Mozilla With Enigmail and GnuPG Mini Howto

LeRoy D. Cressy
leroy@lrcressy.com

v1.4 July 17, 2003

Editors:

Rita J. Cressy
Sibylla C. Cressy
Patrick Brunschwig

Contents

1 Introduction

1.1 Thanks

The author wants to thank all of the fine developers and the ones who have written the fine documentation for:

GnuPG http://www.gnupg.org/

Mozilla http://www.mozilla.org/

Enigmail http://enigmail.mozdev.org/

Phil Zimmermann http://www.philzimmermann.com/

Without all of the work that has preceded this document, there would have not been the possibility of good solid encryption offered by both PGP and GnuPG. If Phil Zimmermann's code was never published on the Internet, the United States Government would have done everything in its power to prevent the people from having good encryption.

1.2 Overview

The purpose of this document is to help the users who do not like to read documentation familiarize themselves with the concepts of using Mozilla along with Enigmail and GnuPG for both sending and receiving email that is signed, encrypted, or with both features.

The author hopes that the reader will benefit and have a better understanding about using Mozilla and encrypted email.

1.3 History

Mozilla is the free open source version of Netscape Communicator. Enigmail is a separate add-on application to Mozilla that makes sending and receiving signed, encrypted, or both email messages work with a mouse click. Enigmail depends upon GnuPG being installed on the system.

1.4 Feedback

Any suggestions, comments, and constructive criticisms are welcome. I read all of my email, but I don't have the time to respond to every message.

All flames will end up in /dev/null.

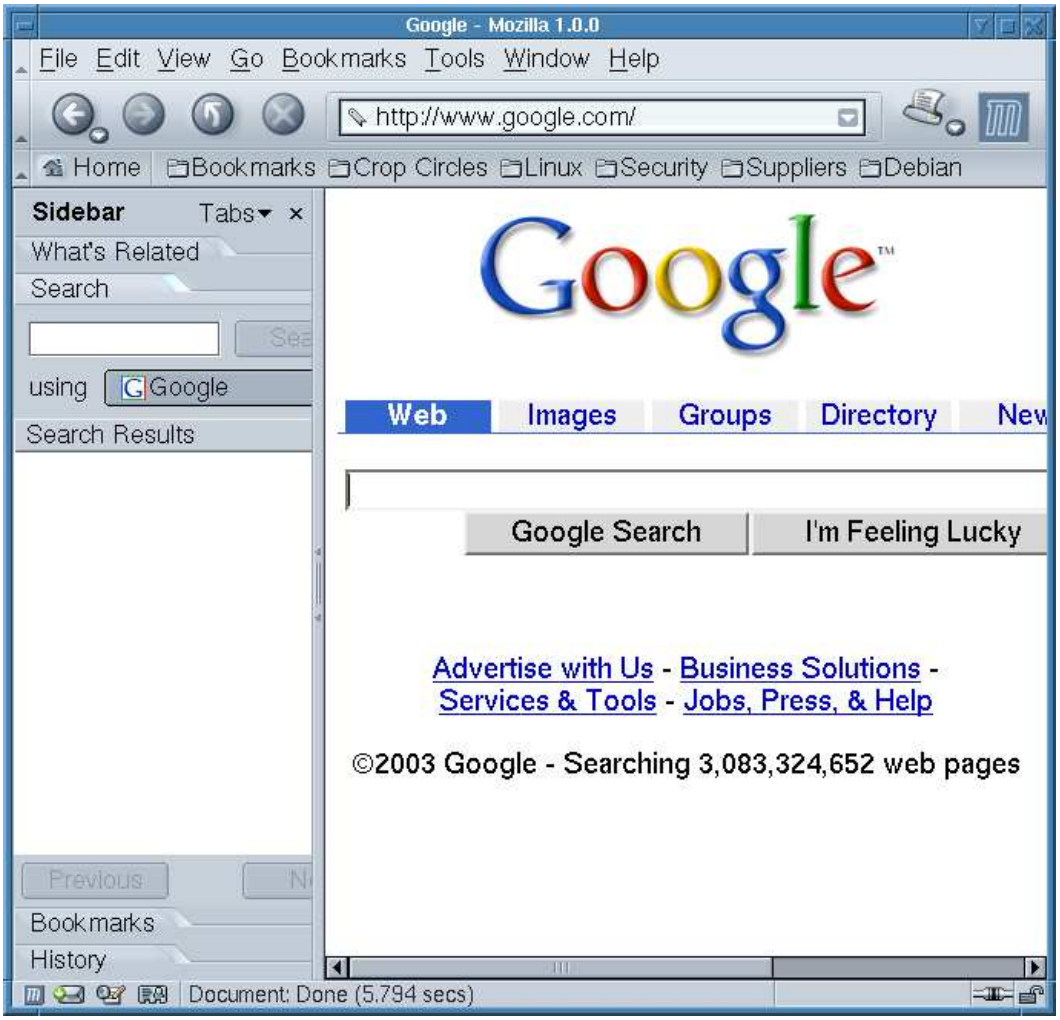
2 What is Mozilla?

Mozilla is a descendent of Netscape Communicator. It contains:

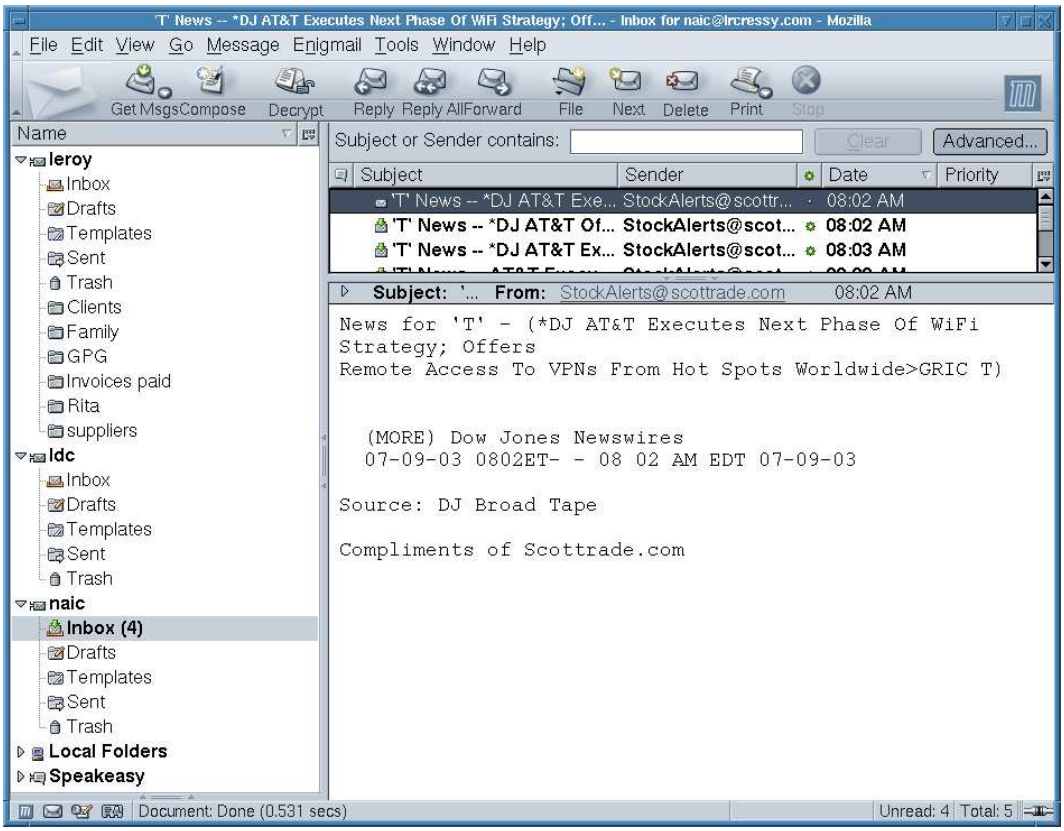
- World Wide Web Browser

- Mail Client
- News Reader
- Address Book
- Html Composer

Mozilla looks like the following graphic:



To open the various applications in Mozilla, click on the menu Window button and choose what application you want to use. For reading and composing email, select Mail & News Groups. This opens the mail and newsgroups window.

