To use PGP to exchange secure emails you have to bring together three programs: 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, and Enigmail is an [add-on[](https://ssd.eff.org/en/glossary/add)](https://ssd.eff.org/en/glossary/add) to Mozilla Thunderbird that ties it all together.

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 Gmail 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[](https://ssd.eff.org/en/glossary/encrypt)](https://ssd.eff.org/en/glossary/encrypt) all aspects of your email: the sender and receiver information is unencrypted. Encrypting the sender and receiver information would break email. For similar reasons, PGP does not encrypt the subject line of your emails so you may want to use a generic subject line when sending encrypted emails. What using Mozilla Thunderbird with the Enigmail add-on gives you is an easy way to encrypt the body of your email.

You will first download all the software needed, install it, and then end with configuration and how to use the result.

**Computer requirements**: An internet connection, a computer running Windows, an email account

**Download Location**:

* [Enigmail](https://www.enigmail.net/index.php/en/)
* [GnuPG](https://gnupg.org/)
* [Mozilla Thunderbird](https://www.mozilla.org/en-US/thunderbird/)

**Versions used in this guide**: Windows: Windows 10 Ultimate; Mozilla Thunderbird 45.2.0; Enigmail 1.9; GnuPG 2.1.14

**License**: [Free Software[](https://ssd.eff.org/en/glossary/open-source-software)](https://ssd.eff.org/en/glossary/open-source-software); mix of Free Software licenses

**Other reading**:

* <https://www.gnupg.org/documentation/guides.html>
* [An Introduction to Public Key Cryptography and PGP Key Verification](https://ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp)
* [Creating Strong Passwords](https://ssd.eff.org/en/module/creating-strong-passwords)
* [Animated Overview: How to Make a Super-Secure Password Using Dice](https://ssd.eff.org/en/module/animated-overview-how-make-super-secure-password-using-dice)
* [Animated Overview: Using Password Managers to Stay Safe Online](https://ssd.eff.org/en/module/animated-overview-using-password-managers-stay-safe-online)

**Level**: Beginner-Intermediate

**Time required**: 30-60 minutes

**Last reviewed:**

6-18-2018

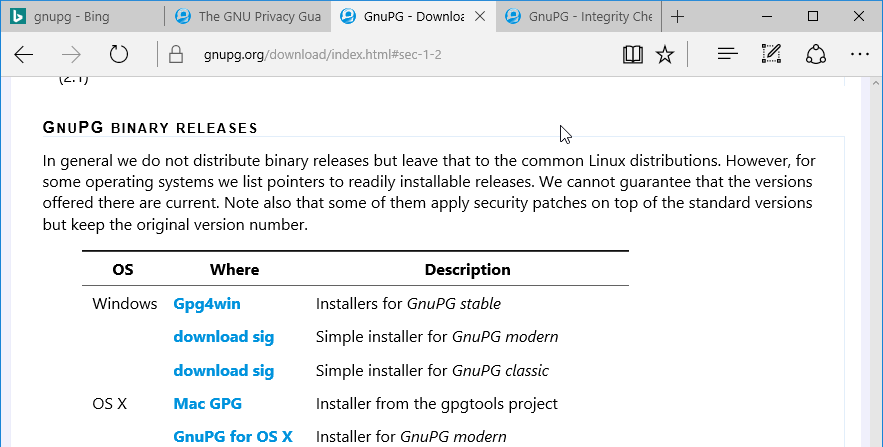
[Pretty Good Privacy[](https://ssd.eff.org/en/glossary/pgp)](https://ssd.eff.org/en/glossary/pgp) ([PGP[](https://ssd.eff.org/en/glossary/pgp)](https://ssd.eff.org/en/glossary/pgp)) is a way to help protect your email communications from being read by anyone except their intended recipients. And, to a lesser extent, it can save your emails from being read if the computer on which they are stored is stolen or broken into.

It can also be used 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.

To use 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[](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key), which you will keep private. The private key is what you will use to [decrypt[](https://ssd.eff.org/en/glossary/decrypt)](https://ssd.eff.org/en/glossary/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.

**Getting GnuPG**[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#1)

You can get GnuPG (also known as GPG) on Windows by downloading the small installer from the [GnuPG download page](https://gnupg.org/download/index.html#sec-1-2).



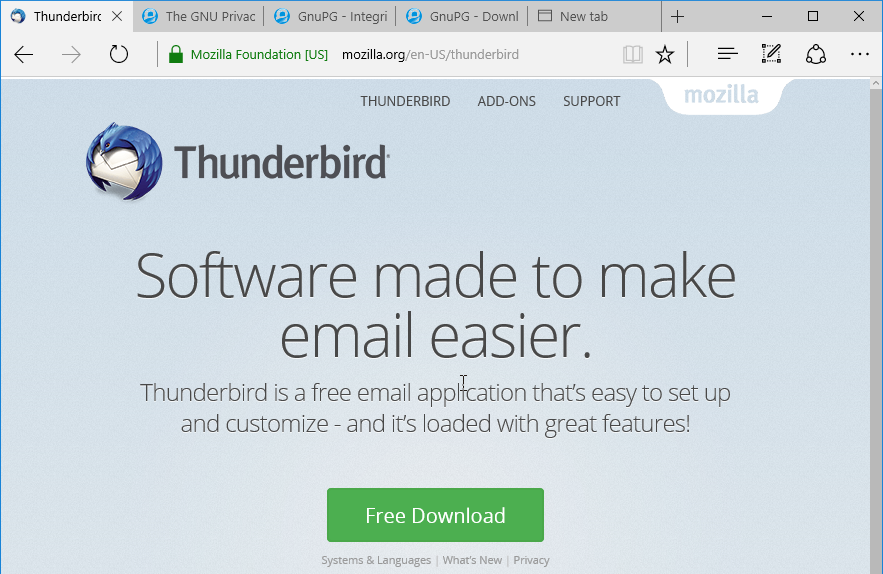
*Click on download* next to “Simple installer for *GnuPG modern*” which will download the GPG installer.

Many browsers will ask you to confirm whether you want to download this file. Microsoft Edge 25 shows a bar at the bottom of the browser window with a blue border.



**Getting Mozilla Thunderbird**[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#2)

Go to the Mozilla Thunderbird [website](https://www.mozilla.org/en-US/thunderbird/).



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

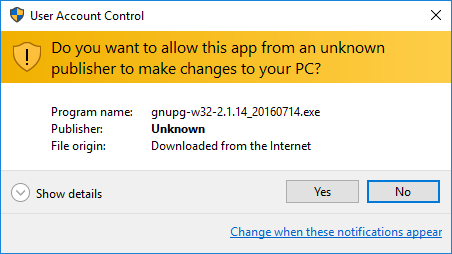
Many browsers will ask you to confirm whether you want to download this file. Microsoft Edge 25 shows a bar at the bottom of the browser window with a blue border.



