Secure your email communication with free software

A guide for installing, configuring and using Mozilla Thunderbird, Enigmail, and GnuPG to provide secure and encrypted email

Jerome Gotangco

Email is one of the most common activities we perform on the internet. However, email is also one of the most vulnerable internet services currently used. Email spam is common, but what most people are not aware of is that email identity theft is common as well. There is also continuous concern over the privacy and security issues surrounding the matter. However, most users dismiss security software as complex and still continue to send email messages with very little or no regard at all to security.

> The larger the key, the longer time it will take for a cracker to decipher your encrypted message

In this article, you'll learn how to install, setup, and use the Mozilla Thunderbird email client for secure, encrypted email using GnuPG and the Enigmail Mozilla Thunderbird extension. The examples in this article are based on Ubuntu 5.10, but any GNU/Linux-based operating system can be used. You'll also get to tackle the basics of using GnuPG with Enigmail—just enough to get you started, as GnuPG is a very powerful suite that can extend to other applications. If you'd like to learn more about cryptography using GnuPG, the man pages are a good place to start. Don't worry though, GnuPG is very well documented and you'll be presented with some links online at the end of this article to get you started.

If you're still using Microsoft Windows, you can still apply the steps presented, but you'll have to download and configure the Win32 counterparts of the software used.

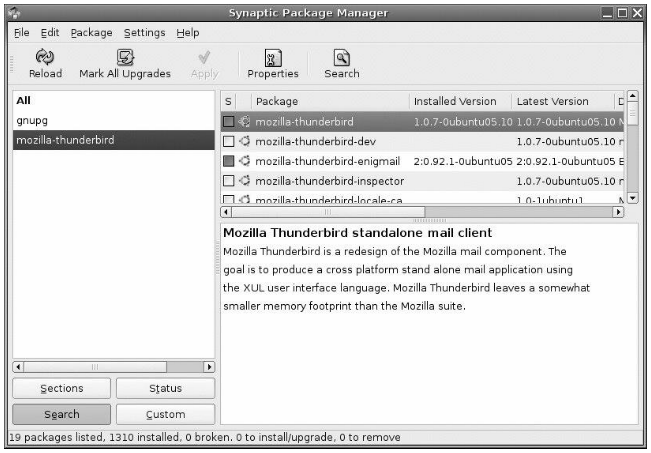
Installing the essential applications

Assuming you're already running Ubuntu 5.10, you need to install three software packages to be able to start sending secure email. These are:

- Mozilla Thunderbird (`http://www.mozilla.com/thunderbird/`)—a free software, full-featured and secure email client from the Mozilla project. It is currently available for GNU/Linux, Windows and MacOSX
- Enigmail (`http://enigmail.mozdev.org/`)—Enigmail is an extension to the mail client of Mozilla Thunderbird which allows users to access the authentication and encryption features provided by GnuPG.
- GnuPG (`http://www.gnupg.org/`)—GnuPG is a complete and free replacement for the PGP (Pretty Good Privacy) suite of cryptographic software; and it's released under the GNU General Public License.

You'll also need an email account that has POP3, SMTP and/or IMAP support. Your Internet Service Provider (ISP) may have provided you one. If you are using a free email account, check your email provider if it has support for such. Gmail (`http://gmail.google.com/`) provides free

Figure 1: The Synaptic Package Manager



S	Package	Installed Version	Latest Version	D
■	mozilla-thunderbird	1.0.7-0ubuntu05.10	1.0.7-0ubuntu05.10	N
□	mozilla-thunderbird-dev		1.0.7-0ubuntu05.10	r
■	mozilla-thunderbird-enigmail	2:0.92.1-0ubuntu05	2:0.92.1-0ubuntu05	E
□	mozilla-thunderbird-inspector		1.0.7-0ubuntu05.10	r
□	mozilla-thunderbird-locale-ca		1.0-1ubuntu1	N

Mozilla Thunderbird standalone mail client

Mozilla Thunderbird is a redesign of the Mozilla mail component. The goal is to produce a cross platform stand alone mail application using the XUL user interface language. Mozilla Thunderbird leaves a somewhat smaller memory footprint than the Mozilla suite.

19 packages listed, 1310 installed, 0 broken. 0 to install/upgrade, 0 to remove

POP3 and SMTP support, so you can make an account (if you haven't already) and use it for this exercise.

Ubuntu officially supports these packages and they can easily be installed from the network. You can use the Synaptic package manager to install them. From your GNOME desktop just click on System → Administration → Synaptic Package Manager. Once selected, you'll be asked for your sudo user password (in Ubuntu, this is normally the first user you create during setup if you did a default install) and then you'll be presented with the Synaptic Package Manager as shown in figure 1.