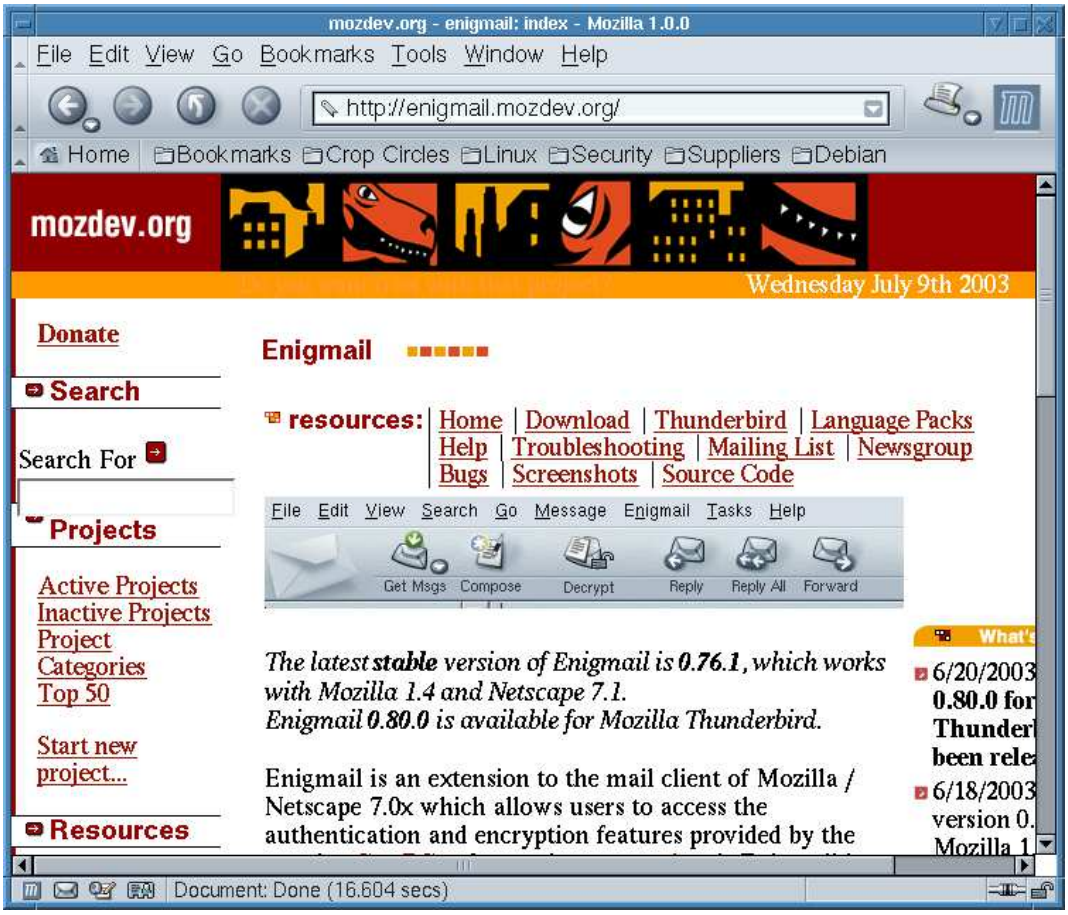


Mozilla allows you to have multiple pop3/IMAP email accounts along with multiple news accounts. Like you can have two on Comcast, one Juno, and another on your company's network. The former versions of Netscape allowed you to only have one pop3 account. This is a tremendous improvement that has also been implemented into the newest release of Netscape.

Later on we will concentrate on the various portions of the Mozilla email client. Now it is time to move on and look at the Enigmail add on application to Mozilla.

3 What is Enigmail?

Enigmail is a separate development add-on package to the Mozilla email client. Enigmail depends on the GnuPG package being installed with a key pair already generated. Enigmail is named after the German Enigma machine in World War II. The home page for the Enigmail project is http://enigmail.mozdev.org/



Enigmail makes sending and receiving secure encrypted messages both easy and reliable. There are other email clients that integrate with GnuPG like mutt, but using a text based email client does not provide graphics support like the browser based email clients. My mother-in-law routinely sends photos of the family with her email messages. So for the person who wants to use both secure encryption and graphics with their email, Mozilla is the way to go.

As stated earlier, you will need to have GnuPG loaded on your system along with a generated key pair to make this application work.

4 What is GnuPG?

GnuPG is the GNU version of PGP (Pretty Good Privacy) developed by Phil Zimmermann. PGP had problems with the U.S. export laws, so the Gnu people started the GnuPG project with the requirements that only developers that have no ties to the United States could

work on the project. This meant that any U.S. citizen could not work on the initial project. Needless to say when the export laws were relaxed, U.S. citizens were welcomed to work on the project.

GnuPG provides true military grade encryption, enabling a very high level of security. This enables a user to send an encrypted message to anyone in the world provided that they have the public key. Only the person who has the private key corresponding to the public key can view the message. Also all of the attachments are encrypted in the message. This level of security provides both the sender and the receiver protection from prying eyes. For the corporate user, this elevates security where corporate espionage is concerned. The present method that the majority of companies use is plain text messages that provide no security at all. If an employee sends an email containing sensitive corporate material outside of the corporate network, everyone along the line to the final destination can view the message. When the recipient downloads the message, there is continued danger from prying eyes.

I have found that most corporations have a very lax concept of computer security and are in grave danger of having their corporate information stolen. Employees send and receive email all over the country while never paying any attention to corporate security policies. Also, many load software on their corporate computers thinking that the virus protector will protect their system. How many times have you lost data and man hours, by some computer being infected by a virus? One time is too much if the infection came from a total disregard to corporate security policies.

Let's take for example an employee sending an email concerning the hot new product that is being developed to a co-worker who is working at another office. If this email is sent without encryption, then everyone along the way can read about the developing product. It could be, that someone will be able to bring this product to market faster with the information provided by the email. Are you ready to take that risk?

Enigmail enables for the default setting to be set at "encrypt + sign" if possible. Also if you are using Linux or UNIX, you can set the file permissions of the configuration files so only the system administrator can edit them. This does not provide total security, but will elevate security to prevent the "normal" user from changing the configuration files in their home directory.

If I have made you contemplate your computer security I have done my job. Now it is time to get on with the show and start using the tools that are available to us.

5 Using GnuPG

The first thing a user should do is generate a key pair. Following the generation of a key pair, the user might grab some keys from the keyserver of his choice in order to communicate with his friends.

For quick help type: `gpg --help`

5.1 Generating a Key Pair

GnuPG uses keys that are divided in half. The first portion of the key pair is the public key. This portion of the key pair can be put on your web site, sent to a key server, and allow everyone to see it. This will enable anyone to use your public key to send you a private encrypted message. Only the holder of the secret key that corresponds to the public key can decrypt the message, provided they know the pass phrase. The second portion of the key pair is the secret key. The secret key **should not** be available to the world. This is your private property and needs to be safeguarded like a key to a safe deposit box in a bank.


```
gpg --gen-key
```

The above command generates a key pair interactively asking you all kinds of questions like the type of key and etcetera as is shown below.

```
~$ gpg --gen-key
gpg (GnuPG) 1.2.0; Copyright (C) 2002 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.

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 keypair will have 1024 bits.
About to generate a new ELG-E keypair.
              minimum keysize is  768 bits
```

```
             default keysize is 1024 bits
    highest suggested keysize is 2048 bits
What keysize do you want? (1024) 2048
Requested keysize is 2048 bits
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)
Key does not expire at all
Is this correct (y/n)? y
```

5.2 Exporting Your Public Key

After you have generated your key pair then you need to export your public key with the command:

```
gpg --export -a > ~/.gnupg/my-key.asc
```

This will create an ASCII armored public key that can be copied to your web site, sent to your co-workers for them to sign and import into their public key ring. In your .gnupg/ directory, there is a file called “pubring.gpg” that contains your public key along with those of your friends, co-workers, and acquaintances. There is also a secring.gpg that contains your secret keys.

These key rings are like the key ring that is in your pocket. You want to make sure that you don’t lose them, so a good back up is vital.

