THUNDERBIRD WORKBOOK

Published : 2012-05-25

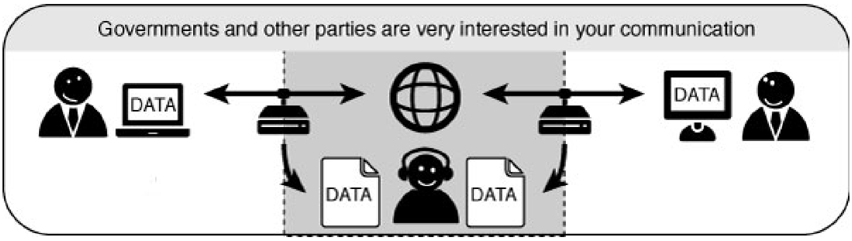
INTRODUCTION

1. ABOUT THIS WORKBOOK
2. INTRODUCTION TO THUNDERBIRD

1. ABOUT THIS WORKBOOK

This workbook is designed to complete specific goals with Thunderbird by providing you with information on how to use the software. This workbook is not aiming to be a complete manual. There is a great online manual online at http://en.flossmanuals.net/thunderbird[1] .

The material in this work book is based on chapters in the manual Basic Internet Security[2] .


Governments and other parties are very interested in your communication
DATA
DATA
DATA
DATA

This workbook is arranged in to groups of chapters called a challenge. Each chapter lists a specific task and gives detailed instructions on how to perform it.

The challenges are designed to be as self contained as possible to make it easier to reuse this material. We imagine that the material in the workbook will be useful for some of the following;

- creating online courses, eg in Peer to Peer University http://p2pu.org
- as printed handouts
- as html pages to be included in other websites
- included in other manuals on related subjects eg Online Security

KEEPING UP TO DATE

Publications about the digital world become outdated fast and a viable solution today could be serious threat tomorrow. Therefore we created this book as open source, so it can be easily updated and will be free for others to update, extend and redistribute. The focus in this book is also on free and open source tools.

There is a wide range of books dealing with different aspects of secure communication in a digital age. We have combined our knowledge with existing publications and our contributions can be re-used and revised as well. This is the advantage of having a growing pool of excellent reusable content at FLOSS Manuals - its becoming easier in this field to make books quickly by combining existing materials using this resource.

Contributing to this Workbook

If you are an educator or if you use this Workbook in other ways and would like to help improve or maintain this resource then please sign up to the Flossmanuals discuss email list[3] and introduce yourself.

1. http://en.flossmanuals.net/thunderbird^
2. http://en.flossmanuals.net/basic-internet-security/^
3. http://lists.flossmanuals.net/listinfo.cgi/discuss-flossmanuals.net^

2. INTRODUCTION TO THUNDERBIRD

These days many people manage their email on the web using services such as Gmail or Hotmail. These services offer access to email accounts through any web browser. It is convenient because you can get your email from almost any computer. If you live in New York and you are backpacking in Thailand, just find an Internet cafe, log on to a computer, and check your email.

Another way to handle your email is to use an *email client* program installed on your own computer. A program like this offers many advantages over using a web email client. It lets you organize your email exactly how you want, it enables you to check email when you are not connected to the Internet, and you can manage multiple email accounts in one place. That said, desktop email clients and web email clients can coexist side-by-side. Using an email client at home doesn't preclude you from using web email when you want to check your account while you are on the road.

Mozilla Thunderbird is a feature-rich, reliable, and secure tool for managing your email.

ENCRYPT AND SIGN YOUR EMAIL

3. WHY ENCRYPT AND SIGN EMAIL

Some background information about email and how you can install software to sign and encrypt it [30-45 mins]

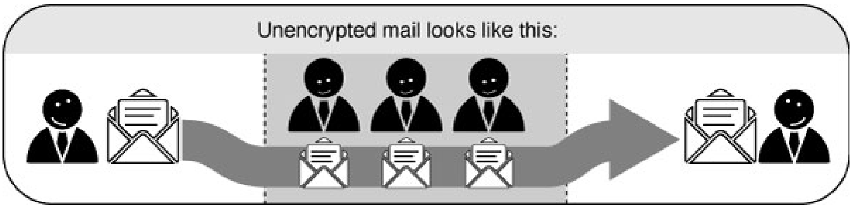
E-mail is one of the oldest forms of communication on the Internet. We often use it to communicate very personal or otherwise sensitive information. It is very important to understand why e-mail in its default configuration is *not secure*. In the following tasks we will describe the different methods necessary to secure your e-mail against known threats.

NO SENDER VERIFICATION: YOU CANNOT TRUST THE 'FROM' ADDRESS

Most people do not realize how trivial it is for any person on the Internet to forge an e-mail by simply changing the identity profile of their own e-mail program. This makes it possibly for anyone to send you an e-mail from some known e-mail address, pretending to be someone else. This can be compared with normal mail; you can write anything on the envelope as the return address, and it will still get delivered to the recipient (given that the destination address is correct). We will describe a method for *signing e-mail messages*, which prevents the possibility of forgery.

E-MAIL COMMUNICATIONS CAN BE TAPPED, JUST LIKE TELEPHONES

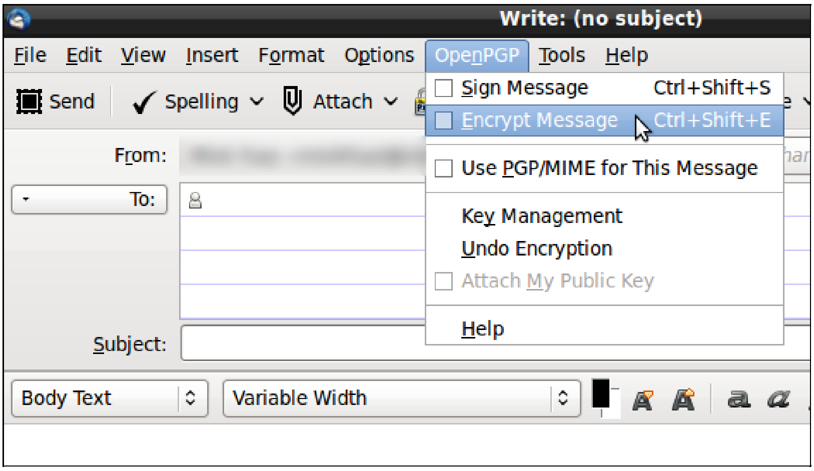
An e-mail message travels across many Internet servers before it reaches its final recipient. Every one of these servers can look into the content of messages, including subject, text and attachments. Even if these servers are run by trusted infrastructure providers, they may have been compromised by hackers or by a rogue employee, or a government agency may seize equipment and retrieve your personal communication.



There are two levels of security that protect against such e-mail interception. The first one is making sure the connection to your e-mail server is secured by an encryption mechanism. The second is by encrypting the message itself, to prevent anyone other than the recipient from understanding the content. This challenge covers E-mail encryption using PGP within Thunderbird.

INSTALLING THUNDERBIRD, ENIGMAIL & PGP / GPG

Thunderbird is an email client which has many options and add ons which give you better email security. One of these add ons is a tool called Enigmail. Enigmail needs another bit of software called GPG (which is also known as PGP) to work. What Enigmail does when it is installed is to add a menu item called OpenPGP to your Thunderbird email client when you are checking or sending emails.


Write: (no subject)
File Edit View Insert Format Options OpenPGP Tools Help
Send
Spelling
Attach
From:
To:
Subject:
□ Sign Message Ctrl+Shift+S
□ Encrypt Message Ctrl+Shift+E
□ Use PGP/MIME for This Message
Key Management
Undo Encryption
□ Attach My Public Key
Help
Body Text
Variable Width

Before we can continue we need to make sure you have the right tools for the job. In some operating systems it is quite easy to install these tools so that they work well together. It should only take you 5 minutes if you are using Ubuntu. However in other operating systems getting these three tools to play nicely together can be a bit tricky. You may have to do some troubleshooting. We really wish that this stage was easier. If you run in problems, try to have patience and read the instruction well help you if you get stuck.

TASK

Install Thunderbird, PGP and Enigmail and set up an email account.

If you don't already have Thunderbird, PGP and Enigmail tools installed then;

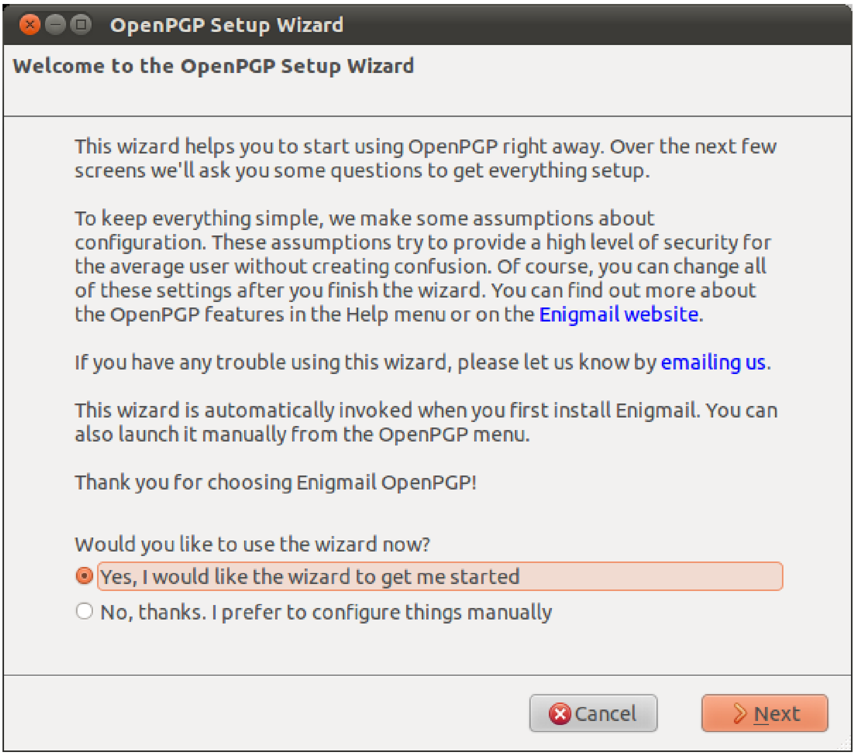
- Read the installation instructions for your operating system in the Thunderbird Workbook here: http://en.flossmanuals.net/thunderbird-workbook/
- Install the latest version of Thunderbird for your operating system.
- Install PGP and the Enigmail plugin for Thunderbird.
- Set up an account with Thunderbird to use an email

4. CREATING YOUR PGP KEYS

How to use Enigmail to create a pair of keys needed before you can sign and encrypt your email [15 mins]

You are now ready to start encryption your mails with PGP. You can do this by using Enigmail *within* Thunderbird. Enigmail comes with a nice wizard to help you with the initial setup and the important aspect of creating a public/private key pair (see the chapter introducing PGP for an explanation). You can start the wizard at any time within Thunderbird by selecting **OpenPGP > Setup Wizard** from the menu on top.

Step 1. This is what the wizard looks like. Please read the text on every window carefully. It provides useful information and helps you setup PGP to your personal preferences. In the first screen, click on Next to start the configuration.



Welcome to the OpenPGP Setup Wizard

This wizard helps you to start using OpenPGP right away. Over the next few screens we'll ask you some questions to get everything setup.

To keep everything simple, we make some assumptions about configuration. These assumptions try to provide a high level of security for the average user without creating confusion. Of course, you can change all of these settings after you finish the wizard. You can find out more about the OpenPGP features in the Help menu or on the Enigmail website.

If you have any trouble using this wizard, please let us know by emailing us.

This wizard is automatically invoked when you first install Enigmail. You can also launch it manually from the OpenPGP menu.

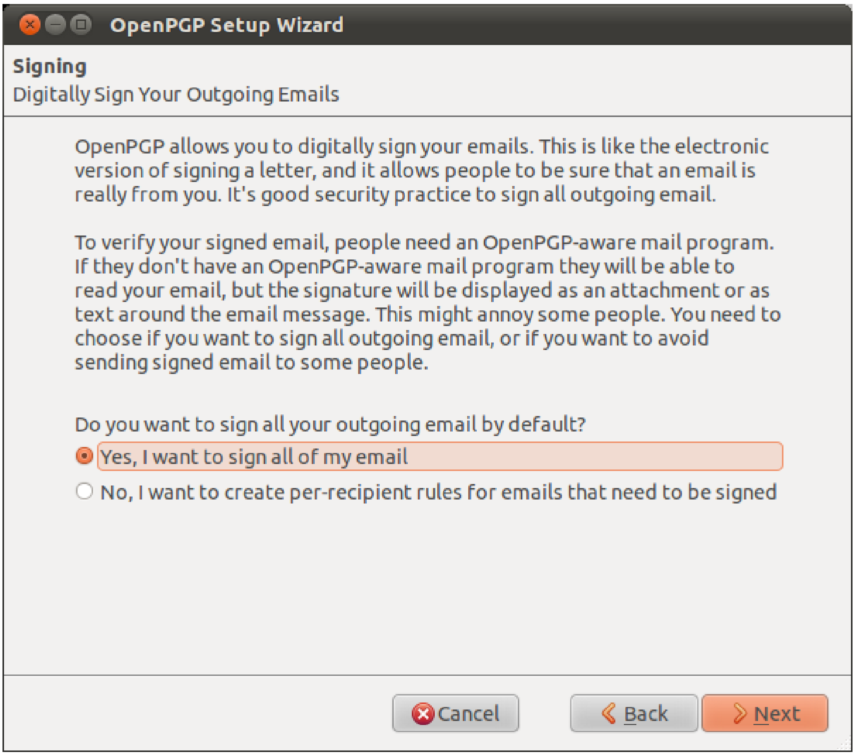
Thank you for choosing Enigmail OpenPGP!

Would you like to use the wizard now?

● Yes, I would like the wizard to get me started

○ No, thanks. I prefer to configure things manually

Step 2. The wizard asks you whether you want to sign all your outgoing mail messages. If you do not chose to sign all your messages, you will have to specify per recipient if you want to sign your e-mail. Signing all your messages is a good choice. Click on the 'Next' button after you have made a decision.



OpenPGP Setup Wizard

Signing

Digitally Sign Your Outgoing Emails

OpenPGP allows you to digitally sign your emails. This is like the electronic version of signing a letter, and it allows people to be sure that an email is really from you. It's good security practice to sign all outgoing email.

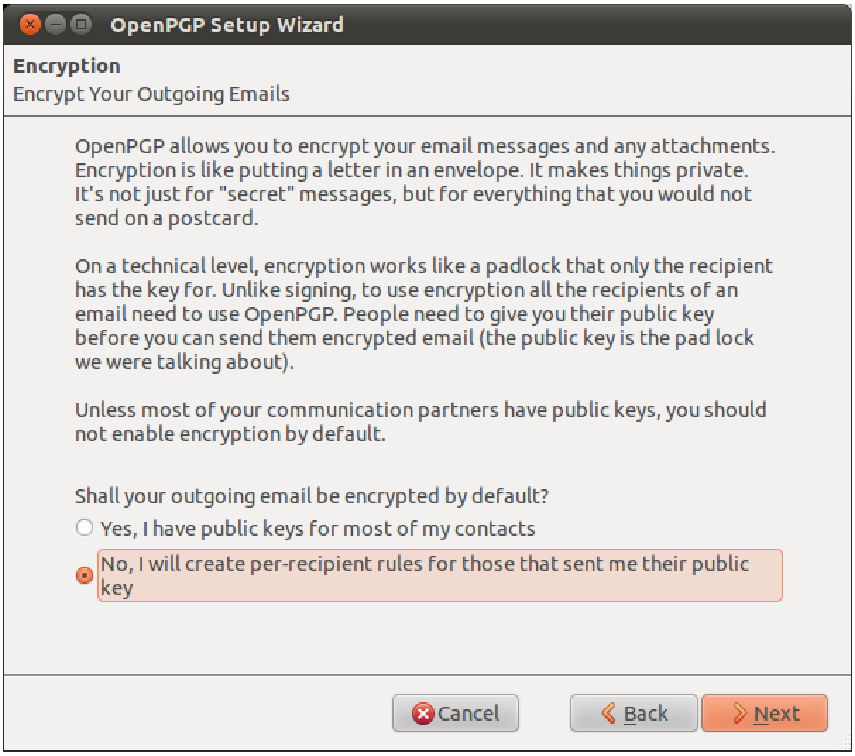
To verify your signed email, people need an OpenPGP-aware mail program. If they don't have an OpenPGP-aware mail program they will be able to read your email, but the signature will be displayed as an attachment or as text around the email message. This might annoy some people. You need to choose if you want to sign all outgoing email, or if you want to avoid sending signed email to some people.

