# PGP FOR LINUX TOOL GUIDE

PGP for Linux Tool Guide  
Encrypted email for Linux -------------------------

**Lesson to read:**  
**?** [**Email**](umbrella://lesson/email)  
**Computer requirements:** An internet connection, a computer running Linux, an email account  
**Version used in this guide:**  
? Linux: Debian 7.0 ("Wheezy")  
? Mozilla Thunderbird 24.8.1  
? Enigmail 1.6  
? GPG4Win 1.4.18  
**License:** Free Software; mix of Free Software licenses  
**Level:** Expert  
**Other reading:** <https://www.gnupg.org/documentation/guides.html>  
**Time required:** 30-60 minutes

**Using PGP will give you:**  
? The ability to protect your email communications from being read by anyone except their intended recipients.  
? The ability to prove that an email came from a particular person, instead of being a fake message sent by another sender (it is otherwise very easy for email to be fabricated). Both of these are important defenses if you're being targeted for surveillance or misinformation.

### 1.0 Before you start

To use Pretty Good Privacy (PGP), you will need to install some extra software that will work with your current email program. You will also need to create a private key, which you will keep private. The private key is what you will use to decrypt emails sent to you, and to digitally sign emails that you send to show they truly came from you. Finally, you'll learn how to distribute your public key?a small chunk of information that others will need to know before they can send you encrypted mail, and that they can use to verify emails you send.

This guide will show you how to use PGP with a Linux-style operating system using Mozilla Thunderbird, a popular open source graphical email client.

You can't currently use PGP directly with a web email service like Gmail, Hotmail, Yahoo! Mail, or Outlook Live. You can still use your webmail address; you?ll just have to configure it with the Thunderbird program on your computer.

**Note that both ends of the email conversation need to be using PGP-compatible software for it to work.**

People will normally use this only on their own personal devices, not on shared devices. Fortunately, PGP is available for most desktop computers and mobile devices, and you can point them to these guides to help them set up their own version.

### 2.0 Installing Thunderbird, GnuPG and Enigmail

PGP is an open standard, which means that more than one piece of software can use it. The software we're going to use for PGP is called GnuPG. We'll also be adding a plug-in to Thunderbird called Enigmail, which lets you use GnuPGP from within Thunderbird. The following instructions require some comfort with the command line.

If you're using using a Red Hat-based distribution such as Red Hat or Fedora Core, open a terminal and run these commands:

*sudo yum install gnupg thunderbird thunderbird-enigmail*

If you are using a Ubuntu-based distribution such as Ubuntu, or Linux Mint, open a terminal and type these commands to make sure you have the right software installed:

*sudo apt-get install gnupg thunderbird enigmail*

If you're using the Debian distribution, you'll find that Thunderbird is called ?Icedove.? Like Debian in general, this is for entirely reasonable but somewhat obscure reasons. Apart from the name, it's exactly the same program: we'll not mention Icedove again, but you can just replace ?Thunderbird? with Icedove in the rest of this guide, and everything should still work.

Use this command in the Terminal to install it:

*sudo apt-get install gnupg icedove enigmail*

### 2.1 Configuring Thunderbird

Now that you've installed Thunderbird, open it as you would another application on your machine (you might pick it from a list of applications on a menu, or type its name into an application search). You will see the first run wizard appear.

To set up your existing email address, click "Skip this and use my existing email,? and then enter your name, email address, and the password to your email account.

If you use a popular free email service like Gmail, Thunderbird should be able to automatically detect your email settings when you click ?Continue.?

**If you use two-factor authentication with Google (and depending on your threat model you probably should!) you cannot use your standard Gmail password with Thunderbird. Instead, you will need to create a new application-specific password for Thunderbird to access your Gmail account. See** [**Google's own guide**](https://support.google.com/mail/answer/1173270?hl=en)**for doing this.**

If it doesn't, you may need to manually configure your IMAP and SMTP settings. If you don?t know how to do this, talk to your email provider, or ask someone technical who is familiar with your email provider (so, an IT person at work, or a technical friend who uses the same ISP as you; they don't need to know how to use PGP, but you can ask them ?Do you know the IMAP and SMTP settings for my email address??).

