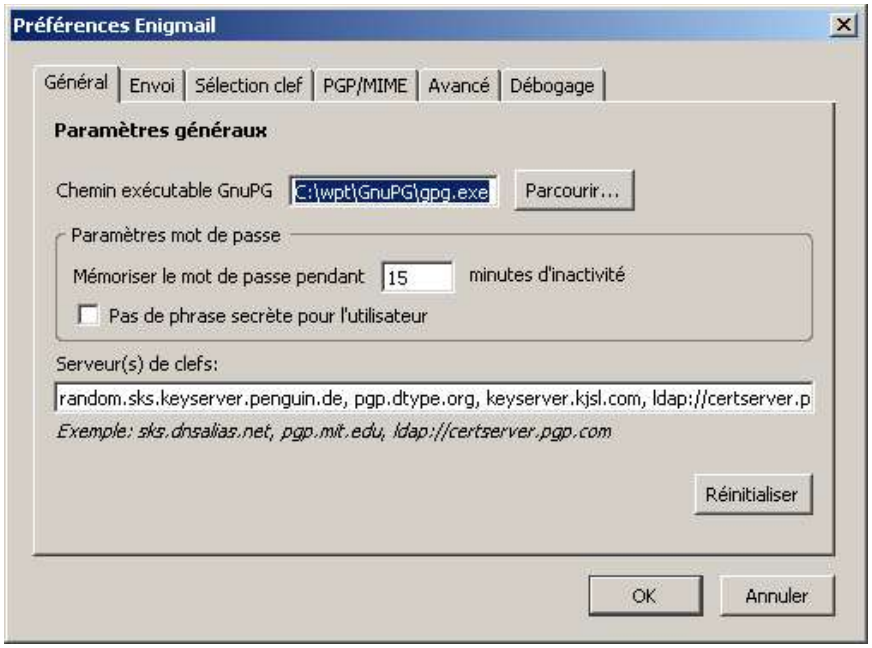
    4. **IMPORTANT:** Quittez Thunderbird complètement afin que l'extension voulue soit activée

    5. Répétez pour une autre extension

6. Une fois les trois extensions installées, redémarrez Thunderbird *une autre fois*. Le menu Enigmail devrait être visible parmi les menus disponibles.

4 Le processus de signatures numériques des extensions Mozilla n'est pas encore en place. Lors du lancement de la version 1.0 de Firefox il est à prévoir qu'il sera finalisé

7. Ouvrez le menu « Enigmail », puis sélectionnez « Préférences »:



   Il n'est pas conseillé d'utiliser l'option « Mémoriser le mot de passe pendant... » si quelqu'un d'autre peut accéder à votre poste informatique. Dans ce cas indiquez « 0 » (zéro) comme valeur des minutes d'inactivité.

8. Dans l'onglet « Général », assurez-vous que « le chemin d'accès au fichier exécutable GPG » est bien **`c:\wpt\GnuPG\gpg.exe`** .

9. Ouvrez le menu « Outils » puis sélectionnez « Paramètres des comptes » et trouvez la section correspondant au compte de messagerie électronique que vous avez configuré. Cliquez sur la sous-catégorie « Rédaction et envoi » et décochez « Rédiger les messages en HTML ».

10. Allez dans la sous-catégorie « Sécurité OpenPGP » et choisissez « Activer la support OpenPGP (Enigmail) pour ce compte »

11. À l'aide du bouton « Choisir une clé », choisissez la clé que vous avez générée pour cette installation.