5.3 Importing a Public Key

When someone sends you their public key in an email or you download the key from their web site then you can import the key to your public key ring.

```
gpg --import filename
```

The “filename” argument is whatever name you saved the key. I like to use the format “name.gpg.asc” for the file names of the ASCII armored keys that I am importing to my public key ring. After the key is imported there is no need to keep the key on your hard drive.

If someone emails you a key and you are using Enigmail, then you can click on the menu Enigmail and select Import public key item. This will automatically import the key to your public key ring.

5.4 Checking Your Key Ring

To see what keys are on your key ring type:

```
gpg --list-keys
```

If there are keys on your key ring that have a photo signature, you can run the command and not only see the keys on your key ring, but also the photographs of some of the individuals on your key ring.

```
gpg --show-photo --list-key
```

If you want to see the fingerprint of one or all of the keys on your key ring then type:

```
gpg --fingerprint leroy@lrcressy.com
pub  1024D/8501AFEA 2003-01-03 LeRoy D. Cressy (ldc)
    <ldc@lrcressy.com>
Key fingerprint = 62DE 6CAB CEE1 B1B3 359A  81D8 3FEF E6DA 8501 AFEA
uid                  LeRoy D. Cressy (ldc) <leroy@lrcressy.com>
uid                  LeRoy d. Cressy (ldc) <ldc@lrcressy.com>
sub  2048g/B16A47D6 2003-01-03
```

5.5 Editing a Key

Let’s say I want to edit my key.

```
gpg --edit-key 8501AFEA
gpg (GnuPG) 1.2.0; Copyright (C) 2002 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.

Secret key is available.

gpg: checking the trustdb
gpg: checking at depth 0 signed=12 ot(-/q/n/m/f/u)=0/0/0/0/0/2
gpg: checking at depth 1 signed=22 ot(-/q/n/m/f/u)=10/0/0/0/2/0
gpg: checking at depth 2 signed=0 ot(-/q/n/m/f/u)=16/0/0/0/1/0
gpg: next trustdb check due at 2004-02-21
pub  1024D/8501AFEA  created: 2003-01-03 expires: never      trust: u/u
sub  2048g/B16A47D6  created: 2003-01-03 expires: never
(1)  LeRoy D. Cressy (ldc) <leroy@lrcressy.com>
(2). LeRoy D. Cressy (ldc) <ldc@lrcressy.com>
(3)  LeRoy d. Cressy (ldc) <ldc@lrcressy.com>

Command> ?
quit       quit this menu
save       save and quit
help       show this help
fpr        show fingerprint
list       list key and user IDs
uid        select user ID N
key        select secondary key N
check      list signatures
sign       sign the key
lsign      sign the key locally
nrsign     sign the key non-revocably
nrlsign    sign the key locally and non-revocably
adduid     add a user ID
addphoto   add a photo ID
deluid     delete user ID
addkey     add a secondary key
delkey     delete a secondary key
addrevoker add a revocation key
delsig     delete signatures
expire     change the expire date
primary    flag user ID as primary
toggle     toggle between secret and public key listing
pref       list preferences (expert)
showpref   list preferences (verbose)
setpref    set preference list
updpref    updated preferences
passwd     change the passphrase
trust      change the ownertrust
revsig     revoke signatures
```

```
revkey     revoke a secondary key
disable    disable a key
enable     enable a key
showphoto  show photo ID

Command> q
```

When you enter the command `gpg --edit-key` gpg first checks to see if a secret key is available and then checks the levels of trust. At the prompt `Command>` entering a '?' will produce a list of all the commands that are available. Entering 'q' will quit. Now you can edit any key that is on your key ring. If someone has requested that you sign their key, then you need to use this command to sign the key. For details you need to read the GnuPG manual.

5.6 Keyservers

Keyservers allow you to post and receive public keys. All of the keyservers sync with each other daily so you only need to work with one. My favorite is "pgp.mit.edu." For a list of keyservers and their status, see http://pgp.uni-mainz.de/bigbrother/.

When you find a keyserver that you like, edit `~/.gnupg/options` file with `keyserver pgp.mit.edu` or whatever keyserver you are going to use as your default.

5.6.1 Finding a Public Key on a Keyserver

There are several methods to use a keyserver. The easiest is if the keyserver is a "http" keyserver where they have a nice interface for searching keys. The method I use is
`gpg --keyserver pgp.mit.edu --search-keys ldc@lrcressy.com`
which produces the following:

```
gpg: searching for "ldc@lrcressy.com" from HKP server pgp.mit.edu
Keys 1-3 of 3 for "ldc@lrcressy.com"
(1)     LeRoy D. Cressy (ldc) <leroy@lrcressy.com>
          1024 bit DSA key 8501AFEA, created 2003-01-03
(2)     LeRoy D. Cressy (ldc) <ldc@lrcressy.com>
          1024 bit DSA key 8501AFEA, created 2003-01-03
(3)     LeRoy d. Cressy (ldc) <ldc@lrcressy.com>
          1024 bit DSA key 8501AFEA, created 2003-01-03
Enter number(s), N)ext, or Q)uit >
```

You will notice that there are three responses for my search. All three are actually the same key with different self signatures. GnuPG prompts you to enter a number, N)ext, or Q)uit. Entering the number '1' produced:

```
gpg: key 8501AFEA: "LeRoy D. Cressy (ldc) <ldc@lrcressy.com>"
not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
```

Let's say you just enter your last name like "Cressy."

```
gpg --keyserver pgp.mit.edu --search-keys Cressy
gpg: searching for "Cressy" from HKP server pgp.mit.edu
Keys 1-6 of 6 for "Cressy"
(1)     Sibylla Cressy (Billie) <scressy@comcast.net>
          1024 bit DSA key AAA49F65, created 2003-07-07
(2)     LeRoy D. Cressy (ldc) <leroy@lrcressy.com>
          1024 bit DSA key 8501AFEA, created 2003-01-03
(3)     LeRoy D. Cressy (ldc) <ldc@lrcressy.com>
          1024 bit DSA key 8501AFEA, created 2003-01-03
(4)     LeRoy d. Cressy (ldc) <ldc@lrcressy.com>
          1024 bit DSA key 8501AFEA, created 2003-01-03
(5)     Rita J. Cressy (rita) <rita@lrcressy.com>
          1024 bit DSA key BCDCEEF1, created 2002-12-30
(6)     Colin J. Cressy <Colin.Cressy@jcu.edu.au>
          1024 bit DSA key B60E5883, created 1998-05-04
Enter number(s), N)ext, or Q)uit > 6
gpg: key B60E5883: public key
"Colin J. Cressy <Colin.Cressy@jcu.edu.au>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

You see that there are six responses. The number that I enter will be imported to my public key ring if it is not already there.

If you specified a keyserver in the configuration file, then you do not need to specify the keyserver on the command line.

5.6.2 Receiving a Public from a Keyserver

The output from the above section specified a key ID number like **AAA49F65**. To receive a key from the keyserver, we need the key ID number. To receive a key from a keyserver, we need to type:

```
gpg --recv-key AAA49F65
gpg: key AAA49F65: "Sibylla Cressy (Billie)
<scressy@comcast.net>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
```

Since the key was already on my key ring, there were no changes made; but if the key wasn't on my key ring, it would have been added.

5.6.3 Sending Your Public Key to a Keyserver

Sending your key to the keyserver is just as easy.

```
gpg --send-key leroy@lrcressy.com
gpg: success sending to 'pgp.mit.edu' (status=200)
```

Every time someone signs your key, the web of trust becomes larger. Thus the more people that have signed your key, the greater the trust level. So the key grows in size with every signature.

5.7 Signing Keys

Now you may not think that it is very important to sign keys and have others sign your key. Where key signing is important comes in when you do not personally know someone you wish to correspond with, but you have a couple of friends who know the individual. They have both signed his key, thus you can be reasonably sure that the individual that you wish to correspond with is who he says he is.

This is called building up a web of trust. The more people who sign your key, the more you are trusted by others who do not know you. Also when you sign your friends' keys, you are helping them build up a web of trust.

5.7.1 Method of Key Signing

1. Print Your Fingerprint

   There is an excellent package that helps in exchanging fingerprints called signing-party which has the utility gpg-key2ps.