Do you want to sign all your outgoing email by default?

● Yes, I want to sign all of my email

○ No, I want to create per-recipient rules for emails that need to be signed

Step 3. On the following screen, the wizard asks you whether you want to encrypt *all* your outgoing mail messages. Unlike signing of mails, encryption requires the recipient to have PGP software installed. Therefore you should answer 'no' to this question, to make sure you can still send normal mails. Only answer 'yes' here if you want to prevent Thunderbird from ever sending unencrypted mails. After you have made your decision, click on the 'Next' button.



OpenPGP Setup Wizard

Encryption

Encrypt Your Outgoing Emails

OpenPGP allows you to encrypt your email messages and any attachments. Encryption is like putting a letter in an envelope. It makes things private. It's not just for "secret" messages, but for everything that you would not send on a postcard.

On a technical level, encryption works like a padlock that only the recipient has the key for. Unlike signing, to use encryption all the recipients of an email need to use OpenPGP. People need to give you their public key before you can send them encrypted email (the public key is the pad lock we were talking about).

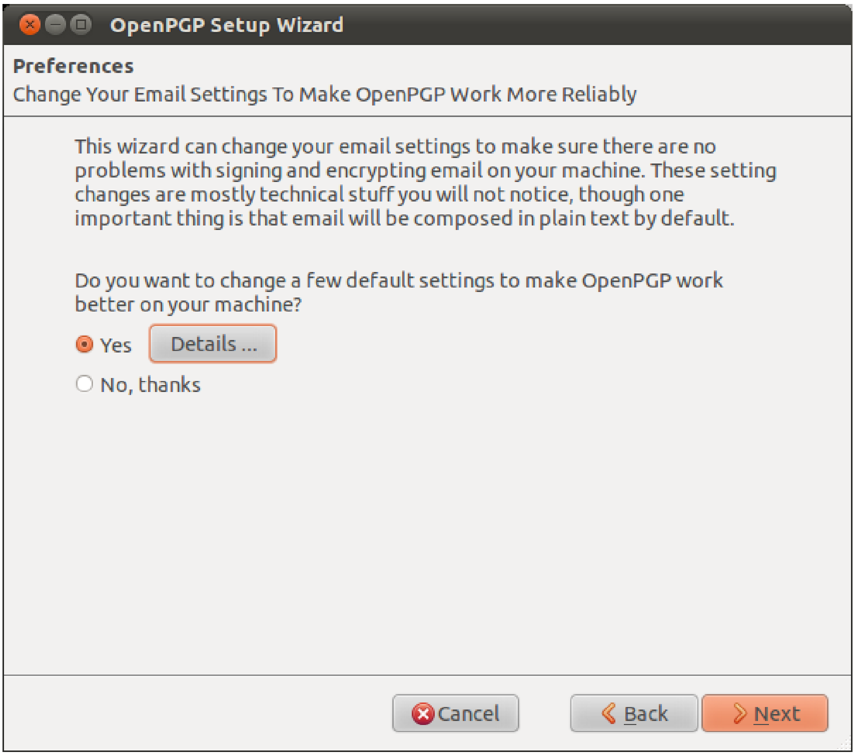
Unless most of your communication partners have public keys, you should not enable encryption by default.

Shall your outgoing email be encrypted by default?

○ Yes, I have public keys for most of my contacts

● No, I will create per-recipient rules for those that sent me their public key

Step 4: On the following screen the wizard asks if he can change some of your mail formatting settings to better work with PGP. It is a good choice to answer 'Yes' here. The only serious thing is that it will prevent you from doing is sending HTML mail messages. Click on the 'Next' button after you have made your decision.



Preferences

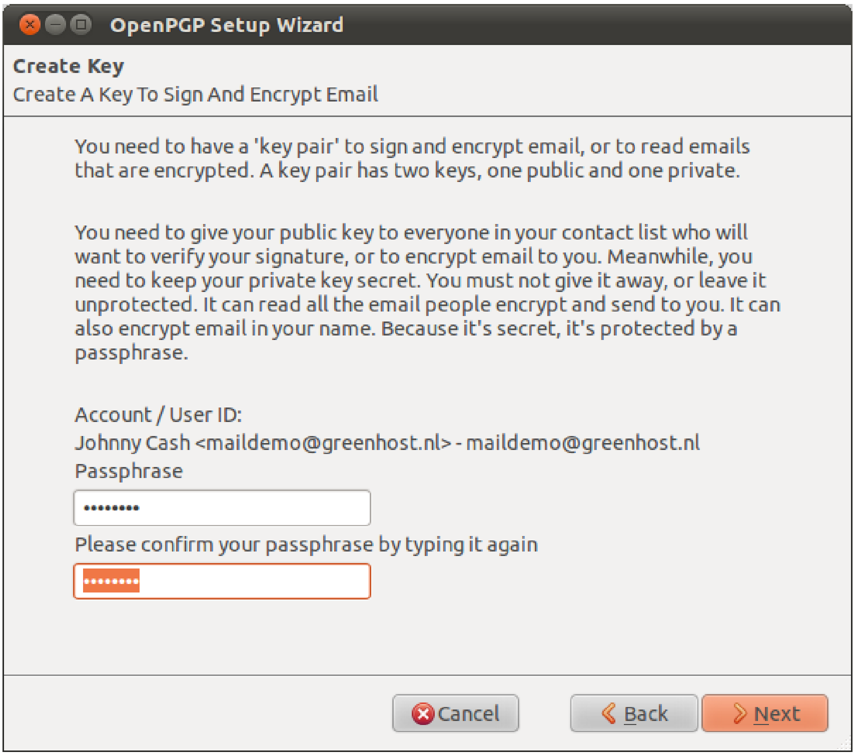
Change Your Email Settings To Make OpenPGP Work More Reliably

This wizard can change your email settings to make sure there are no problems with signing and encrypting email on your machine. These setting changes are mostly technical stuff you will not notice, though one important thing is that email will be composed in plain text by default.

Do you want to change a few default settings to make OpenPGP work better on your machine?

● Yes
○ No, thanks

Step 5: Now it is time to start creating the keys. In the following screen you can select one of your mail accounts, or the default one is selected for you if you have only one mail account. In the 'Passphrase' text box you have to give a password. This is a *new* password which is used to protect your private key. It is **very important** both to remember this password, because you cannot read your own encrypted emails any more when you lose it, and to make it a **strong** password. It should be at least 8 characters long, not contain any dictionary words and it should preferably be a **unique** password. Using the same password for multiple purposes severely increases the chance of it being intercepted at some point. After you have selected your account and created a passphrase, click on the 'Next' button.



Create Key

Create A Key To Sign And Encrypt Email

You need to have a 'key pair' to sign and encrypt email, or to read emails that are encrypted. A key pair has two keys, one public and one private.

You need to give your public key to everyone in your contact list who will want to verify your signature, or to encrypt email to you. Meanwhile, you need to keep your private key secret. You must not give it away, or leave it unprotected. It can read all the email people encrypt and send to you. It can also encrypt email in your name. Because it's secret, it's protected by a passphrase.

Account / User ID:

Johnny Cash <maildemo@greenhost.nl> - maildemo@greenhost.nl

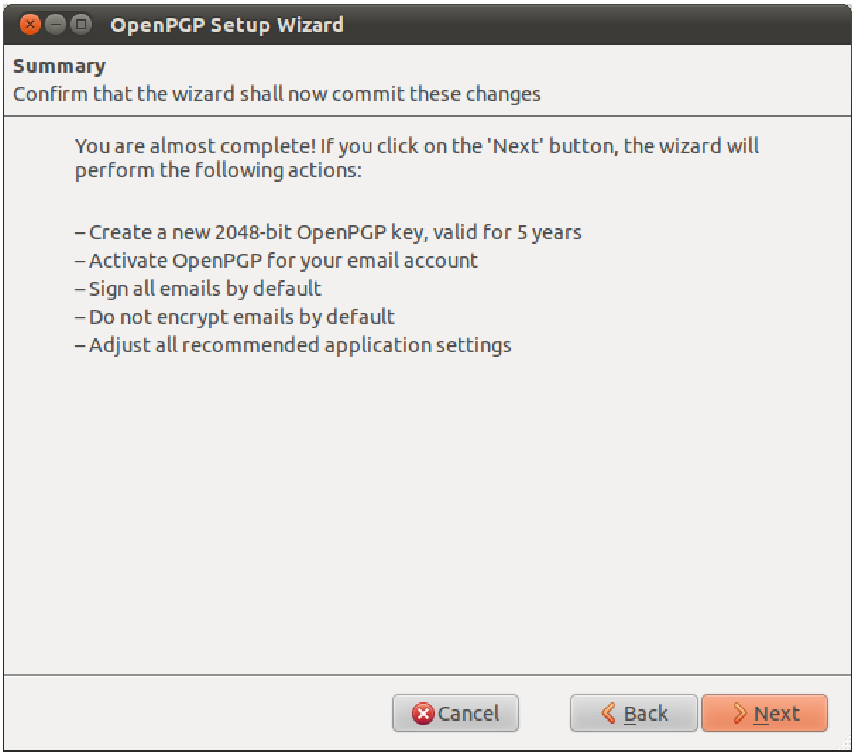
Passphrase

••••••••

Please confirm your passphrase by typing it again

••••••••

Step 6: In the following screen the wizard basically wraps up what actions it will take to enable PGP encryption for your account. If you are satisfied with the options you chose in the previous windows, click on the 'Next' button.



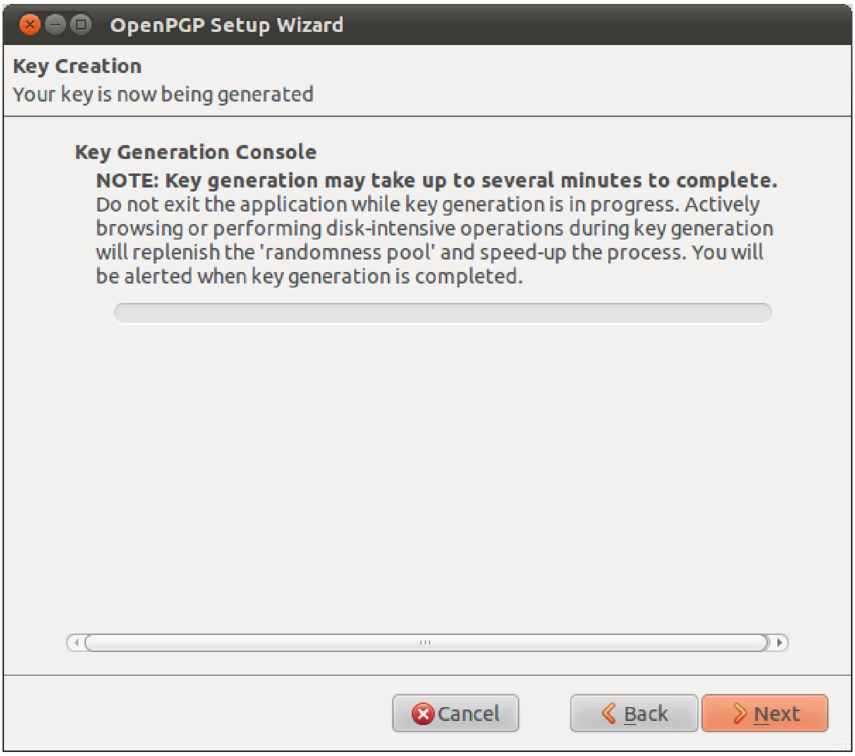
Summary

Confirm that the wizard shall now commit these changes

You are almost complete! If you click on the 'Next' button, the wizard will perform the following actions:

– Create a new 2048-bit OpenPGP key, valid for 5 years
– Activate OpenPGP for your email account
– Sign all emails by default
– Do not encrypt emails by default
– Adjust all recommended application settings

Step 7: Your keys are being created by the wizard. Have some patience. The progress bar should slowly fill up to the right. The wizard will tell you when the keys have been successfully created, then you can click on the 'Next' button again.



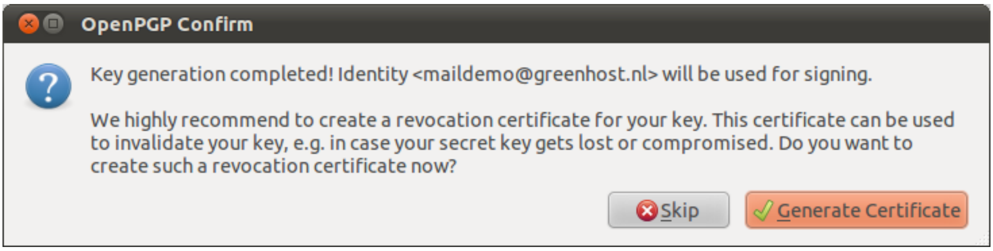
Key Creation

Your key is now being generated

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.

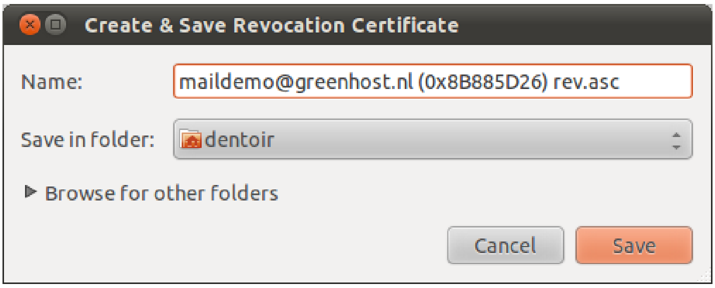
Step 8: You now have your own PGP key-pair. The wizard will ask you if you also want to create a special file, called a 'Revocation certificate'. This file allows you to inform others that your key-pair should no longer be considered valid. Think of it as a 'kill switch' for your PGP identity. You can use this certificate in case you have generated a new set of keys, or in case your old key-pair has been compromised. It is a good idea to create the file and keep it somewhere in a safe place. Click on the 'Generate Certificate' button if you want to create the file, otherwise 'Skip'.



Key generation completed! Identity <maildemo@greenhost.nl> 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?

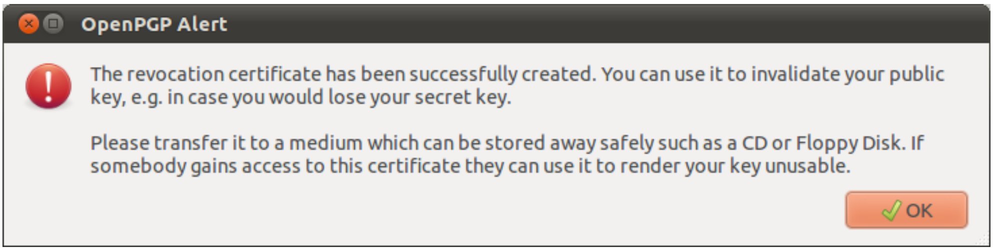
Step 9: Assuming you have decided to generate a revocation certificate, the wizard will ask you where the file should be saved. The dialog may appear a bit different on your particular operating system. It is a good idea to rename the file to something sensible like my_revocation_certificate. Click on 'Save' when you you have decided on a location.