### 2.2 Configuring Enigmail

Enigmail is a plugin for Thunderbird that encrypts and decrypts PGP-encoded emails, and makes handling private and public keys a little easier. If you have the latest version of Enigmail, you should be presented with the Enigmail Setup Wizard.

If you don't see it, you can use this menu option from Thunderbird to make it appear. Click on the three horizontal lines (the ?hamburger menu?) on the right of the Thunderbird window.

Here's the first option that Enigmail offers you: three options for handling when to encrypt your mail.

The default option is to encrypt emails if you have the ?public key? of another person, Enigmail will encrypt the email you send but leave emails unencrypted if you don't have the public key of the recipient yet. You also have the option to encrypt emails all the time to everyone with PGP keys, which means that you will have to find the public keys for people for whom you don't have them already, or turn off automatic encryption completely and only use PGP when directed.

We don't know what the appropriate option is for you, but believe the ?Convenient auto encryption? option to be a good choice. If you are in doubt, choose ?Don't encrypt my messages by default.?

Click the ?Next? button.

Now you have an option to digitally sign all outgoing emails. Signing your email with PGP allows the recipient to check that you sent the message, and that the contents of the message were not tampered with. Click the ?Sign my messages by default? button to turn this feature on.

The downside of doing this, however, is that it can also flag to anyone you send mail to that you use PGP. [In some parts of the world](www.cryptolaw.org/) (including China, Iran, Belarus, and some Middle-East states) using unlicensed encryption, even for personal use, is illegal, so you might have very good reasons to not let others know you use PGP.

Click the ?Next? Button.

Now you'll see an option to have Enigmail make some changes to the configuration of Mozilla Thunderbird.

If you click the Details button you can review what those changes are.

The following options can be unchecked (reenabled), for a more seamless transition, if you use PGP/Mime by default (we'll set that later):  
? Disable flowed text  
? View message body as plain text  
? Do not compose HTML messages

The final option prevents potential problems in the encryption and decryption of your email. Be aware that selecting this box will remove the ability to send text that is bolded, underlined or colored. After reviewing the changes, click the ?OK button.?

Now you will start creating your private key and public key.

### 2.3 Creating a public key and private key

Installation and setup of the Enigmail add-on is complete. Now you'll have the option of creating your public and private key pair. This assumes you have not created a private key before.

Click the ?Next? button.

Unless you have already configured more than one email account, Enigmail will choose the email account you've already configured. The first thing you'll need to do is come up with a strong passphrase for your private key. See the [**Passwords lesson**](umbrella://lesson/passwords) for more information on how to do this.

Enigmail will display some information about your private key as well as the configuration settings. We recommend creating 4096-bit length keys. Click the ?Next? button.

**Your key will expire at a certain time; when that happens, other people will stop using it entirely for new emails to you, though you might not get any warning or explanation about why. So, you may want to mark your calendar and pay attention to this issue a month or so before the expiration date.**

It's possible to extend the lifetime of an existing key by giving it a new, later expiration date, or it's possible to replace it with a new key by creating a fresh one from scratch. Both processes might require contacting people who email you and making sure that they get the updated key; current software isn't very good at automating this. So make a reminder for yourself; if you don't think you'll be able to manage it, you can consider setting the key so that it never expires, though in that case other people might try to use it when contacting you far in the future even if you no longer have the private key or no longer use PGP.

Enigmail will generate the key and when it is complete, a small window will open asking you to generate a revocation certificate. This revocation certificate is important to have as it allows you to make the private key and public key invalid. It is important to note that merely deleting the private key does not invalidate the public key and may lead to people sending you encrypted mail that you can't decrypt.

Click the ?Generate Certificate? button.

A window will open to provide you a place to save the revocation certificate. While you can save the file to your computer, we recommend saving the file on a USB drive that you are using for nothing else and storing the drive in a safe spot. We also recommend removing the revocation certificate from the computer with the keys, just to avoid unintentional revocation.

Even better, save this file on a separate encrypted disk. Choose the location where you are saving this file and click the ?Save? button.