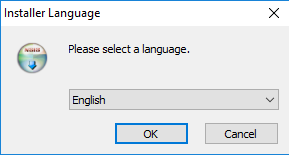
For any browser it is best to first save the file before proceeding, so *click the “Save” button*. By default, most browsers save downloaded files in the Downloads folder.

**Installing GnuPG**[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#3)

Keep the Windows Explorer window open and double-click on gnupg-w32-2.1.14\_20160714.exe. You'll be asked if you want to allow the installation of this program. *Click the “Yes” button.*



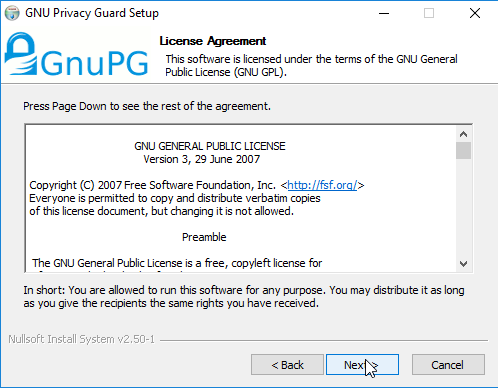
A window will open, asking what language you want to use. You can stick with English. Click the “OK” button.



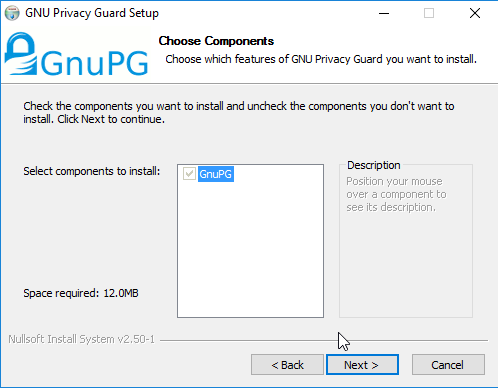
A window will open, giving you an overview of what will be installed. Click the “Next” button.



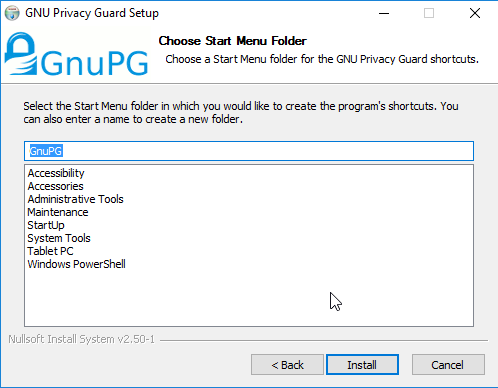
A window with the license agreement will open up. *Click the “Next” button.*



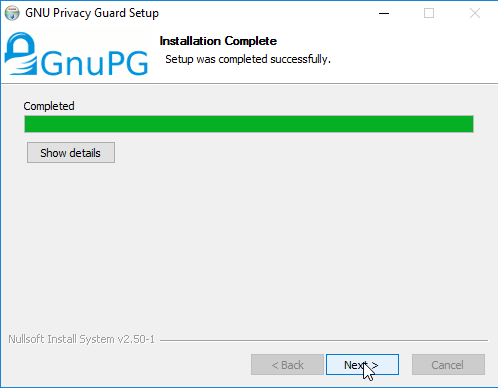
The GnuPG package doesn't have components to select, so *click the “Next“ button again.*



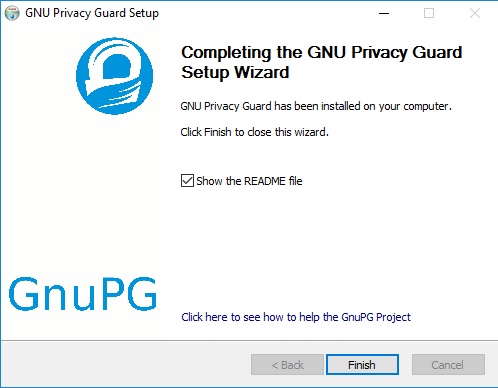
The next window allows you to choose the name in the menu. Leave the default as it is. *Click the “Install” button:*



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



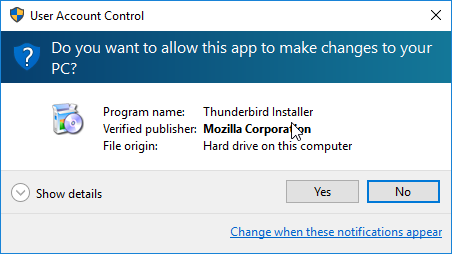
Finally, you are at the last installation step. Remove the check mark next to “Show the README file” and *click the “Finish” button.*



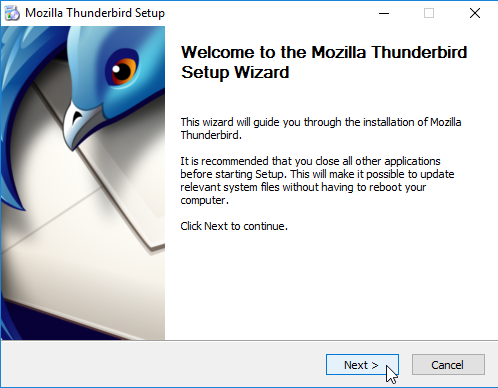
**Installing Mozilla Thunderbird**[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#4)

Similar to GnuPG, you install Mozilla Thunderbird by double-clicking the Thunderbird Setup 45.2.0 file. As usual, you will be asked if you want to run this file. *Click the “Run” button*.

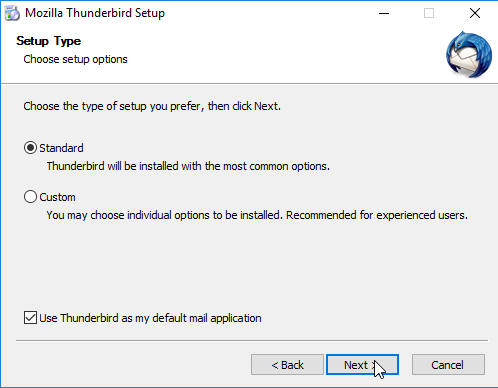
You will be asked if you want to allow Mozilla Thunderbird to make a change to your computer by installing software. *Click the “Yes” button*.