Create & Save Revocation Certificate

Name: maildemo@greenhost.nl (0x8B885D26) rev.asc

Save in folder: dentoir

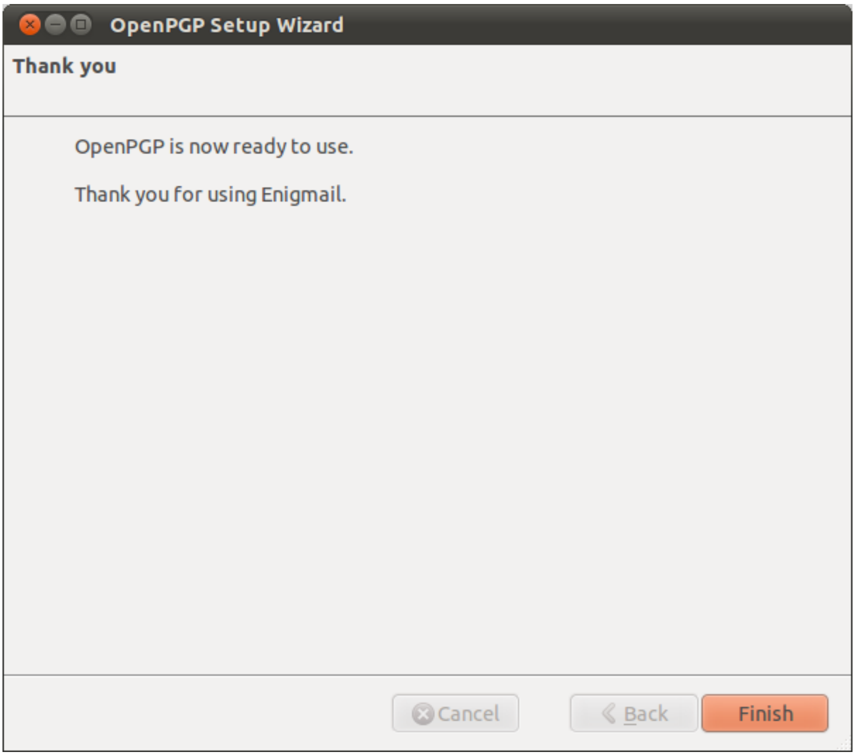
Step 10: Assuming you have decided to generate a revocation certificate, the wizard informs you it has been successfully stored.


OpenPGP Alert

The revocation certificate has been successfully created. You can use it to invalidate your public key, e.g. in case you would lose your secret key.

Please transfer it to a medium which can be stored away safely such as a CD or Floppy Disk. If somebody gains access to this certificate they can use it to render your key unusable.

Step 11: The wizard will inform you it has completed its setup.


OpenPGP Setup Wizard

Thank you

OpenPGP is now ready to use.

Thank you for using Enigmail.

TASK

Follow the instructions above to;

- Create a PGP key pair
- Create a revocation certificate

5. SEND AND RECEIVE PUBLIC KEYS

Add keys to your keyring and send your public key [25 mins]

Our task is to send and receive encrypted and signed email. To do this we will need to exchange public keys with the person that we want to send emails to. Normally to exchange public keys you will contact that person and ask them to send you their key via email or you will download it from the Internet. Conversely, you can then send them your key via email or put in online for them to download.

RECEIVING PUBLIC KEYS AND ADDING THEM TO YOUR KEYRING

Downloading keys from the web

Many people put their public keys on the web so that it is possible for others to download their key. Later challenges will cover the use of **key servers** as another way of receiving and sending keys.

To continue with this task you may want to use the following key and email to test your ability to send encrypted mail.

> **PGP key:** http://clearerchannel.org/keys/mickfuzz.gpg
> **Associated email:** mickfuzz@clearerchannel.org

To be able to send an encrypted email to this address you first need to add that key to your ***keyring*** in Thunderbird. To do this click on the link to the PGP key and download that file to your computer.

Then, in the Thunderbird application go to **OpenPGP > Key Management**

In the Key Management window select **File > Import Keys from File**

Browse to the place where you saved the public key you downloaded and then select it and click on the **Open** button

You should then receive an alert message saying that The key(s) were successfully imported.

You should now be able to progress to sign and encrypt email.

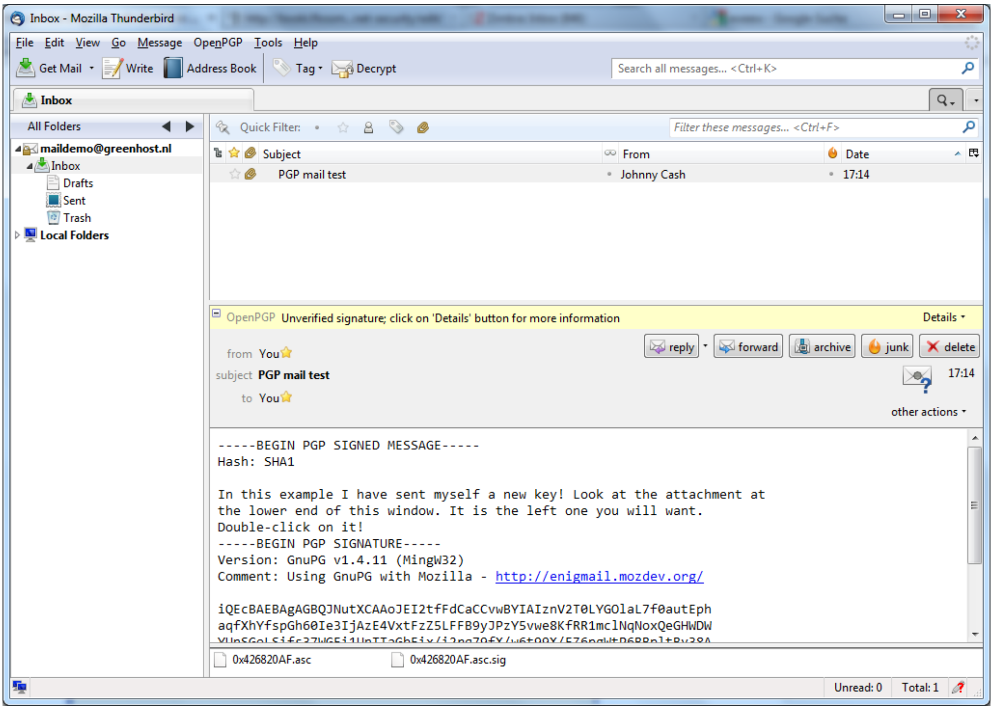
Receiving keys by email

Let's say are able to request and receive a public key from a friend by mail. The key will show up in Thunderbird as an *attached file*. Scroll down the message and below you will find tabs with one or two file names. The extension of this public key file will be .asc, different from the extension of an attached PGP signature, which ends with .asc.sig

Look at the example email in the next image, which is a received, signed PGP message containing an attached public key. We notice a yellow bar with a warning message: 'OpenPGP: Unverified signature, click on 'Details' button for more information'. Thunderbird warns us that the sender is not known yet, which is correct. This will change once we have accepted the public key.

What are all those strange characters doing in the mail message? Because Thunderbird does not recognize the signature as valid, it prints out the entire raw signature, just as it has received it. This is how digitally signed PGP messages will appear to those recipients who do not have your public key.

The most important thing in this example is to find the attached PGP public key. We mentioned it is a file that ends with an .asc. In this example it's the first attachment on the left, which is in the red circle. Double-clicking on this attachment would make Thunderbird recognize the key.



OpenPGP Unverified signature; click on 'Details' button for more information

from You

subject **PGP mail test**

to You

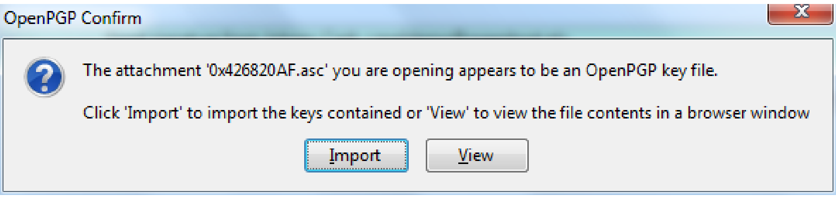
17:14

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

In this example I have sent myself a new key! Look at the attachment at
the lower end of this window. It is the left one you will want.
Double-click on it!
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (MingW32)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org/

iQEcBAEBAgAGBQJNutXCAAoJEI2tfFdCaCCvwBYIAIznV2T0LYGOlaL7f0autEph
aqfXhYfspGh60Ie3IjAzE4VxtFzZ5LFFB9yJPzY5vwe8KfRR1mclNqNoxQeGHWDW
```

0x426820AF.asc 0x426820AF.asc.sig

In the example image above, we should double-click on the attached .asc file to import the PGP public key.

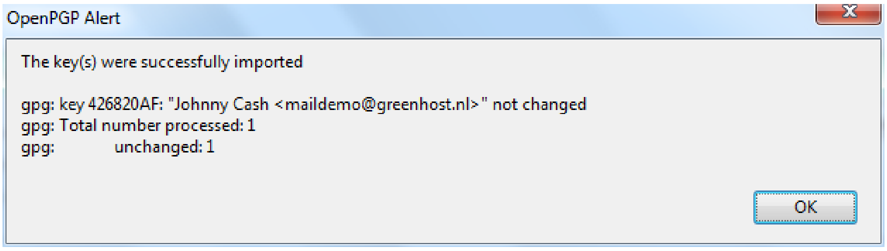
After we have clicked on the attachment, the following pop-up will appear.



The attachment '0x426820AF.asc' you are opening appears to be an OpenPGP key file.

Click 'Import' to import the keys contained or 'View' to view the file contents in a browser window

Thunderbird has recognized the PGP public key file. Click on 'Import' to add this key to your keyring. The following pop-up should appear. Thunderbird says the operation was successful. Click on 'OK' and you are done. You now have the ability to send this friend encrypted messages.



```
The key(s) were successfully imported

gpg: key 426820AF: "Johnny Cash <maildemo@greenhost.nl>" not changed
gpg: Total number processed: 1
gpg:           unchanged: 1
```

SENDING PUBLIC KEYS

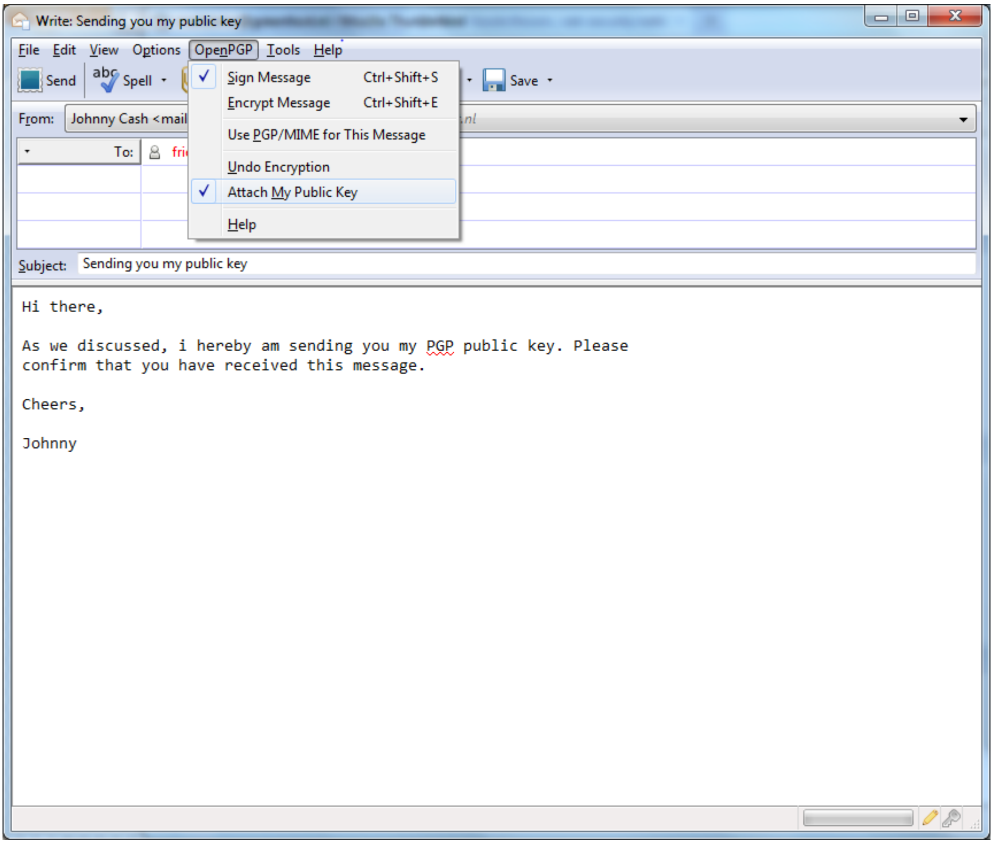
There are multiple ways to distribute your public key to friends or colleagues. By far the simplest way is to attach the key to a mail. In order for your friend to be able to *trust* that the message actually came from you, you should inform them in person (if possible) and also require them to reply to your mail. This should at least prevent easy forgeries. You have to decide for yourself what level of validation is necessary. This is also true when receiving emails from third-parties containing public keys. Contact your correspondent through some means of communication other than e-mail. You can use a telephone, text messages, Voice over Internet Protocol (VoIP) or any other method, but you must be absolutely certain that you are really talking to the right person. As a result, telephone conversations and face-to-face meetings work best, if they are convenient and if they can be arranged safely.

Sending your public key is easy.

1. In Thunderbird, click on the Write icon.

2. Compose a mail to your friend or colleague and tell them you are sending them your PGP public key. If your friend does not know what that means, you may have to explain them and point them to this documentation.

3. Before actually sending the mail, click to **OpenPGP > Attach My Public Key** option on the menu bar of the mail compose window. Next to this option a marked sign ✓ will appear. See the example below.


Write: Sending you my public key
File
Edit
View
Options
OpenPGP
Tools
Help
Send
Spell
Save
✓ Sign Message Ctrl+Shift+S
Encrypt Message Ctrl+Shift+E
Use PGP/MIME for This Message
Undo Encryption
✓ Attach My Public Key
Help

From: Johnny Cash <mail

To: fri

Subject: Sending you my public key

```
Hi there,

As we discussed, i hereby am sending you my PGP public key. Please
confirm that you have received this message.

Cheers,

Johnny
```

4. Send your mail by clicking on the Send button.

TASK

- Import someone else's public key via email or by downloading it from the web
- Send your public key to someone. You can try mickfuzz@clearerchannel.org

6. SEND AN ENCRYPTED AND SIGNED EMAIL

Send and sign encrypted mail in Thunderbird [10 mins]

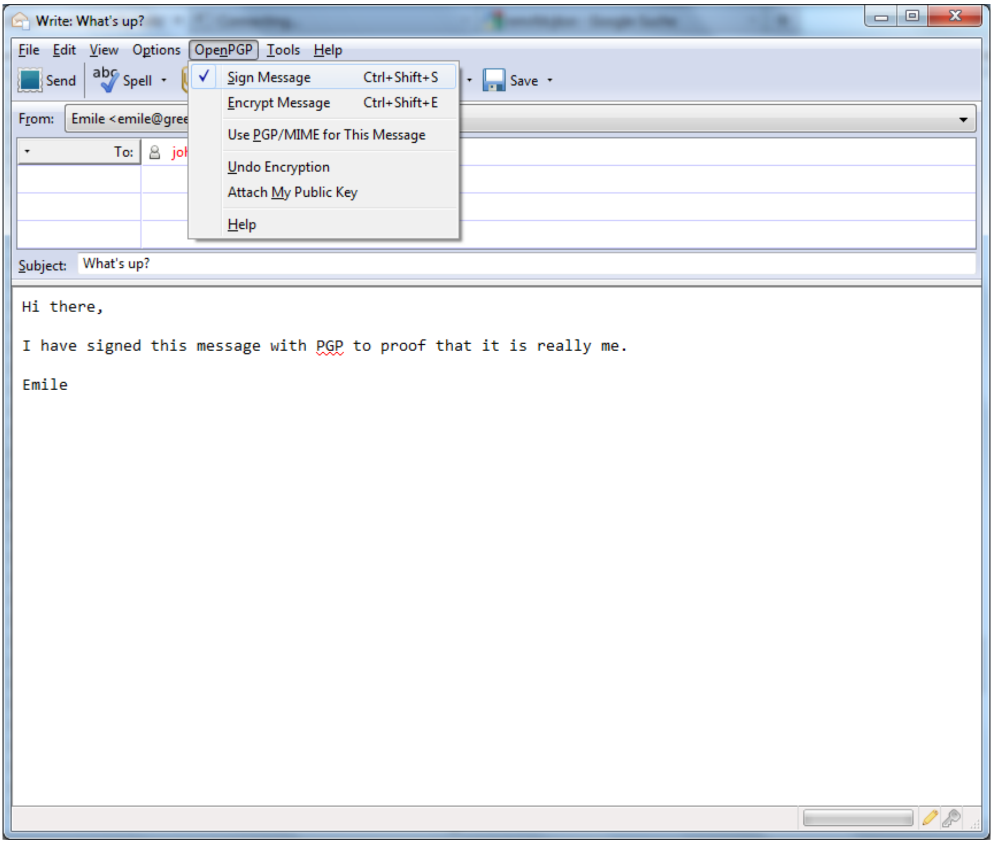
SIGNING EMAILS TO AN INDIVIDUAL

Digitally signing email messages is a way to prove to recipients that you are the actual sender of a mail message. Those recipients who have received your public key will be able to *verify* that your message is authentic.

1. Offer your friend your public key, using the method described earlier in this chapter.

2. In Thunderbird, click on the Write icon.

3. Before actually sending the mail, enable the **OpenPGP > Sign Message** option via the menu bar of the mail compose window, if it is not enable already. Once you have enabled this option, by clicking on it, a marked sign ✓ will appear. Clicking again should disable encryption again. See the example below.



Write: What's up?
File Edit View Options OpenPGP Tools Help
Send
Spell
Save
✓ Sign Message Ctrl+Shift+S
Encrypt Message Ctrl+Shift+E
Use PGP/MIME for This Message
Undo Encryption
Attach My Public Key
Help

From: Emile <emile@gree

To: joh

Subject: What's up?

