**Tools**

*These links are for your use only, as sources of images used below if they are not high quality enough in this doc.*

1. Adium tool guide [– Link](https://ssd.eff.org/en/module/how-use-otr-mac)
2. Basic Security Setup for Android - [Link](https://securityinabox.org/android_basic)
3. ChatSecure tool guide - [Link](https://ssd.eff.org/en/module/how-install-and-use-chatsecure)
4. Cobian Backup Guide - [Link](https://securityinabox.org/cobian_main)
5. How to change your Facebook privacy settings - [Link](https://www.eff.org/deeplinks/2013/01/how-protect-your-privacy-facebooks-graph-search)
6. How to opt-out of Facebook's data broker relationships – [Link](https://www.eff.org/deeplinks/2013/02/howto-opt-out-databrokers-showing-your-targeted-advertisements-facebook)
7. How to opt-out of Twitter's data broker relationships – [Link](https://www.eff.org/deeplinks/2013/07/how-opt-out-twitters-tailored-advertisements-and-more)
8. Jitsi Tool guide – [Link](https://securityinabox.org/jitsi)
9. K9 & APG tool guide – [Link](https://securityinabox.org/k9_apg_main)
10. KeePassX tool guide – [Link](https://www.keepassx.org/screenshots/)
11. ObscuraCam Tool guide – [Link](https://securityinabox.org/obscuracam_main)
12. Orbot & Orweb tool guide – [Link](https://securityinabox.org/Orbot_main), [Link](https://securityinabox.org/orweb_main)
13. PGP for Linux tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-linux)
14. PGP for Mac O SX tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-mac-os-x)
15. PGP for Windows tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-windows-pc)
16. Pidgin tool guide – [Link](https://ssd.eff.org/en/module/how-use-otr-windows)
17. Psiphon3 tool guide – [Link](https://www.level-up.cc/leading-trainings/training-curriculum/deepening/psiphon3)
18. Recuva – File Recovery Guide – [Link](https://securityinabox.org/recuva_main)
19. Redphone Tool guide – [Link](https://ssd.eff.org/en/module/how-use-redphone-android)
20. Signal Tool guide – [Link](https://ssd.eff.org/en/module/how-use-signal-%E2%80%93-private-messenger)
21. TextSecure tool guide – [Link](https://ssd.eff.org/en/module/how-use-textsecure-android)
22. Tor for Mac tool guide – [Link](https://www.torproject.org/projects/torbrowser.html.en#macosx)
23. Tor for Windows tool guide – [Link](https://ssd.eff.org/en/module/how-use-tor-windows#overlay=en/node/57/)
24. TrueCrypt Tool Guide – [Link](https://securityinabox.org/truecrypt_main)

**PGP FOR MAC O SX TOOL GUIDE**

# ****PGP for Mac O SX**** Tool Guide

# Encrypted email for Mac

**Lesson to read:**

* **Email**

**Download Location:**

* [GPG Suite](https://gpgtools.org/" \t "_blank)
* [Mozilla Thunderbird](https://www.mozilla.org/thunderbird/" \t "_blank)
* [Enigmail](https://www.enigmail.net/home/index.php" \t "_blank)

**Computer requirements:** An internet connection, a computer running Mac OS X, an email account

**Version used in this guide:**

* GPG Suite Beta 4
* Mozilla Thunderbird 31.2.0
* Enigmail 1.7.2

**License:** Free Software; mix of Free Software licenses

**Level:**Advanced

**Other reading**: <http://support.gpgtools.org/>

**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 an Apple Mac (but not iPad or iPhone), with either the Mac's built-in Mail program, or with Mozilla Thunderbird, a popular alternative email program.

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. This guide is for Mac users.

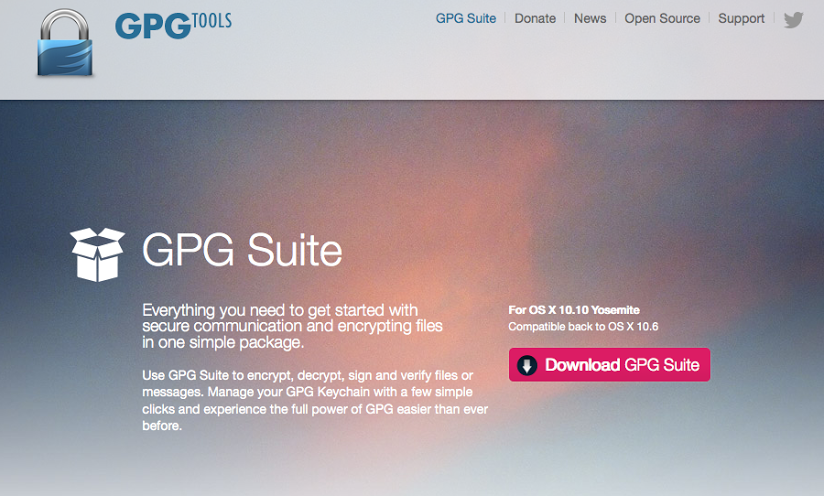
## 2.0 Installing GPGTools on your Mac

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 the GPG Suite, from GPG Tools, because it works on Macs, is free for anyone to use, and it's open source: the underlying source code is available for anyone to check for bugs and backdoors.

Once the GPG Suite is installed, you can set up your keys for the first time, and then enable PGP on Apple Mail and, optionally, Thunderbird.

### Step 1: Install the program.

First, go to <https://www.gpgtools.org/> in your browser and choose “Download GPG Suite.



You'll end up with a disk image that you can click on to install the software. If you're not accustomed to installing third-party software on your computer, ask a nearby Mac expert – this is a step most techies can help you with, even if they don't know PGP or encryption.



Clicking on install will give you a list of tools that will be added to your computer.

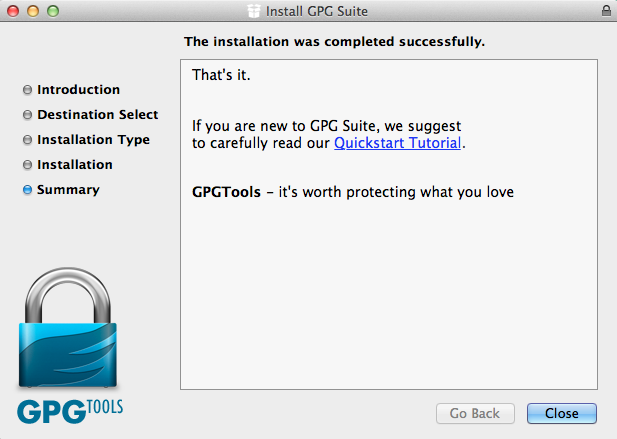


**What exactly am I installing here?**

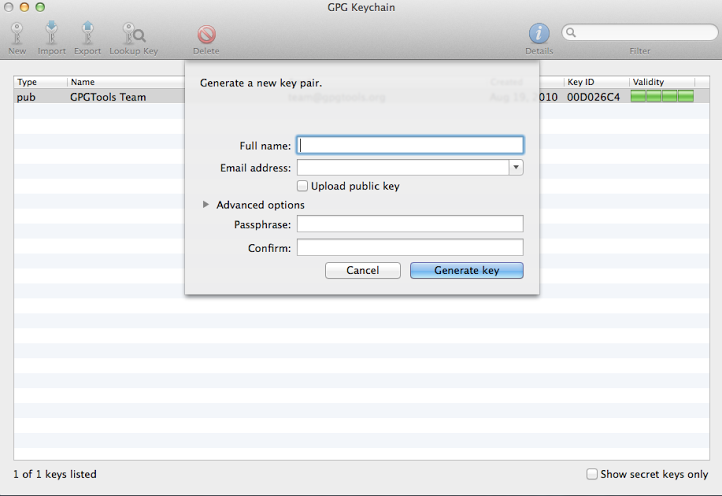
These are tools will mostly work behind the scenes so that more than one program on your Mac can use PGP. Think of them as programs that other programs can use, rather than applications that you will use directly. GPGMail lets Apple Mail send and read PGP emails, GPG Keychain Access lets you keep your private and public keys in the same manner as you can save other passwords on your Mac. GPGServices optionally adds a feature to OS X to let you use PGP directly in programs other than email (for instance, in a word processor). GPGPreferences is for changing PGP settings in Apple's preferences. Finally, MacGPG2 is the basic tool that any program needs to use to do encryption or signing.

In October 2014, the GPG Tools team announced that they would soon be charging for GPGMail, the part of their package that lets you use GPG with Apple's Mail application. This tutorial is about using GPG with Thunderbird, so it doesn't use that component. You can just use the zero-cost part of the GPG Suite, as outlined here, if you like. This option has the added benefit that all of these tools are "free software" meaning you are still allowed to freely examine, edit and redistribute GPG Mail's underlying source code, so they are even more secure. For more information, see GPG Tools' [own FAQ](https://gpgtools.org/news.html" \t "_blank) on their decision.

Click "Continue" to install GPG Suite.



When the installation is complete, open GPG Keychain (found in your applications folder) if it doesn't automatically open and prompt you to generate your PGP keys after installation.  Click "New" to generate your PGP keys.