Now Enigmail will give you further information about saving the revocation certificate file again. Click the ?OK? button.

Finally, you are done with generating the private key and public key. Click the ?Finish? button.

### 2.4 Optional steps

### 2.4.1 Display long key-IDs

The next steps are completely optional but they can be helpful when using OpenPGP and Enigmail. Briefly, the Key ID is a small part of the fingerprint. When it comes to verifying that a public key belongs to a particular person the fingerprint is the best way. Changing the default display makes it easier to read the fingerprints of the certificates you know about. Click the configuration button, then the Enigmail option, then Key Management.

A window will open showing two columns: Name and Key ID.

On the far right there is a small button. Click that button to configure the columns. Unclick the Key ID option and click the Fingerprint option.

Now change the width of the Fingerprint column by moving the mouse to the lines between each column heading (that is, just to the left of the ?Key ID? header at the top of the list of keys), and dragging the line to the left. Keep moving left until you can see all of the Key ID, like this:

Now the columns will look like this:

Now you are set up to send and receive regular and encrypted email. Next you will go through the steps of actually finding the people to exchange encrypted mail with.

**Using PGP doesn't completely encrypt your email so that the sender and receiver information is encrypted. Encrypting the sender and receiver information would break email. Using Thunderbird with the Enigmail add-on gives you an easy way to encrypt and decrypt the content of your email.**

### 3.0 Letting others know you are using PGP

**a) Let people know you are using PGP with an email**

You can easily email your public key to another person by sending them a copy as an attachment.

Click the ?Write? button in Mozilla Thunderbird.

Fill in an address and a subject, perhaps something like ?my public key,? click the Enigmail menu and select the ?Attach My Public Key? option.

You can now the email and the recipient will be able to download and use the public key you sent.

**If this method is used, it's a good idea to have the recipient verify your public key's fingerprint over some other form of communication, in case email is already being intercepted and tampered with.**

**b) Let people know you are using PGP on your website**

In addition to letting people know via email, you can post your public key on your website. The easiest way is to upload the file and link to it. This guide won't go into how to do those things, but you should know how to export the certificate as a file to use in the future.

Click the configuration button, then the Enigmail option, then Key Management.

Highlight your certificate in bold, then right-click to bring up the menu and select Export keys to file.

A small window will pop up with three buttons. Click the ?Export Public Keys Only? button.

**Make sure you don't click the ?Export Secret Keys? button because exporting the secret key could allow others to impersonate you if they are able to guess your password.**

Now a window will open so you can save the file. In order to make it easier to find in the future please save the file to the Documents folder.

Now you can use this file as you wish.

**c) Uploading to a keyserver**

Keyservers make it easier to search for and download public keys. Most modern keyservers are synchronizing, meaning that a public key uploaded to one server will eventually reach all servers.

Although uploading your public key to a keyserver might be a convenient way of letting people know that you have a public PGP certificate, you should know that due to the nature of how keyservers work, there is no way to delete public keys once they are uploaded, you can only mark them as revoked.

**Before uploading your public key to a keyserver, it is good to take a moment to consider whether you want the whole world to know that you have a public key without the ability to remove this information at a later time.**

If you choose to upload your public key to keyservers, you will go back to the Enigmail Key Management window.

Click the Keyserver menu item and select the Upload Public Keys option.

### 3.1 Finding other people who are using PGP

**a) Getting a public key by email**

You might get a public key sent to you as an email attachment.

Notice the attachment at the bottom of the window. Right-click on the attachment and select ?Import OpenPGP Key.? A small window will open giving you the results of the import. Click the OK button.

If you open up the Enigmail key management window again, you can check the result. Your PGP key is in bold because you have both the private key and the public key. The public key you just imported is not bold because it doesn't contain the private key.

**b) Getting a public key as a file**

It's possible that you get a public key by downloading it from a website or someone might have sent it through chat software. In a case like this, you will assume you downloaded the file to the Downloads folder.

Open the Enigmail Key Manager and click on the ?File? menu. Select ?Import Keys from File.?

The public key might have very different file name endings such as .asc, .pgp, or .gpg. Select the file and click the ?Open? button. A small window will open, giving you the results of the import. Click the ?OK? button.