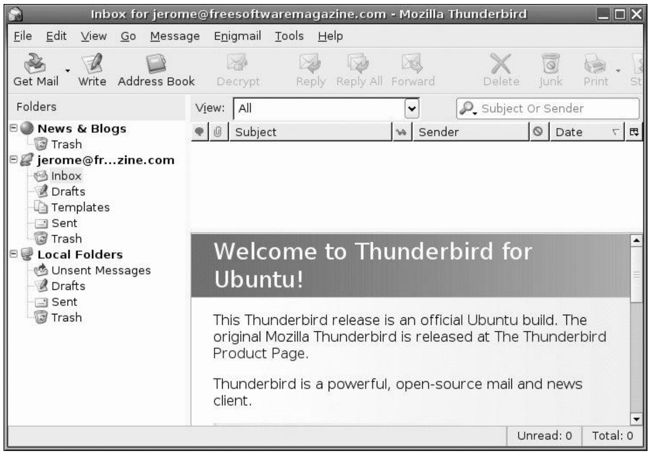
In Synaptic, click on "Search" and look for the following packages: `mozilla-thunderbird`, `mozilla-thunderbird-enigmail` and `gnupg`. The package `gnupg` was most likely installed already during your initial setup of Ubuntu, so you can skip this; but in case it wasn't or you've removed it, you'll have to include it.

Once you have selected the three packages, click on "Apply". Synaptic will then check for package dependencies and install them as needed. Once you have the packages installed, you can now close Synaptic.

Setting up your email client

Now that Thunderbird, Enigmail and GnuPG are installed, you can open up Thunderbird and create your first key pair. From your desktop, click on Applications → Internet → Thunderbird Mail Client. This will open up Mozilla Thunderbird. You will be asked to create your email account when you open up Thunderbird for the first time. If you haven't created one, it's a good time to set it up now. Thunderbird provides a wizard to help you setup your email account. For this article, I'm going to use a fictitious email account named `jerome@freesoftwaremagazine.com`. Figure 2 shows how Thunderbird looks after setting up the email account.

Figure 2: The Mozilla Thunderbird email client with Enigmail installed



Welcome to Thunderbird for Ubuntu!

This Thunderbird release is an official Ubuntu build. The original Mozilla Thunderbird is released at The Thunderbird Product Page.

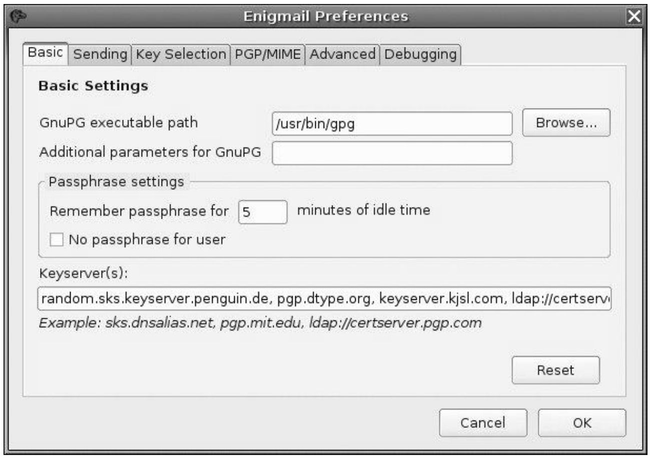
Thunderbird is a powerful, open-source mail and news client.

Setting up Enigmail and creating your Key Pair

Once your email account is ready, you need to generate a new "key pair". A key pair consists of two keys: the public and the private key. This pair (along with the other pairs used by other people worldwide) is essential to make Public Key Infrastructure (PKI) possible. To put it simply, people can send secure, encrypted email to you using your public key but you need your private key to decipher it, and vice-versa. All of this is made possible while using an unsecured public network such as the internet.

If you've used Thunderbird before, you'll notice that after installing the `mozilla-thunderbird-enigmail` package, a new menu entry appeared: "Enigmail". Before creating your first key pair, you need to configure Enigmail to use GnuPG by adding its executable path. Select "Enigmail" and click on "Preferences" and the Enigmail Preferences window will appear (as shown in figure 3).

Figure 3: Adding the GnuPG path in Enigmail preferences



Basic Settings

GnuPG executable path: /usr/bin/gpg

Additional parameters for GnuPG:

Passphrase settings

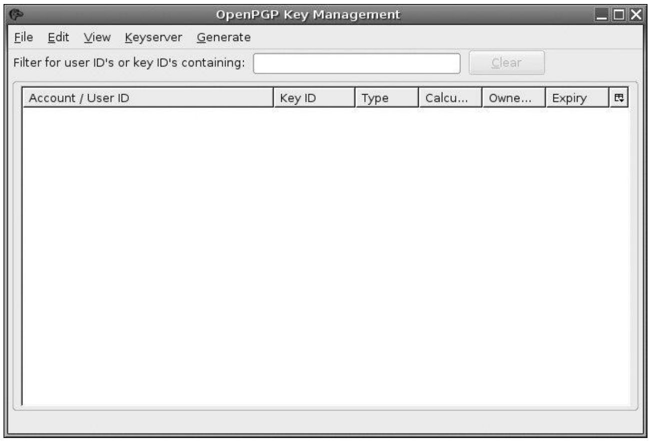
Remember passphrase for 5 minutes of idle time

□ No passphrase for user

Keyserver(s): random.sks.keyserver.penguin.de, pgp.dtype.org, keyserver.kjsl.com, ldap://certserv