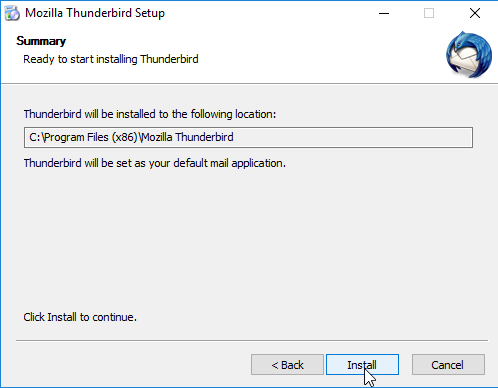
Now the Mozilla Thunderbird starts. Click the “Next” button.



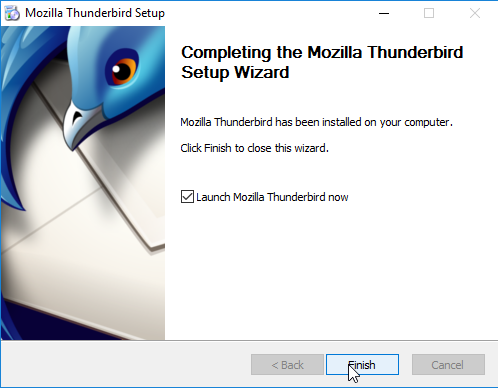
Next, you will get a choice between a Standard setup and a Custom setup. Keep the Standard setup selection and click the “Next” button.



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

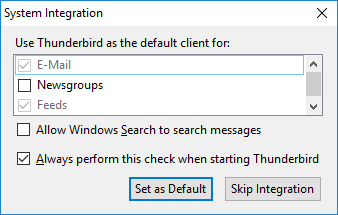


When the installation process is complete, you will see a final window that enables you to launch Mozilla Thunderbird. Click the “Finish” button.

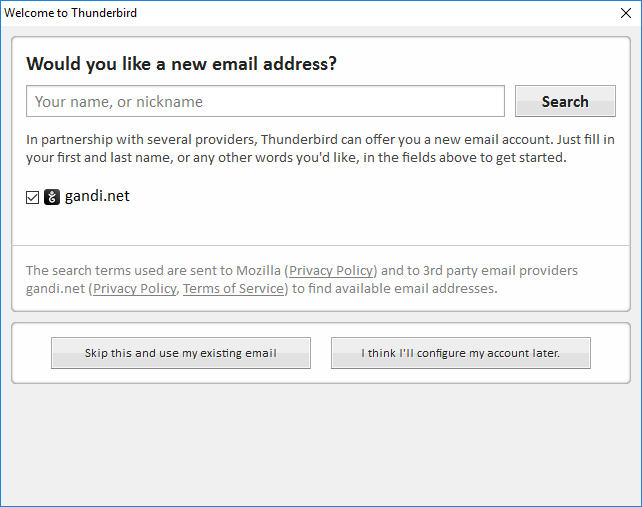


**Preparation for Enigmail Installation**[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#5)

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*.

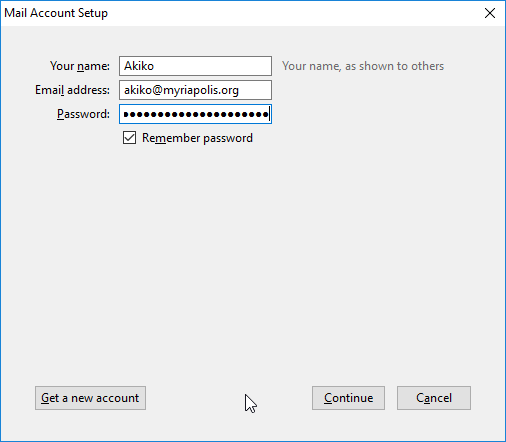


When Mozilla Thunderbird launches for the first time, you will be asked whether you would like a new email address*. Click the “Skip this and use my existing email” button*. Now you will configure Mozilla Thunderbird to be able to receive and send email. If you are used to only reading and sending email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



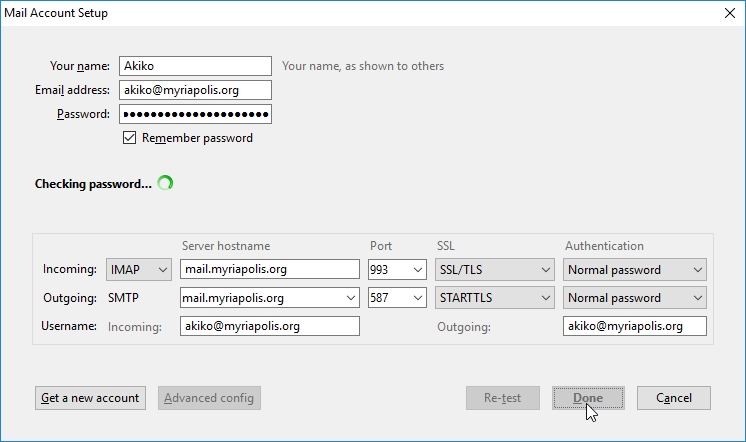
**Adding a Mail Account to Mozilla Thunderbird**

A new window will open:



Enter your name, your email address, and the [password[](https://ssd.eff.org/en/glossary/password)](https://ssd.eff.org/en/glossary/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.

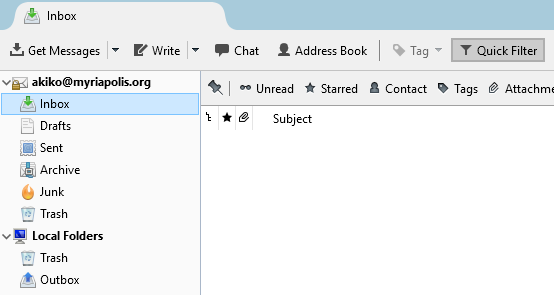


In some cases Mozilla Thunderbird doesn't have complete information and you'll need to enter it yourself. Here is an example of the instructions Google provides for Gmail:

* 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[](https://ssd.eff.org/en/glossary/pseudonym)](https://ssd.eff.org/en/glossary/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[](https://ssd.eff.org/en/glossary/two-factor-authentication)](https://ssd.eff.org/en/glossary/two-factor-authentication) with Google (and depending on your [threat model[](https://ssd.eff.org/en/glossary/threat-model)](https://ssd.eff.org/en/glossary/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/185833?hl=en&rd=1) for doing this.

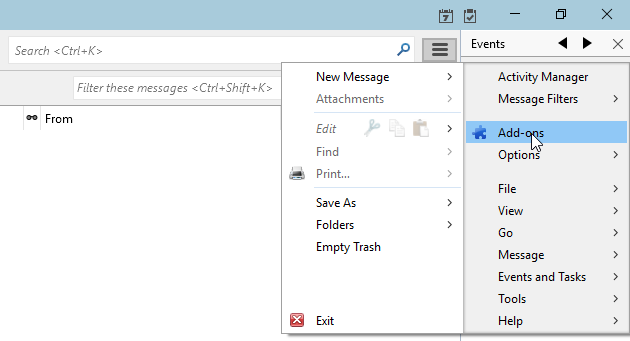
When all the information is entered correctly, *click the “Done” button*.