### Step 2: Create your PGP key

Sometimes when you install new software, your computer will pester you with questions that have no obvious answer, without actually giving you any advice on how to reply. This is one of those times.

It's important to spend a little time thinking about the answers you'll give here, because changing your PGP key details can be difficult later, and if you’ve chosen to publish your key somewhere, you won’t be able to unpublish it. (There are still thousands of old public keys from the 1990’s floating around, with the names and old email addresses of the people who made them back then.)

PGP keys contain a name and an email address that link the key to you. The email address will be one of the ways others can discover which key to use when they are encrypting a message to you.

**When should I not put my real name or email address on my PGP key? When shouldn't I upload my key?**

For most people, it makes sense to add a real email address to your key, and upload it to the public keyservers – it's how people will match the right key to you. They can send you an email directly, and know it will be encrypted with the right key, and when they receive a signed email from you, the digital signature will be marked with your name.

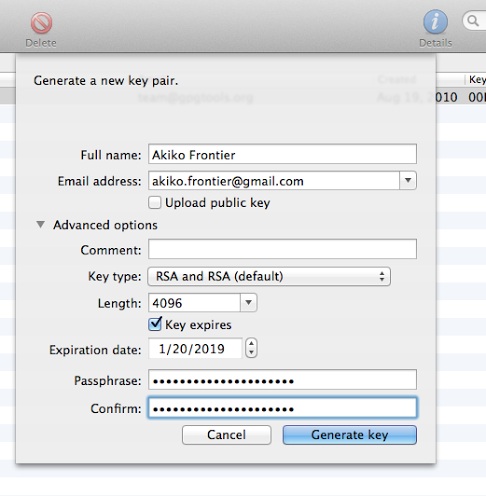
For some people, though, it will not make sense to add your real name to your key, for instance if your threat model means that having your identity publicly attached to your key (and the linked email address) is not a good idea. Edward Snowden communicated with journalists using PGP and an anonymous email address before he revealed his identity; his PGP key certainly wasn't marked with his name.

Uploading your key is normal practice, but it can reveal that you're using encryption, even if you don't use your own name. Also, as we'll see, others might upload your key and associate their own key with it, implying that you and they have a connection. That can be harmful if you are communicating and don't want people to know it. It can also be troublesome if you're not communicating, but your attacker wants people to think that you are associated.

Here's a rough guideline: if you're thinking about using a pseudonym generally, use that pseudonym (and alternative email) when labeling your key. If you are in a more dangerous environment, when you don't want people to know you're using PGP at all, or know who you are communicating with, don't upload your key to the public keyservers – and make sure the small group of people you're communicating with know not to upload your key either. There are other ways of verifying keys that don't rely on them being available on the public key server – see EFF’s guide to [Key Verification](https://ssd.eff.org/en/module/key-verification" \l "overlay=en/node/37/" \t "_blank) for more information.

Click the "Upload public key after generation" box if you'd like to let others find your key quickly so that they can send you encrypted messages. It's like adding your phone number to a public phone directory: you don't need it, but it's convenient for others.

Before generating the key, expand "Advanced options." You can leave the comment blank, and leave the key type "RSA and RSA (default)." But make sure to change the Length field to 4096.

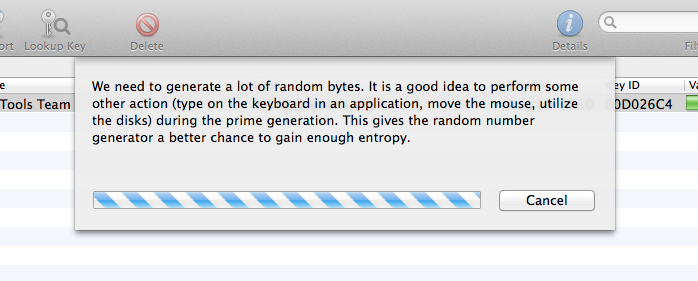


Your key will expire at a certain time; when that happens, other people will stop using it entirely for new emails to you, though you might not get any warning or explanation about why. So, you may want to mark your calendar and pay attention to this issue a month or so before the expiration date.

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.

When you're ready, click the "Generate key" button.

You computer will start generating both your public and private key. It shouldn't take any more than a couple of minutes to finish (it takes a while because to create your keys, your computer needs to gather random numbers. Think of it as your computer throwing a pair of dice many, many, many times.)



When you're done generating your key, you'll see it key listed in GPG Keychain Access. You can double-click on your key to see information about it, including its "fingerprint ”—a unique way to identify your PGP key.

Now is a good time to generate a **revocation certificate**. (A revocation certificate is a file that you can generate that announces that you no longer trust that key. You generate it when you still have the secret key, and keep it for any future disaster.) In the future, if you ever worry that your private key has been copied by someone, you accidentally delete or lose your private key, or you forget your passphrase, you can tell everyone it has been revoked, or cancelled, by using a revocation certificate.

It's better to create one now, because you need the private key and passphrase to create a revocation certificate. If you leave it until later, you might lose one or the other, and then it will be too late. So create a certificate by clicking on your key, choosing the “Key” menu entry, and then “Create Revocation Certificate.” You'll be prompted for somewhere to save the file. You might want to keep it with a backup copy of the key (see next step).

### Step 3: Back up your PGP key

If you lose access to your private key, you won't be able to decrypt any incoming PGP mail, or your old mail. On the other hand, you want to keep your private key as securely as you can.

You might want to save a backup copy to a USB key, which you keep safely hidden. You will only need it if you lose your original key, but for safety you will want to keep it out of the hands of your potential attackers.

**Is everything lost if my attackers get hold of my PGP private key?**

What if you get your Mac stolen, or your backup key is taken from you? Does that mean your PGP messages are vulnerable? No: if you've chosen a good passphrase and nobody has been able to learn what it is, you should still be mostly protected. To be safe, you may want to revoke your old key, and create a new PGP key. This won’t stop your old key from being able to decrypt your old email, but it will discourage other people from using the old key for their new emails to you.

To backup your key, open GPG Keychain Access. Select your key, and click “Export” in the toolbar. Put your USB drive into the machine, and choose it in the “Where” part of the “Save As...” dialog. Check the “Allow secret key export” checkbox.

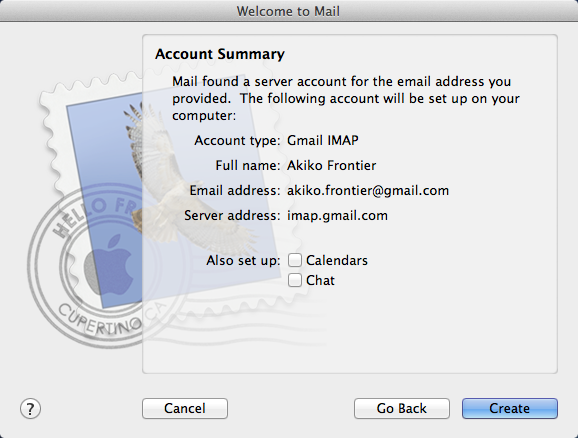
## OPTION A) Configuring Apple Mail

When you first open Apple Mail, you'll see a first run wizard that helps you set up your email address. Fill out your name, email address, and your email password and click "Create."



### Mail account setup wizard

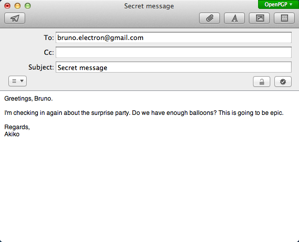
If you use popular free email services like Gmail, Mail should be able to automatically detect your email settings when you click Continue. If it doesn't, you may need to manually configure your IMAP and SMTP settings. Talk to the company you use for email, or ask someone technical who is familiar with 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 about PGP, but you can ask them “Can you set up Apple Mail for me?”).



### Mail account setup auto-detect

When you're composing a new message, there are two icons just beneath the Subject field. There's a padlock (encrypt email) and a star (digitally sign email). If the padlock is closed it means this email will be encrypted, and if the star has a check in it, it means this email will be digitally signed.

## Sending PGP Signed or Encrypted Email



You can always sign your email, even if the recipient doesn’t use PGP. Because digitally signing emails requires your secret key, Mail will pop up a window asking for your passphrase when you first sign an email.

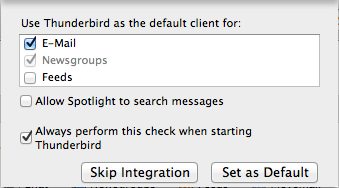
You can only encrypt emails if the person you’re emailing uses PGP and you have that person’s public key. If the encryption padlock icon is unlocked and greyed out so you can't click on it, this means you first need to import the recipient's public key. Either ask them to send it to you, or use the GPG Keychain Access app to find the key to from a public keyserver.

To be absolutely safe, you'll need to verify the keys you get from the keyserver or your colleague. See EFF’s guide to [Key Verification](https://ssd.eff.org/en/module/key-verification" \l "overlay=en/node/37/" \t "_blank) for more information.

