Configurer GnuPG sous Mac OS X

Vous trouverez ici les instructions pour installer et configurer Mac OS X afin d'encrypter vos mails et fichiers texte. De plus, nous vous présentons d'autres outils intéressants pour faciliter votre travail. Des informations plus détaillées sur GnuPG se trouvent également sur le site web des développeurs du projets.

Si vous cherchez à importer une clé publique dans votre chaine de clés, vous pouvez demander un serveur de clés.

Introduction

GnuPG est un système d'encryption qui fonctionne en lignes de commande, compatible avec PGP 5 et plus, qui a été developpé pour UNIX et ses dérivés. Etant donné que Mac OS X est basé sur un système BSD-UNIX, les utilisateurs de Mac peuvent désormais utiliser GnuPG également.

Les auteurs du projet Mac GNU Privacy Guard ont porté ce software sur les plateformes Mac X et développé divers outils pour que les utilisateurs puissent bénéficier des avantages de toutes les fonctions dans le cadre d'une interface graphique. Tous les outils présentés ici sont encore endéveloppement. Leur fonctionnalité et maniabilité vont s'améliorer de manière constante.

GnuPG est publié sous GPL (GNU Public License) et est donc librement accessible.

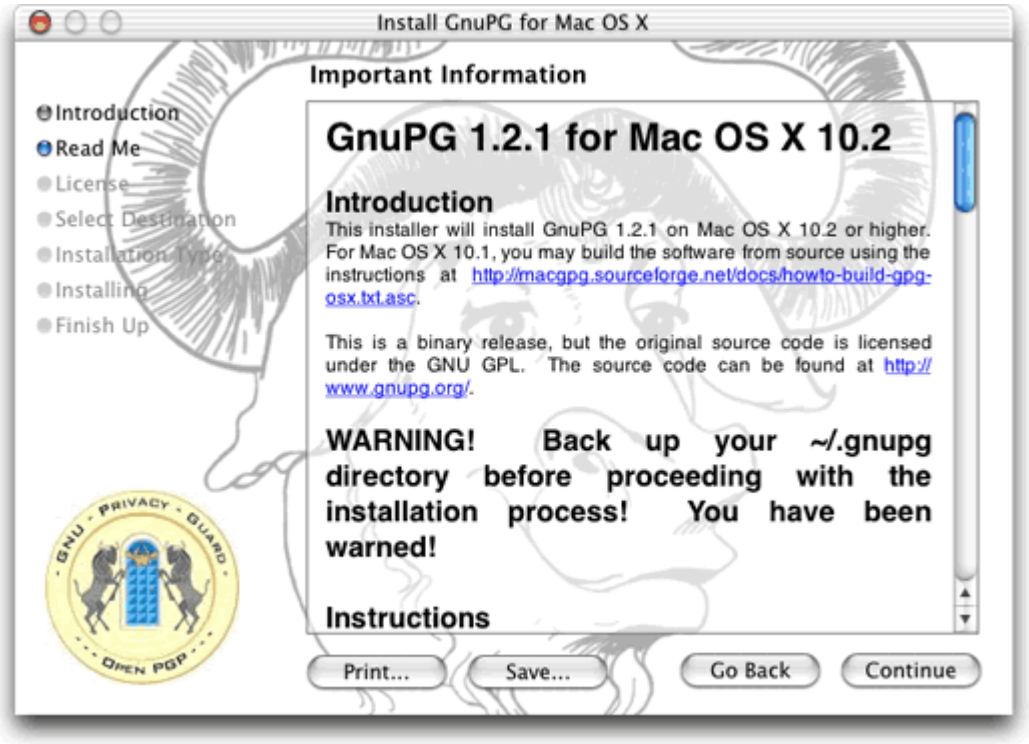
top

Installation

Pour installer GnuPG vous devez avoir le droit d'administrer la machine en tant que Super Utilisateur. Sans être Administrateur du système, vous ne serez pas en mesure d'installer le software.

1. Téléchargez GNU Privacy Guard, décompactez-le (par exemple avec StuffIt Expander), faites monter l'image du disque où il se situe en double-cliquant dessus et ouvrez le lecteur “GnuPG for Mac X” qui est maintenant apparu sue votre bureau.
2. Maintenant double-cliquez sur "GnuPGOSX.pkg". Un fenêtre s'ouvre. Cliquez sur le symbole

du verrou et insérez de mot de passe de l'Administrateur. Confirmez avec OK et suivez les instructions sur l'écran.



top

Génération de clés

Les étapes qui suivent sont aussi expliquées en détails sur [Instructions on GnuPG](#).

Notez que cette démarche doit être effectuée par tous les différents utilisateurs de votre système qui n'ont pas déjà de clés pour Mac !

Si vous n'avez jamais utilisé PGP ou tout autre software d'encryption compatible basé sur un système de codage assymétrique auparavant, vous devrez générer une paire de clés directement après l'installation du software.