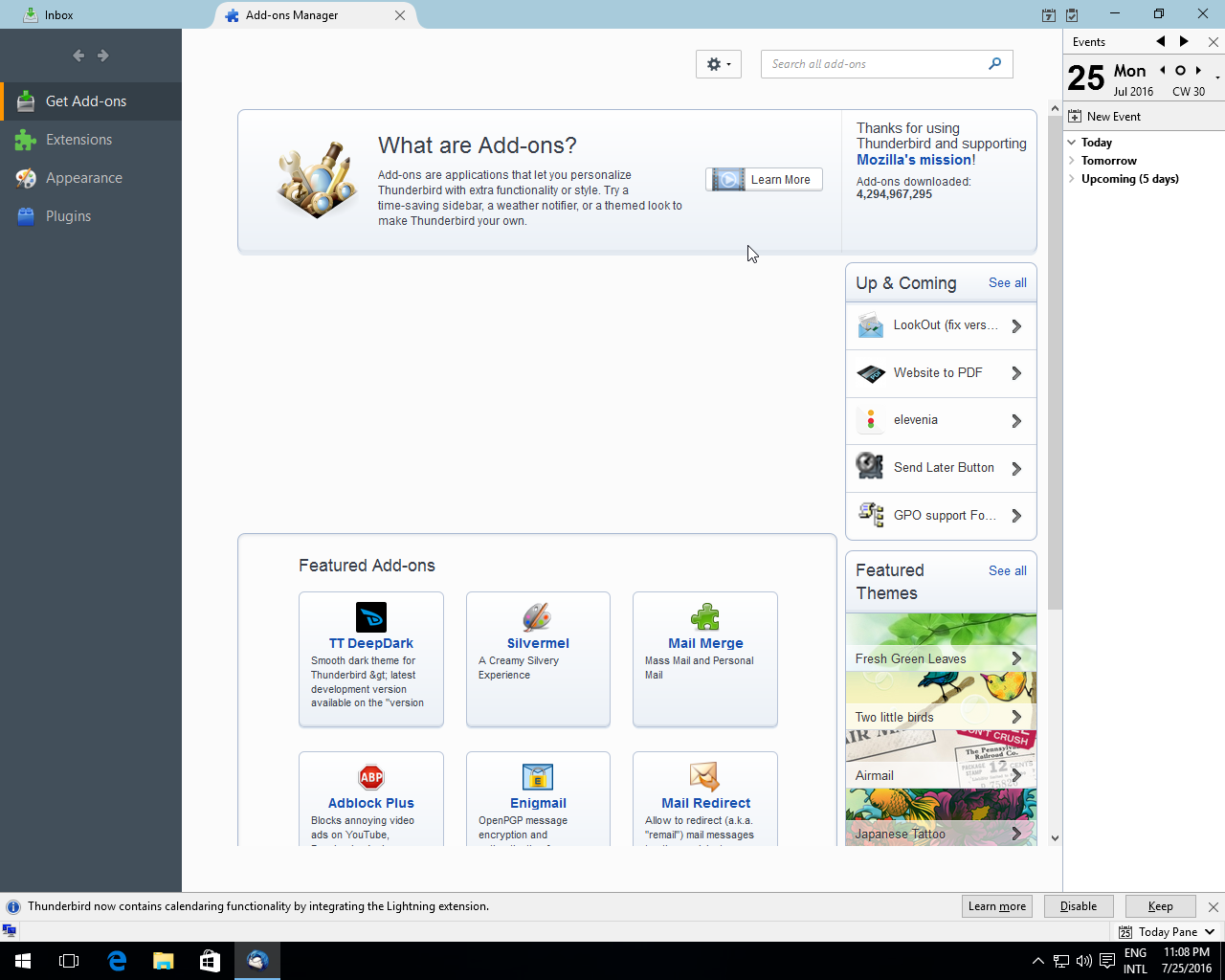
Mozilla Thunderbird will start downloading copies of your email to your computer. Try sending a test email to your friends.

**Installing Enigmail**[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#6)

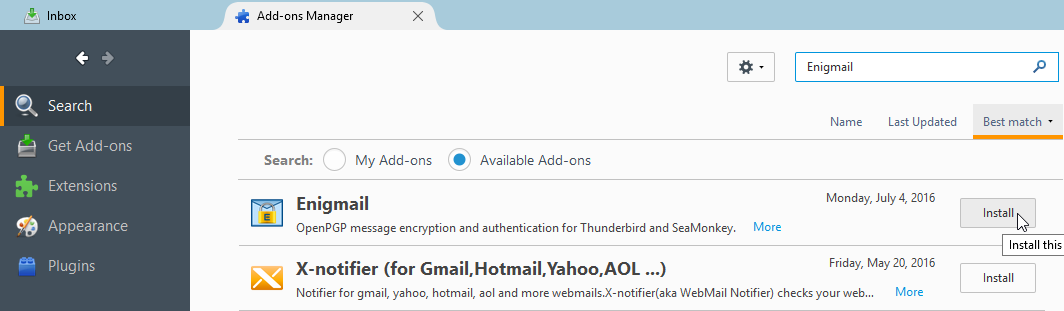
Enigmail is installed in a different way from Mozilla Thunderbird and GnuPG. As mentioned before, Enigmail is an [Add-on[](https://ssd.eff.org/en/glossary/add)](https://ssd.eff.org/en/glossary/add) for Mozilla Thunderbird. *Click the “Menu button,” also called the Hamburger button and select “Add Ons.”*



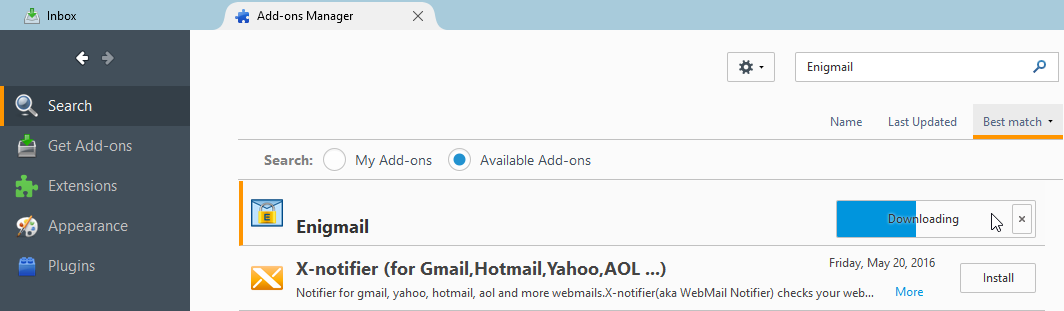
You'll be taken to an Add-ons Manager tab.