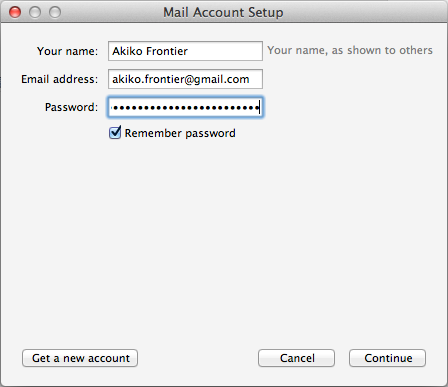
## OPTION B) Using PGP with Mozilla Thunderbird

This walkthrough shows how to use GPG with the free, open source, Thunderbird mail client from Mozilla, together with the Enigmail plugin for email encryption.

First, download Thunderbird from [https://www.mozilla.org/thunderbird](https://www.mozilla.org/thunderbird/), mount the disk image as you did with GPG Tools, and drag the Thunderbird into Applications. When you open it for the first time it will ask if you want to set it as your default email client. Go ahead and click "Set as Default.”

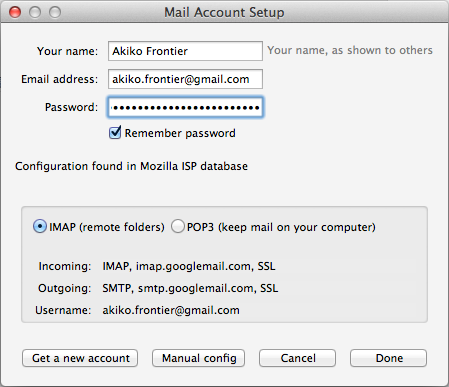


Then you will see the first run wizard. To set up your existing email address, click "Skip this and use my existing email." Then enter your name, email address, and the password to your email account.



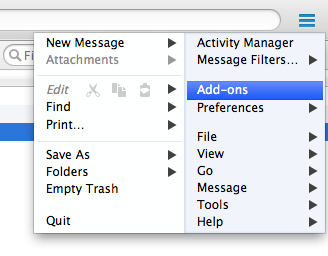
If you use popular free email services like Gmail, Thunderbird should be able to automatically detect your email settings when you click Continue. If it doesn't, you may need to manually configure your IMAP and SMTP settings—ask your ISP, or a technical friend who knows about setting up email, to help. Sometimes, Thunderbird can just guess the correct settings.

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" \t "_blank) for doing this.

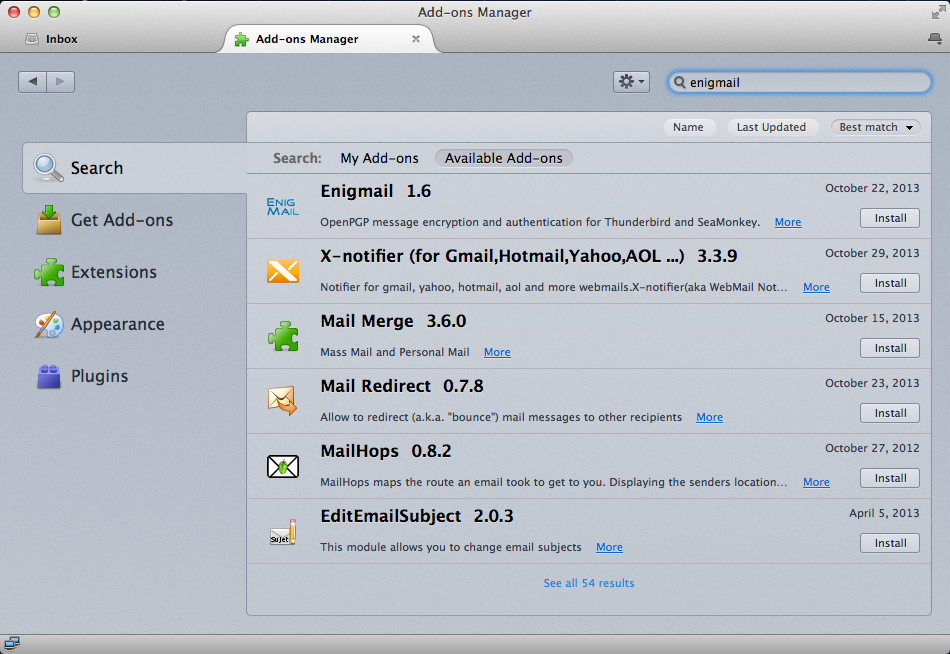


After you're done configuring Thunderbird to check your email, click "Done." Then click on "Inbox" in the top left to load your emails.

Now that you've installed and configured Thunderbird to work with your email, you need to install [Enigmail](https://www.enigmail.net/home/index.php" \t "_blank), the GPG add-on for Thunderbird. In Thunderbird, click the menu icon in the top-right, and choose Add-ons.



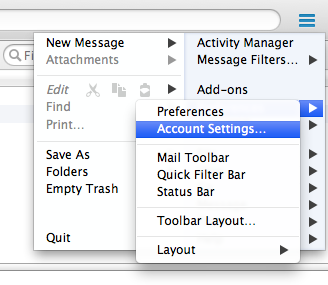
Search for "enigmail" in the search box in the top right.



Click the Install button next to the Enigmail extension to download and install Enigmail. When it's done, click "Restart Now" to restart Thunderbird.

The first time you run Thunderbird with Enigmail enabled it opens the OpenPGP Setup Wizard. Click "Cancel." We will manually configure Enigmail instead.

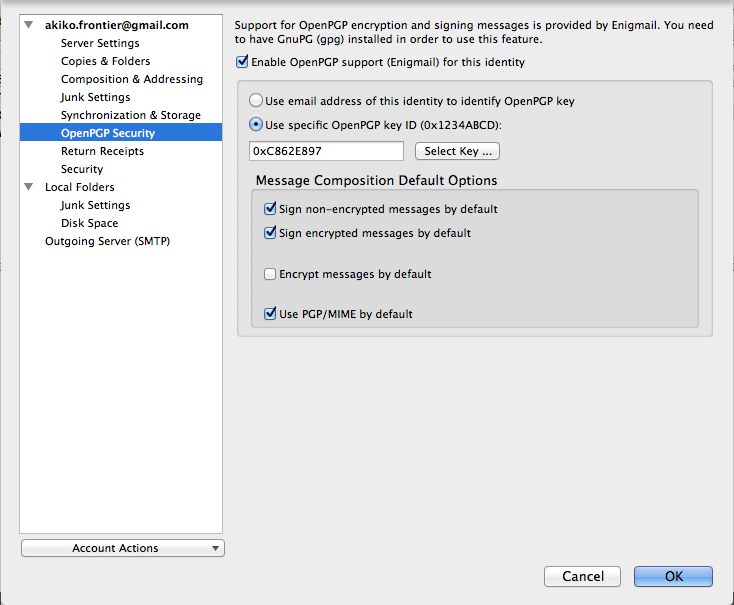
Click the menu button, hover over Preferences, and choose Account Settings.



Go to the OpenPGP Security tab. Make sure "Enable OpenPGP support (Enigmail) for this identity" is checked. "Use specific OpenPGP key ID" should be selected, and if your key isn't already selected you can click "Select Key" to select it.

You should also check "Sign non-encrypted message by default," "Sign encrypted messages by default," and "Use PGP/MIME by default," but not (for most people) "Encrypt messages by default."

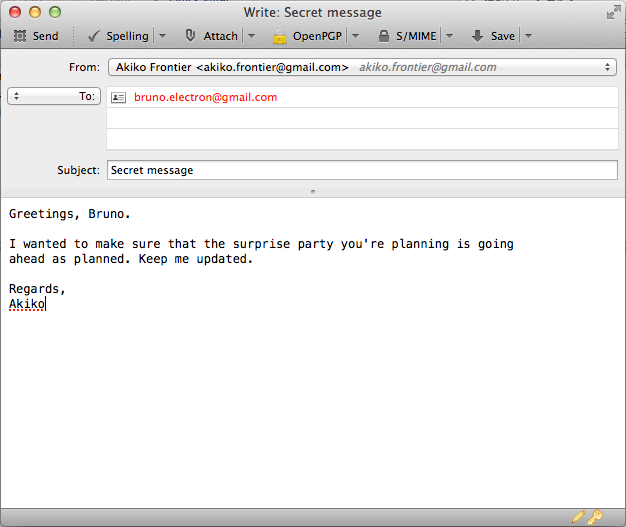
If most of the people that you email use PGP (or you would like to encourage them to do so), you may wish to encrypt by default. It would be ideal to encrypt all the emails you send, but that is not always possible. Remember that you can only send encrypted email to other people who use PGP, and you need to have their public keys in your keychain. For most people, manually choosing to encrypt each email you send will probably work best.



Then click "OK" to save all of the settings.

Congratulations, you now have Thunderbird and Enigmail set up! Here are a couple of quick pointers:

* You can click the menu button, hover over OpenPGP, and open Key Management to see the PGP key manager that's build-in to Enigmail. It's very similar to GPG Keychain Access, and it's your choice which you use.
* When you're composing a new message, there are two icons in the bottom right corner of the window: a pen (digitally sign email) and a key (encrypt email). If the icons are gold it means they are selected, and if they're silver it means they're not selected. Click on them to toggle signing and encrypting the email you're writing.