Example: sks.dnsalias.net, pgp.mit.edu, ldap://certserver.pgp.com

Figure 4: Empty keyring in OpenPGP Management

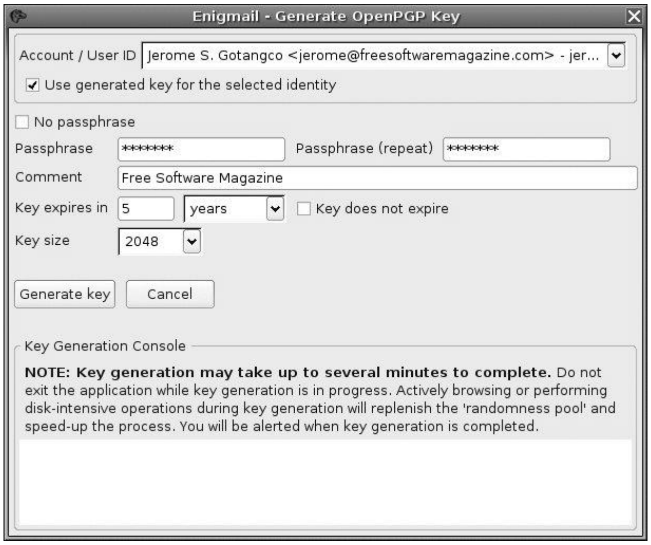


To begin with, just focus on the “Basic” settings to get Enigmail running. First, you’ll need to add the executable path of GnuPG. In Ubuntu, this is located at `/usr/bin/gpg`. So, add that to the “GnuPG executable path” field and click on “Ok”. Other settings such as additional parameters, passphrase settings and keyservers can be left as is for now. You can go back to those settings later when our key pair is done.

After adding the executable path of GnuPG. You’re now ready to create your first key pair. From Thunderbird click on “Enigmail” and select “OpenPG Key Management”. (This is shown in figure 4.)

Notice that you still have an empty keyring here. You’ll get to populate it later after creating your first key pair.

Figure 5: Generating a new key pair



Account / User ID: Jerome S. Gotangco <jerome@freesoftwaremagazine.com> - jer...

☑ Use generated key for the selected identity

□ No passphrase

Passphrase: ******* Passphrase (repeat): *******

Comment: Free Software Magazine

Key expires in: 5 years □ Key does not expire

Key size: 2048

Key Generation Console

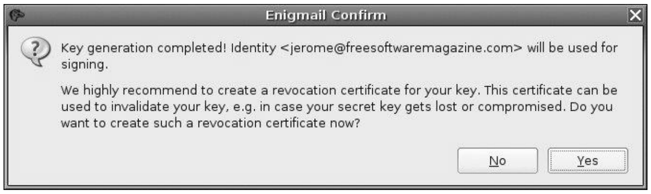
NOTE: Key generation may take up to several minutes to complete. Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.

From this window, click on “Generate”, and select “New Key Pair”. A new window should appear with your default email account for your new key pair already selected. If you have multiple email accounts in Thunderbird, you can select which key to use, or, if you prefer, have your key pair use different email accounts (as shown in figure 5) as additional User IDs (I’ll cover this more later).

> A key pair consists of two keys: the public and the private key. This pair (along with the other pairs used by people worldwide) is essential to make Public Key Infrastructure (PKI) possible

From here, select the email account that you want to create your first key pair for. Selecting “Use generated key for the selected identity” makes this key your default if you have multiple keys installed. Since you’ll be using Enigmail to secure your email, it’s a good idea to assign a passphrase for your key pair. Your passphrase will be used everytime you sign, encrypt and decrypt email. Keep the passphrase to yourself and make sure you don’t forget it. If you need to write it down, make sure you place it in a secure place (don’t even think of putting it in your wallet or purse). Your passphrase is very important since your use of the key depends upon it. You can also opt to disable passphrases but

Figure 6: Dialog box confirming the creation of a new key pair and recommending the creation of a revocation certificate



Key generation completed! Identity <jerome@freesoftwaremagazine.com> will be used for signing.

We highly recommend to create a revocation certificate for your key. This certificate can be used to invalidate your key, e.g. in case your secret key gets lost or compromised. Do you want to create such a revocation certificate now?

this is not a good idea especially if you're going to use your key to send and receive sensitive information.

You can add a comment to your key if you want to. Comments are useful if have multiple keys installed in your machine. Make your comment descriptive enough that people will easily identify you with it. If you don't want to add a comment, you can leave this field blank.

You can also choose if you'd like your key to expire in a given period of time. Enigmail defaults this at 5 years, but you can also choose to increase or decrease the duration or to have a non-expiring key. Key size pertains to the length of the key which can determine how long it takes to encrypt an email message; hence using a 2048 bit key to encrypt a message will take much longer than using a 1024 bit key. The larger the key, the longer time it will take for a cracker to decipher your encrypted message. You are given the choice between 1024, 2048 and 4096 bit keys. Determining the size of key to use depends entirely upon your requirements, but 1024 bits is reasonable enough for everyday use.

Once you have filled up the required fields, it's time to generate your key! Click on "Generate key" to create it!

It'll take a few minutes to generate your key—much longer if you chose a higher key size. Feel free to continue on with your work and let the system run and generate the key from the background. When the key creation is done, you'll be notified about it and asked if you want to create a revocation certificate. A revocation certificate is useful for if the secret key of your key pair gets lost. Just click "Yes" and Enigmail will prompt you to choose a location where you want your revocation certificate to be saved. (This is shown in figure 6.)