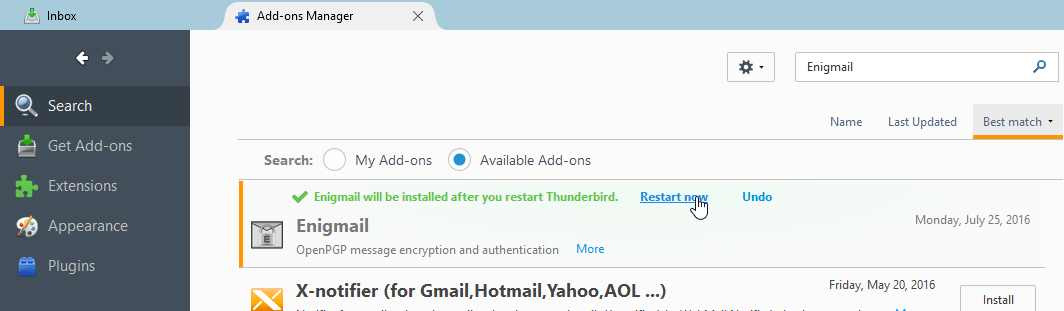


Enter "Enigmail" into the Add-on search field to look for Enigmail on the Mozilla Add-on site.

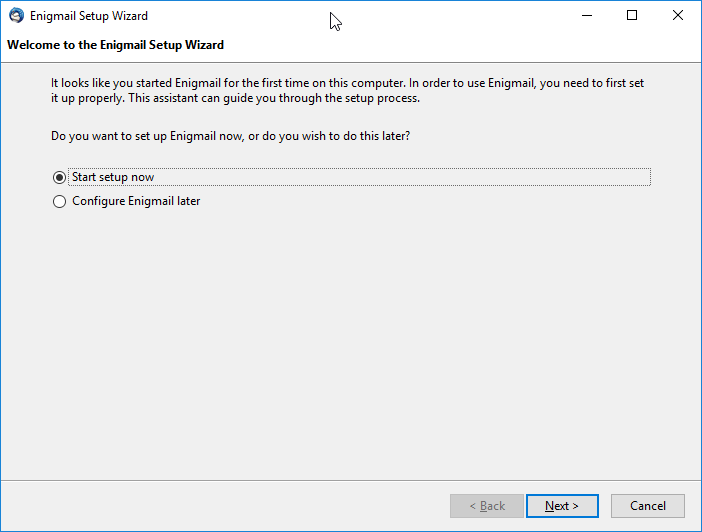


Enigmail will be the first option. *Click the "Install" button.*

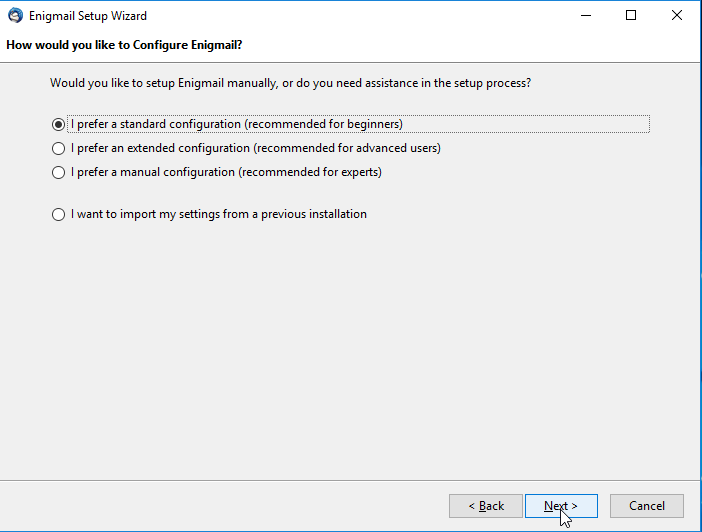




After the Enigmail add-on is installed Mozilla Thunderbird will ask to restart the browser to activate Enigmail. *Click the “Restart Now” button and Mozilla Thunderbird will restart*.



When Mozilla Thunderbird restarts an additional window will open up that will start the process of setting up the Enigmail add-on. *Keep the “Start setup now” button selected and click the “Next” button.*



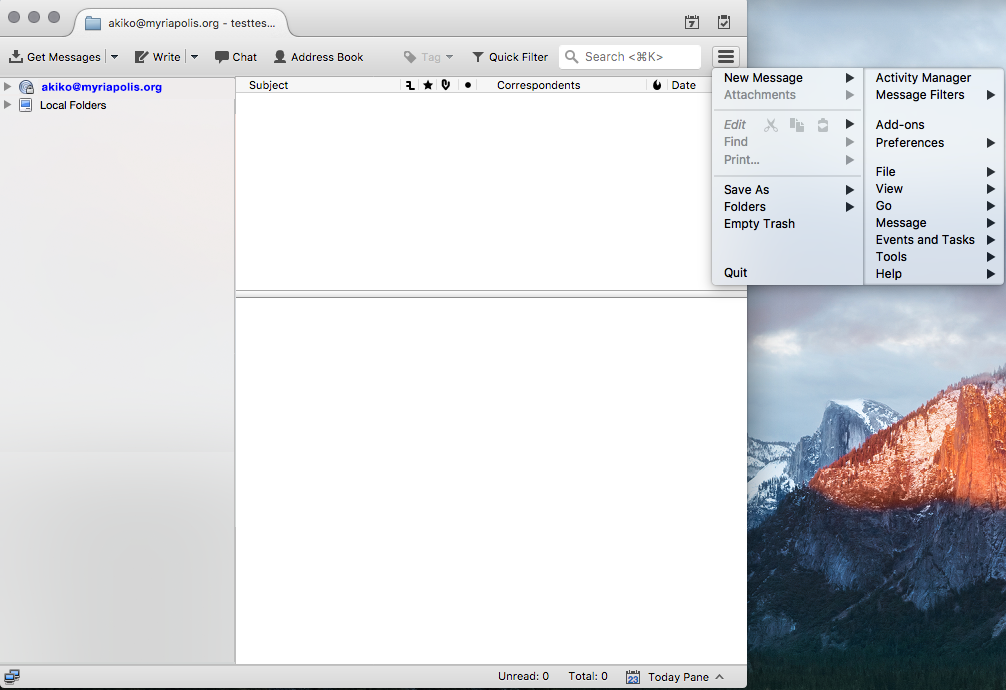
**Required Configuration Steps**[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#6)

In May 2018 researchers [revealed](https://efail.de/) several vulnerabilities in [PGP[](https://ssd.eff.org/en/glossary/pgp)](https://ssd.eff.org/en/glossary/pgp) (including GPG) for email, and theorized many more which others could build upon.