**PGP FOR WINDOWS PC TOOL GUIDE**

# ****PGP for Windows PC**** Tool Guide

# Encrypted email for Windows

**Lesson to read:**

* **Email**

**Download Location:**

* [GPG4Win](http://www.gpg4win.org/" \t "_blank)
* [Mozilla Thunderbird](https://www.mozilla.org/en-US/thunderbird/" \t "_blank)
* [Enigmail](https://www.enigmail.net/home/index.php" \t "_blank)

**Computer requirements:** An internet connection, a computer running Mac OS X, an email account

**Version used in this guide:**

* Windows: Windows 7 Ultimate
* Mozilla Thunderbird 24.6.0
* Enigmail 1.7
* GPG4Win 2.2.1

**License:** Free Software; mix of Free Software licenses

**Level:**Advanced

**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.

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. This guide is for Windows users.

## 1.1 Overview

To use PGP to exchange secure emails you have to bring together three programs: GPG4Win (GNU Privacy Guard for Windows known as GnuPG), Mozilla Thunderbird and Enigmail.

* GnuPG is the program that actually encrypts and decrypts the content of your mail.
* Mozilla Thunderbird is an email client that allows you to read and write emails without using a browser.
* Enigmail is an add-on to Mozilla Thunderbird that ties it all together.

Note! What this guide teaches is how to use PGP with Mozilla Thunderbird, an email client program that performs a similar function to Outlook. You may have your own favorite email software program (or use a web mail service like Google Mail or Outlook.com). This guide won't tell you how to use PGP with these programs. You can choose either to install Thunderbird and experiment with PGP with a new email client, or you can investigate other solutions to use PGP with your customary software. We have still not found a satisfactory solution for these other programs.

Using PGP doesn't completely encrypt your email: the sender and receiver information is still unencrypted and so is the subject line!

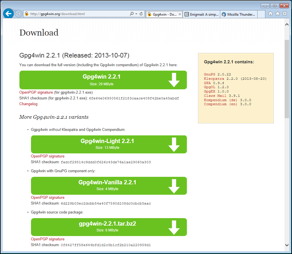
Encrypting the sender and receiver information isn’t possible in the existing email system. What using Mozilla Thunderbird with the Enigmail add-on gives you is an easy way to encrypt the *content* of your email. Someone spying on your emails may still see the identities of the people you communicate with and when you email them.

You will first download all the software needed, install it, and then end with configuration and usage.

## 2 Downloading the software

## 2.1 Getting GPG4Win

You can get GnuPG (also known as GPG) on Windows by downloading the small installer from the GPG4Win download page.



Click on the most recent version of GPG4Win with GnuPG component only (Vanilla or Light) to download the GPG installer.

Note: This version of GPG is available only on a web site that offers “http” downloads, not secure “[https](https://ssd.eff.org/en/glossary/https)” downloads. If you are concerned that you may be targeted for surveillance by an organization that can tamper with your Internet connection, you may want to investigate more drastic solutions, such as downloading and running Tails, a secure [operating system](https://ssd.eff.org/en/glossary/operating-system) that replaces Windows.

Many browsers will ask you to confirm whether you want to download this file. Internet Explorer 11 shows a bar at the bottom of the browser window with an orange border.

For any browser it is best to first save the file before proceeding, so click the “Save” button. By default, most browsers save downloaded files in the Downloads folder.

## 2.2 Getting Mozilla Thunderbird

Go to the Mozilla Thunderbird website.



Click on the green button labelled “Thunderbird Free Download.”

The Mozilla Thunderbird website will have detected your preferred language. If you want to use Thunderbird in another language click on the “Other Systems & Languages” link and make your selection from there.

Many browsers will ask you to confirm if you want to download this file. Internet Explorer 11 shows a bar at the bottom of the browser window with an orange border.

https://ssd.eff.org/files/field/image/pgpwindows4.png

For any browser, it is best to first save the file before proceeding, so click the “Save” button. By default, most browsers save downloaded files in the Downloads folder.

## 2.3 Getting Enigmail

You can get Enigmail from the Enigmail website.

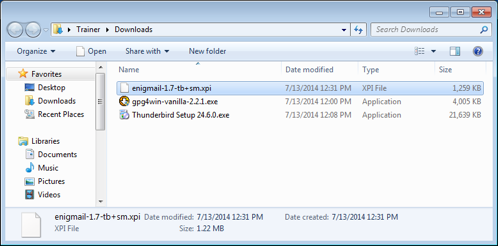


Many browsers will ask you to confirm if you want to download this file. Internet Explorer 11 shows a bar at the bottom of the browser window with an orange border.

https://ssd.eff.org/files/field/image/pgpwindows6.png

For any browser it is best to first save the file before proceeding, so click the “Save” button. By default, most browsers save downloaded files in the Downloads folder.

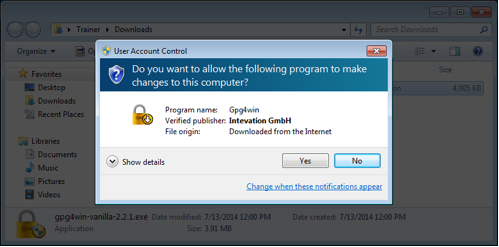
After downloading Enigmail, GPG4Win, and Mozilla Thunderbird you should have three new files in your Downloads folder:



## 3 Installing the software

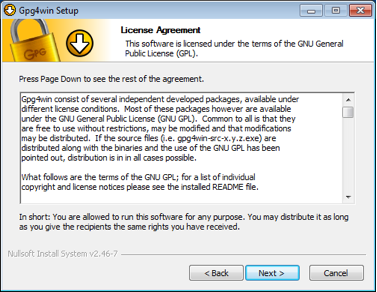
## 3.1 Installing GPG4Win

Keep the Windows Explorer window open and double-click on gpg4win-xxx-x.x.x.exe. You'll be asked if you want to allow the installation of this program. Click the “Yes” button.

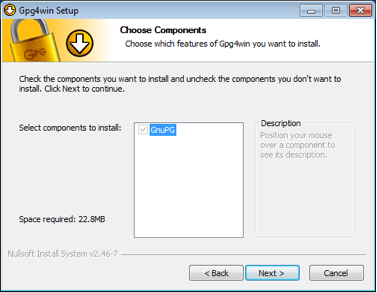


A window will open, giving you an overview of what will be installed. Click the “Next” button.

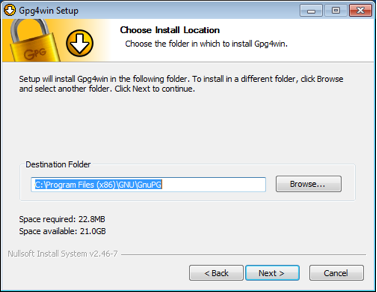
A window with the license agreement will open up. Click the “Next” button.



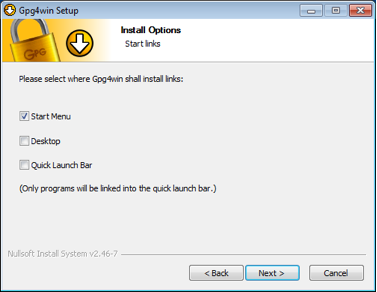
The GPG4Win Vanilla package doesn't have components to select, so click the “Next “button again. For the GPG4Win-Light package, unselect all optional components to install GnuPG only.

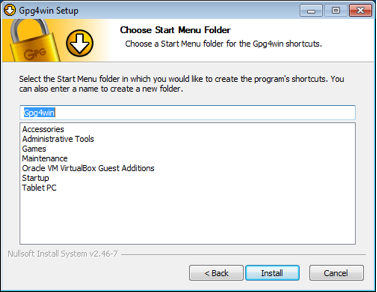


Next, you'll have the ability to choose where GPG is installed. Don't change the default setting. Click the “Next” button.

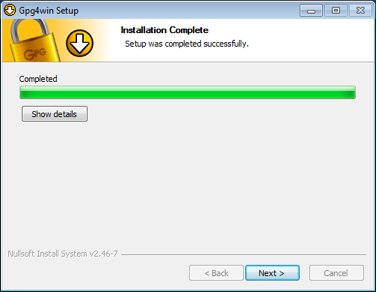


The next two windows will have some installation options. Click the “Next” button and then click the "Install" button:





You will see a window with a progress bar—when it's done it will say “Installation Complete.” Click the “Next” button again.



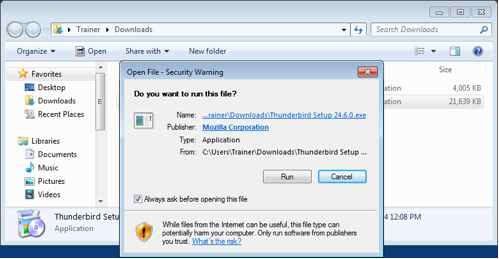
Finally, you are at the last installation step. Remove the check mark next to “Show the README file” and click the “Finish” button.