```
# Get Your Key-ID
gpg --fingerprint "Your Name"
# Print A nice sheet of tags with your fingerprint
gpg-key2ps -p letter key-ID | lpr
```

2. Verification

   The first step in signing keys is to verify that the person whose key you are going to sign is who they say they are. To do this requires verifying the photo ID issued by the state, or checking the passport and making sure that the picture matches the person whose key you are signing.

3. Exchange Fingerprint Tags

4. Email Your Public Key

   ```
   gpg --export -a Key-ID > filename.gpg.asc
   ```

   Email filename.gpg.asc as an attachment to the person that you are signing keys with.

5. Exchange a Secret Message

   This verifies that the person that you have the fingerprint of is really the one who can decrypt your message. Conversely, they should be doing the same thing.

6. Edit the Key You Are Signing

   When the person that you are exchanging keys with sends you their key, import their key to your key ring.

   ```
   gpg --import filename.gpg.asc

   gpg --edit-key scressy@comcast.net
   gpg (GnuPG) 1.2.0; Copyright (C) 2002 Free Software Foundation,
   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.


   pub  1024D/AAA49F65  created: 2003-07-07 expires: never
        trust: -/f
   sub  2048g/CAB78B8E  created: 2003-07-07 expires: never
   (1). Sibylla Cressy (Billie) <scressy@comcast.net>

   Command>sign
   ```

7. Export the Signed Key

```
gpg --export -a AAA49F65 > scressy.gpg.asc
```

8. Email the Signed Key as an Attachment

NOTE:

All the communication between the key signing parties should be signed and encrypted email. This will ensure that you are dealing with the right person, for they are the only ones who can read your messages.

5.8 Generate a Revocation Certificate

The next thing you want to do is generate a revocation certificate. This certificate should not be stored on the hard drive of your computer since you don't need a pass phrase to use it.