Pour continuer, veuillez ouvrir un "Terminal" (fenêtre pour entrer des instructions en lignes de commande).

Lorsqu'invoqué pour la première fois, GnuPG va créer un répertoire dans le “home directory” à la racine de votre système de fichiers pour souvegarder vos clés privées et publiques ainsi que le fichier de configuration. Ce répertoire sera caché, vous ne serez pas en mesure de le voir dans le Finder!

1. D'abord, il faudra générer une paire de clés. Vous aurez à répondre à différentes questions. Nous allons essayer de vous aider ici pour un mieux. Exécutez les commandes suivantes en lignes de commande (les commandes à introduire sont indiquées en rouge. En noir : la réponse du système. N'oubliez pas qu'il faut toujours confirmer vos commandes en tapant sur la touche Enter :

```
[localhost:~] user% gpg --gen-key
gpg (GnuPG) 1.4.0; Copyright (C) 2004 Free Software Foundation, Inc.
```

```
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

gpg: directory `/Users/hans/.gnupg' created
gpg: new configuration file `/Users/hans/.gnupg/gpg.conf' created
gpg: WARNING: options in `/Users/hans/.gnupg/gpg.conf' are not yet active
during
this run
gpg: keyring `/Users/hans/.gnupg/secring.gpg' created
gpg: keyring `/Users/hans/.gnupg/pubring.gpg' created
Please select what kind of key you want:
   (1) DSA and Elgamal (default)
   (2) DSA (sign only)
   (5) RSA (sign only)
Your selection? 1
```

DSA est le standard pour la signature de textes, ElGamal est un puissant algorithme d'encryption. C'est pourquoi nous vous incitons à choisir l'option 1.

```
DSA keypair will have 1024 bits.
ELG-E keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 4096
Requested keysize is 4096 bits
```

Ici vous devez choisir une longueur de 4096 bits pour votre clé. En résumé : plus longue est la clé, plus elle est protégée contre les attaques en force brute.

```
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct (y/N)? y
```

Ici vous devez indiquer au système si et quand une clé doit venir à expiration. En général vous n'aurez pas besoin d'une clé qui expire, aussi vous choisirez 0, la valeur par défaut. Il vous faudra juste le confirmer.

Si vous pensez que votre clé devrait être juste valide pour une certaine période de temps, enterez un chiffre suivi si nécessaire par le code de la période désirée : 5w pour 5 weeks (semaines), 8m pour 8 months (mois), 2y pour 2 years (années). Si vous entrer simplement un chiffre, cela indiquera juste le nombre de jours avant que votre clé n'exprire.

```
You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Jean Smets
Email address: jean.smets@all2all.be
Comment: no secrets
You selected this USER-ID:
    "Jean Smets (no secrets) <jean.smets@all2all.be>"
```

```
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
```

Maintenant votre identité d'utilisateur va être crée. Vous pourrez en créer d'autres plus tard. Votre identité consiste en votre nom complet, votre adresse e-mail et un commentaire optionnel. Vous devez porter attention à votre identité d'utilisateur car elle ne pourra pas être modifiée plus tard !

```
You need a Passphrase to protect your secret key.

Enter Passphrase: 1 phr@se de reconnaissance doit être longue et compliquée!
Repeat Passphrase: 1 phr@se de reconnaissance doit être longue et compliquée!
```

Afin d'éviter que votre clé soit frauduleusement utilisée par d'autres, GnuPG va l'encrypter avec un algoritme symetrique. aussi devrez-vous choisir votre phrase de reconnaissance avec beacoup de soin également.

N'utilisez dans aucun cas la phrase donnée dans cet exemple ! N'employez pas non plus le nom de vos proches, des dates d'anniversaire ou n'importe quel mot issu du dictionnaire. Veuillez trouver plus d'information sur la manière de choisir de meilleures phrases de reconnaissance à la section Informations techniques.

Pour votre propre protection, l'introduction de votre phrase de reconnaissance s'opère de manière cachée. Vous ne serez pas capable de lire ce que vous tapez. Pour des raisons de sécurité, il faut introduire le phrase de reconnaissance une seconde fois.