You can move this revocation certificate to a USB flash disk along with your private and public key and store it in a secure place in case your machine dies along with your keys. That way, you'll still be able to move to a new machine and just import your existing keys to be used again.

Once this is done, you'll get back to OpenPGP Key Management. But this time around, your key pair is now visible (and highlighted, which means it is your default key pair). But before you use it, it would be a good idea to make a backup of your key pair first and store it along with your revocation certificate which you did a while ago. From the OpenPGP Key Management window, select your default key pair, right-click and choose "Export Keys to File". You'll then be asked if you want to include your secret key.

If you're backing up your key pair for the first time since generating it, you should include your secret key. Click on "Yes" and store it in your computer; then, make sure you back it up in a USB flash disk or backup media that you're familiar with. The secret key is very important and when your only copy gets lost (stolen machine, disk failure, etc.) your key pair becomes useless.

You can export your public key to be sent to a peer or coworker to add to their own keyrings. For this, do not include your secret key when exporting. Your secret key is for your own use and is needed when decrypting secure email. If someone gets hold of your secret key, it is already compromised and you'll have to send the revocation certificate to people in your keyring to let them know that your key can no longer be trusted.

Adding keys of other people

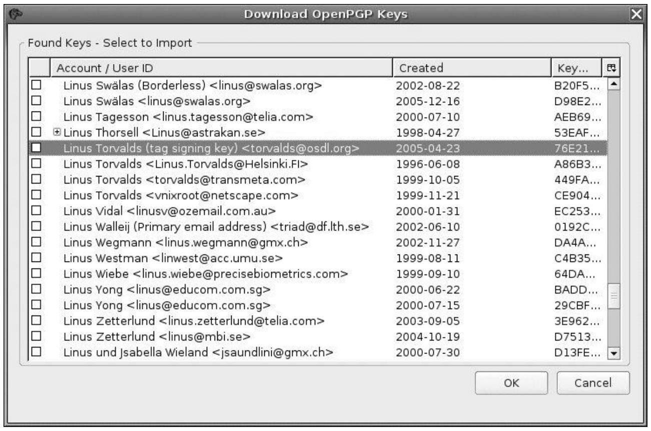
Now that you have generated and backed up your key pair, it's time to add the public keys of other people you want to be in your keyring. For this, you'll have to download their public keys from a public keyserver (or to receive their signed emails), and then add their key to your own key ring.

To be able to send an encrypted email message to someone, first, you need to obtain his public key. A person's public key can be obtained in two ways:

- You have received the public key via email, or have it on file.
- You have searched and downloaded the public key from a keyserver.

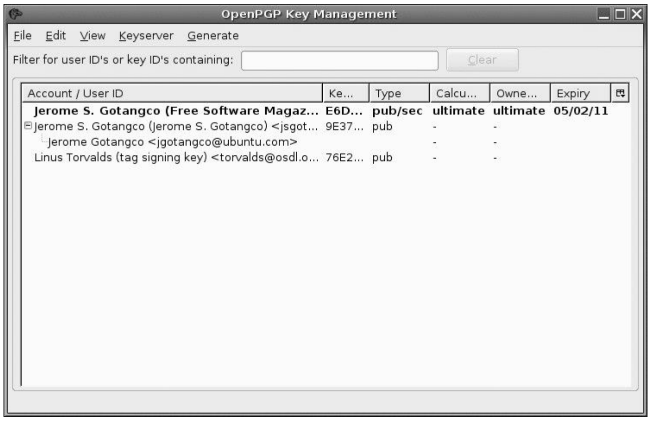
If you have received another person's public key via email or have it on file, you can import the key using OpenPGP

Figure 7: A list of public keys from the search result



	Account / User ID	Created	Key...
□	Linus Swälas (Borderless) <linus@swalas.org>	2002-08-22	B20F5...
□	Linus Swälas <linus@swalas.org>	2005-12-16	D98E2...
□	Linus Tagesson <linus.tagesson@telia.com>	2000-07-10	AEB69...
□	⊞ Linus Thorsell <Linus@astrakan.se>	1998-04-27	53EAF...
□	Linus Torvalds (tag signing key) <torvalds@osdl.org>	2005-04-23	76E21...
□	Linus Torvalds <Linus.Torvalds@Helsinki.FI>	1996-06-08	A86B3...
□	Linus Torvalds <torvalds@transmeta.com>	1999-10-05	449FA...
□	Linus Torvalds <vnixroot@netscape.com>	1999-11-21	CE904...
□	Linus Vidal <linusv@ozemail.com.au>	2000-01-31	EC253...
□	Linus Walleij (Primary email address) <triad@df.lth.se>	2002-06-10	0192C...
□	Linus Wegmann <linus.wegmann@gmx.ch>	2002-11-27	DA4A...
□	Linus Westman <linwest@acc.umu.se>	1999-08-11	C4B35...
□	Linus Wiebe <linus.wiebe@precisebiometrics.com>	1999-09-10	64DA...
□	Linus Yong <linus@educom.com.sg>	2000-06-22	BADD...
□	Linus Yong <linus@educom.com.sg>	2000-07-15	29CBF...
□	Linus Zetterlund <linus.zetterlund@telia.com>	2003-09-05	3E962...
□	Linus Zetterlund <linus@mbi.se>	2004-10-19	D7513...
□	Linus und Jsabella Wieland <jsaundlini@gmx.ch>	2000-07-30	D13FE...