```
gpg --output revoke.asc --gen-revoke mykey
```

> The argument mykey must be a key specifier, either the key ID of your primary keypair or any part of a user ID that identifies your keypair. The generated certificate will be left in the file revoke.asc. If the –output option is omitted, the result will be placed on standard output. Since the certificate is short, you may wish to print a hardcopy of the certificate to store somewhere safe such as your safe deposit box. The certificate should not be stored where others can access it since anybody can publish the revocation certificate and render the corresponding public key useless.[1]

6 Configuring Mozilla Mail

Mozilla enables you to have several pop email accounts. Each one has its own configuration parameters. We will first take you through the process of setting up a new account.

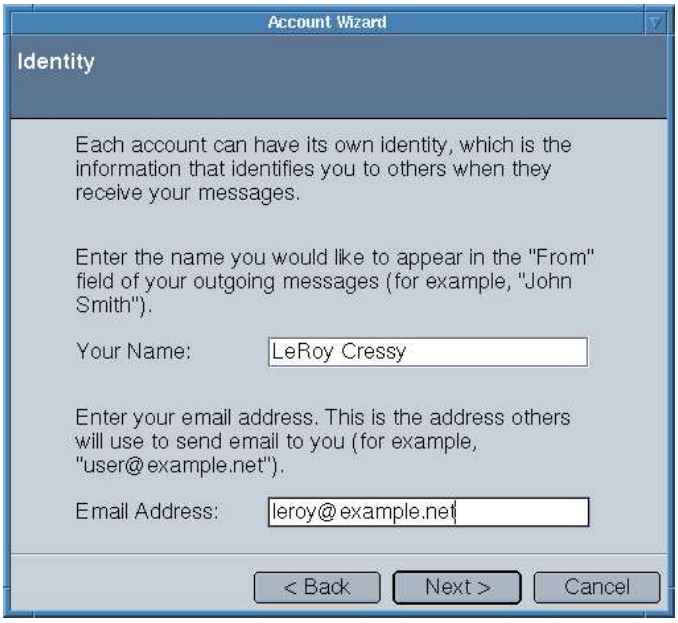
[1] http://www.gnupg.org/gph/en/manual/c14.html, The GnuPG Manual

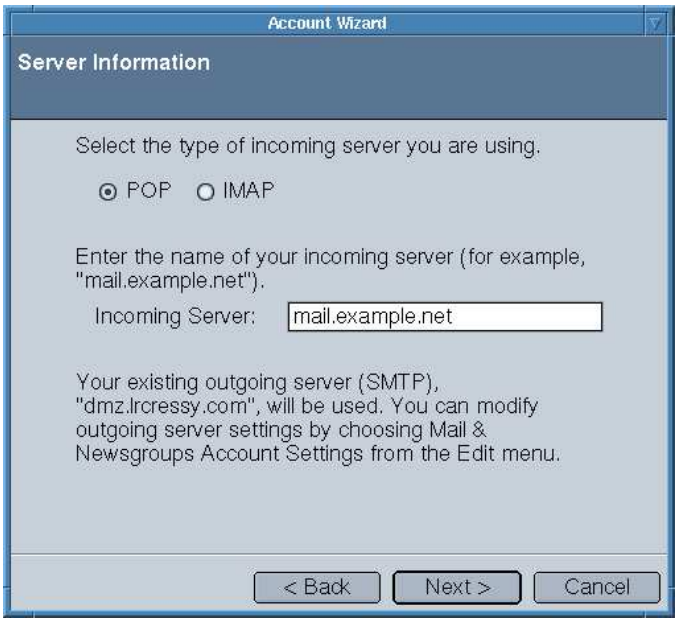
6.1 Creating a New Mail Account

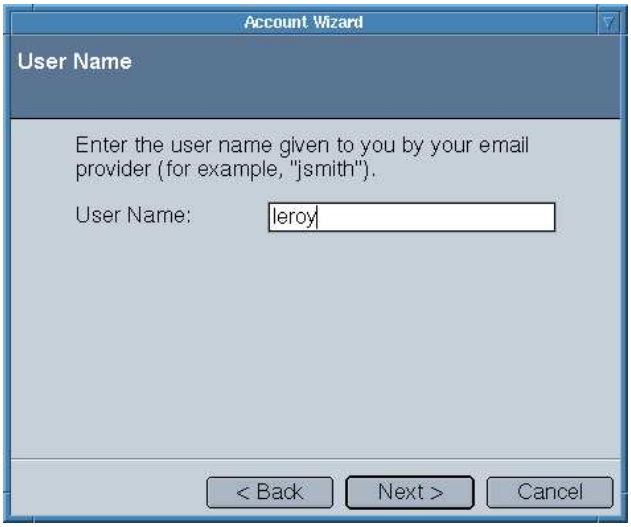
The first step is to click on the top user mail entry of the Mozilla mail client.

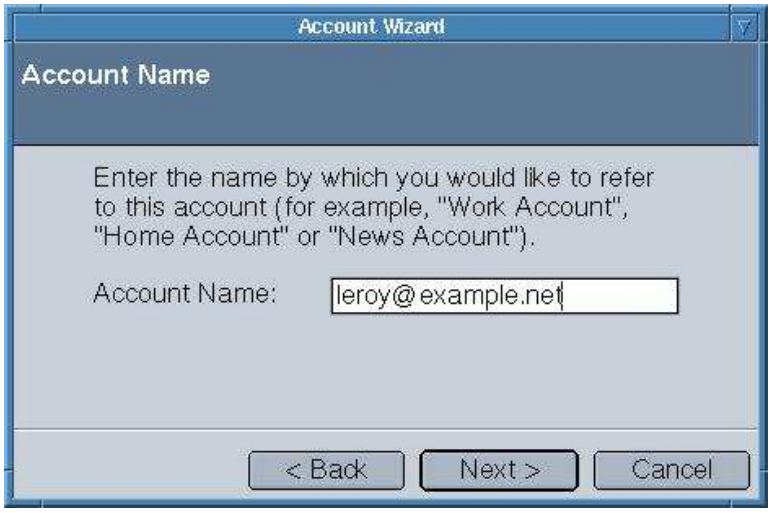
Since we are creating a new account, we will click on Create New Account which opens up the mail account creation wizard.

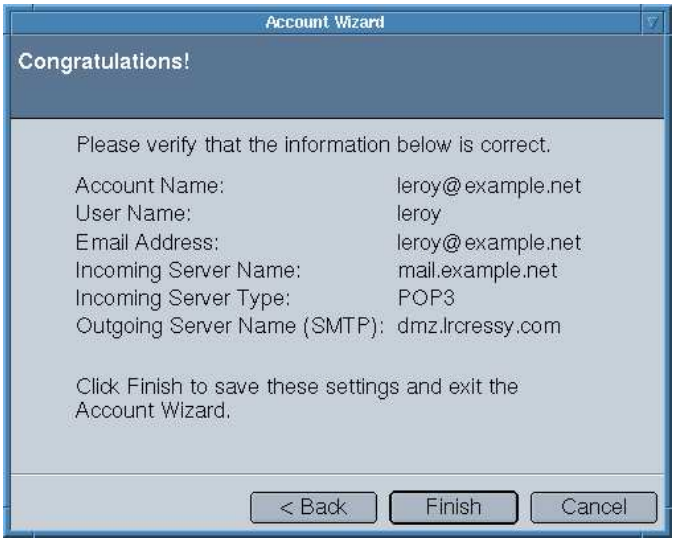
Since this is a new mail account, we will click on email account.







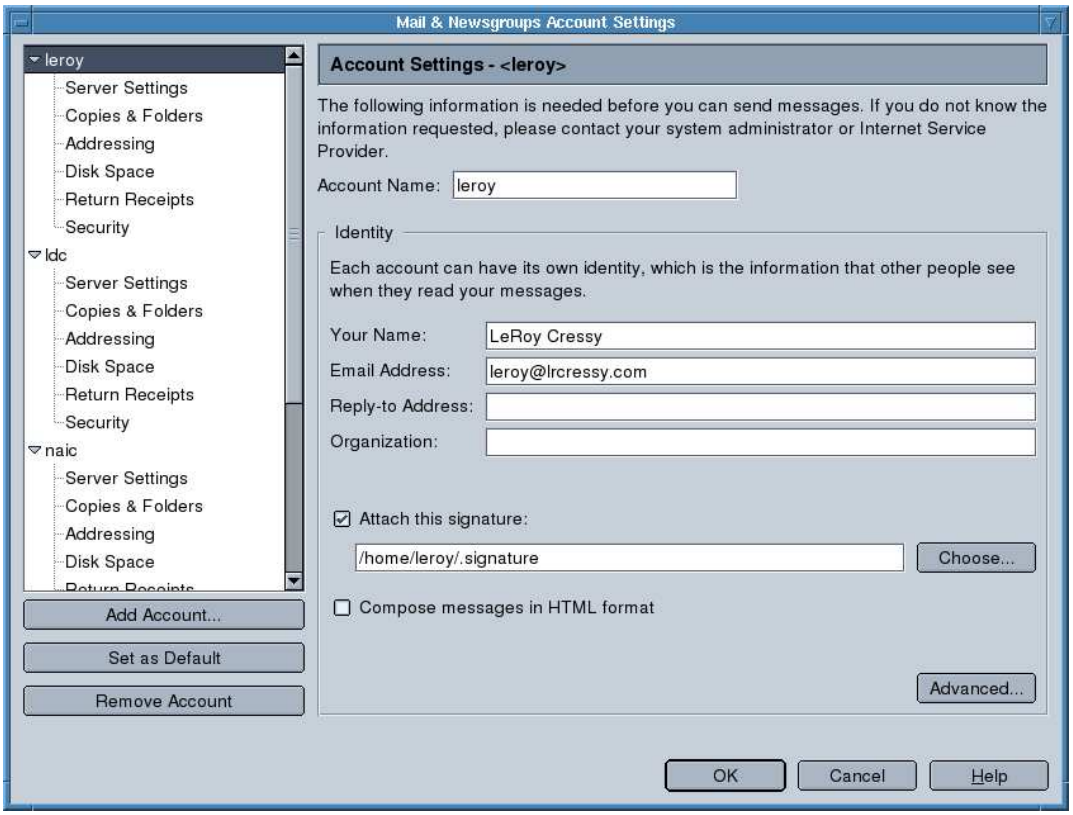




As you can see, the account wizard has most of the help right on each screen. It is mostly self explanatory.

NOTE:

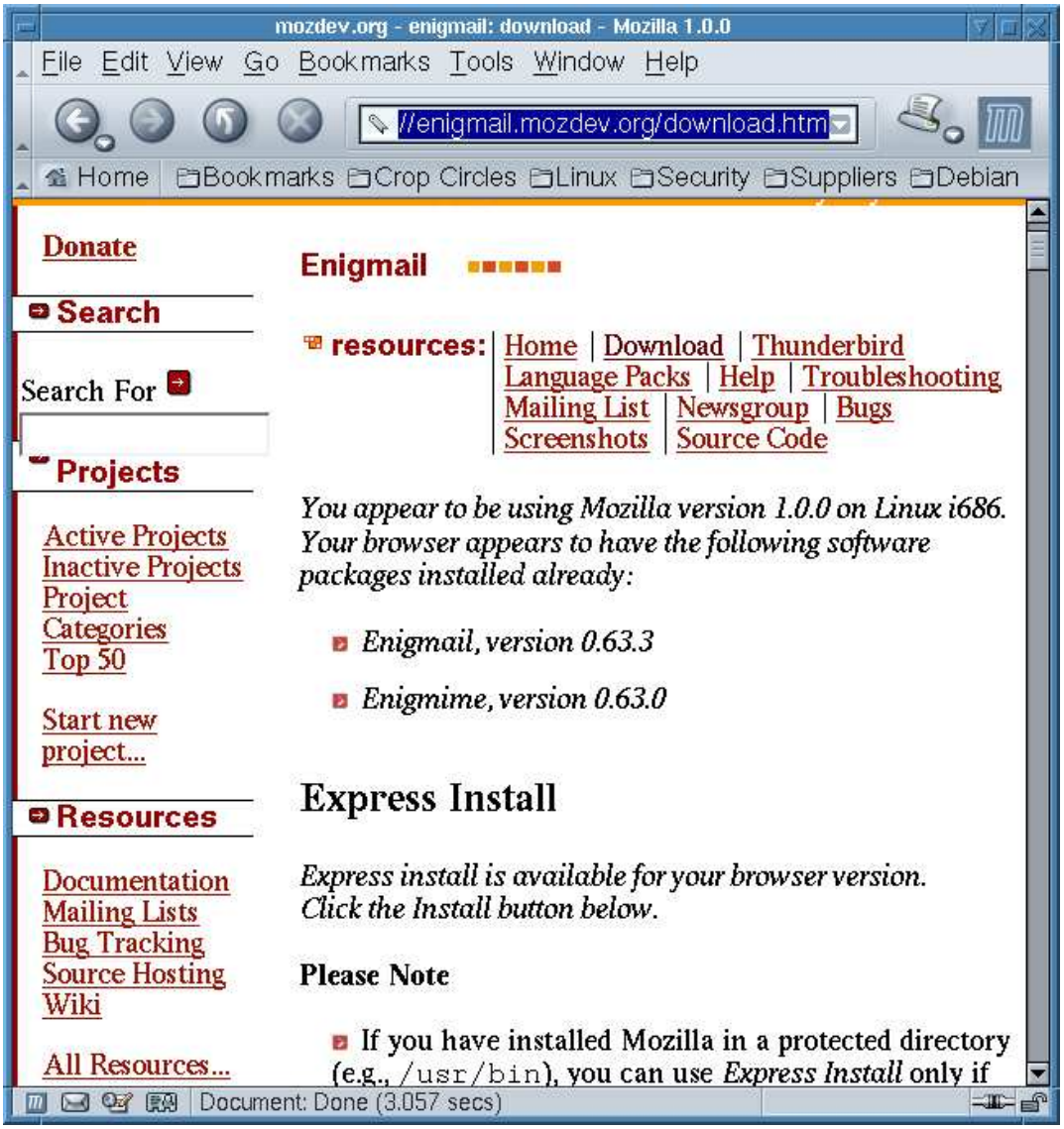
You need to make sure that your account settings do not compose email in html format. Right click your mouse on the email or news account and select Properties. The account settings window will pop up.



If the ☐ Compose messages in HTML format is checked, you will not be able to sign outgoing mail with Enigmail.

7 Getting and Installing Enigmail

The first thing to installing Enigmail is to download the version that matches your browser. To find out exactly what version of Mozilla or Netscape you are using, click on the help menu and choose “About Mozilla” or “About Netscape.” Enigmail supports Netscape 7 and Mozilla. The web site http://enigmail.mozdev.org/download.html is where you will find the download page for enigmail.



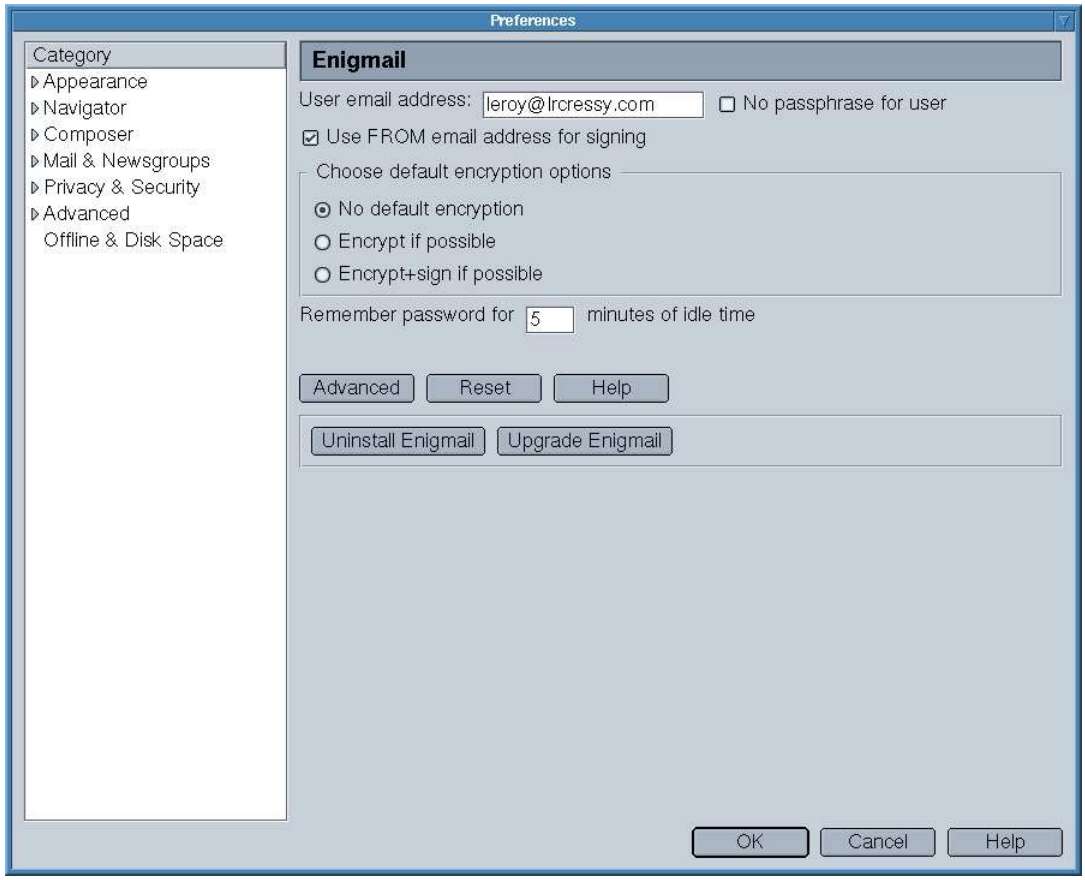
CAUTION

You must read the entire download page to determine the correct version for your browser. Also, you need to ensure that you have root privileges along with /usr mounted as rw.

8 Configuring and Testing Enigmail

8.1 Preferences

After you have Enigmail installed on your system in the mail + newsgroups window, you will see a new menu item Enigmail. Clicking on preferences of the enigmail menu produces:



There is a little check box next to the user email address that says, "No passphrase for user." Checking this box is not safe and can lead to security troubles. Let's say you walk away from your computer without logging out or setting the lock screen password. You are only going to the coffee machine to get a quick cup of go juice. A co-worker comes around and uses your computer to send some email, and it is signed with your signature. This can have drastic consequences for you if the co-worker was intending some damage.