Félicitations! Vous avez à présent terminé. GnuPG va maintenant créer votre clé privée (secrète) et votre clé publique. Cela peut prendre un certain temps en fonction de la taille de votre clé. Soyez donc patient ! Après cela, vous pourrez utiliser un système d'encryption puissant sur votre Mac OS X.

```
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
++++++++++++++.++++++++++++++...+++++++++++++++++++++++++++++.++++++
++++++++++++++++++.++++++++++++++++++.++++++++++++++++++++.+++++....
+++++...>+++++..............>+++++.<+++++........+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
..+++++.+++++.+++++++++++++++++++++++++++.+++++.++++++++++.++++++++++.+++
++++++++++++++++++++++++++++++++++++++++++..++++++++++++++++++++++++++++
+++.+++++...+++++>++++++++++>+++++.................+++++^^^^^
gpg: /Users/hans/.gnupg/trustdb.gpg: trustdb created
gpg: key 80EEFCB2 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
pub   1024D/80EEFCB2 2004-12-17
      Key fingerprint = 526B 9A10 AC4E DF93 D097  914E 9B55 76CA 80EE FCB2
uid                  Jean Smets (no secrets) <jean.smets@all2all.be>
```

```
sub   4096g/06A49AE2 2004-12-17
```

top

Importer des clé existantes dans PGP sous Mac OS

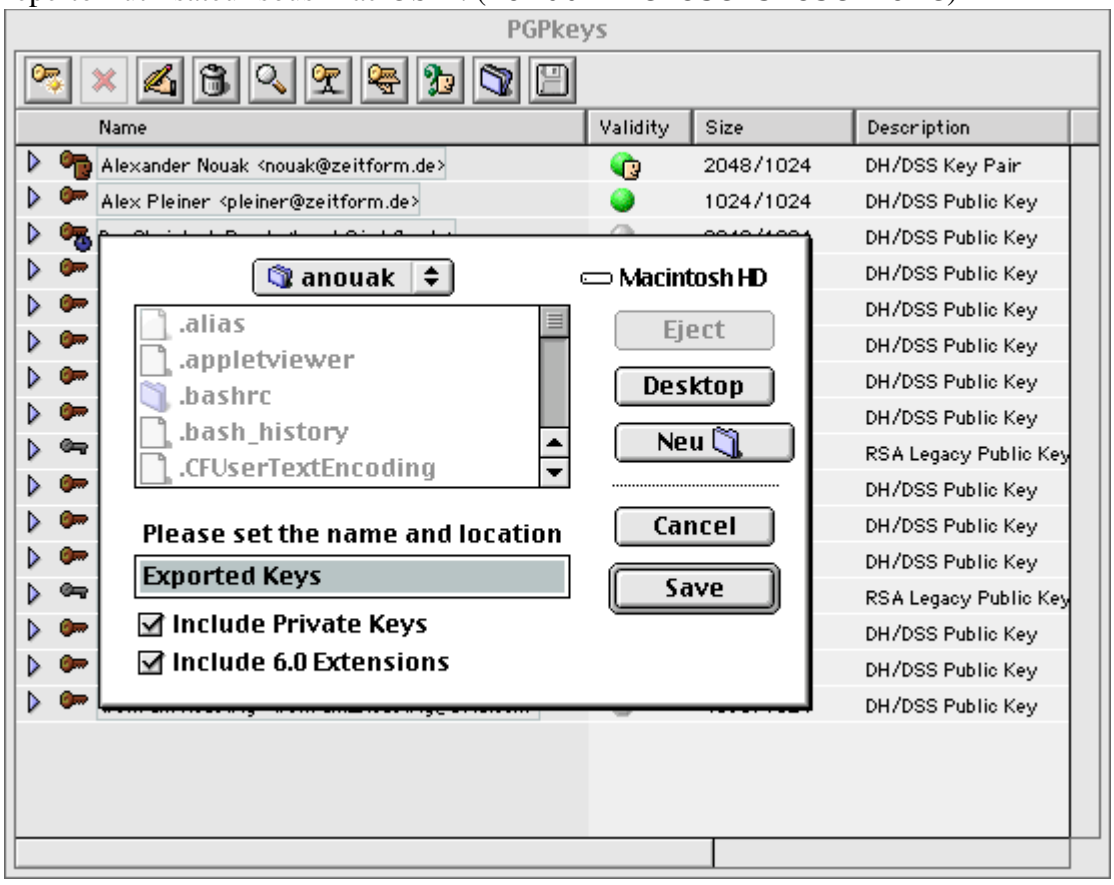
Notez que cette démarche doit être effectuée par tous les utilisateurs de votre système qui ont déjà une clé, par exemple de PGP pour Mac !

Veuillez noter en outre que pour que l'opération réussisse, PGP pour Mac doit être installé dans l'environnement Classic avec toutes ses extensions système.

Si vous travailliez déjà avec un programme d'encryption sous Mac, vous pourrez toujours utiliser votre clé privée et toutes vos clés publiques. Vous devez juste exporter les clés existantes et les importer dans GnuPG.