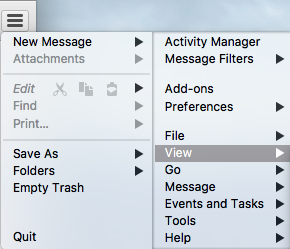
Thunderbird and Enigmail’s developers have been working on ways to protect against the EFAIL vulnerabilities. As of [version 2.0.6](https://sourceforge.net/p/enigmail/forum/announce/thread/5772757e/) (released May 27, 2018), Enigmail has released patches that defend against all known exploits described in the EFAIL paper, along with some new ones in the same class that other researchers were [able to devise](https://twitter.com/hanno/status/997138771194859521), which beat earlier Enigmail fixes. Each new fix made it a little harder for an attacker to get through Enigmail’s defenses. We feel confident that, if you update to this version of Enigmail (and keep updating!), Thunderbird users can turn their PGP back on.

But, while Enigmail now defends against most known attacks even with HTML on, the EFAIL vulnerability demonstrated just how dangerous HTML in email is for security. Thus, we recommend that Enigmail users also turn off HTML by going to View > Message Body As > Plain Text.

1. First click on the Thunderbird **hamburger menu** (the three horizontal lines).



2. Select “**View**” from the right side of the menu that appears.



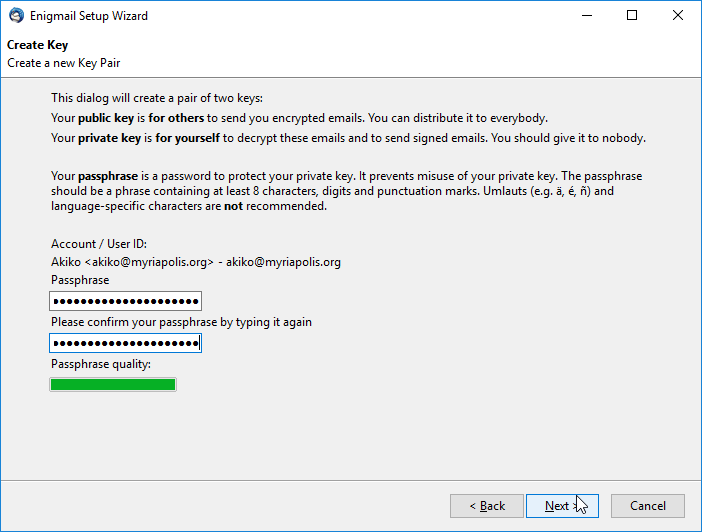
3. Select “**Message Body As**” from the menu that appears, then select the “**Plain Text**” radio option.



Viewing all email in plaintext can be hard, and not just because many services send only HTML emails. Turning off HTML mail can pose some usability problems, such as [some attachments failing to show up](https://twitter.com/micahflee/status/998984671995166721). Thunderbird users shouldn't have to make this trade-off between usability and security, so we hope that Thunderbird will take a closer look at supporting their plaintext community from now on. As the software is now, however, users will need to decide for themselves whether to take the [risk[](https://ssd.eff.org/en/glossary/risk-assessment)](https://ssd.eff.org/en/glossary/risk-assessment) of using HTML mail; the most vulnerable users should probably not take that risk, but the right choice for your community is a judgment call [based on your situation](https://ssd.eff.org/en/module/assessing-your-risks).

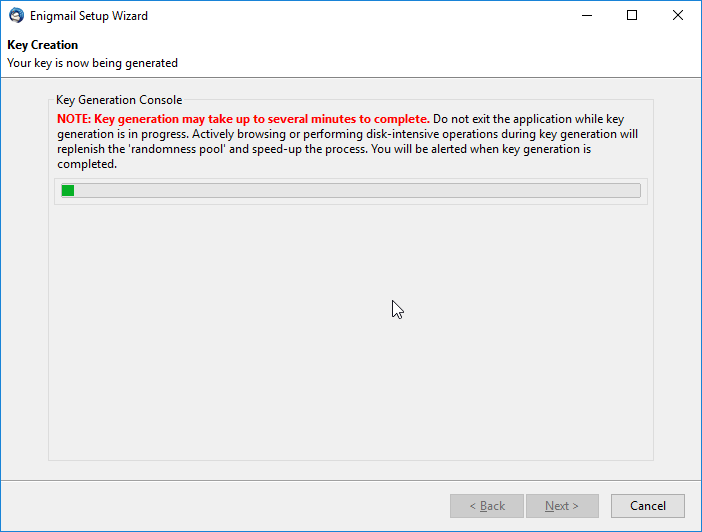
Now you will start creating your private [key[](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key) and public key. Learn more about keys, and what they are, in our [Introduction to Public Key Cryptography and PGP guide](https://ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp#1).

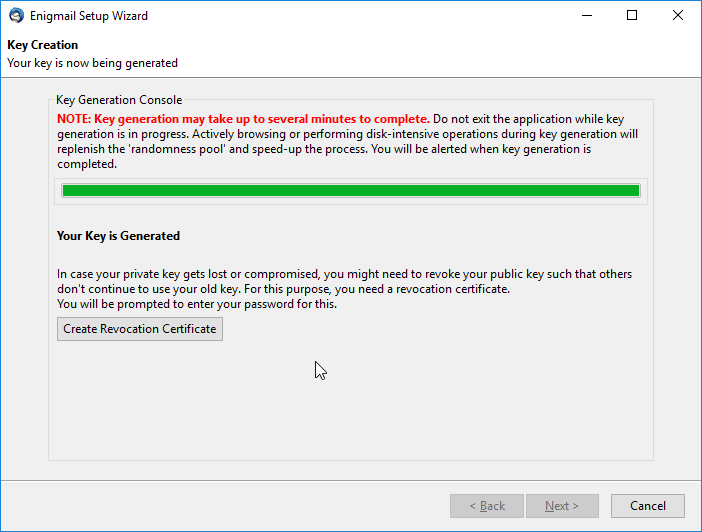
**Creating a Public Key and Private Key**[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#7)



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) for your private key.