```
Hi there,

I have signed this message with PGP to proof that it is really me.

Emile
```

5. Click on the Send button and your signed mail will be sent.

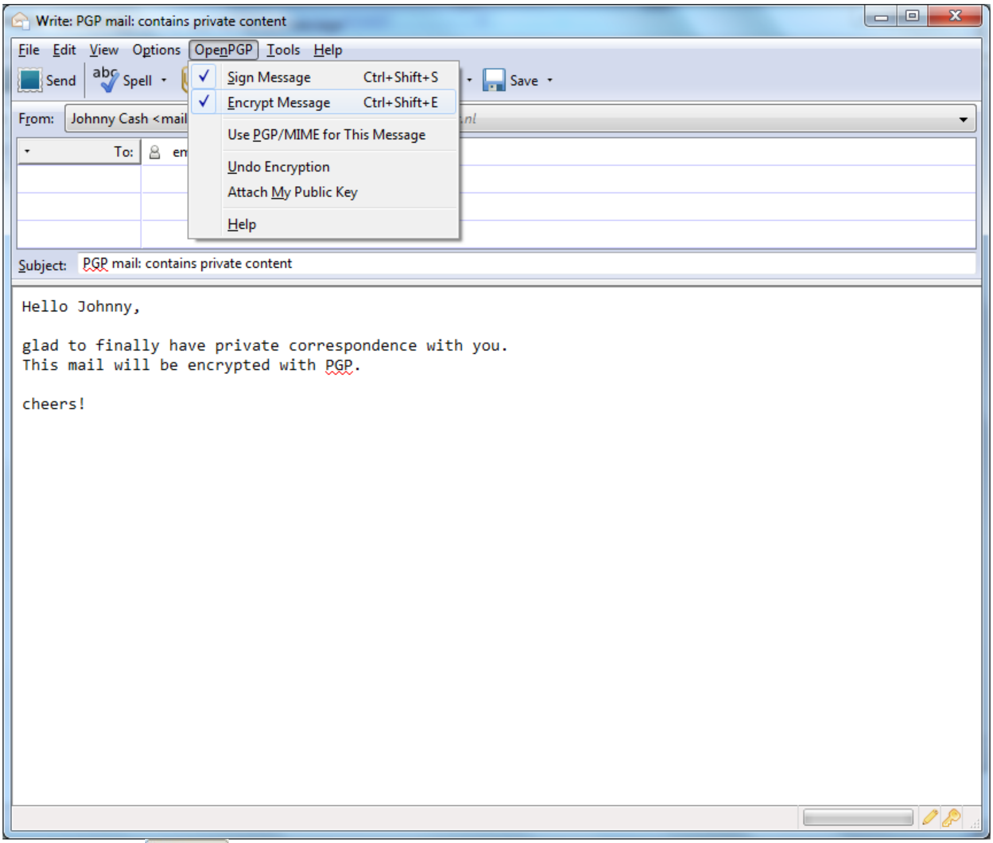
SENDING ENCRYPTED MAILS TO AN INDIVIDUAL

1. You should have received the public key from the friend or colleague you want to email and you should have accepted their public key, using the method describe earlier in this chapter.

2. In Thunderbird, click on the Write icon.

3. Compose a mail to the friend or colleague, from who you have previously received their public key. **Remember the subject line of the message will <u>not</u> be encrypted**, only the message body itself, and any attachments.

4. Before actually sending the mail, enable the **OpenPGP > Encrypt Message** option via the menu bar of the mail compose window, if it is not enabled already. Once you have enabled this option, by clicking on it, a marked sign ✓ will appear. Clicking again should disable encryption again. See the example below.


Write: PGP mail: contains private content
File Edit View Options OpenPGP Tools Help
Send
Spell
Save
✓ Sign Message Ctrl+Shift+S
✓ Encrypt Message Ctrl+Shift+E
Use PGP/MIME for This Message
Undo Encryption
Attach My Public Key
Help
From:
To:

From: Johnny Cash <mail

Subject: PGP mail: contains private content

```
Hello Johnny,

glad to finally have private correspondence with you.
This mail will be encrypted with PGP.