**c) Getting a public key from a key server**

Keyservers can be a very useful way of getting public keys. Try looking for a public key. Open up the key manager then click the ?Keyserver? menu and select ?Search for Keys.?

A small window will pop up with a search field. You can search by a complete email address, a partial email address, or a name. In this case, you will search for certificates containing ?eff.org.?

A larger window will pop up with many options. If you scroll down you'll notice some certificates are italicized and grayed out. These are certificates that have either been revoked or expired on their own.

Let's take the public keys of Danny O'Brien for example, he has one expired or revoked certificate and one valid certificate. Select the valid certificate by clicking the box on the left then press the OK button.

In some cases a person may have more than one certificate, all appearing valid. Note that it's possible for anyone to upload a public certificate for anyone else, and that one of these keys may not belong to the person that owns the email address associated with it. In this case, verifying the fingerprint is extremely important.

A small notification window will pop up letting you know if you succeeded, and the Enigmail Key Manager will now show you the added certificates:

### 4.0 Sending PGP encrypted mail

Now you will send your first encrypted email to a recipient. In the main Mozilla Thunderbird window click the ?Write? button. A new window will open.

Write your message, and enter a recipient. For this test, select a recipient whose public key you already have. Enigmail will detect this and automatically encrypt the email (you can tell it will be encrypted by the golden key at the bottom right of the email).

**Note that the subject line won't be encrypted, so choose something innocuous, like ?hello.?**

When you click the ?Send? button, you'll be given a window to enter the password to your PGP Key. Remember this is different from your email password!

Enter your password then click the ?OK? button and your email will be encrypted and sent.

The body of the email was encrypted and transformed. For example our text above, was converted to this:

### 4.1 Receiving PGP encrypted mail

Let's go through what happens when you receive encrypted email. First, click on the message.

A small window opens asking you for the password to the PGP key. Remember: Don't enter your email password. Click the ?OK? button.

Now the message will show up decrypted

### 5.0 Revoking the PGP Key

**a) Revoking your PGP Key through the Enigmail interface**

The PGP keys generated by Enigmail automatically expire after five years. So if you lose all your files, you can hope that people will know to ask you for another key once the key has expired.

You might have a good reason to disable the PGP key before it expires. Perhaps you want to generate a new, stronger PGP key. The easiest way to revoke your own PGP key in Enigmail is through the Enigmail Key Manager. Right-click on your PGP key (it's in bold), and select the ?Revoke Key? option.

A window will pop up letting you know what happens and asking for your confirmation. Click the ?Revoke Key? button.

The password window opens, enter your password for the PGP key and click the ?OK? button.

Now a new window will open up letting you know you succeeded. Click the ?OK? button.

When you go back to the Enigmail Key Management window you'll notice a change to your PGP key. It is now grayed out and italicized.

**b) Revoking a PGP Key with a revocation certificate**

As mentioned before, the PGP keys generated by Enigmail automatically expire after five years. So if you lose all your files you can be sure that people will know to ask you for another key once the key has expired.

Like we mentioned before, you might have a good reason to disable the PGP key before it expires.

Similarly, others might have good reasons to revoke an existing key.

You might get sent revocation certificates from friends as a notice that they want to revoke their key.

In the previous section you might have noticed that Enigmail generates and imports a revocation certificate internally when you use the Enigmail Key Manager to revoke a key. Since you already have a revocation certificate, you will use the one you generated earlier to revoke your own key.

Start with the Enigmail Key Manager and click the ?File? menu and select ?Import Keys from File.?

A window will open up so you can select the revocation certificate. Click on the file, and click the ?Open? button. You'll get a notification that the certificate was imported successfully and that a key was revoked. Click the ?OK? button.

Once you click the ?OK? button, you'll be taken back to the Enigmail Key Manager and you see the certificate you revoked greyed out and italicized.

If the key you revoked is your own, and you previously uploaded your public key to the key servers, you will want to re-upload the now-revoked key to the key servers, so that others see not to use it anymore.

Now that you have all the proper tools, try sending your own PGP-encrypted email.