*Click the "Next" button.*



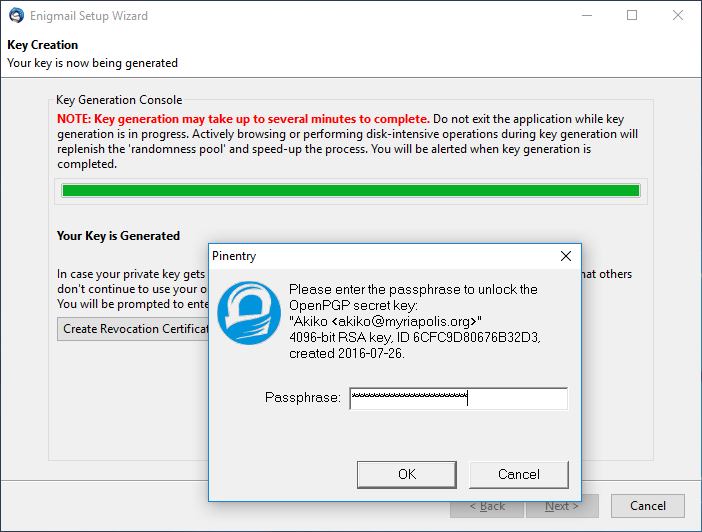


Your key will expire at a certain time; when that happens, other people will stop using it entirely for new emails to you, though you might not get any warning or explanation about why. So, you may want to mark your calendar and pay attention to this issue a month or so before the expiration date.

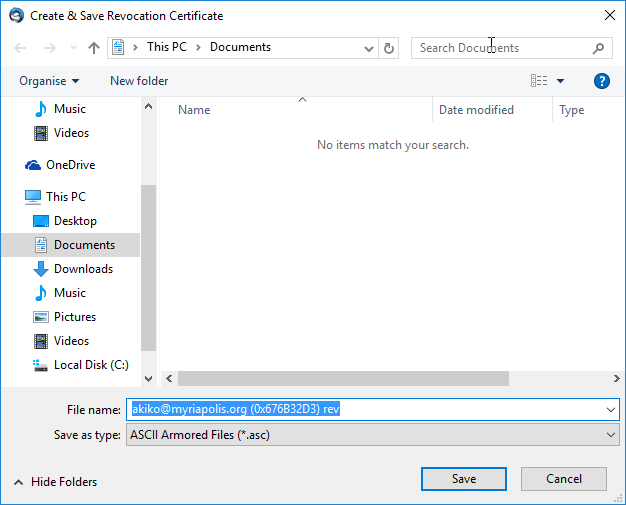
It's possible to extend the lifetime of an existing key by giving it a new, later expiration date, or it's possible to replace it with a new key by creating a fresh one from scratch. Both processes might require contacting people who email you and making sure that they get the updated key; current software 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[](https://ssd.eff.org/en/glossary/pgp)](https://ssd.eff.org/en/glossary/pgp).

To check your key's expiration date in Thunderbird, click the Enigmail menu and select "Key Management." Search for your key in the Enigmail Key Management window and double click on it. A new window will open and your key's expiration date will be displayed in the field called "Expiry." To set a new expiration date, click the "Change" button next to your key's current expiration date. Remember to send your updated public key to your contacts or publish it to a keyserver if you update your key's expiration date.

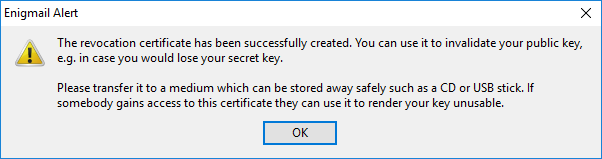
Enigmail will generate the key and when it is complete, a small window will open asking you to generate a [revocation certificate[](https://ssd.eff.org/en/glossary/revocation-certificate)](https://ssd.eff.org/en/glossary/revocation-certificate). This revocation certificate is important to have as it allows you to make the private key and public key invalid in the event you lose your private key or it gets stolen. For this reason, store your revocation certificate separately from your private key; burn it to a CD or put it on a USB drive and keep it somewhere safe. Publishing the revocation certificate to a keyserver will let other PGP users know not to use or trust that public key. It is important to note that merely deleting the private key does not invalidate the public key and may lead others to sending you encrypted mail that you can't [decrypt[](https://ssd.eff.org/en/glossary/decrypt)](https://ssd.eff.org/en/glossary/decrypt). *Click the “Generate Certificate” button*.



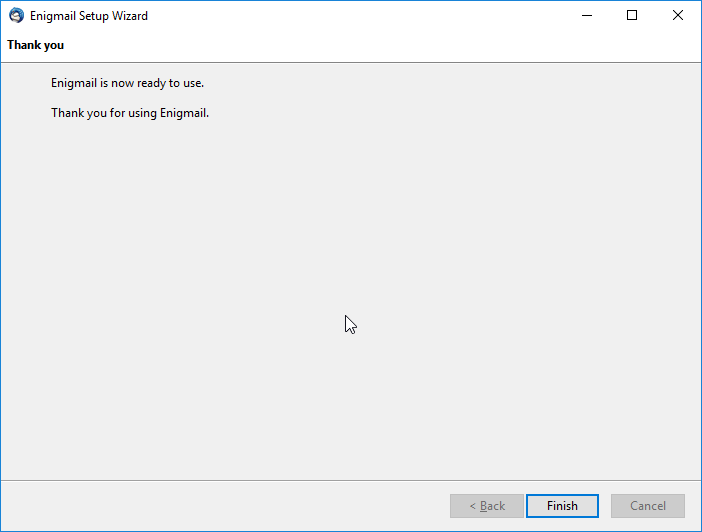
First you will be asked to provide the [passphrase[](https://ssd.eff.org/en/glossary/passphrase)](https://ssd.eff.org/en/glossary/passphrase) you used when you created the PGP key. *Click the “OK” button.*



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 to a USB drive that you are using for nothing else and storing the drive in a safe space. We also recommend removing the revocation certificate from the computer with the keys, just to avoid unintentional revocation. Even better, save this file on an 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.*

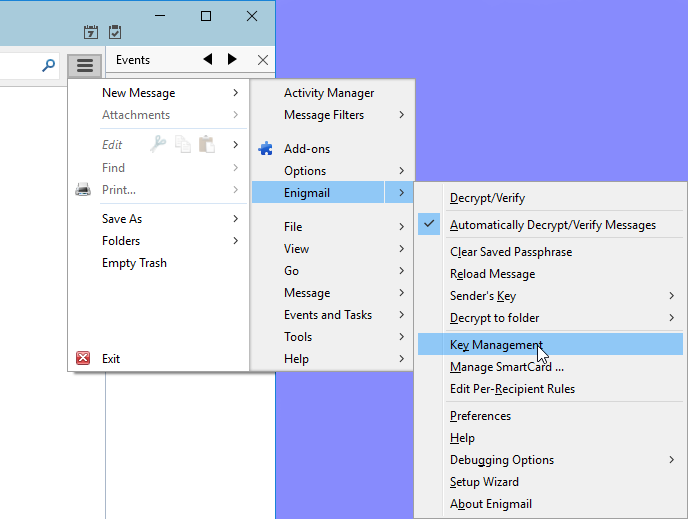


Finally, you are done with generating the private key and public key. *Click the “Finish” button.*