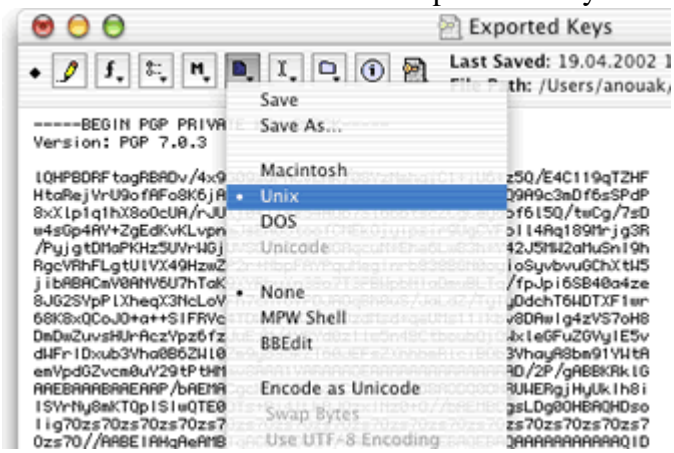
Si vous utilisez un système d'encryption pour la première fois, lisez d'abord le chapitre Génération de clés.

1. Ouvrez l'applikation "Keys". Selectionez toutes les clés que vous avez l'intention d'employer avec GnuPG. Choisissez "Export" dans le menu "Keys".
2. Soyez sûr d'avoir activé l'option "Include Private Keys" et "Include 6.0 Extensions" dans la bôite de dialogue qui s'ouvre. Sauvez le fichier sous "Exported Keys" à l'intérieur de votre répertoir utilisateur sous Mac OS X. (`Harddrive:Users:Username`)



3. Ouvrez le fichier qui vient juste d'être généré avec un éditeur de texte, avec BBEdit lite par

exemple, et changez les retours à la ligne Macintosh en retours à la ligne UNIX. Sauvegardez ensuite le fichier sous le nom "Importable Keys".



Alternativement, vous pouvez aussi ouvrir un "Terminal" et taper les commandes suivantes (en rouge ci-dessous, à confirmer avec la touche Enter) :

```
[localhost:~] user% tr -d '\r' < "Exported Keys" > "Importable Keys"
```

4. Lorsqu'invoqué pour la première fois, GnuPG va créer un répertoire dans le “home directory” à la racine de votre système de fichiers pour souvegarder vos clés privées et publiques ainsi que le fichier de configuration. Ce répertoire sera caché, vous ne serez pas en mesure de le voir dans le Finder!

   Pour importer toutes les clés publiques dans GnuPG, introduiser la commande suivante dans le Terminal :

   ```
   [localhost:~] user% gpg --import "Importable Keys"
   ```

5. Pour importer votre clé privée dans GnuPG, exécutez la commande suivante :

   ```
   [localhost:~] user% gpg --import --allow-secret-key-import "Importable Keys"
   ```

   Félicitations ! Vous avez installé GnuPG avec succès et pouvez maintenant encrypter vos messages. Poursuivez en lisant comment configurer les options pour GnuPG au chapitre GPGPreferences – Options GnuPG.

top

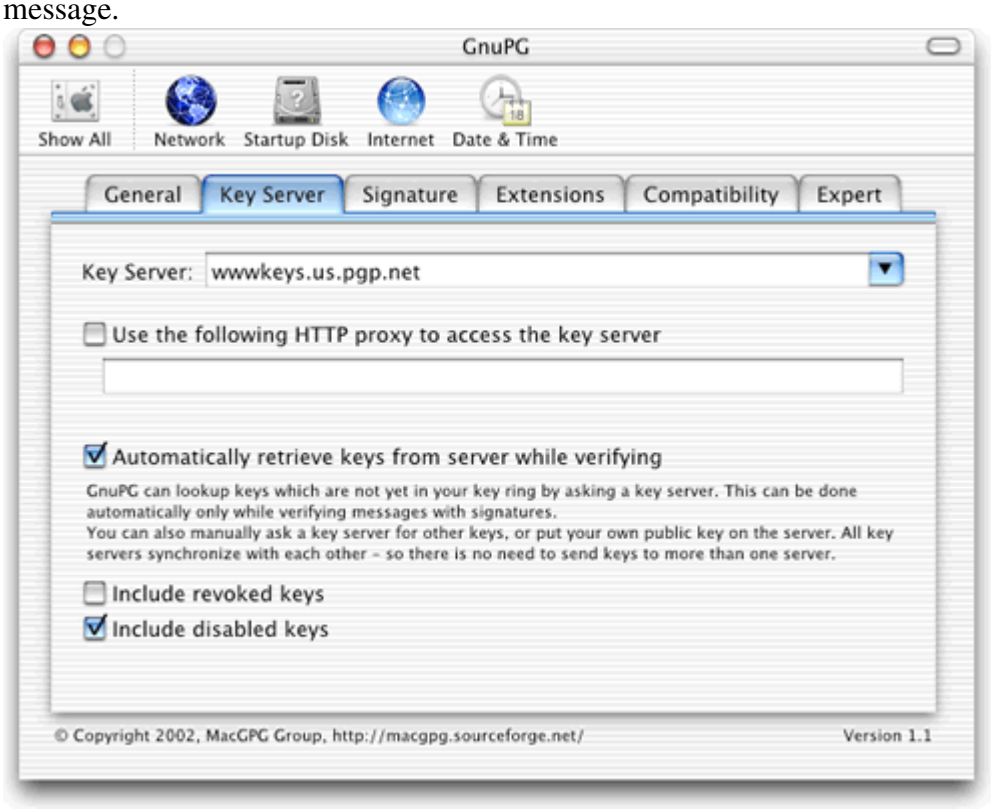
GPGPreferences – Options GnuPG

Normallement vous éditez les fichiers d'options avec un éditeur de texte pour changer les options définies par des programmes qui fonctionnent en lignes de commande.