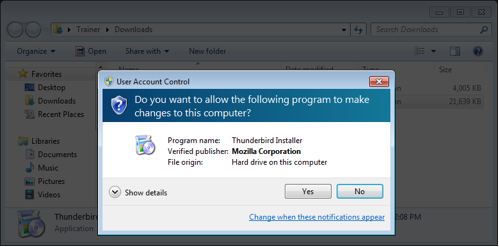
That's it. Now let's move on to installing Mozilla Thunderbird.

## 3.2 Installing Mozilla Thunderbird

Similar to GPG4Win, you install Mozilla Thunderbird by double-clicking the Thunderbird Setup 24.6.0.exe file. As usual, you will be asked if you want to run this file. Click the “Run” button.



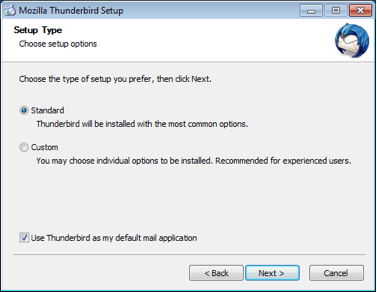
You will be asked if you want to allow Mozilla Thunderbird to make a change to your computer by installing software. Click the “Yes” button.



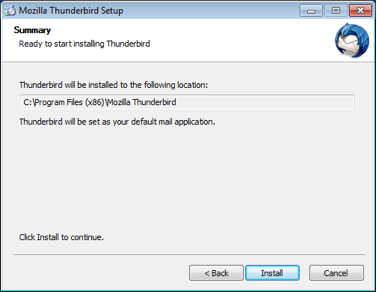
You will see the Mozilla Thunderbird Setup window. Click the “Next” button.



Next, you will get a choice between a Standard setup and a Custom setup. Keep the Standard setup selection and click the “Next” button.



You will be given a summary of where Mozilla Thunderbird's files will be installed. Click the “Install” button.



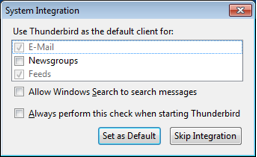
When the installation process is complete, you will see a final window that enables you to launch Mozilla Thunderbird. Click the “Finish” button.



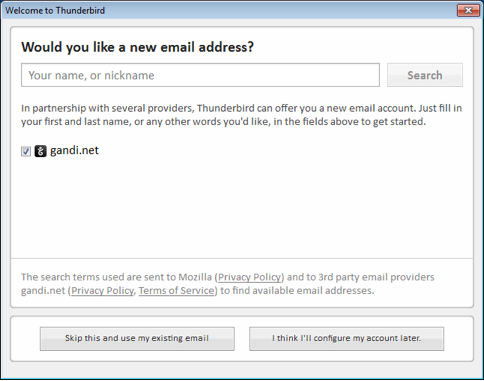
## 3.3. Enigmail installation

## Step 1. Preparation

When Mozilla Thunderbird launches for the first time, you will see this small confirmation window asking about some default settings. We recommend clicking the “Set as Default” button.

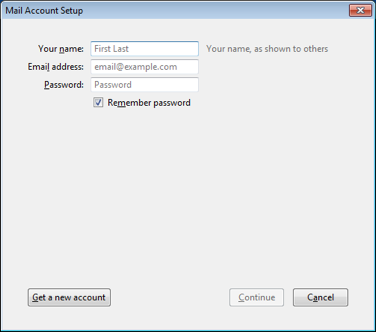


Next, you will be asked whether you would like a new email address. Click the “Skip this and use my existing email” button. Now you will configure Mozilla Thunderbird to send and receive email. If you are used to only reading and sending email through gmail.com, outlook.com, or yahoo.com, Mozilla Thunderbird will be a new experience, but it isn't that different overall.

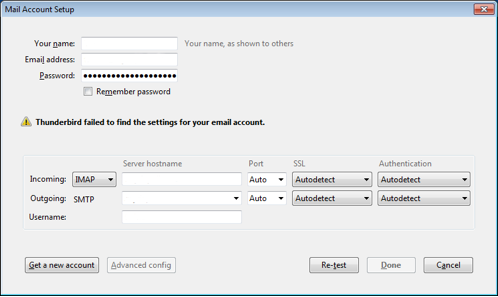


## Step 2. Adding a mail account to Mozilla Thunderbird

A new window will open.



Enter your name, email address, and the password to your email account. Mozilla doesn't have access to your password or your email account. Click the “Continue” button.



In many cases Mozilla Thunderbird will automatically detect the necessary settings. In some cases Mozilla Thunderbird doesn't have complete information and you'll need to enter it yourself. Here is an example of the instructions Google provides for Gmail:

### Incoming Mail (IMAP) Server - Requires SSL

* imap.gmail.com
* Port: 993
* Requires SSL:Yes

### Outgoing Mail (SMTP) Server - Requires TLS

* smtp.gmail.com
* Port: 465 or 587
* Requires SSL: Yes
* Requires authentication: Yes
* Use same settings as incoming mail server

**Full Name or Display Name**: [your name or pseudonym]

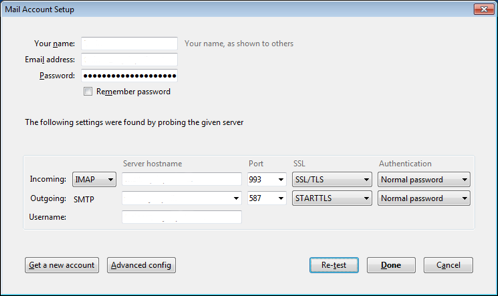
**Account Name or User Name**: your full Gmail address ([username@gmail.com](mailto:username@gmail.com)). Google Apps users, please enter [username@your\_domain.com](mailto:username@your_domain.com)

**Email address**: your full Gmail address ([username@gmail.com](mailto:username@gmail.com)) Google Apps users, please enter [username@your\_domain.com](mailto:username@your_domain.com)

**Password**: your Gmail password

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" \t "_blank) for doing this.

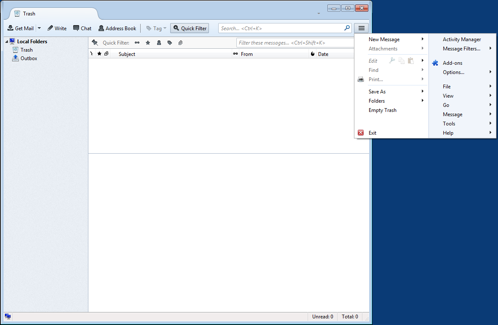
When all the information is entered correctly, click the “Done” button.



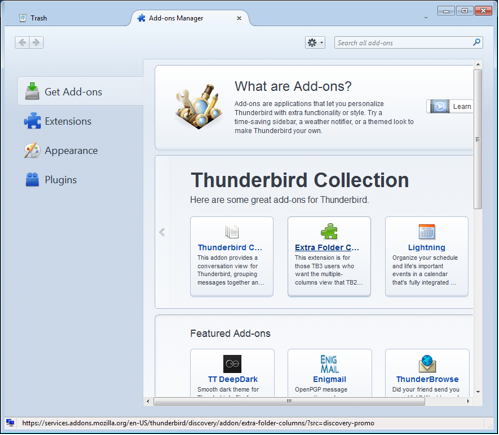
Mozilla Thunderbird will start downloading copies of your email to your computer. Try sending a test email to your friends.

## Step 3. Installing Enigmail

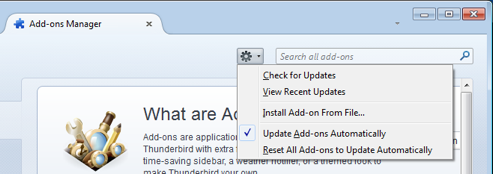
Enigmail is installed in a different way from Mozilla Thunderbird and GPG4Win. As mentioned before, Enigmail is an Add-on for Mozilla Thunderbird. Click the “Menu button,” also called the Hamburger button, and select “Add Ons.”



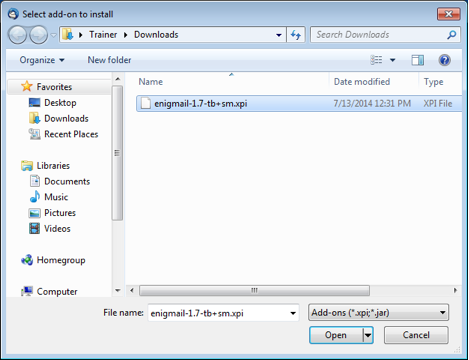
You'll be taken to the Add-ons Manager tab.



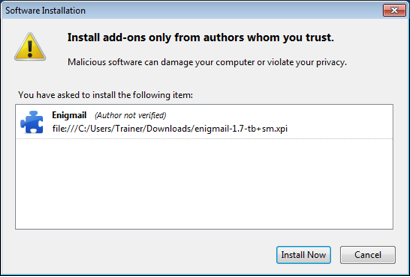
Click the cog to bring up a small menu and select “Install add-on from file” which will bring up a file-selection window.