cheers!
```

5. Click on the Send button and your encrypted mail will be sent.

TASK

Follow the instructions above to;

- Send an encrypted and signed email to someone to who you have sent your public key.
- Ask them to check back with you to tell you if they can read it.

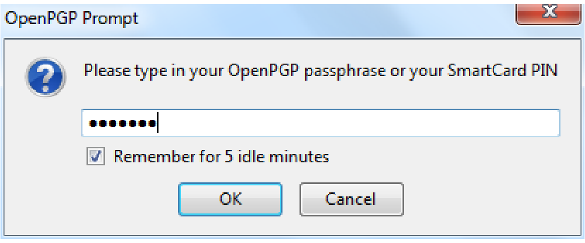
7. RECEIVE ENCRYPTED MAIL

Using Thunderbird and Enigmail to receive encrypted e-mails [5 mins]

The decryption of e-mails is handled automatically by Enigmail, the only action that may be needed on your behalf is to enter the pass-phrase to your secret key. In order to complete this part of the challenge you will need to ask someone you have exchanged keys with to send you an encrypted email.

ENTERING YOUR PASS-PHRASE

For security reasons, the pass-phrase to your secret key is stored temporarily in memory. Every now and then the dialog window below will pop-up. Thunderbird asks you for the pass-phrase to your secret key. This should be different from your normal email password. It was the pass-phrase you have entered when creating your key-pair in the previous chapter. Enter the pass-phrase in the text-box and click on 'OK'


OpenPGP Prompt

Please type in your OpenPGP passphrase or your SmartCard PIN

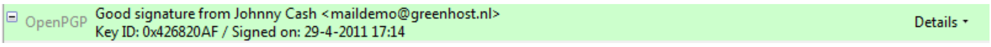
•••••••

☑ Remember for 5 idle minutes

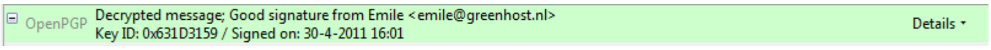
VERIFYING INCOMING E-MAILS

Decrypting email messages sent to you will be fully automatic and transparent. But it is obviously important to see whether or not a message to you *has* in fact been encrypted or signed. This information is available by looking at the special bar above the message body.

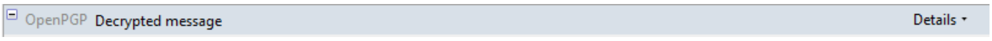
A valid signature will be recognized by a green bar above the mail message like the example image below.


Good signature from Johnny Cash <maildemo@greenhost.nl>
Key ID: 0x426820AF / Signed on: 29-4-2011 17:14

The last example message was signed but *not* encrypted. If the message had been encrypted, it would show like this:

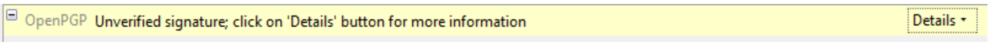

Decrypted message; Good signature from Emile <emile@greenhost.nl>
Key ID: 0x631D3159 / Signed on: 30-4-2011 16:01

When a message which has been encrypted, but *not* signed, it could have been a forgery by someone. The status bar will become gray like in the image below and tells you that while the message was sent securely (encrypted), the sender could have been someone else than the person behind the email address you will see in the 'From' header. The signature is necessary to verify the real sender of the message. Of course it is perfectly possible that you have published your public key on the Internet and you allow people to send you emails anonymously. But is it also possible that someone is trying to impersonate one of your friends.



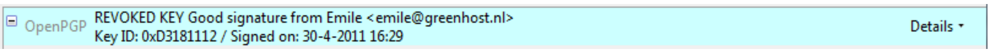
Decrypted message

Similarly if you receive a *signed* email from somebody you know, and you have this persons public key, but still the status bar becomes yellow and displays a warning message, it is likely that someone is attempting to send you forged emails!



Unverified signature; click on 'Details' button for more information

Sometimes secret keys get stolen or lost. The owner of the key will inform his friends and send them a so-called revocation certificate (more explanation of this in the next paragraph). Revocation means that we no longer trust the old key. The thief may afterwards still try his luck and send you a falsely signed mail message. The status bar will now look like this:



REVOKED KEY Good signature from Emile <emile@greenhost.nl>
Key ID: 0xD3181112 / Signed on: 30-4-2011 16:29

Strangely enough Thunderbird in this situation will still display a green status bar! It is important to look at the contents of the status bar in order to understand the encryption aspects of a message. PGP allows for strong security and privacy, but only if you are familiar with its use and concepts. Pay attention to warnings in the status bar.

TASK

Test your learning by following the instructions above to;

- Send them a signed and encrypted email and ask them if it worked

INSTALLING ON WINDOWS

8. INSTALLING THUNDERBIRD ON WINDOWS

Thunderbird runs on Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows 7. Thunderbird will run on a computer with at least the following hardware:

- Pentium 233 MHz. Mozilla recommends Pentium 500 MHz or greater
- Windows 7, Windows Vista, and Windows XP: 768 MB of memory. Mozilla recommends 1 GB of memory or more
- Windows 2000: 256 MB of memory or more
- 52 MB of hard drive space

INSTALLING THUNDERBIRD

Installing Thunderbird involves two steps: first, downloading the software and then running the installation program. Here is how to do that:

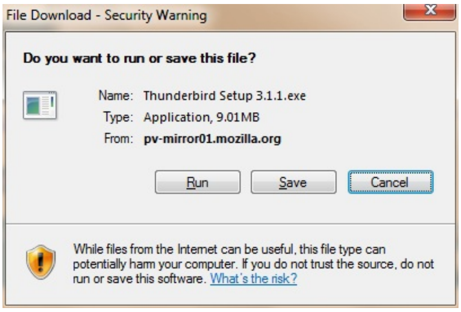
1. Use your web browser to visit the Thunderbird download page at https://www.mozilla.org/en-US/thunderbird/. This page detects your computer's operating system and language, and it recommends the best version of Thunderbird for you to use.

   If you want to use Thunderbird in a different language or with a different operating system, click the *Other Systems and Languages* link and select the version that you need.

2. Click the download button to save the installation program to your computer.

   The web browser displays a message asking you to start the download:

   Internet Explorer 8



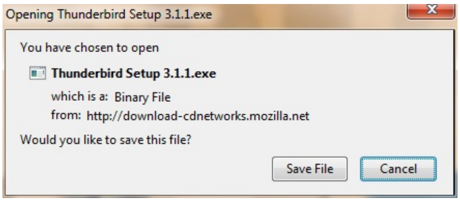
File Download - Security Warning

Do you want to run or save this file?

Name: Thunderbird Setup 3.1.1.exe
Type: Application, 9.01MB
From: pv-mirror01.mozilla.org

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

   Firefox 3.6



Opening Thunderbird Setup 3.1.1.exe

You have chosen to open

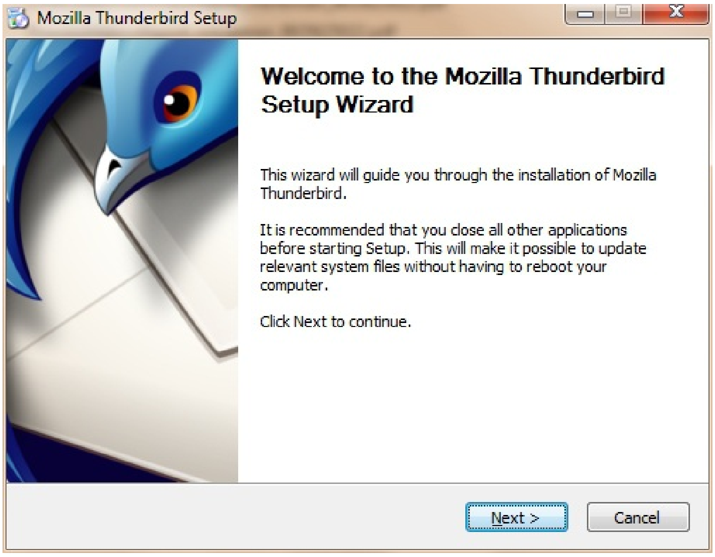
Thunderbird Setup 3.1.1.exe

which is a: Binary File
from: http://download-cdnetworks.mozilla.net

Would you like to save this file?

   Click the **Save** button to save the Thunderbird Setup file to your computer.

3. Close all applications running on your computer.
4. Find the setup file on your computer (it's usually in the Downloads folder) and then double-click it to start the installation. The first thing that the installer does is display the **Welcome to the Mozilla Thunderbird Setup Wizard** screen.



Welcome to the Mozilla Thunderbird Setup Wizard

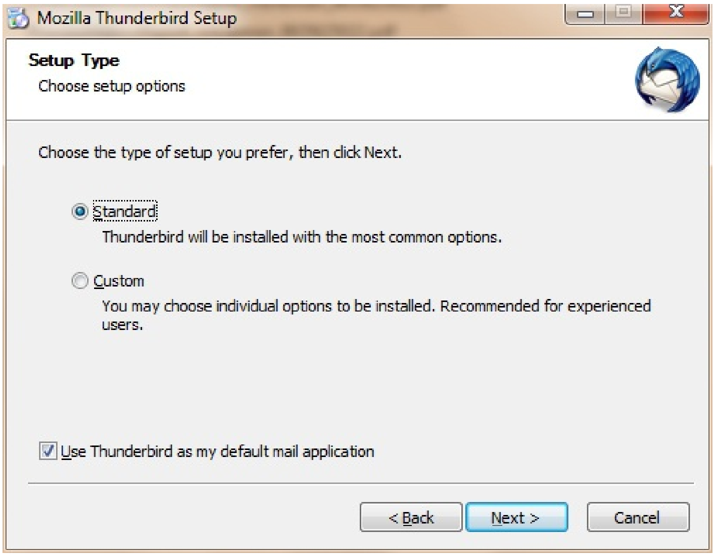
This wizard will guide you through the installation of Mozilla Thunderbird.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Click the **Next** button to start the installation. If you want to cancel it, click the **Cancel** button.

5. The next thing that you see is the **Setup Type** screen. For most users the Standard setup option is good enough for their needs. The Custom setup option is recommended for experienced users only. Note that Thunderbird installs itself as your default mail application. If you do not want this, clear the checkbox labeled **Use Thunderbird as my default mail application**.



Setup Type

Choose setup options

Choose the type of setup you prefer, then click Next.

● Standard

Thunderbird will be installed with the most common options.

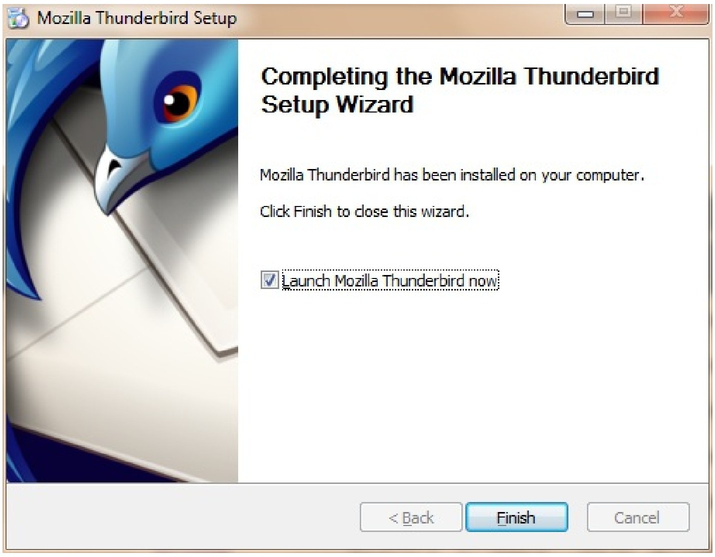
○ Custom

You may choose individual options to be installed. Recommended for experienced users.

☑ Use Thunderbird as my default mail application

Click the **Next** button to continue the installation. The **Back** button takes you to the Welcome screen and the Cancel button stops the installation.

6. After Thunderbird has been installed, click the **Finish** button to close the setup wizard.



Mozilla Thunderbird Setup

Completing the Mozilla Thunderbird Setup Wizard

Mozilla Thunderbird has been installed on your computer.

Click Finish to close this wizard.

☑ Launch Mozilla Thunderbird now

If the **Launch Mozilla Thunderbird now** checkbox is selected, Thunderbird starts after it has been installed.

9. INSTALLING PGP ON WINDOWS

To complicate matters a little - PGP is the protocol used for encrypting e-mail by various softwares. To get PGP to work with Thunderbird we need to install GPG - a free software implementation of PGP *and* Enigmail - an extension of Thunderbird that allows you to use GPG... Confused?! Don't worry about it, all you have to know is how to encrypt your email with PGP and you need to install *both* GPG and Enigmail. Here is how to do it...

INSTALLING PGP (GPG) ON MICROSOFT WINDOWS

The GNU Privacy Guard (GnuPG) is software which is required to send PGP encrypted or signed emails. It is necessary to install this software before being able to do any encryption.

Head to the website of the Gpg4win project. Go to http://gpg4win.org/

On the left side of the website, you will find a 'Download' link. Click on it.

This will take you to a page where you can download the Gpg4Win. Click on the button which offers you the latest stable version (not beta) of Gpg4Win.

This will download you an .exe file. Depending on your browser, you may have to double-click on this downloaded file (which will be called something like gpg4qin-2.1.0.exe) before something happens. Windows will ask you if you are sure you want to install this program. Answer yes.

Then complete the installation by agreeing to the license, choosing appropriate language and accepting the default options by clicking 'Next', unless you have a particular reason not to.

The installer will ask you where to put the application on your computer. The default setting should be fine but make a note of it as we may need this later. Click on 'Next' when you agree.

INSTALLING WITH THE ENIGMAIL EXTENSION

After you have successfully installed the **PGP** software as we described above you are now ready to install the **Enigmail** add-on.

Enigmail is a Thunderbird add-on that lets you protect the privacy of your email conversations. Enigmail is simply an interface that lets you use PGP encryption from within Thunderbird.