Figure 8: A populated keyring in OpenPGP Management window



Account / User ID	Ke...	Type	Calcu...	Owne...	Expiry
Jerome S. Gotangco (Free Software Magaz...	**E6D...**	**pub/sec**	**ultimate**	**ultimate**	**05/02/11**
⊟ Jerome S. Gotangco (Jerome S. Gotangco) <jsgot...	9E37...	pub	-	-	
Jerome Gotangco <jgotangco@ubuntu.com>			-	-	
Linus Torvalds (tag signing key) <torvalds@osdl.o...	76E2...	pub	-	-	

Key Management by selecting File → Import Keys from File, and then selecting the key that you want to import (the key uses 3 possible file extensions: `*.asc`, `*.gpg`, and `*.pgp`). The public key should then be added to your default keyring.

Obtaining public keys with this method is not practiced that much, since people can upload their public keys to a public keyserver available from the internet. You can just search the keyserver for a person's public key then import it to your keyring. This is one of the compelling reasons why PKI is very useful from a global perspective.

You can easily add a new public key to your keyring using Enigmail. Let's say you want to add Linus Torvald's key to your personal keyring. To do this, just open up OpenPGP Key Management and click "Keyserver" then select "Search for Keys". A small window will open up asking you what key you want to search for and what keyserver to use. For the keyserver, just leave the defaults as they are since this will work (you can add more keyservers later). As for the key you want to search for, you can use a person's whole name, email address, or the key ID itself. For this example, I just wrote "Linus Torvalds", used the default keyservers listed and clicked "Ok". Figure 7 shows the result of this example search.

From the search results, you see a lot of keys with the name Linus Torvalds. Let's assume that you personally know his public key (in reality, I don't; we're just using this key for the exercise), so click on the box bearing the email address `torvalds@osdl.org` and click "OK". This public key will then be retrieved from the online keyserver and then added to your personal keyring. When the process is complete, your OpenPGP Key Management window will now look like figure 8.

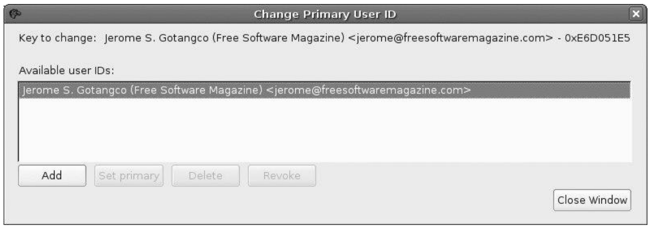
Notice that I've also added my real public key for this exercise using the same method. When you are done importing public keys from a keyserver, you will have a simple keyring that can be used to send secure email to people as long as they are part of it.

Adding User IDs

Some of us maintain more than one email address. The most common scenario is having one account for home, then another for work. You can create a key for each account that you maintain, but that would mean you'll have to remember a lot of passphrases and Key IDs. What you can do, though, is have all those email addresses use one single Key ID and create multiple User IDs as needed. To do that, make sure OpenPGP Key Management is open, then right-click in the window and select Manage User IDs. Then select the key pair that you wish to add a new User ID (shown in figure 9).

Select the key that you want to add a User ID to, then click "Add". A window will appear where you can add your new User ID. From here, add your email address, name and comment to the User ID. You will then be asked for your passphrase before adding the new User ID to your key. Adding a new entry also makes it your new Primary User ID, but you can change this anytime by going back to the window and selecting the ID that you wish to become your primary.

Figure 9: Creating a new User ID



Change Primary User ID

Key to change: Jerome S. Gotangco (Free Software Magazine) <jerome@freesoftwaremagazine.com> - 0xE6D051E5

Available user IDs:

Jerome S. Gotangco (Free Software Magazine) <jerome@freesoftwaremagazine.com>

Now that you've created your key, made your backup and downloaded the public key of one popular free software personality, you're all set to send secure messages—all of this without touching the command line! For sending email, you won't use the command line anymore because your'e going to use Thunderbird.

Sending your public key by email or to a keyserver

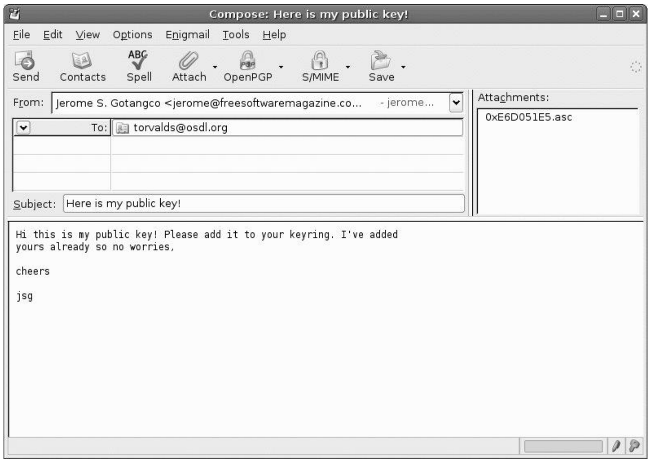
The next step, after adding a new user id to your primary key, is to make sure people all over the world will be able to get your public key and use it to communicate with you in a secure manner. Remember the key pair right? As I have said earlier, it has 2 parts: the public key and the private key. Again, the private key belongs to you and it should never be given to anyone at all. However, you do want people to know your public key and there are two ways for people to get it.