The file selection window will very likely open to the Downloads folder. If it doesn't, go to the Downloads folder (where Enigmail was saved to) click on enigmail-1.7-tb+sm.xpi then click the “Open” button.



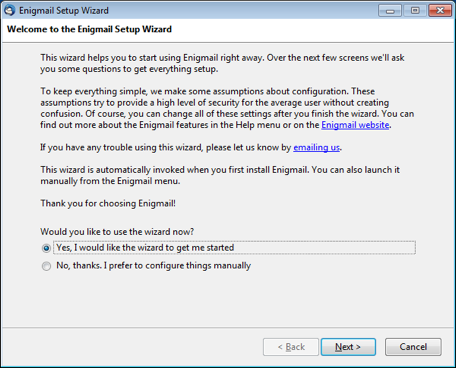
Now you will see a small window asking you to confirm whether you want to install Enigmail. Click the “Install Now” button.



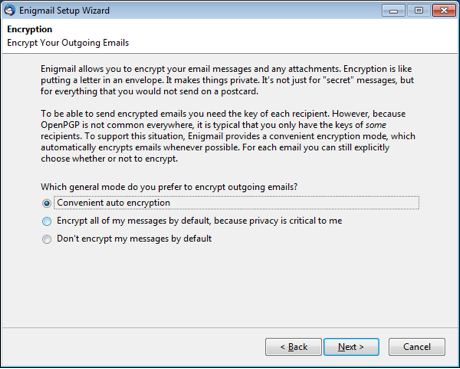
After the Enigmail add-on is installed, Mozilla Thunderbird will ask to restart the browser to activate Enigmail. Click the “Restart Now” button and Mozilla Thunderbird will restart.



When Mozilla Thunderbird restarts, an additional window will open up that will start the process of setting up the Enigmail add-on. Keep the “Yes, I would like the wizard to get me started” button selected and click the “Next” button.



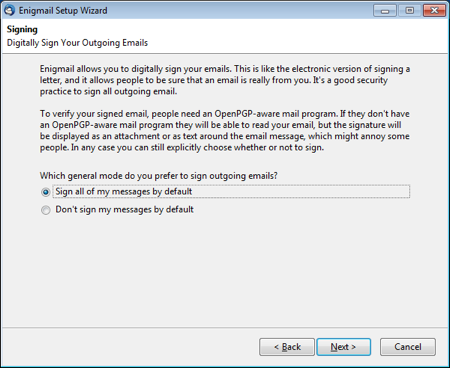
Enigmail provides you with three options for handling mail. The default option is to encrypt emails if you have the “public key” of another person, Enigmail will encrypt the email you send but leave emails unencrypted if you don't have the public key of the recipient yet. You also have the option to 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.



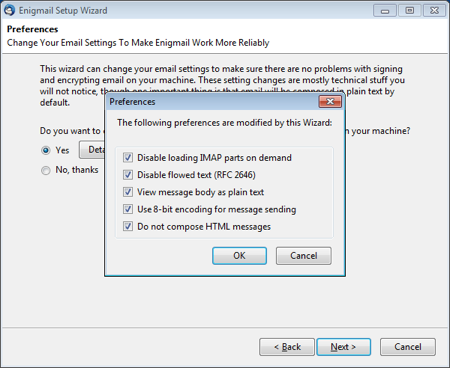
We don't know what the appropriate option is for you, but believe the “Convenient auto encryption” option to be a good choice. If you are in doubt, choose “Don't encrypt my messages by default.” Click the “Next” button.

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](http://www.cryptolaw.org/" \t "_blank)(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.

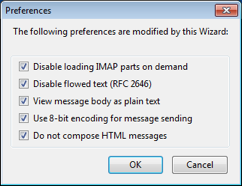
Click the “Next” Button.



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.”

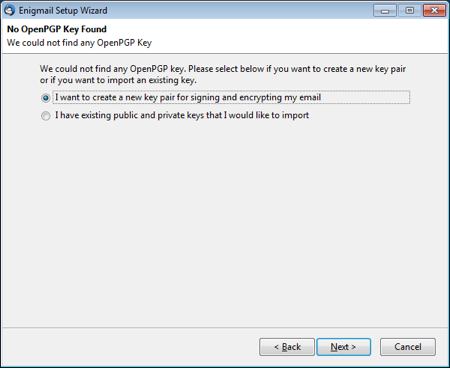
The small window will close. Click the “Next” button.

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

## 4 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.

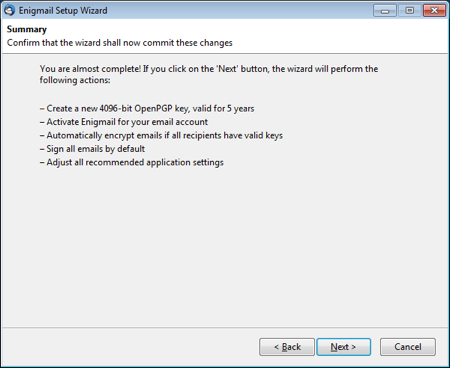


Unless you have already configured more than one email account, Enigmail will choose the email account you've already configured. The first thing you'll need to do is come up with a strong [passphrase](https://ssd.eff.org/en/module/creating-strong-passwords" \l "overlay=en/node/23/" \t "_blank) for your private key. See the **Passwords lesson** for more information on how to do this.

Make sure that you've written down this passphrase on paper until you have memorized it. Keep it somewhere where you can tell if it has been taken or viewed (like your wallet or purse). Just make sure you don't leave this paper lying around.

Click the “Next” button.

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.

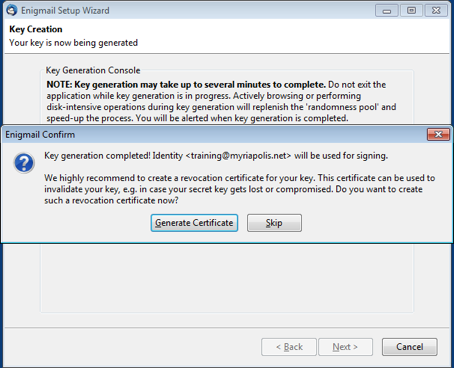


Your key will expire at a certain time; when that happens, other people will stop using it entirely for new emails to you, though you might not get any warning or explanation about why. So, you may want to mark your calendar and pay attention to this issue a month or so before the expiration date.

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.

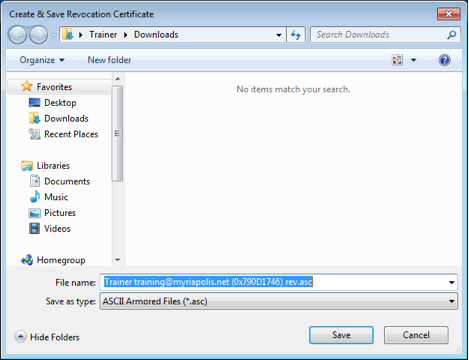
Enigmail will generate the key and when it is complete, a small window will open asking you to generate a revocation certificate. This revocation certificate is important to have as it allows you to make the private key and public key invalid. It is important to note that merely deleting the private 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.

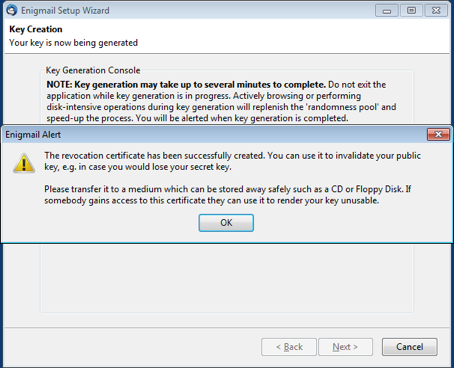


A window will open to provide you a place to save the revocation certificate. While you can save the file to your computer, we recommend saving the file on a USB drive that you are using for nothing else and storing the drive in a safe spot. We also recommend removing the revocation certificate from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

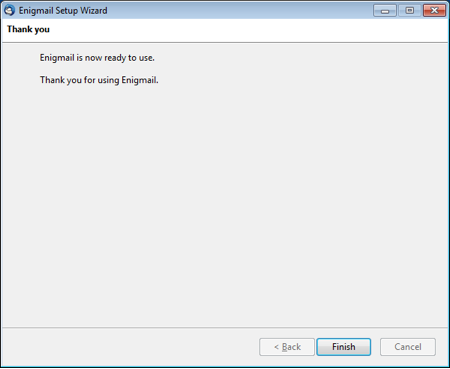
Even better, save this file on a separate encrypted disk. Choose the location where you are saving this file and click the “Save” button.



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



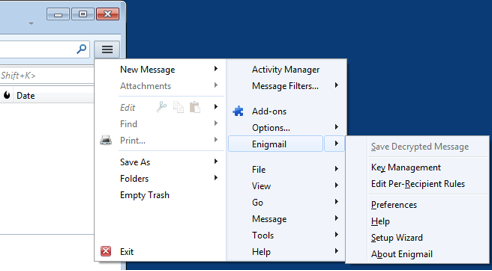
Finally, you are done with generating the private key and public key. Click the “Finish” button.