Enigmail is based on public-key cryptography. In this method, each individual must generate her/his own personal key pair. The first key is known as the private key. It is protected by a password or passphrase, guarded and never shared with anyone.

The second key is known as the public key. This key can be shared with any of your correspondents. Once you have a correspondent's public key you can begin sending encrypted e-mails to this person. Only she will be able to decrypt and read your emails, because she is the only person who has access to the matching private key.

Similarly, if you send a copy of your own public key to your e-mail contacts and keep the matching private key secret, only you will be able to read encrypted messages from those contacts.

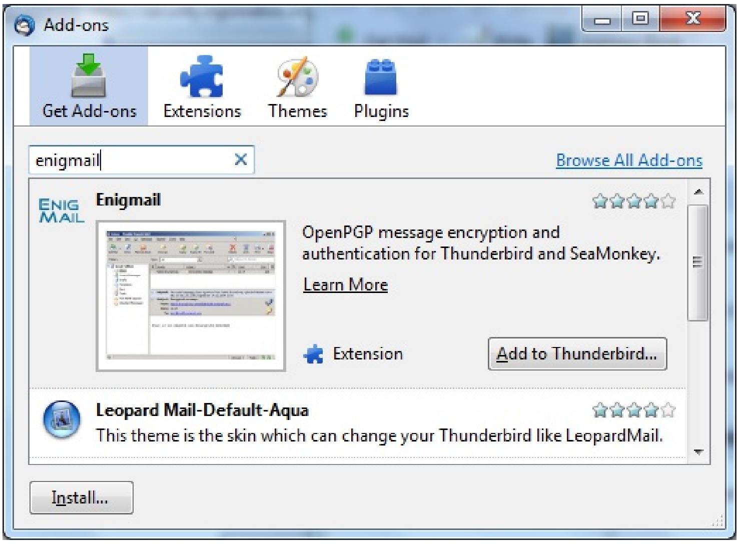
Enigmail also lets you attach digital signatures to your messages. The recipient of your message who has a genuine copy of your public key will be able to verify that the e-mail comes from you, and that its content was not tampered with on the way. Similarly, if you have a correspondent's public key, you can verify the digital signatures on her messages.

INSTALLATION STEPS

To begin installing **Enigmail**, perform the following steps:

Step 1. Open Thunderbird, then **Select Tools > Add-ons** to activate the *Add-ons* window; the *Add-ons* window will appear with the default *Get Add-ons* pane enabled.

Step 2. Enter enigmail in the search bar, like below, and click on the search icon.



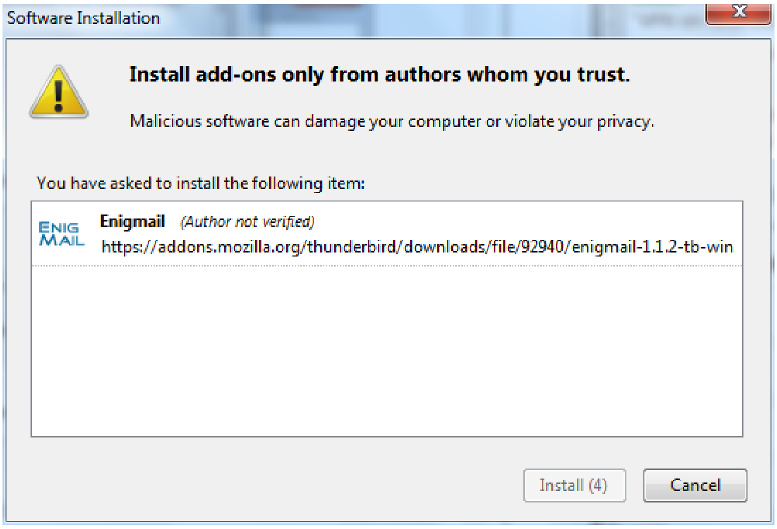
enigmail

OpenPGP message encryption and authentication for Thunderbird and SeaMonkey.

This theme is the skin which can change your Thunderbird like LeopardMail.

Step 3. Simply click on the 'Add to Thunderbird' button to start the installation.

Step 4. Thunderbird will ask you if you are certain you want to install this add-on. We trust this application so we should click on the 'Install now' button.



Software Installation

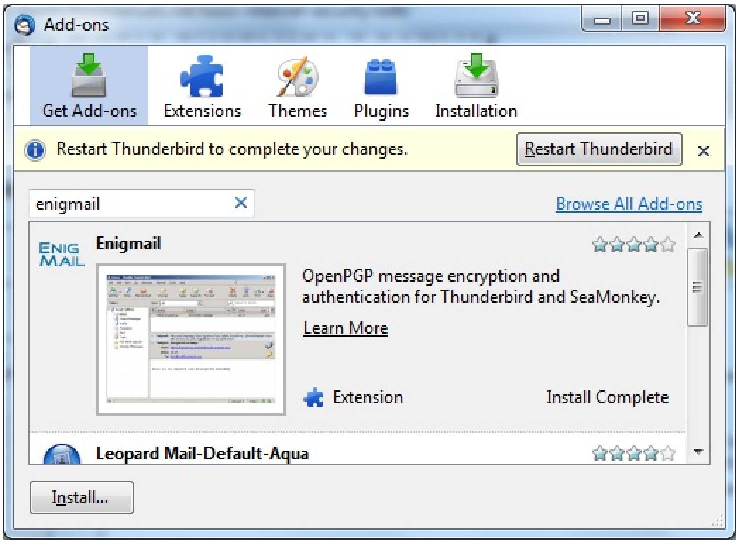
Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:

Enigmail *(Author not verified)*
https://addons.mozilla.org/thunderbird/downloads/file/92940/enigmail-1.1.2-tb-win

Step 5. After some time the installation should be completed and the following window should appear. Please click on the 'Restart Thunderbird' button.



Add-ons

Restart Thunderbird to complete your changes.

enigmail

Enigmail

OpenPGP message encryption and authentication for Thunderbird and SeaMonkey.

Extension Install Complete

Leopard Mail-Default-Aqua

Be aware that you will have to restart Thunderbird to use the functionality of this extension!

TESTING AND TROUBLESHOOTING

To test if this has been successful you can progress to the next part of this challenge and try to generate a keypair. If you get errors when you try to do this then either share them with the person leading this course or post them to the Enigmail forum.[1]

One Common Installation Problem

One common problem when using Windows is that Enigmail can't find the GPG programme. If this is the case you can try to solve this by updating where Enigmail goes to try to find GPG.

In the main window you should go **OpenGPG > Preferences > Advanced** (you may need to tick Expert Settings) and in the **Override With** box browse to the gpg.exe file in the folder where you installed GPG. If this doesn't help then try the Enigmail forum.

1. http://www.mozilla-enigmail.org/forum/^

INSTALLING ON UBUNTU

10. INSTALLING THUNDERBIRD ON UBUNTU

11. INSTALLING PGP ON UBUNTU

10. INSTALLING THUNDERBIRD ON UBUNTU

There are two procedures for installing Thunderbird on Ubuntu: one for version 10.04 or later, and one for earlier versions of Ubuntu. We take a look at both below:

Thunderbird will not run without the following libraries or packages installed on your computer:

- GTK+ 2.10 or higher
- GLib 2.12 or higher
- Pango 1.14 or higher
- X.Org 1.0 or higher

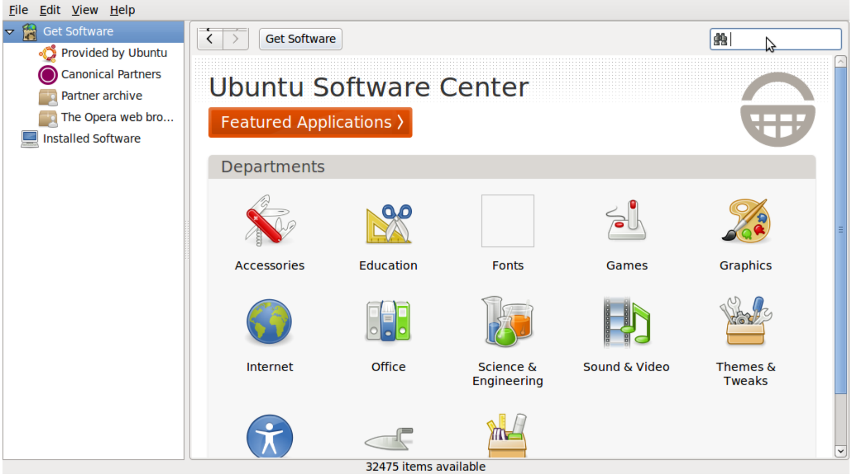
Mozilla recommends that a Linux system also has the following libraries or packages installed:

- NetworkManager 0.7 or higher
- DBus 1.0 or higher
- HAL 0.5.8 or higher
- GNOME 2.16 or higher

INSTALLING THUNDERBIRD ON UBUNTU 10.04 OR NEWER

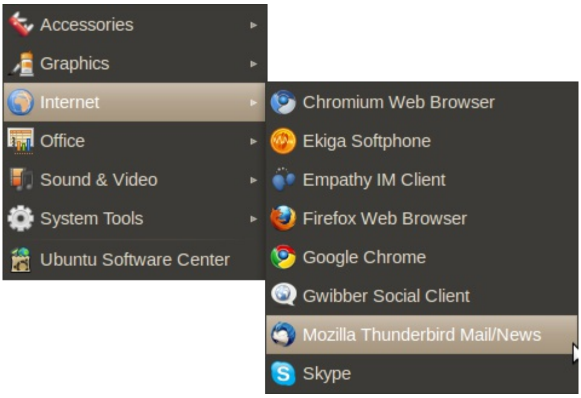
If you're using Ubuntu 10.04 or newer, the easiest way to install Thunderbird is through the Ubuntu Software Center.

1. Click **Ubuntu Software Center** under the Applications menu.



2. Type "Thunderbird" in the search box and press the Enter on your keyboard. The Ubuntu Software Center finds Thunderbird in its list of available software.
3. Click the **Install** button. If Thunderbird needs any additional libraries, the Ubuntu Software Center alerts you and installs them along with Thunderbird.

You can find the shortcut to start Thunderbird in the Internet option under the Applications menu:



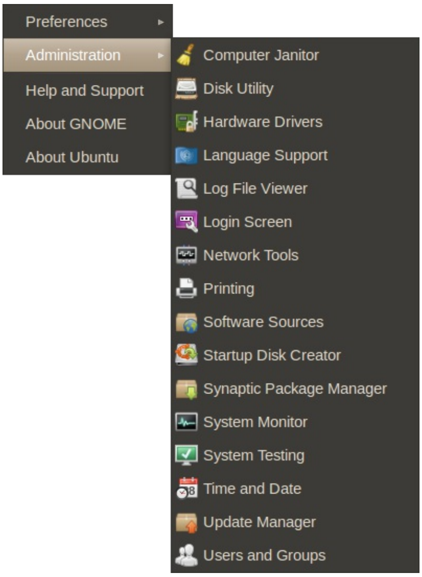
INSTALLING THUNDERBIRD ON OLDER VERSIONS OF UBUNTU

If you are installing Thunderbird under a version of Ubuntu older than 10.04, you can do it with either

the Ubuntuzilla package or with Synaptic Package Manager. You can get more information about Ubuntuzilla here: http://sourceforge.net/apps/mediawiki/ubuntuzilla/index.php.

To install Thunderbird using the Synaptic Package Manager

1. Click **Administration** under the System menu, then click **Synaptic Package Manager**.



2. You'll be asked to enter your root password. This is the password that you use to log into Ubuntu.
3. In the Quick search box, type "Thunderbird" and then press Enter on your keyboard.
   A list of software that you can install (called *packages*) appears.
4. Find Thunderbird in the list, right click on it, and then click on **Mark for installation** from the menu that appears.
5. If Thunderbird needs any additional libraries, Synaptic Package Manager alerts you and marks those packages for installation along with Thunderbird.
6. Click the **Apply** button.

INSTALLING FROM A PERSONAL PACKAGE ARCHIVE

If you want to stay on the cutting edge of Thunderbird, you can install it from a Personal Package Archive (PPA). A PPA is special repository for Ubuntu software that's separate from ones you would normally use either with the Ubuntu Software Center or Synaptic Package Manager. A PPA contains more frequent updates to software -- updates which are often created nightly.

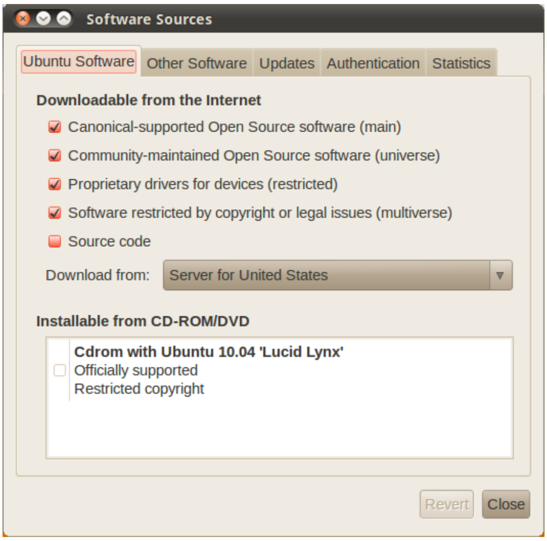
Remember that the software that you get from a PPA is 'cutting edge'. It may be buggy or unstable. Use it at your own risk.

To install Thunderbird from a PPA

1. Go to the Mozilla PPA at https://launchpad.net/~ubuntu-mozilla-daily/+archive/ppa.
2. At the Mozilla PPA site, select your version of Ubuntu from the **Display sources.list entries for:** list. Two lines, which look like the following, appear below the list:

   deb http://ppa.launchpad.net/ubuntu-mozilla-daily/ppa/ubuntu maverick main
   deb-src http://ppa.launchpad.net/ubuntu-mozilla-daily/ppa/ubuntu maverick main

3. In Ubuntu, click **Administration** under the System Menu and then click **Software Sources**.
4. You'll be asked to enter your root password. This is the password that you use to log into Ubuntu. The Software Sources window appears.



Downloadable from the Internet

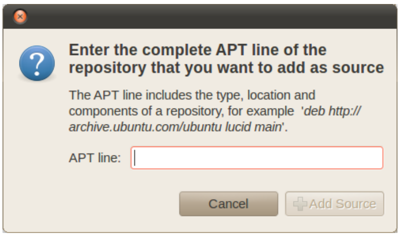
☑ Canonical-supported Open Source software (main)
☑ Community-maintained Open Source software (universe)
☑ Proprietary drivers for devices (restricted)
☑ Software restricted by copyright or legal issues (multiverse)
□ Source code

Download from: Server for United States

Installable from CD-ROM/DVD

□ Cdrom with Ubuntu 10.04 'Lucid Lynx'
Officially supported
Restricted copyright

5. In the Software Sources window, click the **Other Software** tab and then click **Add**.



Enter the complete APT line of the repository that you want to add as source

The APT line includes the type, location and components of a repository, for example *'deb http://archive.ubuntu.com/ubuntu lucid main'*.

APT line:

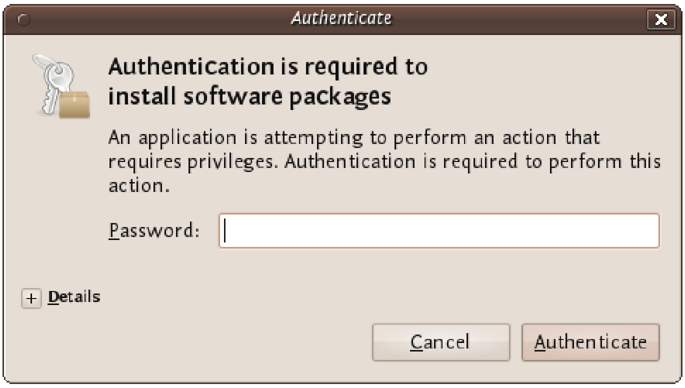
6. Copy the first line from list of sources that you created in step 2, paste it into the **APT Line** field, and then click **Add Source**.
7. Repeat steps 5 and 6 for the second line from list of sources that you created in step 2.
8. In the Software Sources window, click **Close**. Ubuntu will update the list of software sources that it uses.
9. Once that's done, you can install Thunderbird using Synaptic Package Manager.

11. INSTALLING PGP ON UBUNTU

We will use the Ubuntu Software Centre for installing PGP (Enigmail and accessories). First open the Ubuntu Software Center through Applications -> Ubuntu Software Center:

Type into the search field 'Enigmail' and search results should be returned automatically:

Highlight the Enigmail item (it should be highlighted by default) and click 'Install' and you will be asked to authenticate the installation process.



Authentication is required to install software packages

An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

Password:

Enter your password and click 'Authenticate'. The installation process will begin.

When the process is completed you get very little feedback from Ubuntu. The progress bar at the top left disappears. The 'In Progress' text on the right also disappears. Enigmail should now be installed.

INSTALLING ON OSX

12. INSTALLING THUNDERBIRD ON MAC OS X

Thunderbird runs on Mac OS X 10.4.x and later. Thunderbird will run on a computer with at least the following hardware:

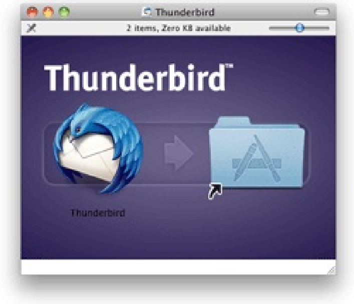
- An Intel x86 or PowerPC G3, G4, or G5 processor
- 256 MB of memory. Mozilla recommends 512 MB of memory or more
- 200 MB hard drive space

DOWNLOAD AND INSTALL THUNDERBIRD

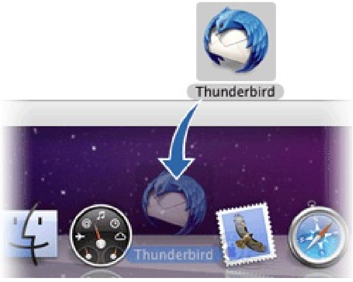
