# Table of Contents

Linux......................................................................................................................................................... 2
  Install GNUPG........................................................................................................................................ 2
  Configure the software ............................................................................................................................ 3
    Configure GnuPG files .......................................................................................................................... 3
    Create your own set of keys .................................................................................................................. 6
    Upload key to keyserver ....................................................................................................................... 10
  Import keys ............................................................................................................................................... 13
    Fetched keys .......................................................................................................................................... 13
    Manually import keys ............................................................................................................................ 14
    Validate keys ......................................................................................................................................... 15
  Email encryption in Thunderbird on Linux ............................................................................................... 18
    Settings .................................................................................................................................................. 18
    Sign and Encrypt emails ......................................................................................................................... 20
    Decrypt and Verify emails ......................................................................................................................... 22
  Files ........................................................................................................................................................... 26
    Sign and Encrypt files ............................................................................................................................. 26
    Decrypt and verify files ........................................................................................................................... 27
Linux

Install GNUPG

This documentation is for Debian distributions and Thunderbird.

The core GNUPG package is installed by default on Ubuntu systems, but if it isn’t, then install it from the command line (fig. 73).

```
marilena@marilena-VirtualBox:~$ sudo apt-get install gnupg
```

*fig. 1 Install gnupg*

Install Thunderbird as your email client with the command `sudo apt-get install thunderbird`.

Configure your email account and install the add-on Enigmail. In Thunderbird, go to Tools → Add-ons and search for Enigmail. From the Available Add-ons click on Install (fig. 74).
After the add-on installation a new tab called Enigmail will appear in your menu bar.

**Configure the software**

**Configure GnuPG files**

Before creating your own set of keys, you need to adjust the gnupg configuration.

In a terminal window enter the following:

- `apt-get remove gnome-keyring`
- `killall gpg-agent`

Check the version of your gpg-agent with the commands (fig. 75):

```
gpg-connect-agent <<EOT
GETINFO version
EOT
```
Check the gpg-agent version (fig. 3):

```
gpg-connect-agent <<EOT
GET_CONFIRMATION Hello
EOT
```

Check your gpg-agent (fig. 4):

If you receive an error check if your pinentry program is working (fig. 77):

```
pinentry <<EOT
SETDESC Hello World
CONFIRM
EOT
```
Check the location of the pinentry program:

```
whereis pinentry
```

Create the gpg-agent.conf and gpg.conf files and type in the following lines:

```
nano .gnupg/gpg-agent.conf
```

```
pinentry-program /usr/bin/pinentry-gtk-2
use-standard-socket
```

```
nano .gnupg/gpg.conf
```

```
keyserver-options no-honor-keyserver-url
keyserver-options auto-key-retrieve,verbose,timeout=120
utf8-strings
use-agent
auto-key-locate local,keyserver
keyserver ldap://keys.uwo.ca
```

Change the permissions in the gnupg files:

```
chmod 600 .gnupg/*
chmod 700 .gnupg
```
Create your own set of keys
Now you can create your own set of keys.

Go To Enigmail → Setup Wizard (fig. 78). A window that will help you configure email with encryption will appear. Leave the default settings unless otherwise required, enter a passphrase (fig. 79) and wait for the software to create the private and public keys for you (fig. 80).
Create Key
Create a new Key Pair

This dialog will create a pair of two keys:
Your public key is for others to send you encrypted emails. You can distribute it to everybody.
Your private key is for yourself to decrypt these emails and to send signed emails. You should give it to nobody.

Your passphrase is a password to protect your private key. It prevents misuse of your private key. The passphrase should be a phrase containing at least 8 characters, digits and punctuation marks. Umlauts (e.g. ä, é, ñ) and language-specific characters are not recommended.

Account / User ID:
Marilena <menus@uwo.ca> - menus@uwo.ca
Passphrase

Please confirm your passphrase by typing it again

Passphrase quality:

fig. 7 Enter passphrase
In Enigmail ➜ Preferences in the Basic tab click on Display Expert Settings and Menus, go to Keyserver and enter ldap://keys.uwo.ca, pool.sks-keyservers.net, keys.gnupg.net, pgp.mit.edu in the Specify your keyservers field and ldap://keys.uwo.ca in the Automatically download keys for signature verification field (fig. 81).
fig. 9 Enigmail Keyserver preferences

Now try to send a signed and encrypted email to yourself (fig. 82).
If you receive any errors, then debug the gpg agent and try to find out what causes the error. In a terminal enter the commands:

```
killall gpg-agent
gpg-agent --debug-level expert --use-standard-socket --daemon /bin/sh
```

**Upload key to keyserver**

Now that everything is working and you have your own keys, you can upload your public key to the server. Go to Thunderbird, click on Enigmail → Key Management, right click your name (fig. 83), choose Export Keys to File → Export Public Keys Only (fig. 84), choose a location for the file and click on Save.
fig. 11 Export your public key
This is how a public key looks like:
Now, go to [http://keys.uwo.ca/vkd/GetWelcomeScreen.event](http://keys.uwo.ca/vkd/GetWelcomeScreen.event) and Publish Your Key twice.