> You'll need an email account that has POP3/SMTP and/or IMAP support to be able to download your email messages to Thunderbird

The first method is send your public key to your contact by email. Since Thunderbird is an email client, it can send the email itself along with the public key in one click. From OpenPGP Key Management, click on your default key pair and select "Send Public Keys by Email" (see figure 10).

This action creates an ASCII-armored file that contains your public key and is ready to be sent to your contact. Once your contact receives it, they'll be able to add your public key and then connect with you using secure email.

Figure 10: Sending an ASCII-armored public key by email



Compose: Here is my public key!

From: Jerome S. Gotangco <jerome@freesoftwaremagazine.co... - jerome...

To: torvalds@osdl.org

Subject: Here is my public key!

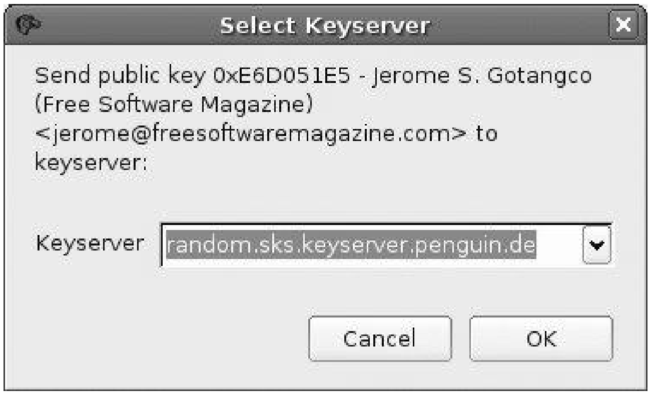
Attachments: 0xE6D051E5.asc

```
Hi this is my public key! Please add it to your keyring. I've added
yours already so no worries,

cheers

jsg
```

Figure 11: Selecting a keyserver before uploading the public key



Select Keyserver

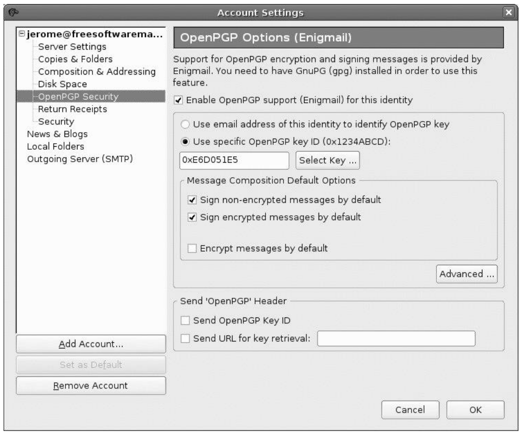
Send public key 0xE6D051E5 - Jerome S. Gotangco (Free Software Magazine) <jerome@freesoftwaremagazine.com> to keyserver:

Keyserver: random.sks.keyserver.penguin.de

The second method is to send your public key to a keyserver. This is the most convenient way for people to obtain your public key, rather than asking for it from you via email or other forms of communication. When you get to sign keys, you'll be uploading the updated public keys of other people. Both actions employ the same routine on uploading the public key to the keyserver. To do this, from OpenPGP Manager, select your default key, right click and choose "Upload Public Keys to Keyserver". This will open up a window where you can put what keyserver you want to use (as shown in figure 11).

The default keyservers work, but you can indicate any keyserver you want such as `pgp.mit.edu`, `keyserver.ubuntu.com` and more. Don't worry about what keyserver to use; all of them should work

Figure 12: OpenPGP options in your account



OpenPGP Options (Enigmail)

Support for OpenPGP encryption and signing messages is provided by Enigmail. You need to have GnuPG (gpg) installed in order to use this feature.

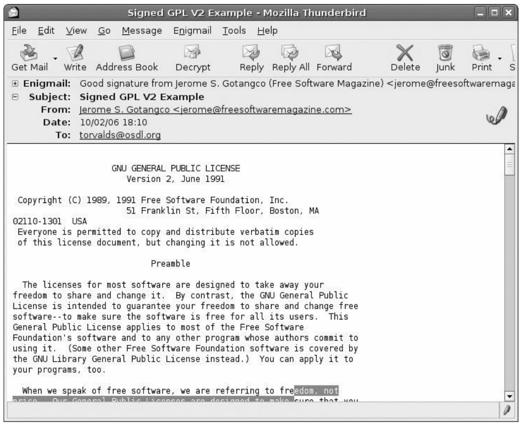
☑ Enable OpenPGP support (Enigmail) for this identity

○ Use email address of this identity to identify OpenPGP key
● Use specific OpenPGP key ID (0x1234ABCD): 0xE6D051E5

Message Composition Default Options
☑ Sign non-encrypted messages by default
☑ Sign encrypted messages by default
□ Encrypt messages by default