12. Afin de minimiser les problèmes de compatibilité, consultez les paramètres suggérés à l'Annexe A

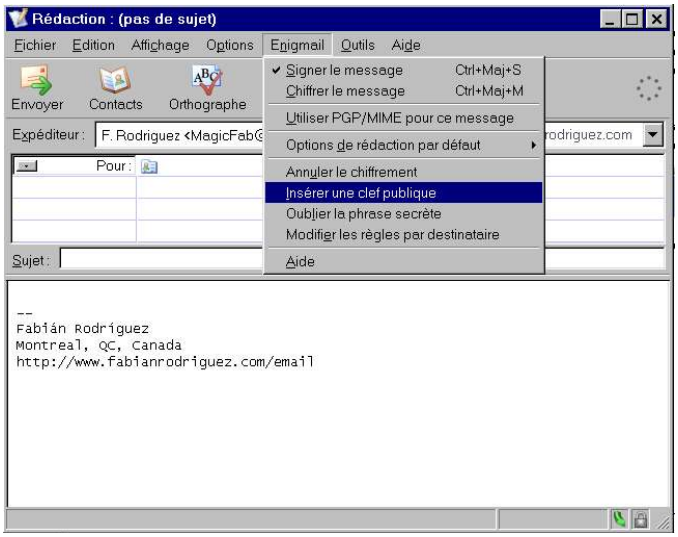
Utilisation

Envoi de votre clé publique à l'aide de Enigmail

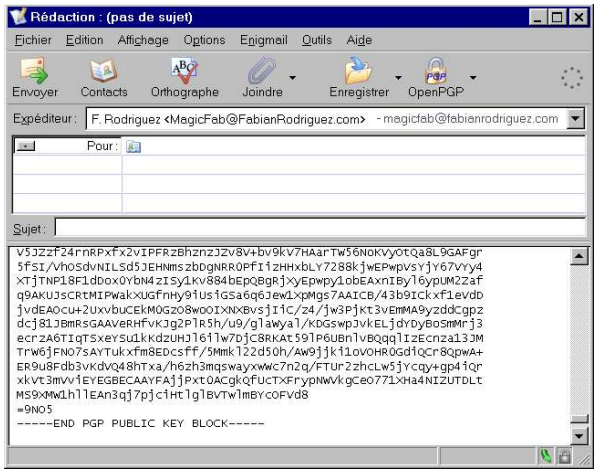
Il est maintenant temps d'envoyer votre clé publique à vos correspondants, de façon à ce qu'ils puissent vous envoyer des fichiers chiffrés et vérifier votre signature. N'importe quelle personne qui a votre clé publique peut chiffrer et vous envoyer du courrier que vous seul pourrez lire en utilisant votre clé privée.

1. Créez un nouveau message en appuyant sur le bouton « Écrire » ou sur les touches raccourci CTRL-M.

2. Ouvrez le menu « Enigmail » et choisissez « Insérer une clé publique »:



3. Choisissez votre clé publique parmi la liste présentée. S'il s'agît de votre première installation, il est probable que seule votre clé apparaisse. Voici ce à quoi ressemblerait le résultat:



4. Lorsque votre interlocuteur recevra votre clé publique, il pourra l'importer en utilisant l'option « Déchiffrer » sous Enigmail ou une option similaire selon le logiciel utilisé.

Envoi de messages chiffrés avec Thunderbird

Vous pouvez également envoyer un message chiffré avec Thunderbird.

1. Rédigez normalement votre message dans Thunderbird :

2. Une fois que c'est fait, cliquez sur le bouton OpenPGP de la barre d'outils et cochez les cases « Signer le message » et « Chiffrer le message ». Cochez aussi l'option « Utiliser PGP/MIME pour ce message » si votre interlocuteur utilise aussi Enigmail. Cela facilitera l'encodage de fichiers attachés.

3. Si le destinataire utilise un webmail, il pourra déchiffrer le message à l'aide WinPT Tray par exemple.

Envoi de messages chiffrés avec un webmail

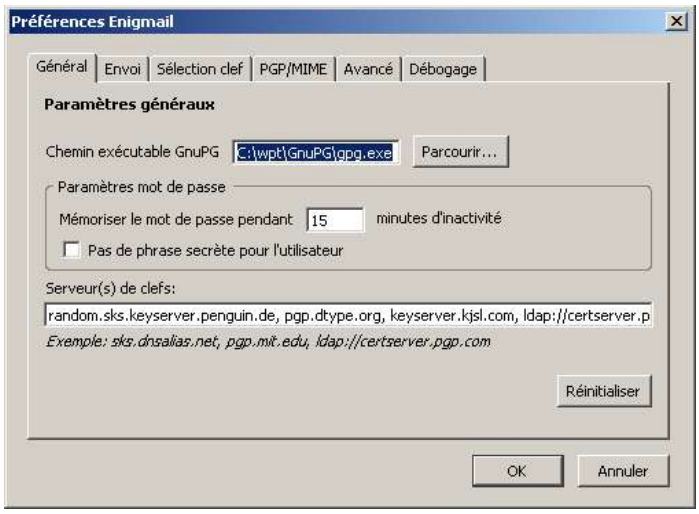
Si vous avez un compte de courriel sur un service web gratuit comme GMail, à partir duquel vous voulez envoyer des messages chiffrés, c'est possible à l'aide de WinPT Tray.

Vous pouvez utiliser les mêmes clés utilisées avec Enigmail, mais vous devrez réinstaller WinPT et importer ces clés sur le poste à partir duquel vous voulez chiffrer vos messages. **Attention:** s'il s'agît d'un poste informatique public (bibliothèque, etc), n'oubliez pas que malgré toutes les précautions que vous prendrez, si vos clés y sont enregistrées il serait possible pour un autre utilisateur de les récupérer et/ou de mettre sous écoute ce poste pour récupérer votre mot de passe.