So making you type in the pass phrase for each message that you send may seem like an onerous task, but the consequences of making it easy for yourself can be disastrous.

8.1.1 Default Encryption Options

There are three default encryption options:

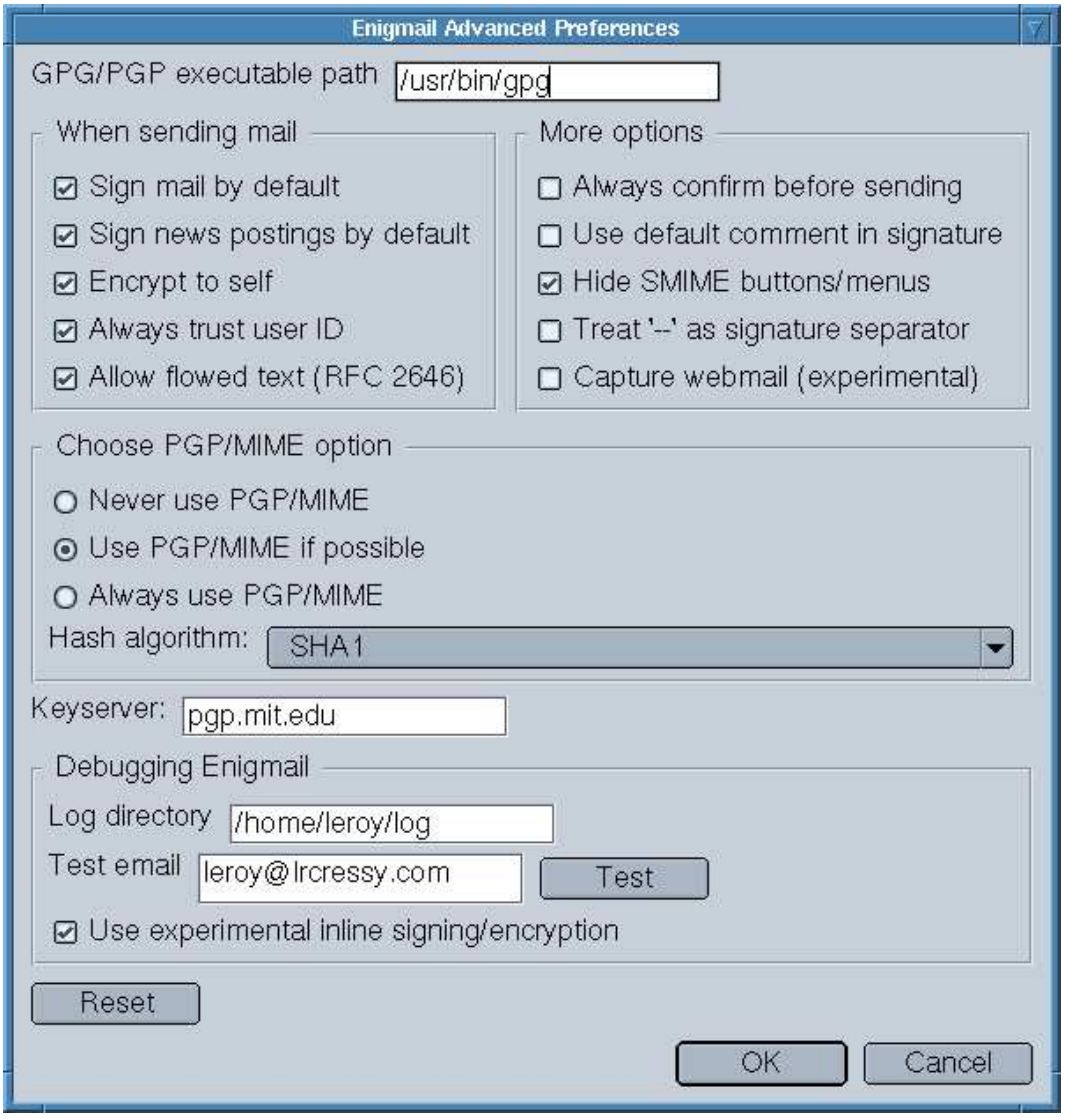
- No default encryption

- Encrypt if possible
- Encrypt + sign if possible

The choice that you make depends on the level of security level that you want to achieve. Careful consideration should be made before changing the default settings. With the new key selection window enabled, possibly the most secure method would be Encrypt + sign if possible. How about if the recipient is away on vacation and not receiving email where their secret key is available? Thus for me it is best to leave the default as No default encryption.

8.2 Advanced Preferences

Clicking on the Advanced gives you the details of your enigmail configuration.



Careful consideration should be taken when changing any of the default settings.

8.2.1 When Sending Mail

□ **Sign mail by default** This is a good setting where all of the mail that you send will be signed with your signature assuring the recipients that you're the sender. Also, the recipient does not need to have their secret key to view the message.

□ **Sign news postings by default** The same advice holds true as for signing mail.

□ **Encrypt to self** This is a good choice if you are sending a message to yourself, causing the message to be encrypted by default. Why would you want to encrypt a message to yourself? Let's say you have a password file that contains all of the various passwords for all of the accounts you have on line. These may include the New York Times, Wall Street Journal, Credit Card accounts, Stock broker, and Various suppliers. Now I know that maintaining a password file is stupid, and against all advice about computer security, but many people have such files in a plain text or some word processor format. Thus sending this file to yourself encrypted would provide a reasonable level of safety.

□ **Always trust user ID** By default, Enigmail enables the –always-trust option for GPG to allow outgoing mail to be encrypted to any key, even untrusted ones. If you would like to encrypt only to trusted keys, you should disable this option in the Advanced Preferences. (This setting does not affect signature verification on received messages: you will always be warned if the signing key is untrusted.)

On my system I stick with the default, but in a corporate environment the security policy might be to turn this option off. Depending on the level of security that you want to achieve, you might want to turn the default option off.

□ **Allow flowed text (RFC 2646)** If you are sending ASCII Art and the image gets messed up, you might want to turn this option off. For normal operations, it is safe to leave this option on.

8.2.2 More Options

□ **Always confirm before sending** This option is off by default, and turning it on will normally cause fatigue and frustration to the end user. Most people will just click the OK button without rereading what they are sending. So it is wise that the default setting should be left alone.

□ **Use default comment in signature** I have not been able to verify this, but I think this adds the gpg comment to the gpg signature.

□ **Hide SMIME buttons/menus** The default is to turn this feature off, but you may choose to have the mime buttons and menus available.