**Import keys**

**Fetched keys**

Thanks to our configuration, Enigmail and GnuPg will automatically download the public keys of the people who have sent you a signed email from the keyserver `ldap://keys.uwo.ca`. You can modify this by going to *Thunderbird → Enigmail → Preferences* and changing the entry in the field *Automatically download keys for signature verification from the following server* with the server that you want (fig.86).

![Enigmail Preferences](image)

*fig. 14 Modify the keyserver entry*
Manually import keys
You can import public keys from the server by going to `Enigmail → Key Management → Keyserver → Search for Keys` (fig. 87). Type in the name or email address of the person whose public key you need and click on `OK`. If the search returned the key you were looking for then select the key and click `OK` to import it (fig. 88). This new key will appear in your local database.
You can change the keyserver you wish to manually lookup keys by choosing another keyserver from the drop-down list or just type in the name of the keyserver (fig. 89).

**Validate keys**
A valid key is a key which you’re sure belongs to the right person.
The keys that are fetched by the software or that you manually import from a server come by default as “untrusted” (fig. 80). That means that you’ll have to check with that person if they actually sent that email and that’s their right key.

Fig. 18 Untrusted key

After you make sure that the owner of the key is who he/she claims to be, then you can Sign Sender’s Key to validate it (fig. 91 - 92). Every time you receive a signed email from that person, the software will compare the key with the one you validated and if they match, Enigmail will notify you that the key is valid (fig. 93). If the message has been tampered with, you’ll see a “Bad signature” message.

Fig. 19 Click on Details to Sign Sender’s Key
fig. 20 Sign key

fig. 21 Valid key
Email encryption in Thunderbird on Linux

Settings
You can modify or check the default settings by going to Thunderbird → Enigmail (fig. 94).

![Enigmail settings](image)

Under Preferences (fig. 95), among other things, you can modify your keyservers entries and export your public and secret keys and your GPG configuration files (fig. 96) which you can later import on another machine.
fig. 23 Enigmail preferences
Sign and Encrypt emails
To encrypt an email for someone you’ll need their public key. Make sure you have it downloaded in your local database.

In Thunderbird when you write a new email, the buttons for signing and encrypting should be in the ribbon (fig. 97). Enable them accordingly before you send the email. If you want to attach a file, it is recommended you encrypt it and sign it separately and then attach it. If you attach an unencrypted file, Enigmail will ask if you want the file to be encrypted for you (fig. 98).
Secret content

*fig. 25 Writing a signed and encrypted email*
Encrypting attachments

fig. 26 Encrypting attachments

Decrypt and Verify emails

Enigmail will detect the encrypted email and will ask for your passphrase to decrypt it.

fig. 27 Enter passphrase for signing

If for some reason the add-on doesn’t detect the encryption (fig. 100), then copy and paste the content of the email in a text file. Save it and decrypt it with the command line (fig. 101):

```
gpg /path/to/the/saved/text/file
```

The decrypted message (fig. 102) will be saved in a file in the same location as the encrypted original message file.
fig. 28 No encryption detected
Fig. 29 Decrypting from the command line
Very secret.

- Matt

On 2016-04-12 12:56 PM, Marilena wrote:

```plaintext
>=20
> Secret content
>=20
```

Matthew Feeney
mfeeney7@uwo.ca
519-661-2111x82870
Security Analyst - ITS
Support Services Building Rm.4300, Western University

```plaintext
--qoGXX9fXW1SK83fvMWumGGk9SPHRavpm9--
--rTM6uugu8q5nRkaR4FEmRN4UH9h13mfbV--
```

*fig. 30 Decrypted message*
Files

Sign and Encrypt files
You can sign and encrypt a file from a terminal windows using the command (fig. 103):

`gpg --s --e /path/to/your/file`

Choose your recipients’ keys and your key and hit enter twice. The encrypted file will be saved in the same location as the original file.

![encrypting file from command line](image)

*fig. 31 Encrypting files from the command line*
Decrypt and verify files
When you receive an encrypted file (fig. 104), save it and decrypt and verify it with the command (fig. 105):

```
gpg /path/to/your/file
```

![Fig. 32 Encrypted file attached](image1)

![Fig. 33 Decrypting a file from the command line](image2)