Send 'OpenPGP' Header
□ Send OpenPGP Key ID
□ Send URL for key retrieval:

Figure 13: Signed email from Thunderbird



Enigmail: Good signature from Jerome S. Gotangco (Free Software Magazine) <jerome@freesoftwaremaga
Subject: **Signed GPL V2 Example**
From: Jerome S. Gotangco <jerome@freesoftwaremagazine.com>
Date: 10/02/06 18:10
To: torvalds@osdl.org

```
                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
                       51 Franklin St, Fifth Floor, Boston, MA
02110-1301  USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The licenses for most software are designed to take away your
freedom to share and change it.  By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users.  This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it.  (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.)  You can apply it to
your programs, too.

  When we speak of free software, we are referring to freedom, not
```

fine because they synchronize with each other almost instantaneously.

When signing another key, you'll also be requested to upload the public key that you signed to a keyserver. The same actions apply here when uploading a signed public key.

Signing an email message with your key

Unless you're in a very sensitive position that involves national security, you'll have very little need to encrypt all email messages to your contact list. Sometimes, you just want to make sure that your contacts are aware that it really was you who sent the email message that they just received. This is where GnuPG key signatures come in handy.

You can also opt to have all messages signed by default with your key. You can do this by going to your Thunderbird Account Properties (Edit—Account Properties) and select your account. You'll see a folder named "OpenPGP Security" (see figure 12)

From this window, make sure "Sign non-encrypted messages by default" is checked. This will mean that any email correspondence that is sent using this account are signed. Once you have filled out the details, click on "Ok" to close the window.

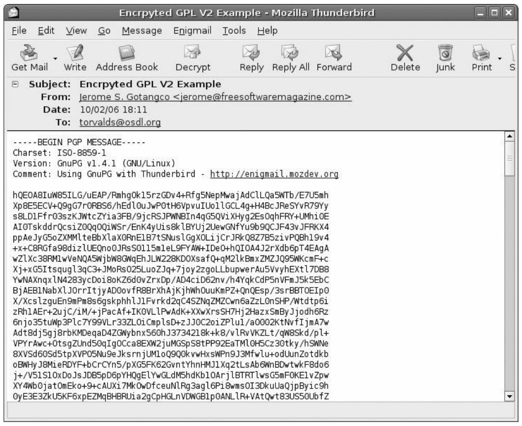
With this setting, every email message that you send outside will be signed by your key. From Thunderbird, click on "Write" and you'll get to compose an email; however, notice at the lower right side of the picture has a green pencil: this means the email will be signed using your key. For this example, I am sending a copy of the GPL V2 to Linus Torvalds, but I'm going to sign this email so that he'll know that it was actually me who sent the email to him. When your email is done and about to be sent to your contact, you will be asked for your passphrase. When you are authenticated, the email will be sent to your recipient but will be signed as seen in figure 13.

The email recipient will then be able to retrieve your public key from a keyserver using your signature. Having this email signed also assures the recipient that it was actually your own email account and its corresponding key that signed and sent this email message.

Encrypting and decrypting an email message with your key

Encrypting the above email message which you have already signed is the next step. Fortunately, this is made simple with Enigmail. From the current email composition window, you can just click "OpenPGP" and select "Encrypt Message". You also encrypt this message by just clicking on the small key icon on the lower right side of the composition window. When the key is colored green, it means the message will be encrypted. Once you send this email, you'll then be asked for your passphrase and the message will be encrypted using your key. Encryption makes your email only readable to the person you intend it for—hence the need for the person's public key to encrypt the message. Our GNU GPL V2 message to Linus Torvalds, once encrypted, looks like that shown in figure 14.