- **Treat '- -' as signature separator** Causes the "- -" separator of mail signatures (not to be confused with PGP signatures) to be treated in a way that when replying, the sender's signature is cut.

- **Capture webmail experimental** If you use an isp that uses web mail, then you might want to try this. I run my own server, thus I don't have this feature on my system.

8.2.3 Choose PGP/MIME Option

- **Never Use PGP/MIME** This causes all attachments, encryption, and signatures to be inline.

- **Allow to use PGP/MIME if possible** This is the default setting where if the end user is using mutt or enigmail, the mail will work. Whenever you send a message with attachments, there will be a warning asking if you are sure that the recipient is capable of receiving PGP/MIME messages with PGP attachments.

- **Always use PGP/MIME** This will cause all messages to be sent as MIME attachments, even if the recipient's system cannot use PGP/MIME.

8.2.4 Keyserver

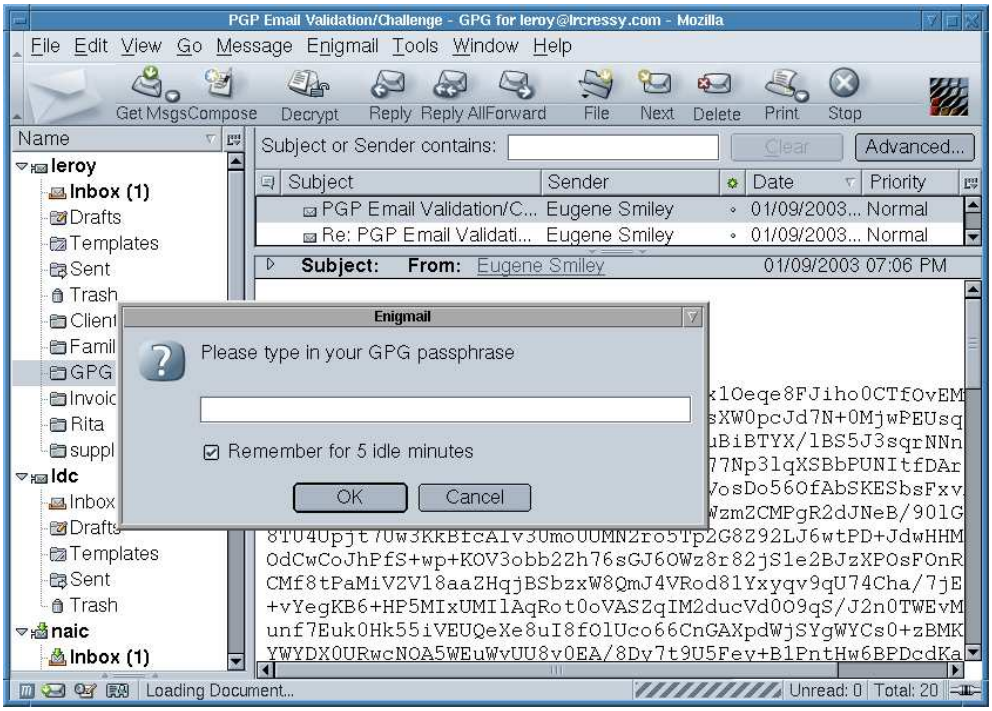
Here you specify a keyserver. The default keyserver www.keyserver.net has never worked for me, so I use pgp.mit.edu which has always worked.

9 Using Mozilla Mail with Enigmail

Finally after all of the installation and configuration, now we are all set to seamlessly use Enigmail, Mozilla, and GnuPG.

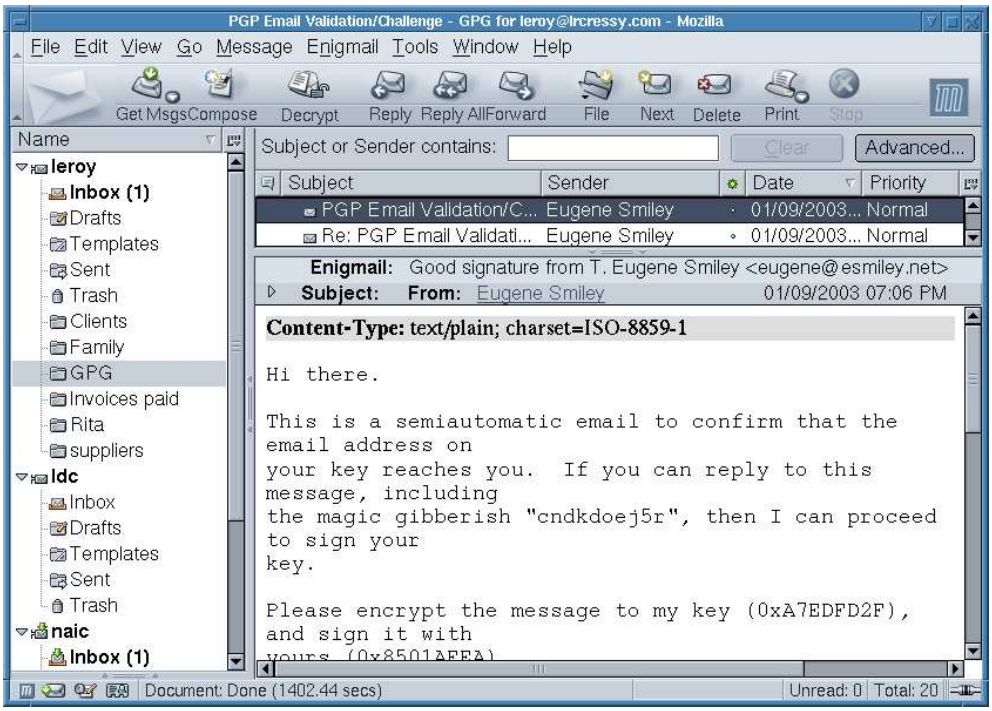
9.1 Receiving Mail

Reading email that has been sent to you encrypted is just as easy as reading other email. All you have to do is enter your pass phrase in the message box as shown.

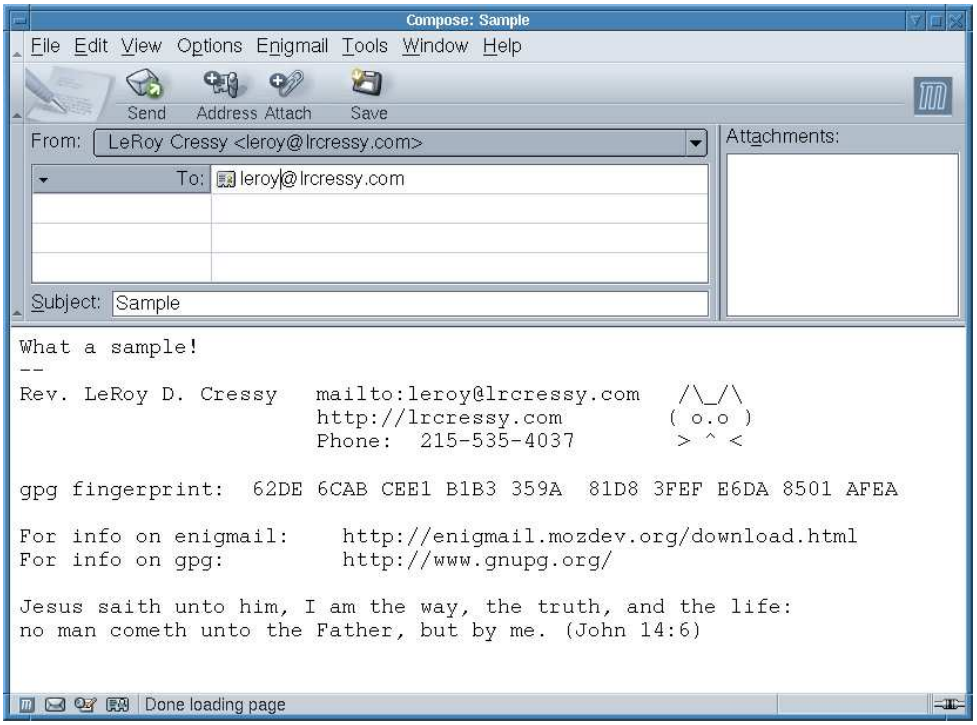


As you can see, the text is totally unintelligible to you until you enter in your pass phrase and click the OK button.

Then the message appears so you can read it.



9.2 Composing Mail



Composing an email message in Mozilla is very easy. The only thing is you now have a choice on how you want to send it.

- Signed send
- Encrypted send
- Encrypted + signed send
- Plain text send

Clicking on the Enigmail menu button gives you the options on how you want to send this message. If you click on the send icon, then whatever the default that was set during the configuration process will indicate how the message is sent. For instance if you have the default set at signed send, then a message box will pop up asking for your pass phrase. If you type the wrong pass phrase, an error box will pop up saying that the message was not sent. If you have a little box checked □ Save pass phrase for 5 minutes then the wrong pass phrase is in Mozilla's memory. In this case you need to click on the Enigmail and click on Clear saved passphrase

9.3 Decrypting and Verifying Signatures

By default, Enigmail will decrypt a file asking you for your pass phrase, but every now and then you may need to click on the Decrypt button to accomplish this.

9.4 Saving Decrypted Mail

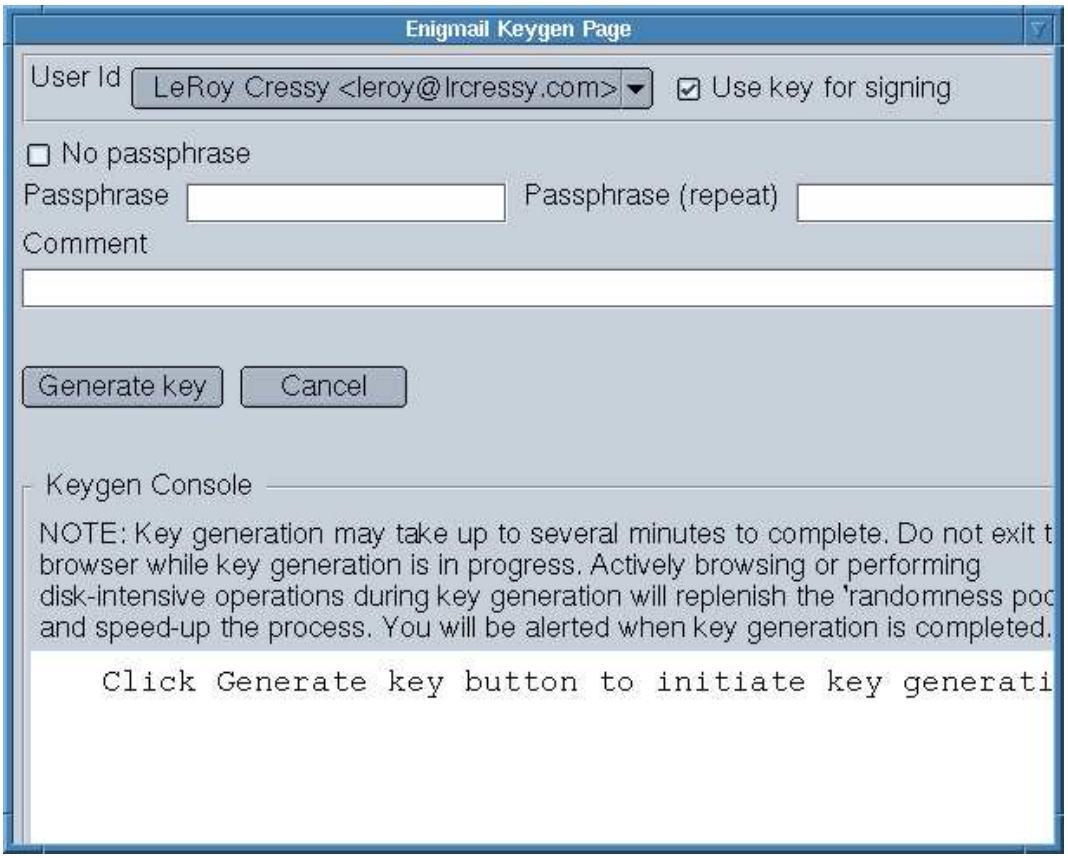
The Enigmail has an option to save a decrypted mail message to a plain text file. You have a choice to either save the message as plain text, or you can save the message as it came and decrypt it every time you want to see it.

9.5 Importing a Public Key

If someone sends you their public key, then you can click on the Enigmail menu button and select Import Public Key and the imported public key will be added to your key ring.

9.6 Generate Key

You can even use Enigmail as a front end to GnuPG to generate a key pair. I have never used this function, so this is a first for me.