Comme ce n'est pas la manière dont travaillent les utilisateurs de Macintosh, vous pouvez employer une autre méthode en installant GPGPreferences. Avec ce programe, vous pouvez changer toutes les options nécessaires à l'aide d'un panneau de configuration dans les "System Preferences".

A priori, vous pouvez laisser les options telles qu'elles sont. Soyez juste certain de choisir un serveur approprié sous "Key Server" (serveur de clés) pour permettre l'importation de nouvelles clés lorsque c'est nécessaire. Si vous choisissez l'option "Automatically retrieve keys from server while verifying"

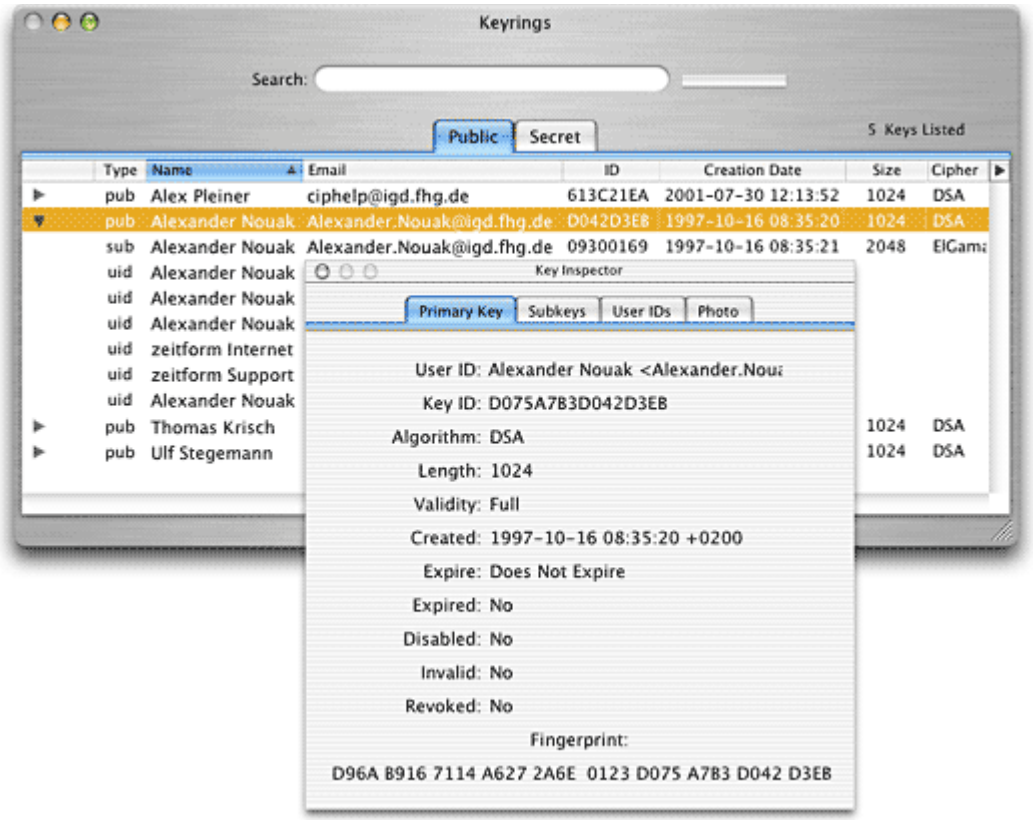
les clés dont vous avez besoin seront chargées automatiquement quand vous vérifiez la signature d'un message.