Figure 14: Encrypted email from Thunderbird

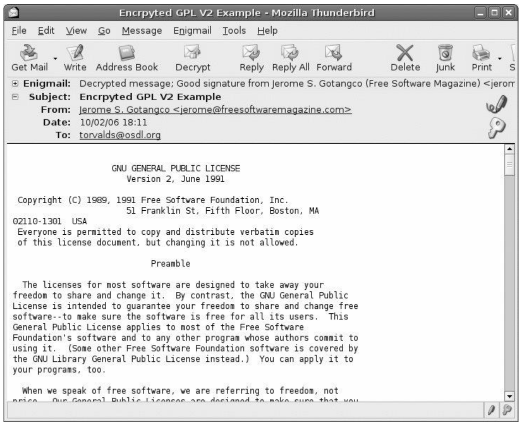


Subject: **Encrpyted GPL V2 Example**
From: Jerome S. Gotangco <jerome@freesoftwaremagazine.com>
Date: 10/02/06 18:11
To: torvalds@osdl.org

```
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG v1.4.1 (GNU/Linux)
Comment: Using GnuPG with Thunderbird - http://enigmail.mozdev.org

hQEOA8IuW85ILG/uEAP/RmhgOkl5rzGDv4+Rfg5NepMwajAdClLQa5WTb/E7U5mh
Xp8E5ECV+Q9gG7r0RBS6/hEdl0uJwP0tH6VpvuIUollGCL4g+H4BcJReSYvR79Yy
s8LDlFfr03szKJWtcZYia3FB/9jcRSJPWNBIn4qG5QViXHyg2EsOqhFRY+UMhi0E
AI0TskddrQcsiZ0Qq0QiWSr/EnK4yUis8klBYUj2UewGNfYu9b9QCJF43vJFRKX4
ppAeJyG5oZXMMlteBbXlaX0RnElB7tSNuslGgXOLijCrJRkQ8Z7B5zivPQBh19v4
+x+C8RGfa98dizlUEQno0JRsS0ll5mleL9FYAW+IDeO+hQIOA4J2rXdb6pT4EAgA
wZlXc38RMlwVeNQA5WjbW8GWqEhJLW228KDOXsafQ+qM2lkBmxZMZJQ95WKcmF+c
Xj+xG5Itsqugl3qC3+JMoRsO25LuoZJq+7joy2zgoLLbupwerAu5VvyhEXtl7DB8
YwNAXnqxlN4283ycDoi8oKZ6d0vZrxDp/AD4ciD62nv/h4YqkCdP5nVFmJ5k5EbC
BjAEBlNabXlJOrrItjyAD0ovfR8BrXhAjKjhWhOuuKmPZ+QnQEsp/3srBBTOEIp0
X/XcslzguEn9mPm8s6gskphhlJlFvrkd2qC4SZNqZMZCwn6aZzL0nSHP/Wtdtp6i
zRhlAEr+2ujC/iM/+jPacAf+IK0VLlPwAdK+XXwXrsSH7Hj2HazxSmByJjodh6Rz
6njo35tuWp3Plc7Y99VLr33ZLOiCmplsD+zJJ0C2oiZPlul/aO002KtNvfIjmA7w
Adt8dj5gj8rbKMDeqaD4ZGWybnx560hJ3734218k+k8/vlRvVKZLt/qW8Skd/pl+
VPYrAwc+OtsgZUnd50qIgOCca8EXW2juMGSpS8tPP92EaTMl0H5Cz30tky/hSWNe
8XVSd60Sd5tpXVPO5Nu9eJksrnjUMloQ9Q0kvwHxsWPn9J3Mfwlu+odUunZotdkb
oBWHyJ8MieRDYF+bCrCYn5/pXG5FK62GvntYhnHMJ1Xq2tLsAb6WnBDwtwkF8do6
j+/V51S1OxDoJsJDB5pD6pYHQgElYwGLdM5hdKb1OArjlBTRTlwsG5mF0KElvZpw
XY4Wb0jatOmEko+9+cAUXi7MkOwDfceuNlRg3agl6Pi8wmsOI3DkuUaQjpByic9h
0yE3E3ZkU5KF6xpEZMqBHBRUia2gCpHGLnVDWGB1p0ANLlR+VAtQwt83US50UbfZ
```

Figure 15: Decrypted email from Thunderbird



Enigmail: Decrypted message; Good signature from Jerome S. Gotangco (Free Software Magazine) <jerom
Subject: **Encrpyted GPL V2 Example**
From: Jerome S. Gotangco <jerome@freesoftwaremagazine.com>
Date: 10/02/06 18:11
To: torvalds@osdl.org

```
                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
                       51 Franklin St, Fifth Floor, Boston, MA
02110-1301  USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The licenses for most software are designed to take away your
freedom to share and change it.  By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users.  This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it.  (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.)  You can apply it to
your programs, too.

  When we speak of free software, we are referring to freedom, not
price.  Our General Public Licenses are designed to make sure that you
```

When Linus receives this encrypted email message, all he has to do is decrypt it using his passphrase and he would be able to read the GNU GPL V2 message that I sent. Assuming I received the same email, I can easily decrypt this email by selecting "Decrypt" from the menu and entering my passphrase when asked. Figure 15 shows how it looks once decrypted.

Now that everything is in place, you can feel comfortable in the thought that you can send secure email messages with very little time and effort. There are still some precautions to consider, like keeping a secure copy of your key pair as well as your passphrase. But, when used properly, the software triumvirate of Mozilla Thunderbird, Enigmail and GnuPG makes a compelling choice for secure email for beginners and seasoned users. Since the software is cross platform, it can also be used in Microsoft Windows, but you will have to configure the software settings differently from what I have done here for Ubuntu.

Bibliography

Mozilla Thunderbird Homepage (`http://www.mozilla.com/thunderbird/`).

Enigmail Homepage (`http://enigmail.mozdev.org/`).

GnuPG Homepage (`http://www.gnupg.org/`).

Ubuntu (`http://www.ubuntu.com`).

The GNU Privacy handbook (`http://www.gnupg.org/gph/en/manual.html`).

GnuPG Key signing Party HowTo (`http://www.cryptnet.net/fdp/crypto/gpg-party.html`).

Biglumber (`http://www.biglumber.com/`)—key signing coordination site.

Copyright information

About the author

Jerome Gotangco is an active member of the Ubuntu Documentation Project, a free software volunteer project that develops and maintains documentation for the Ubuntu operating system. He currently serves as External Vice President of the Philippine Linux Users Group, the oldest Linux users' group in Asia. He is also a frequent speaker and author on the topic of Ubuntu and free software. He can be reached via email at "jgotangco" followed by the at sign followed by "ubuntu.com"