1. Use your web browser to visit the Thunderbird download page at https://www.mozilla.org/en-US/thunderbird/. This page detects your computer's operating system and language, and it recommends the best version of Thunderbird for you to use.

   If you want to use Thunderbird in a different languages or with a different operating system, click the *Other Systems and Languages* link on the right side of the page and select the version you need.

2. Download the Thunderbird disk image. When the download is complete, the disc image may automatically open and mount a new volume called *Thunderbird*.
   If the volume did not mount automatically, open the Download folder and double-click the disk image to mount it. A Finder window appears:

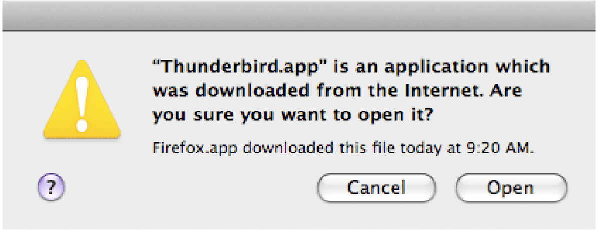


3. Drag the Thunderbird icon into your Applications folder. You've installed Thunderbird!
4. Optionally, drag the Thunderbird icon from the Applications folder into the Dock. Choosing the Thunderbird icon from the Dock lets you quickly open Thunderbird from there.



Note: When you run Thunderbird for the first time, newer versions of Mac OS X (10.5 or later) will warn you that the application Thunderbird.app was downloaded from the Internet.

If you downloaded Thunderbird from the Mozilla site, click the **Open** button.



"Thunderbird.app" is an application which was downloaded from the Internet. Are you sure you want to open it?

Firefox.app downloaded this file today at 9:20 AM.

13. INSTALLING PGP ON OSX

The GNU Privacy Guard (GnuPG) is software which enables you to send PGP encrypted or signed emails. It is necessary to install this software before being able to do any encryption. This chapter covers the installation steps required to install GnuPG on Mac OSX.

Getting started

For this chapter we assume you have the latest version of:

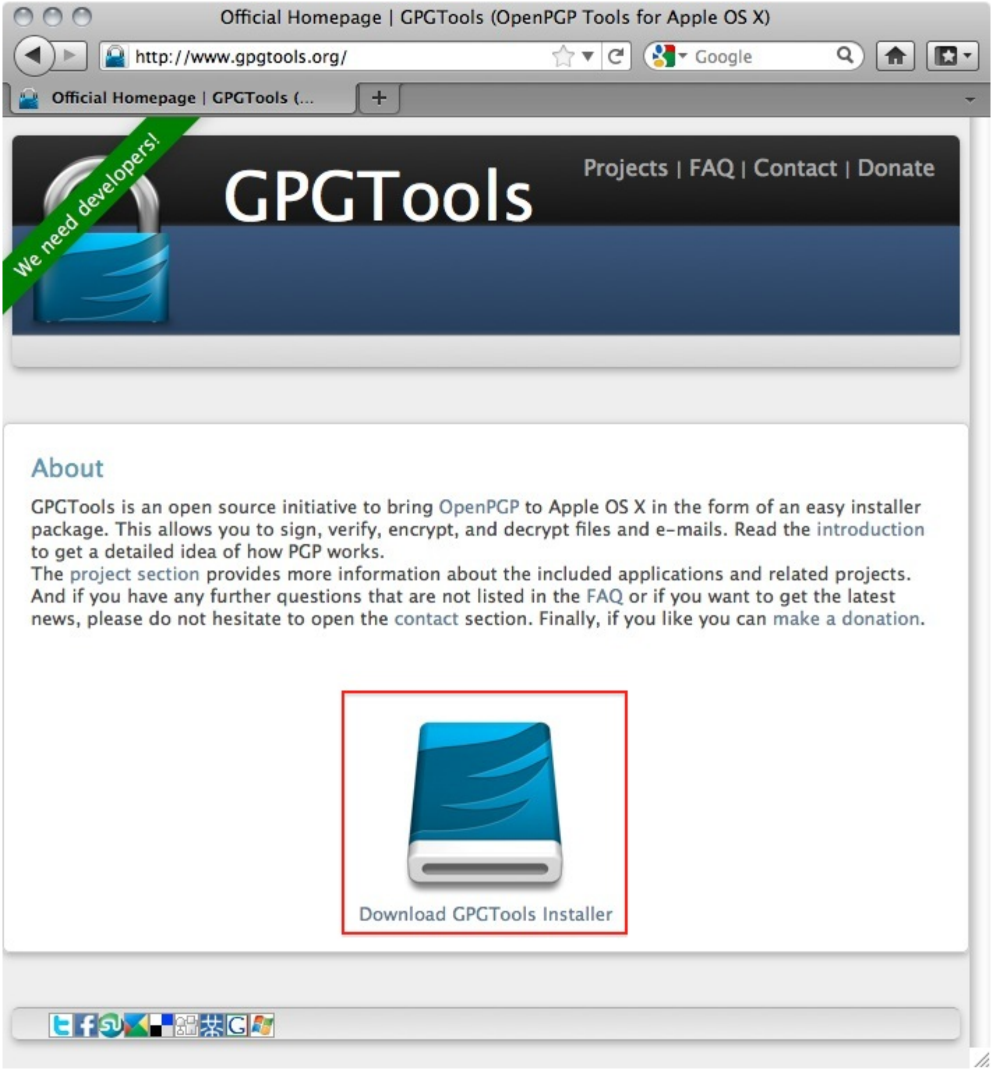
- OSX installed (10.6.7)
- Thunderbird (3.1.10)

Note on OSX Mail: It is possible to use PGP with the build-in mail program of OSX. But we do not recommend this because this option relies on a hack of the program which is neither open or supported by its developer and breaks with every update of the mail program. So unless you really have no other option we advice you to switch to Mozilla Thunderbird as your default mail program if you want to use PGP.

DOWNLOADING AND INSTALLING THE SOFTWARE

For OSX there is a bundle available which will install everything you need in one installation. You can get it by directing your browser to http://www.gpgtools.org/ and clicking on the big blue disk with "Download GPGTools Installer" written under it. It will redirect you to another page on http://www.gpgtools.org/installer/index.html where you can actually download the software.

(*nb. We are using the latest version Firefox for this manual, so the screens might look a little bit different if you are using a different browser*)

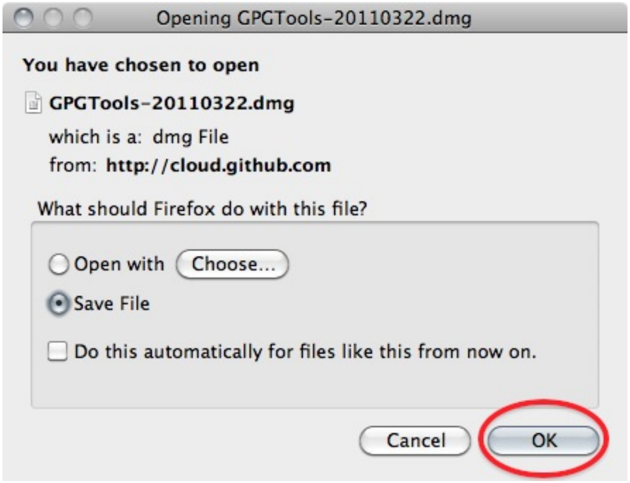


Official Homepage | GPGTools (OpenPGP Tools for Apple OS X)
http://www.gpgtools.org/
Google
Official Homepage | GPGTools (...
We need developers!
GPGTools
Projects | FAQ | Contact | Donate

About

GPGTools is an open source initiative to bring OpenPGP to Apple OS X in the form of an easy installer package. This allows you to sign, verify, encrypt, and decrypt files and e-mails. Read the introduction to get a detailed idea of how PGP works.
The project section provides more information about the included applications and related projects. And if you have any further questions that are not listed in the FAQ or if you want to get the latest news, please do not hesitate to open the contact section. Finally, if you like you can make a donation.

2. Download the software by choosing 'Save File' and clicking 'OK' in the dialogue.



Opening GPGTools-20110322.dmg

You have chosen to open

GPGTools-20110322.dmg

which is a: dmg File

from: **http://cloud.github.com**

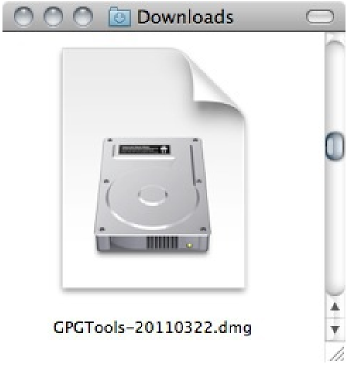
What should Firefox do with this file?

○ Open with Choose...

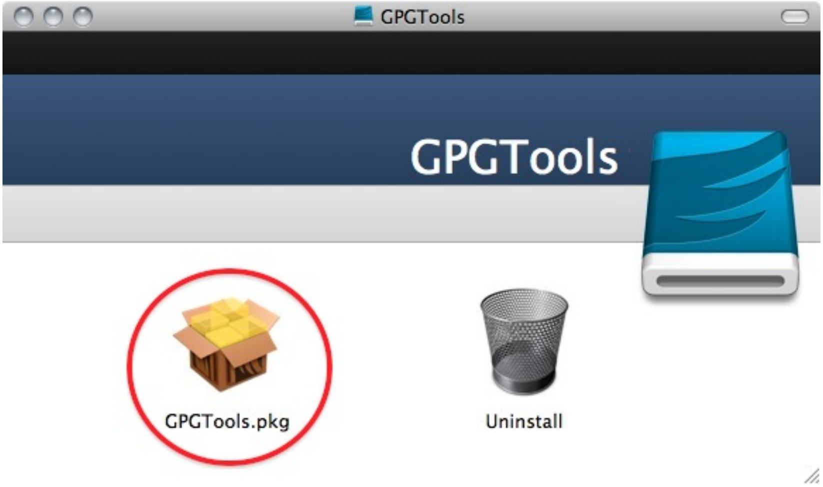
● Save File

□ Do this automatically for files like this from now on.

3. Navigate to the folder where you normally store your downloads (Mostly the desktop or the downloads folder surprisingly) en double click the '.DMG' file to open the virtual disk containing the installer.

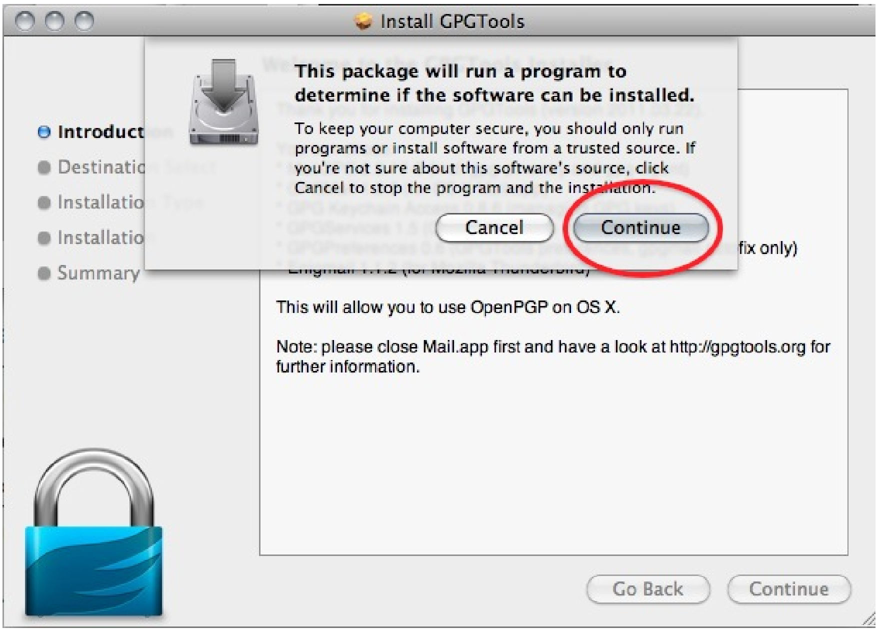


4. Open the installer by double-clicking on the icon.



5. The program will check your computer to see if it can run on the computer.

> *(Note, if you're Mac is bought before 2006 it will not have an intel processor required to run this software and the installation will fail. Sadly it is beyond the scope op this manual to also take into account computers over five year old)*



This package will run a program to determine if the software can be installed.

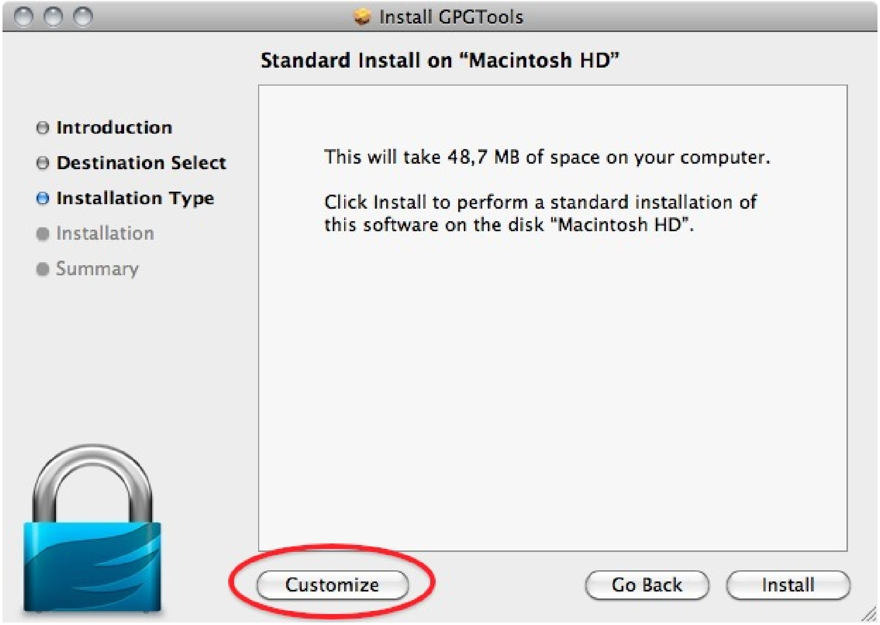
To keep your computer secure, you should only run programs or install software from a trusted source. If you're not sure about this software's source, click Cancel to stop the program and the installation.

fix only)

This will allow you to use OpenPGP on OS X.

Note: please close Mail.app first and have a look at http://gpgtools.org for further information.

You will be guided by the program through the next steps like accepting the license agreement. But stop pressing all the OK's and Agrees as soon as you come to the 'Installation Type' screen:

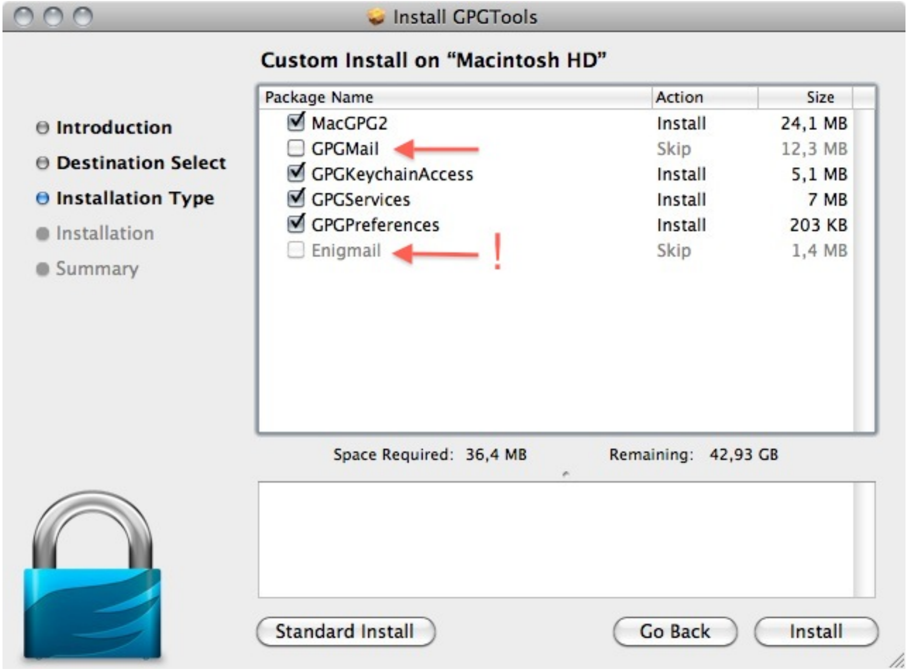


Standard Install on "Macintosh HD"

This will take 48,7 MB of space on your computer.

Click Install to perform a standard installation of this software on the disk "Macintosh HD".

6. Clicking 'Customize' will open this screen where you several options of programs and software to install. You can click on each one of them to get a little bit of information on what is is, what it does and why you might need it.



Custom Install on “Macintosh HD”

Package Name	Action	Size
☑ MacGPG2	Install	24,1 MB
□ GPGMail	Skip	12,3 MB
☑ GPGKeychainAccess	Install	5,1 MB
☑ GPGServices	Install	7 MB
☑ GPGPreferences	Install	203 KB
□ Enigmail	Skip	1,4 MB

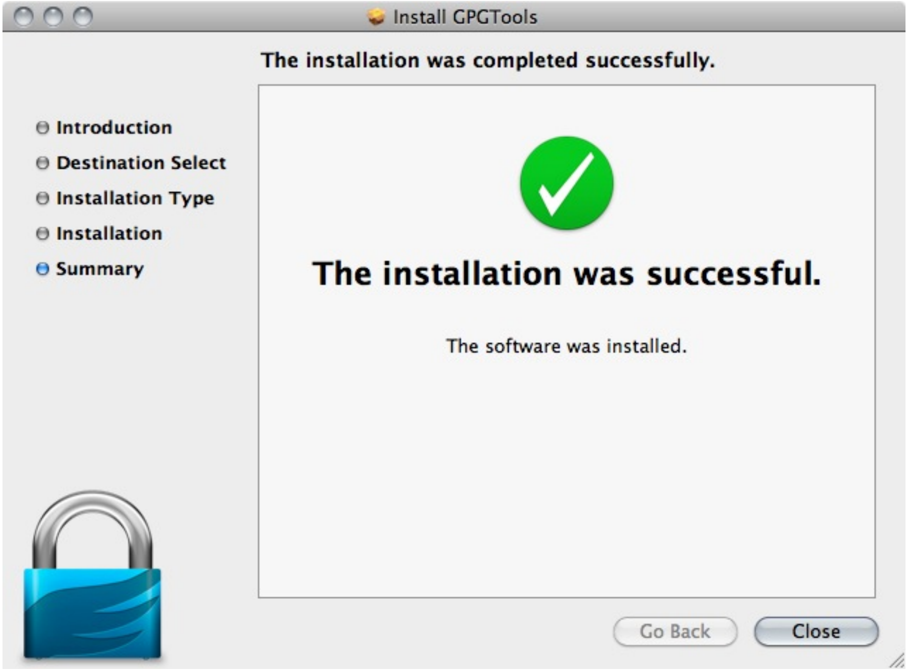
Space Required: 36,4 MB   Remaining: 42,93 GB

As said in the intro; we advice against using Apple Mail in combination with PGP. Therefore you won't be needing 'GPGMail', as this enables PGP on Apple Mail, and you can uncheck it.

'**Enigmail**' on the other hand is very important as it is the component that will enable Thunderbird to use PGP. In the screen shot here it is greyed out as the installer wasn't able to identify my installation of Thunderbird. Since this seems to be a bug. You can also install Enigmail from within Thunderbird as is explained in another chapter.

If the option is not greyed out in your installation, you should tick it.

After you checked all the components you want to install click 'Install' to proceed. The installer will ask you for your password and after you enter that the installation will run and complete; Hooray!



Install GPGTools

The installation was completed successfully.

The installation was successful.

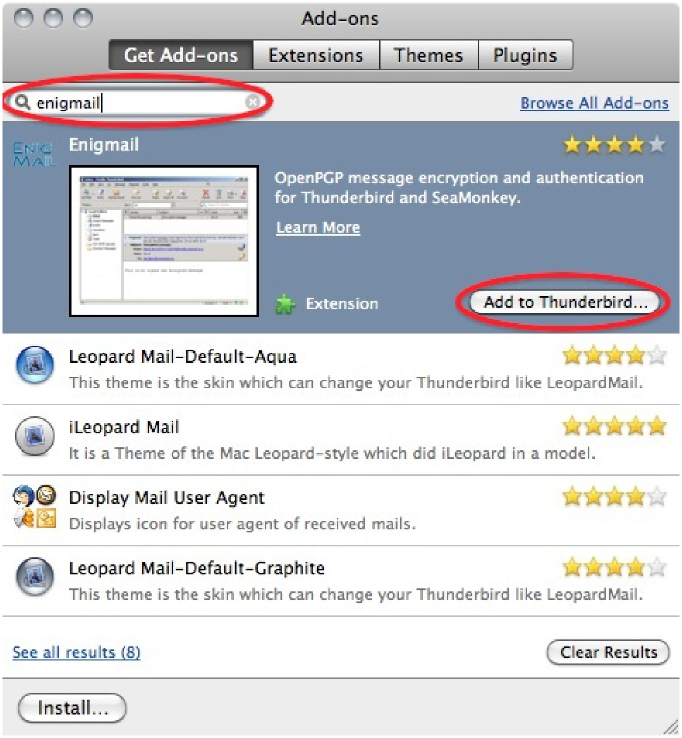
The software was installed.

INSTALLING UP ENGIMAIL

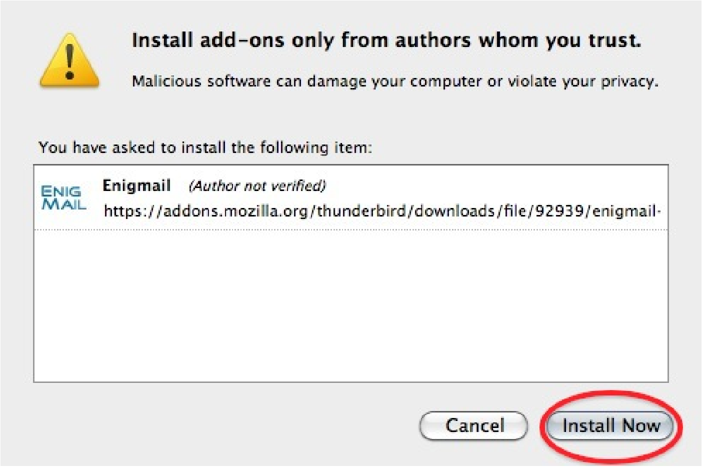
Step 1. **Open Thunderbird**, then **Select Tools > Add-ons** to activate the *Add-ons* window; the *Add-ons* window will appear with the default *Get Add-ons* pane enabled.

In the Add-On window, you can search for 'Enigmail' and install the extension by clicking 'Add to Thunderbird ...'

2. After you open the Add-On window, you can search for 'Enigmail' and install the extension by clicking 'Add to Thunderbird ...'


Add-ons
Get Add-ons
Extensions
Themes
Plugins
enigmail
Browse All Add-ons
Enigmail
OpenPGP message encryption and authentication for Thunderbird and SeaMonkey.
Learn More
Extension
Add to Thunderbird...
Leopard Mail-Default-Aqua
This theme is the skin which can change your Thunderbird like LeopardMail.
iLeopard Mail
It is a Theme of the Mac Leopard-style which did iLeopard in a model.
Display Mail User Agent
Displays icon for user agent of received mails.
Leopard Mail-Default-Graphite
This theme is the skin which can change your Thunderbird like LeopardMail.
See all results (8)
Clear Results
Install...

3. Click on 'Install Now' to download and install the extension.


Install add-ons only from authors whom you trust.
Malicious software can damage your computer or violate your privacy.
You have asked to install the following item:
Enigmail (Author not verified)
https://addons.mozilla.org/thunderbird/downloads/file/92939/enigmail-
Cancel
Install Now

Be aware that you will have to restart Thunderbird to use the functionality of this extension!

TESTING AND TROUBLESHOOTING

To test if this has been successful you can progress to the next part of this challenge and try to generate a keypair. If you get errors when you try to do this then either share them with the person leading this course or post them to the Enigmail forum.[1]

One Common Installation Problem

One common problem when using Mac OSX is that Enigmail can't find the GPG programme. If this is the case you can try to solve this by updating where Enigmail goes to try to find GPG.

In the main window you should go **OpenGPG > Preferences > Advanced** (you may need to tick Expert Settings) and in the **Override With** box browse to the gpg.exe file in the folder where you installed GPG. If this doesn't help then try the Enigmail forum.

1. http://www.mozilla-enigmail.org/forum/^

SET UP AN ACCOUNT

14. ACCOUNT SETUP

14. ACCOUNT SETUP

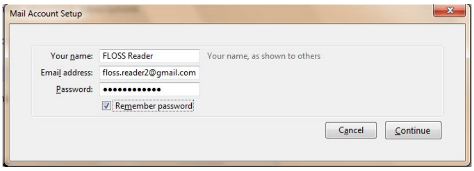
There are two way to create new email accounts in Thunderbird. The first way is an automated process that guides you through the set up routine. The second is manual, where you enter all of the account information yourself. Let's take a look at both.

AUTOMATED SETUP