top

GPGKeys – La gestion des clés

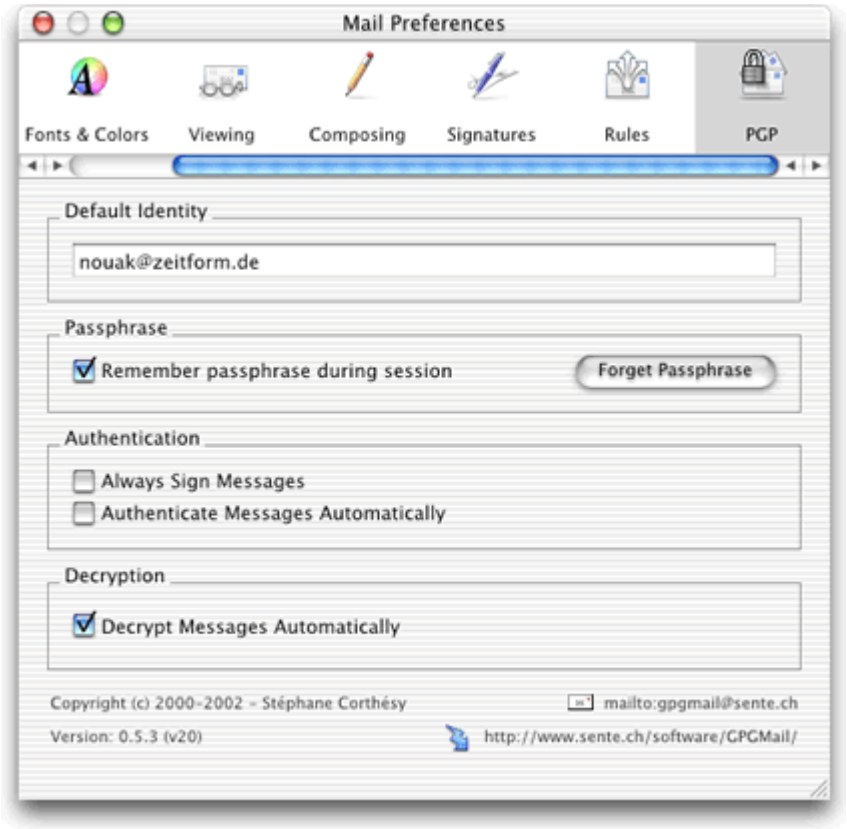
Pour gérer à la fois les clés privées et publiques, vous pouvez utiliser GPGKeys, dont le design et l'interface graphique sont similaires à la Suite PGP pour Mac. Cette application vous permet d'importer et d'exporter des clés publiques pour les transmettre aux personnes avec lesquelles vous voulez communiquer. De plus, vous pouvez générer et signer de nouvelles clés. Vous pouvez même rechercher des clés sur des serveurs de clés.



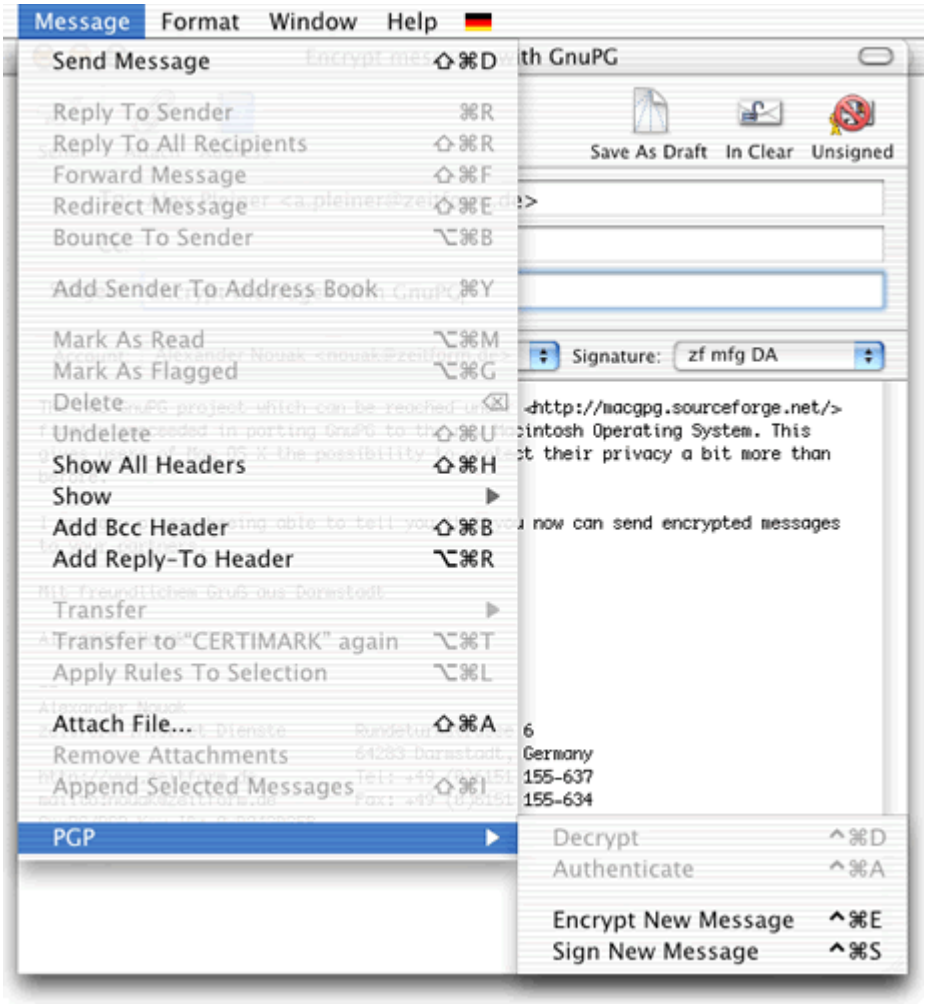
top

GPGMail – GnuPG dans Mail d'Appel

GnuPG est principalement utilisé pour des communications via e-mail. Pour faciliter l'encryption et la signature des e-mails, la société suisse Sen:te a créé GPGMail, un plug-in pour le programme"Mail" livré avec Mac OS X. Un panneau de configuration additionnel vous permet de régler toutes les options.