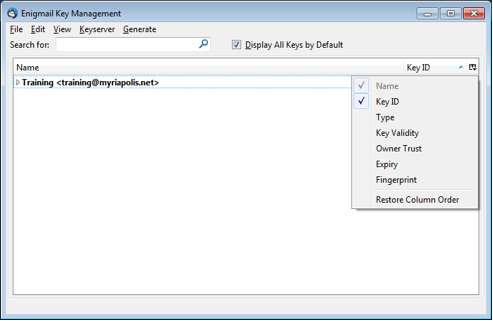
## 5 Optional steps

### 5.1 Display long key-IDs

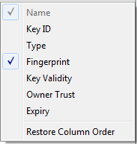
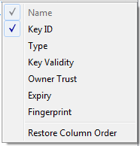
The next steps are completely optional but they can be helpful when using OpenPGP and Enigmail. Briefly, the Key ID is a small part of the fingerprint. When it comes to verifying that a public key belongs to a particular person the fingerprint is the best way. Changing the default display makes it easier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



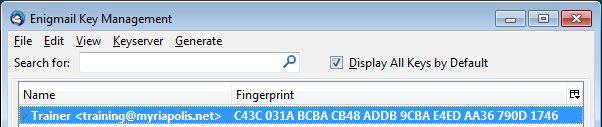
A window will open showing two columns: Name and Key ID.



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 the columns will look like this:

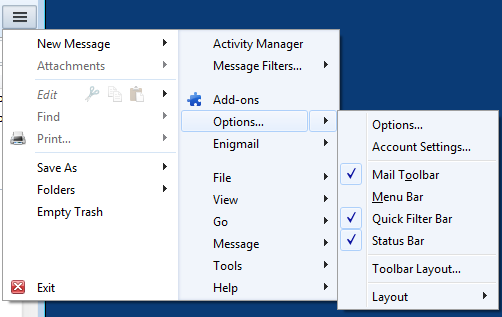


Now you are set up to send and receive regular and encrypted email. Next you will go through the steps of actually finding the people to exchange encrypted mail with.

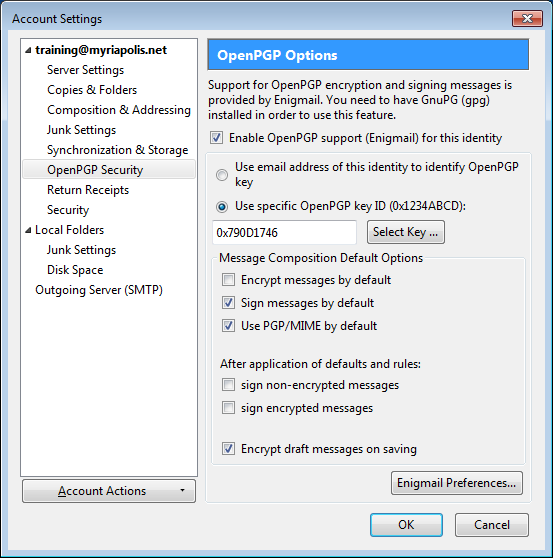
## 5.2 Using PGP/MIME

There is a final optional configuration step is to enable PGP/MIME which makes sending encrypted and signed attachments easier.

You can find this setting by clicking on the Menu Button, hovering over Options, then clicking Account Settings. The Account Settings window will open.



When the Account Settings window opens click the OpenPGP Security tab then click the checkbox next to Use PGP/MIME by default. Next click the OK button. Now Enigmail will use PGP/MIME by default.



Using PGP doesn't completely encrypt your email so that the sender and received 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.

## 6.1 Letting others know you are using PGP

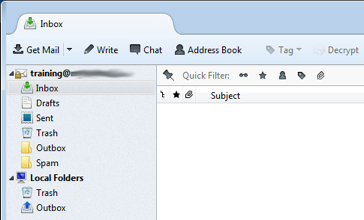
Now that you have PGP, you want to let others know that you are using it so they can also send you encrypted messages using PGP.

Let's look at three different ways you can let people know you are using PGP.

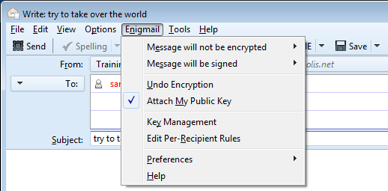
### Let people know you are using PGP with an email

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 send the email and the recipient will be able to download and use the public key you sent.

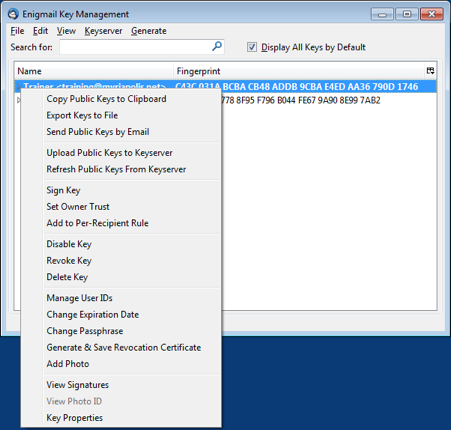
If this method is used, it's a good idea to have the recipient verify your public key's fingerprint over some other form of communication, in case email is already being intercepted and tampered with.

### Let people know you are using PGP on your website

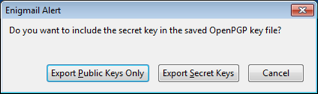
In addition to letting people know via email, you can post your public key on your website. The easiest way is to upload the file and link to it. This guide won't go into how to do those things, but you should know how to export the certificate as a file to use in the future.

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

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

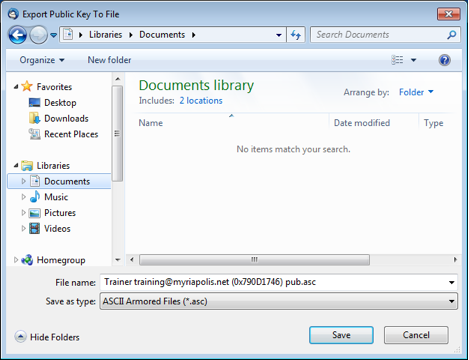


A small window will pop up with three buttons. Click the “Export Public Keys Only” button.



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.

### Uploading to a keyserver

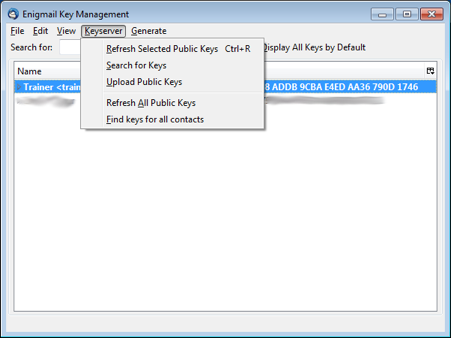
Keyservers make it easier to search for and download public keys. Most modern keyservers are synchronizing, meaning that a public key uploaded to one server will eventually reach all servers.

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.

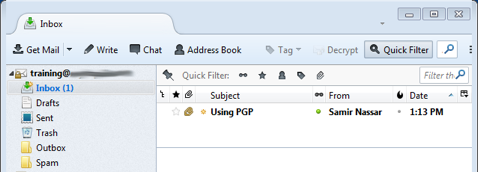
Click the Keyserver menu item and select the Upload Public Keys option.



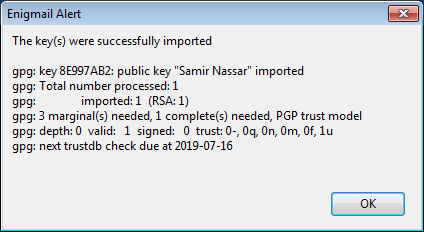
## 6.2 Finding other people who are using PGP

### Getting a public key by email

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



Double-click on the new message, and it'll open a new tab. 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.



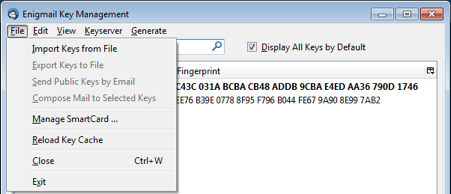
If you open up the Enigmail key management window again, you can check the result. Your PGP key is in bold because you have both the private key and the public key. The public key you just imported is not bold because it doesn't contain the private key.



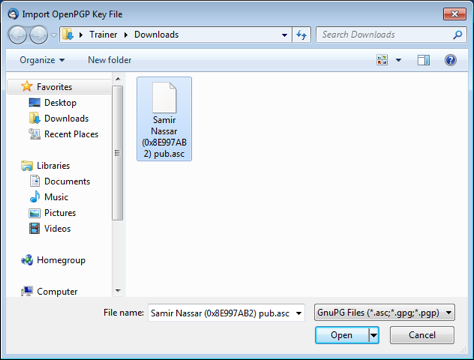
### Getting a public key as a file

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.

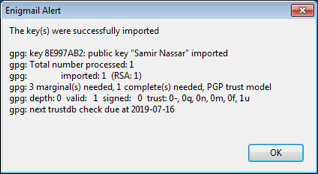
Open the Enigmail Key Manager and click on the “File” menu. Select “Import Keys from File.”