The automated setup process runs the first time that you start Thunderbird. Remember that you can also run the setup at anytime by going to the **File** menu, pointing at **New**, and clicking **Mail Account**.

Here's how to work your way through the automated setup process:

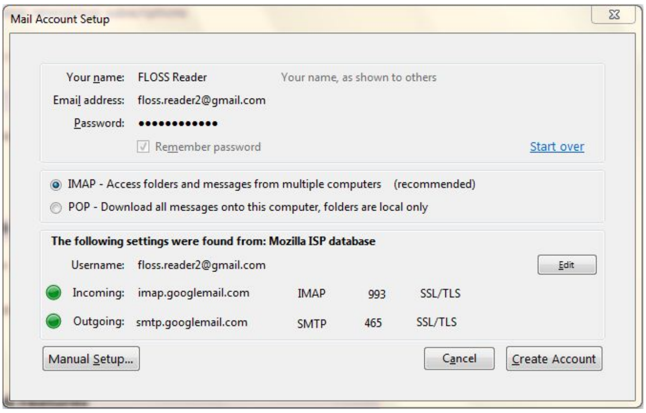
1. Make sure that your computer is connected to the Internet and then start Thunderbird.
2. On the first setup screen, enter your name, your email address, your password. Your password is your current email password. If you want Thunderbird to remember your password (so you don't need to keep typing it every time you check your mail), click the **Remember password** checkbox.



Your name: FLOSS Reader Your name, as shown to others
Email address: floss.reader2@gmail.com
Password: ••••••••••••
☑ Remember password

3. Click the **Continue** button to go to the next step. Click the **Cancel** button to stop the set up process.
4. Thunderbird tries to get your account settings by connecting to the database of Internet Service Providers (ISPs) that is maintained by Mozilla.

   If Thunderbird finds the information for your email provider it automatically enters that information for you. Click the **Create Account** button to add the account. Click the **Cancel** button to stop the set up process.



Your name: FLOSS Reader Your name, as shown to others
Email address: floss.reader2@gmail.com
Password: ••••••••••••
☑ Remember password

● IMAP - Access folders and messages from multiple computers (recommended)
○ POP - Download all messages onto this computer, folders are local only

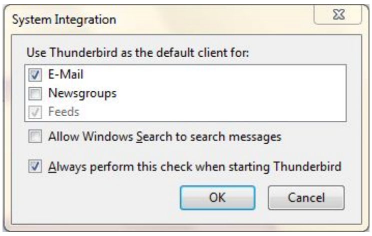
The following settings were found from: Mozilla ISP database

Username: floss.reader2@gmail.com

●	Incoming: imap.googlemail.com	IMAP	993	SSL/TLS
●	Outgoing: smtp.googlemail.com	SMTP	465	SSL/TLS

5. If Thunderbird cannot find information for your email provider, click the **Manual config** button in the Mail Account Setup window. For more information on what to do, read the *Manual Set Up* section below.
6. Once your account is created, Thunderbird asks you if you want it to be the default application for email, newsgroups, or feeds. Make your choices by clicking the checkboxes.

   If you use Microsoft Windows, you use the Windows Search feature to find messages. Do this by selecting the **Allow Windows to search messages** checkbox. Click the **OK** button to save the settings and the **Cancel** button to leave them unchanged.



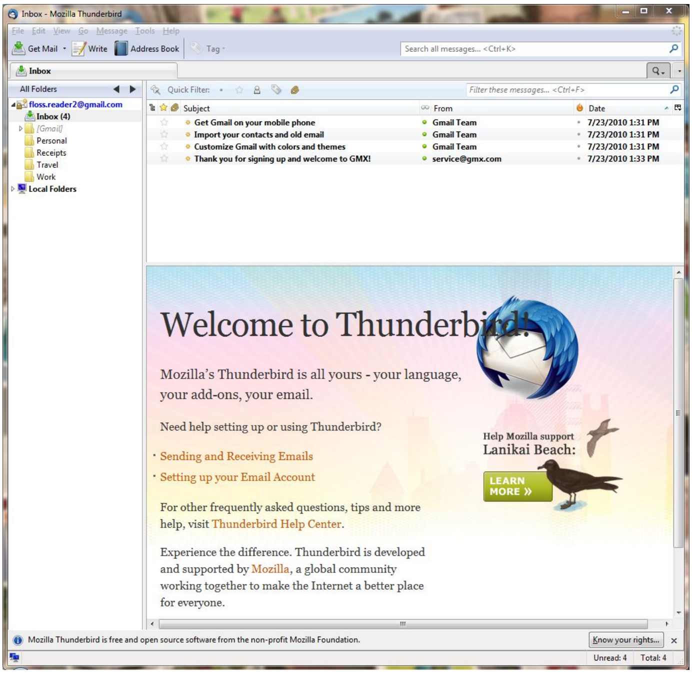
Use Thunderbird as the default client for:
☑ E-Mail
☐ Newsgroups
☑ Feeds

☐ Allow Windows Search to search messages

☑ Always perform this check when starting Thunderbird

Note: Thunderbird will create your account even if you click **Cancel** at this point.

7. Your account has been created and you're ready to go!



Subject	From	Date
Get Gmail on your mobile phone	Gmail Team	7/23/2010 1:31 PM
Import your contacts and old email	Gmail Team	7/23/2010 1:31 PM
Customize Gmail with colors and themes	Gmail Team	7/23/2010 1:31 PM
Thank you for signing up and welcome to GMX!	service@gmx.com	7/23/2010 1:33 PM

Welcome to Thunderbird!

Mozilla's Thunderbird is all yours - your language, your add-ons, your email.

Need help setting up or using Thunderbird?

- Sending and Receiving Emails
- Setting up your Email Account

For other frequently asked questions, tips and more help, visit Thunderbird Help Center.

Experience the difference. Thunderbird is developed and supported by Mozilla, a global community working together to make the Internet a better place for everyone.

Help Mozilla support Lanikai Beach:

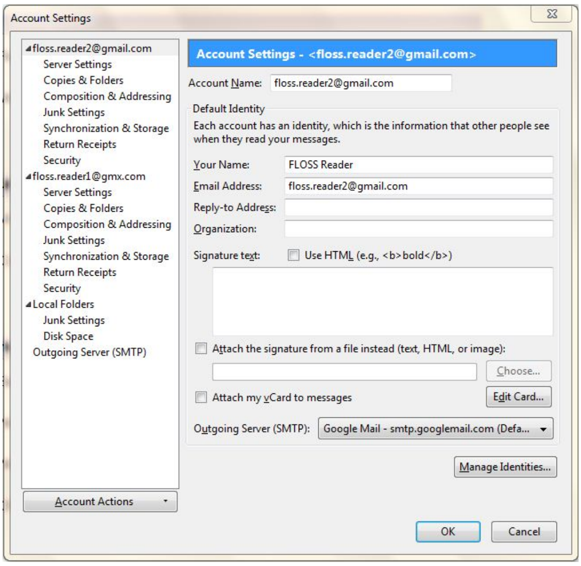
Mozilla Thunderbird is free and open source software from the non-profit Mozilla Foundation.

8. Repeat this process for as many accounts as you want to add to Thunderbird.

MANUAL SET UP

If the automated set up process does not work or if the database of ISPs that Mozilla maintains doesn't contain information about your email provider, you can set up your account manually. Your email provider should supply you with the information that you'll to set up an account. You can usually find this information on your email provider's website, or by contacting their technical support department.

1. Go to the **Tools** menu and click **Account Settings** to open the Account Settings screen.



Account Settings - <floss.reader2@gmail.com>

Account Name: floss.reader2@gmail.com

Default Identity

Each account has an identity, which is the information that other people see when they read your messages.

Your Name: FLOSS Reader

Email Address: floss.reader2@gmail.com

Reply-to Address:

Organization:

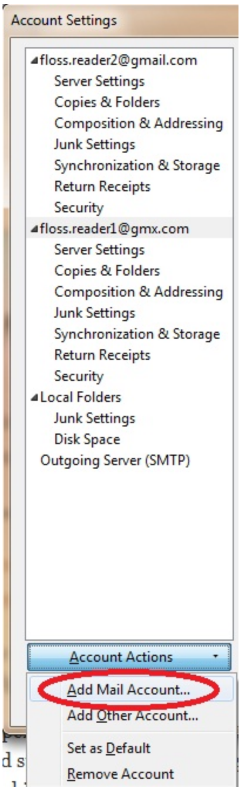
Signature text: □ Use HTML (e.g., <b>bold</b>)

□ Attach the signature from a file instead (text, HTML, or image):

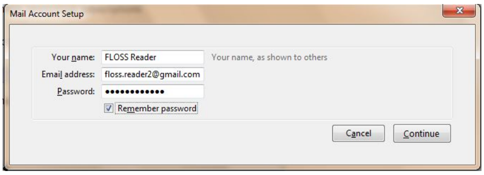
□ Attach my vCard to messages

Outgoing Server (SMTP): Google Mail - smtp.googlemail.com (Defa...

2. Go to Account Actions and click **Add Mail Account**.



3. Thunderbird tries to use the automated process to create your account.


Mail Account Setup

Your name: FLOSS Reader — Your name, as shown to others

Email address: floss.reader2@gmail.com

Password: ••••••••••••

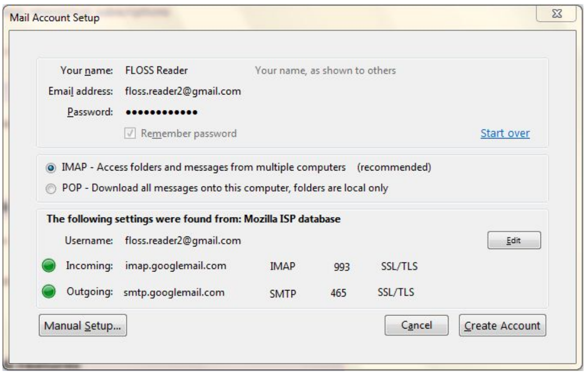
☑ Remember password

Enter your name, your email address, and email password and then click the **Continue** button.

4. Thunderbird will attempt to use database of Internet Service Providers (ISPs) that is maintained by Mozilla to get the account settings. You can stop this process by clicking the **Stop** button.

   At this point, click the **Stop** button to start creating the account manually:

   - Click **POP or IMAP** in the **Incoming** row. You won't be able to change from POP to IMAP or IMAP to POP after you have clicked **Manual Setup** so please double check that you have selected POP or IMAP as appropriate!
   - Click the **Manual Config** button.


Mail Account Setup

Your name: FLOSS Reader — Your name, as shown to others

Email address: floss.reader2@gmail.com

Password: ••••••••••••

☑ Remember password

● IMAP - Access folders and messages from multiple computers (recommended)

○ POP - Download all messages onto this computer, folders are local only

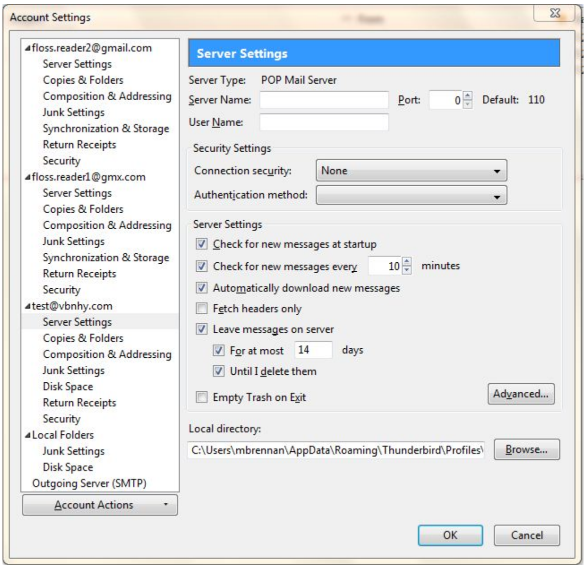
The following settings were found from: Mozilla ISP database

Username: floss.reader2@gmail.com

Incoming: imap.googlemail.com IMAP 993 SSL/TLS

Outgoing: smtp.googlemail.com SMTP 465 SSL/TLS

5. The Account Settings screen will open for your new account. The screen contains your account name, your name, and your email address.
6. Click **Server Settings** to configure your account to receive email.


Account Settings

Server Settings

Server Type: POP Mail Server

Server Name: Port: 0 Default: 110

User Name:

Security Settings

Connection security: None

Authentication method:

Server Settings

☑ Check for new messages at startup

☑ Check for new messages every 10 minutes

☑ Automatically download new messages

□ Fetch headers only

☑ Leave messages on server

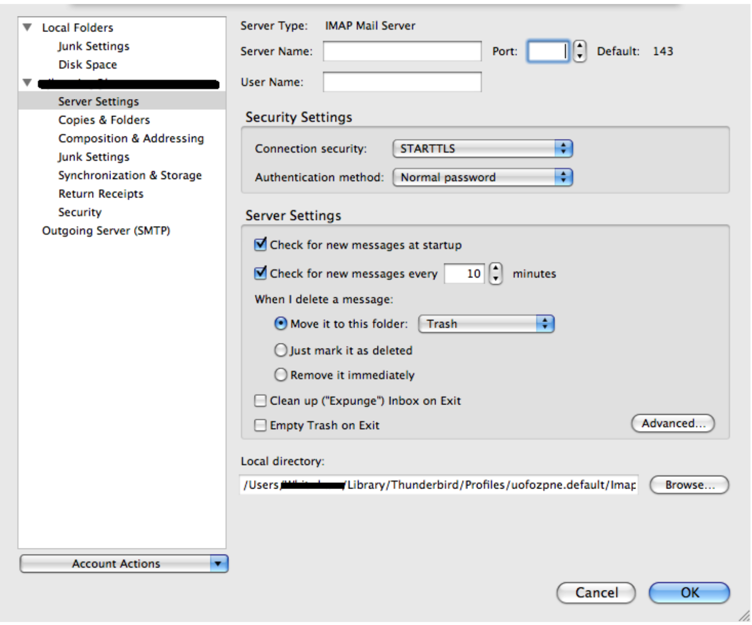
☑ For at most 14 days

☑ Until I delete them

□ Empty Trash on Exit

Local directory: C:\Users\mbrennan\AppData\Roaming\Thunderbird\Profiles\

The IMAP and POP screens look slightly different than the Windows screens. For more information on IMAP and POP, read this short Gmail help article: https://mail.google.com/support/bin/static.py?page=ts.cs&ts=1668960



Server Type: IMAP Mail Server

Server Name: Port: Default: 143

User Name:

Security Settings

Connection security: STARTTLS

Authentication method: Normal password

Server Settings

☑ Check for new messages at startup

☑ Check for new messages every 10 minutes

When I delete a message:

● Move it to this folder: Trash

○ Just mark it as deleted

○ Remove it immediately

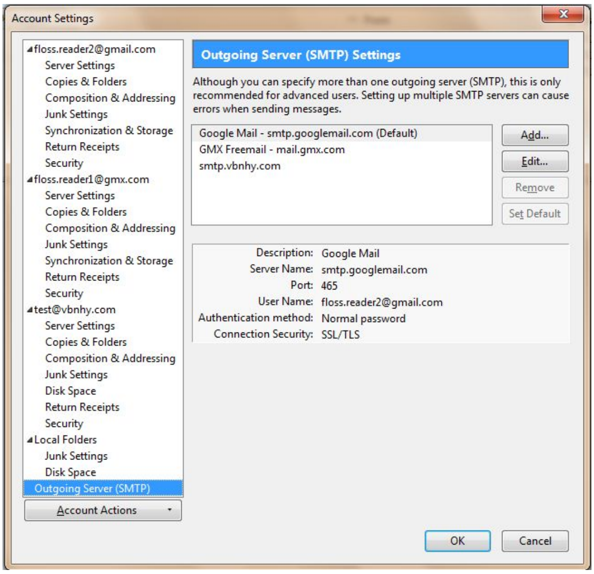
☐ Clean up ("Expunge") Inbox on Exit

☐ Empty Trash on Exit

Local directory:

/Users/[redacted]/Library/Thunderbird/Profiles/uofozpne.default/Imap

7. Enter the following settings for your email provider:
   - Server Name
   - User Name
   - Port
   - Security Settings
8. Click **Outgoing Server (SMTP)** to setup the account to send email.



Outgoing Server (SMTP) Settings

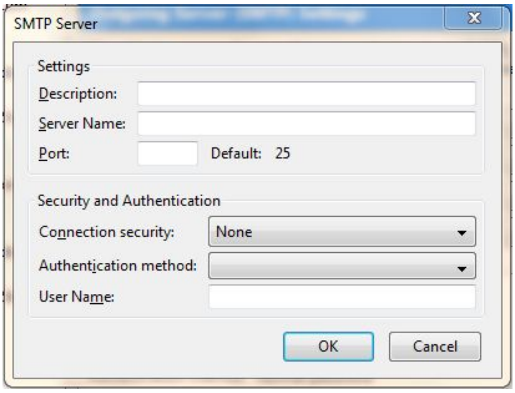
Although you can specify more than one outgoing server (SMTP), this is only recommended for advanced users. Setting up multiple SMTP servers can cause errors when sending messages.

Google Mail - smtp.googlemail.com (Default)
GMX Freemail - mail.gmx.com
smtp.vbnhy.com

Description: Google Mail
Server Name: smtp.googlemail.com
Port: 465
User Name: floss.reader2@gmail.com
Authentication method: Normal password
Connection Security: SSL/TLS

In Outgoing Server (SMTP) Settings click the **Add** button.

9. Enter the settings for sending email that you got from your email provider.



SMTP Server

Settings

Description:

Server Name:

Port: Default: 25

Security and Authentication

Connection security: None

Authentication method:

User Name:

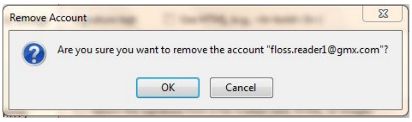
Click the **OK** button to continue.

10. To complete the set up process, click the **OK** button on the Account Settings screen.
11. Thunderbird asks for your password the first time that you try to get or send email. When this happens you can have Thunderbird remember your email.

REMOVE AN ACCOUNT

Here's how to remove an email account from Thunderbird.

1. Go to the account Manual Set Up screen.
2. Select the account that you want to remove.
3. Click **Account Actions** and select **Remove Account** from the list.
4. Thunderbird confirms that you want to remove the account. Click the **OK** button to continue removing the account.



Remove Account

Are you sure you want to remove the account "floss.reader1@gmx.com"?

The account is removed from Thunderbird and is no longer in the Account Settings screen.