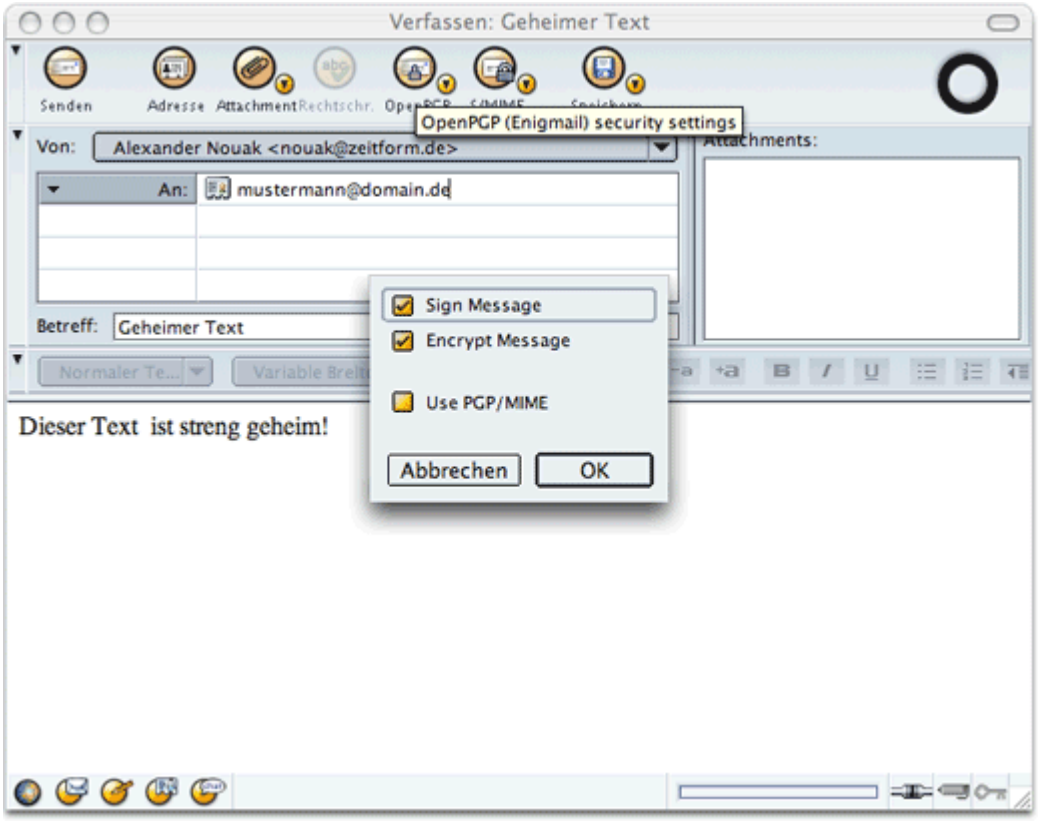
Vous pouvez exécuter les commande pour l'encodage, la signature et le décodage dpuis un menu additionnel dans "E-Mail" ou en utilisant les nouveaux choix dans la barre de menu.



top

Enigmail – GnuPG dans Thunderbird, Mozilla ou Netscape

Avec Enigmail la communauté "Mozilla" a développé une extension pour les clients e-mail à l'intérieur des suites des navigateurs "Mozilla" et "Netscape" aussi bien que pour le client e-mail in dépendant "Thunderbird" qui fournit un nouveau menu doté de toutes les options nécessaires pour encoder, décoder et signer les messages. Des boutons dans la fenêtre des messages font apparaître toutes les fonctions nécessaires.