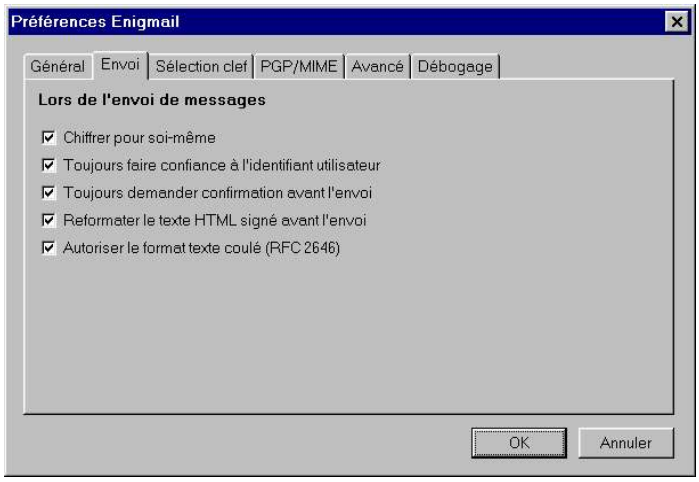
Pour en savoir plus sur le chiffrement et le déchiffrement de messages et fichiers avec WinPT Tray, consultez sa documentation, disponible par le menu **`Démarrer > Programmes > Windows Privacy Tools > Documentation`** .

Annexe A: Paramètres suggérés

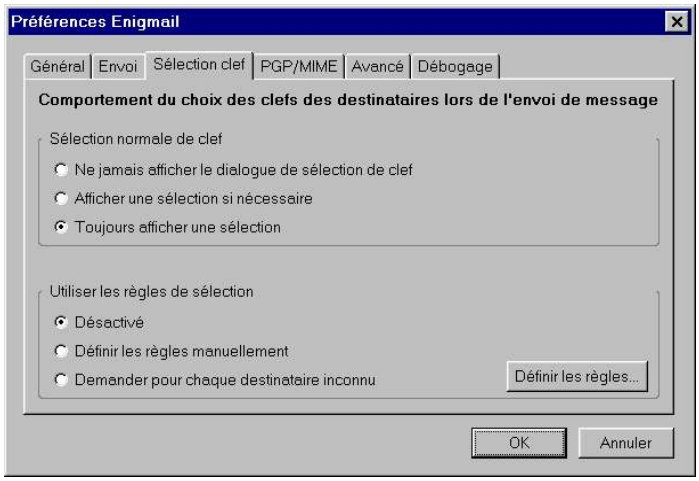
1. Dans **`Options > Paramètres comptes > Sécurité OpenPGP`**, section **`Options de rédaction par défaut`**:
   1. Cochez l'option « **`Signer les messages non-chiffrés par défaut »`**
   2. Cochez l'option « **`Signer les messages chiffrés par défaut`** »
2. Dans **`Enigmail > Préférences > Général`** :



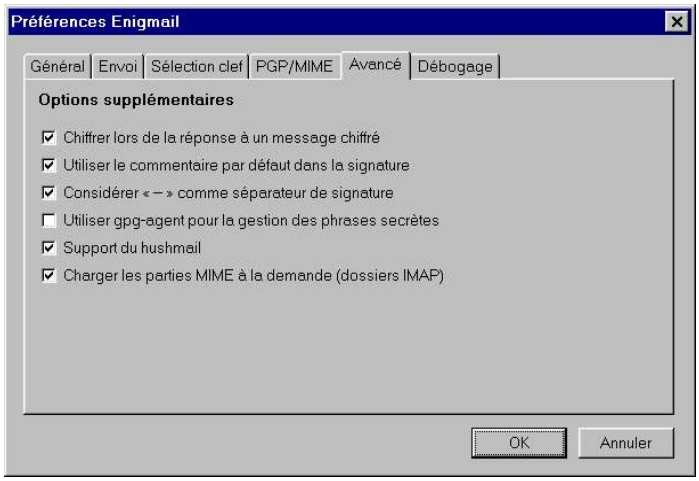
3. Dans **`Enigmail > Préférences > Envoi`**:



4. Dans **`Enigmail > Préférences > Sélection de clé`** :



5. Dans **`Enigmail > Préférences > Avancé`** :



Pour en savoir plus sur chacune des options ici présentées, consultez le guide détaillé de configuration en ligne à **`http://enigmail.mozdev.org/configure.html`** .