I noticed that using the Enigmail front end for generating keys will only generate a 1024 bit key and not prompt you for the key size like GnuPG or PGP does. For most cases this is secure enough, but if you want better security then use gpg –gen-key and follow all of the prompts.

10 Conclusion

When I first switched from Netscape Communicator to the free Mozilla browser, I had a hard time in figuring out how to configure the mail client. This was several years ago when there was not a lot of documentation for Mozilla. Now I have several email accounts on various servers, the main one being mostly on lrcressy.com which I control myself.

When Enigmail came out, I almost stopped using mutt except when I am logged in through ssh. I have found using Mozilla to be very beneficial and rewarding.

11 GNU Free Documentation License

Version 1.2, November 2002

PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

11.1 APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you

copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming

simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

11.2 VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 11.3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

11.3 COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

11.4 MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 11.2 and 11.3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

1. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

2. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

3. State on the Title page the name of the publisher of the Modified Version, as the publisher.

4. Preserve all the copyright notices of the Document.

5. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

6. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

7. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

8. Include an unaltered copy of this License.

9. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

10. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

11. For any section Entitled “Acknowledgements” or “Dedications”, Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

12. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

13. Delete any section Entitled “Endorsements”. Such a section may not be included in the Modified Version.

14. Do not retitle any existing section to be Entitled “Endorsements” or to conflict in title with any Invariant Section.

15. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section Entitled “Endorsements”, provided it contains nothing but endorsements of your Modified Version by various parties–for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

11.5 COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 11.4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

11.6 COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

11.7 AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright

resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 11.3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

11.8 TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 11.4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 11.4) to Preserve its Title (section 11.1) will typically require changing the actual title.

11.9 TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

11.10 FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright © YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.