The public key might have very different file name endings such as .asc, .pgp, or .gpg. Select the file and click the “Open” button.

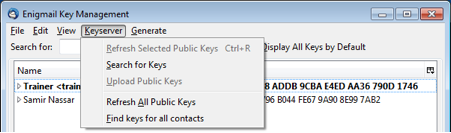


A small window will open, giving you the results of the import. Click the “OK” button.

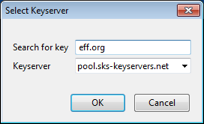


### Getting a public key from a key server

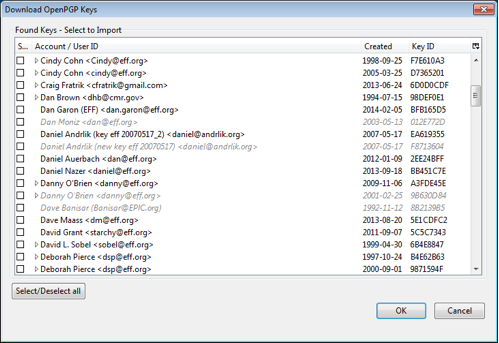
Keyservers can be a very useful way of getting public keys. Try looking for a public key. Open up the key manager then click the “Keyserver” menu and select “Search for Keys.”



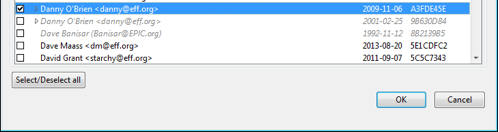
A small window will pop up with a search field. You can search by a complete email address, a partial email address, or a name. In this case, you will search for certificates containing “eff.org.”



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.

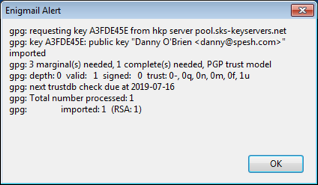


Let's take the public keys of Danny O'Brien for example, he has one expired or revoked certificate and one valid certificate. Select the valid certificate by clicking the box on the left then press the OK button.

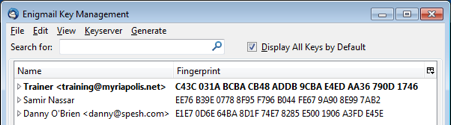


In some cases a person may have more than one certificate, all appearing valid. Note that it's possible for anyone to upload a public certificate for anyone else, and that one of these keys may not belong to the person that owns the email address associated with it. In this case, verifying the fingerprint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

A small notification window will pop up letting you know if you succeeded:

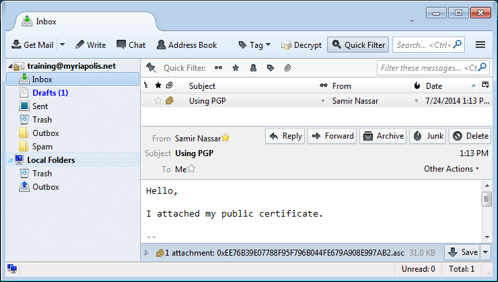


The Enigmail Key Manager will now show you the added certificates:

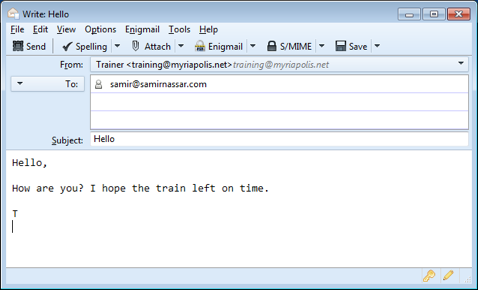


## 7.1 Sending PGP encrypted mail

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.



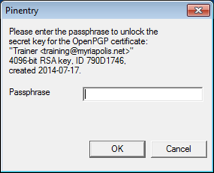
Write your message, and enter a recipient. For this test, select a recipient whose public key you already have. Enigmail will detect this and automatically encrypt the email.



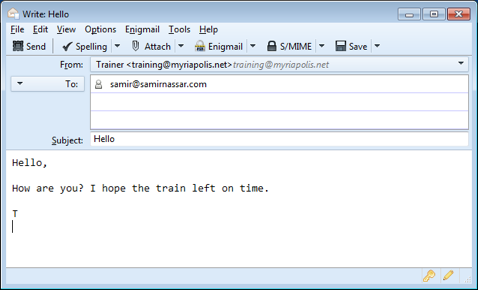
Note that the subject line won't be encrypted, so choose something innocuous, like “hello.”

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 this text:

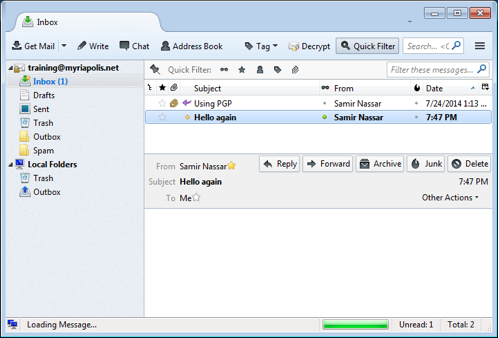


Will be transformed into:

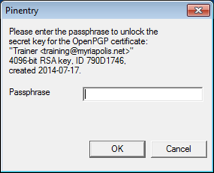


## 7.2 Receiving PGP encrypted mail

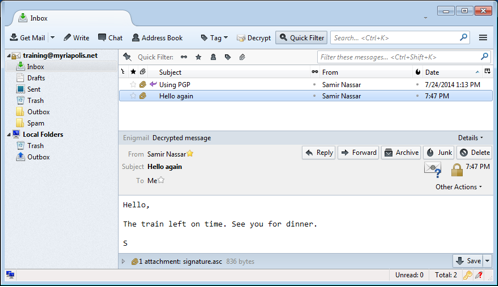
Let's go through what happens when you receive encrypted email. Notice that that Mozilla Thunderbird is letting you know you have new mail. Click on the message.



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

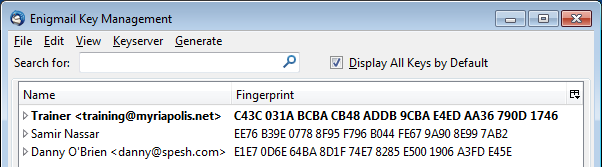


## 8 Revoking the PGP Key

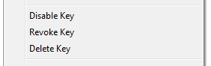
### Revoking your PGP Key through the Enigmail interface

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.

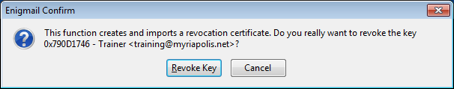
You might have a good reason to disable the PGP key before it expires. Perhaps you want to generate a new, stronger PGP key. The easiest way to revoke your own PGP key in Enigmail is through the Enigmail Key Manager.



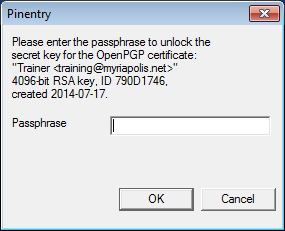
Right-click on your PGP key (it's in bold), and select the “Revoke Key” option.



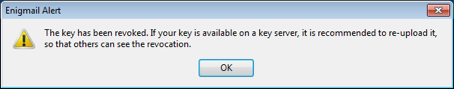
A window will pop up letting you know what happens and asking for your confirmation. Click the “Revoke Key” button.



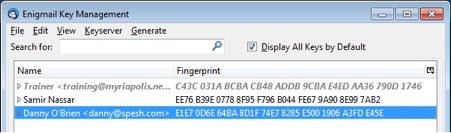
The password window opens, enter your password for the PGP key and click the “OK” button.



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.



## 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.

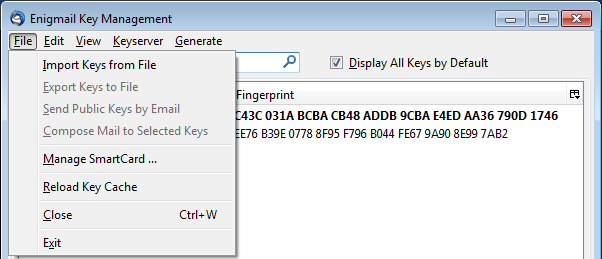
Like we mentioned before, you might have a good reason to disable the PGP key before it expires.

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.

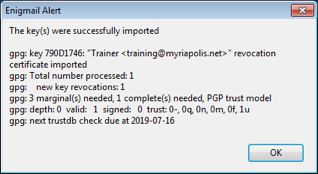
Start with the Enigmail Key Manager and click the “File” menu and select “Import Keys from File.”



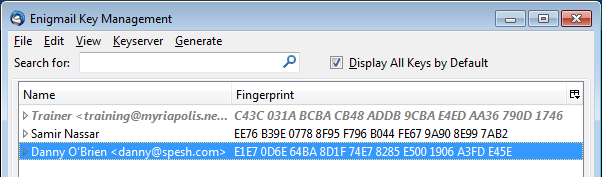
A window will open up so you can select the revocation certificate. Click on the file, and click the “Open” button.



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.