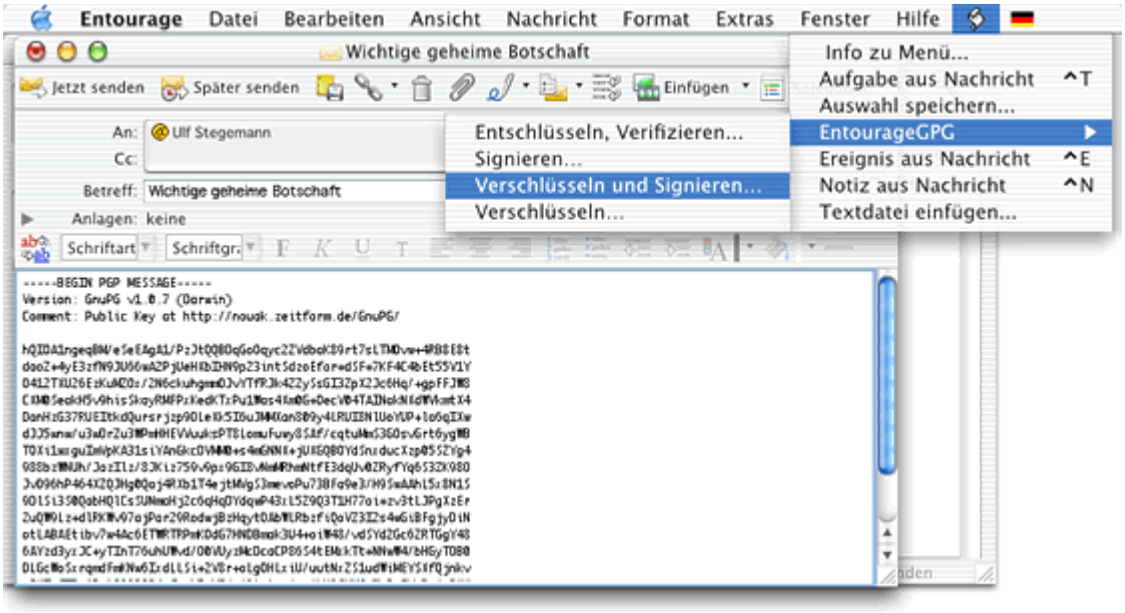


De plus "Enigmail" est livré avec un gestionnaire de clé qui rend l'installation de GPGKeys superflue.

top

EntourageGPG – GnuPG pour MS Entourage

Les utilisateurs d' "Entourage" qui est livré avec MS Office peuvent utiliser également les fonctionnalités principales de GnuPG. can make use of the main functionalities of also. Simon Kornblith a développé une série d'AppleScripts et les offre gratuitement avec un bel installeur sous EntourageGPG.



Après l'installation des AppleScripts, vous pouvez trouver une nouvelle entrée intitulée "EntourageGPG" dans le menu des scripts qui vous donne la possibilité d'appeler les fonctionnalités principales d'encodage et de décodage de vos e-mails.

top

Eudora-GPG – GnuPG dans Qualcomms Eudora

Les utilisateurs de Qualcomms Eudora peuvent utiliser les AppleScripts écrits par Richard Chang qui peuvent se trouver gratuitement sous Eudora-GPG.

top

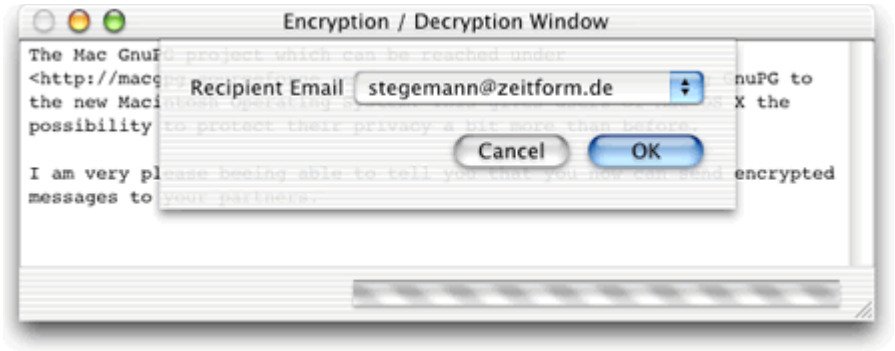
MailSmith-GPG – GnuGP dans BareBones MailSmith

Les utilisateurs de BareBones MailSmith peuvent utiliser les AppleScripts écrits par Alessandro Ranellucci qui peuvent se trouver gratuitement sous MailSmith-GPG.

top

GPGDropThing – L'encryption de fichiers texte

Si vous utilisez un client e-mail qui n'a pas encore d'interface pour GnuPG, ou si vous voulez simplement encoder ou décoder des fichiers texte, vous ne devez pas nécessairement utiliser des lignes de commande. Avec GPGDropThing vous disposez d'une application qui vous permet de taper du texte dans une fenêtre (vous pouvez aussi utiliser l'option “Copier/Coller”) et puis de le signer et de l'encrypter. Ou vice-versa : coller le texte encrypté dans la fenêtre et choisir la commande de décodage. Après avoir introduit votre phrase de reconnaissance, vous pourrez voir l'information apparaître en clair.



Vous pouvez lancer l'application GPGDropThing depuis n'importe quelle autre application capable d'éditer du texte. En utilisant le menu "Services", vous avez accès aux quatre commandes les plus utilisées : Encrypt, Decrypt, Sign et Verify.