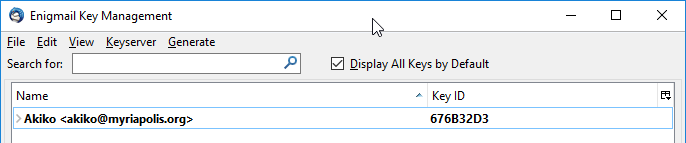
**Optional configuration steps**[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#8)

**Display Fingerprints and**[**Key[](https://ssd.eff.org/en/glossary/key)**](https://ssd.eff.org/en/glossary/key)**Validity**

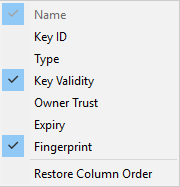
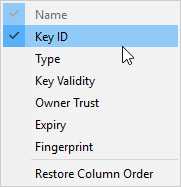
The next steps are completely optional but they can be helpful when using OpenPGP and Enigmail. Briefly, the Key ID is a small part of the [fingerprint[](https://ssd.eff.org/en/glossary/fingerprint)](https://ssd.eff.org/en/glossary/fingerprint). When it comes to verifying that a public key belongs to 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.



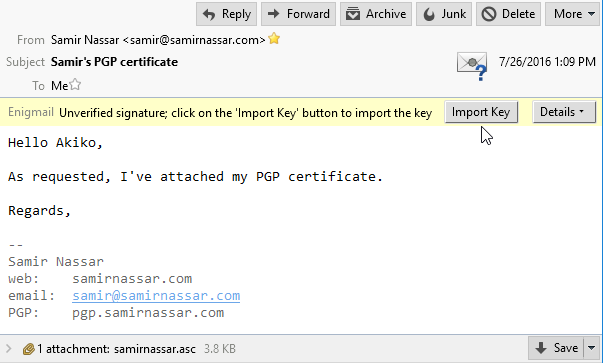
On the far right there is a small button. *Click that button to configure the columns.* *Unclick the Key ID option and click the Fingerprint option and the Key Validity option.*



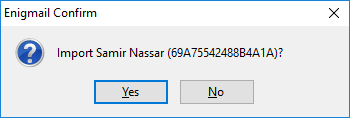
Now there will be three columns: Name, Key Validity, and Fingerprint.

**Finding Other People Who Are Using PGP**[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#9)

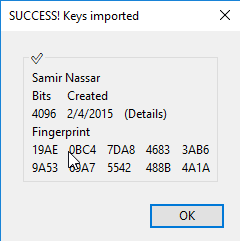
**Getting a Public**[**Key[](https://ssd.eff.org/en/glossary/key)**](https://ssd.eff.org/en/glossary/key)**by Email**



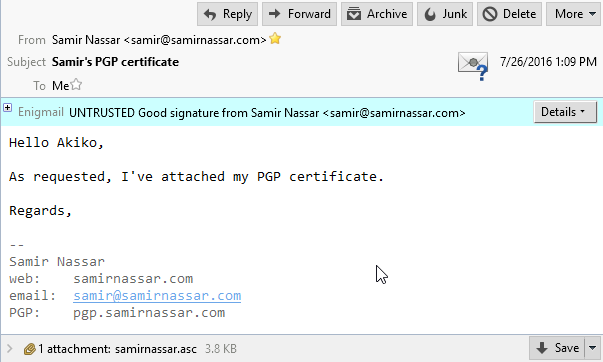
You might get a public key sent to you as an email attachment. *Click on the "Import Key"* button.

****

A small window will open asking you to confirm importing the PGP key. *Click the "Yes" button.*

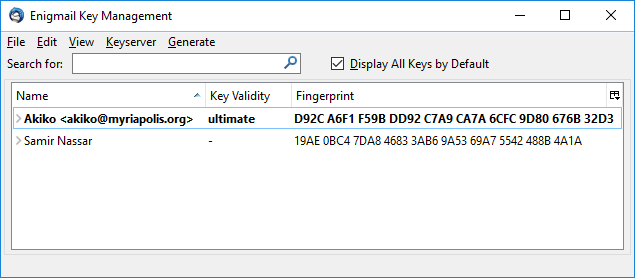


A new window will open with the results of the import. *Click the “OK” button.*



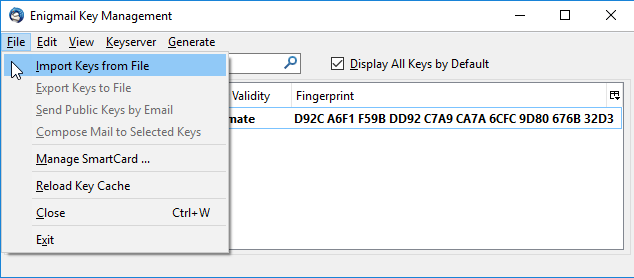
If you reload the original email you’ll see that the bar over the email has changed.

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.

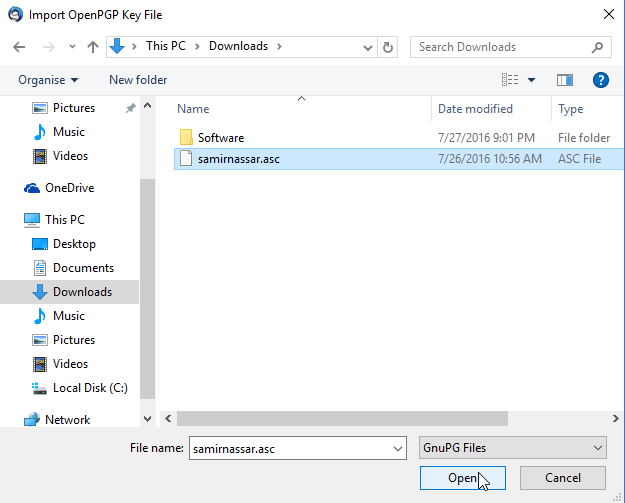


**Getting a Public Key as a File**

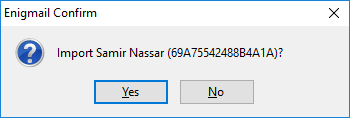
It's possible that you get a public key by downloading it from a website or someone might have sent it through chat software. In a case like this, we will assume you downloaded the file to the Downloads folder.



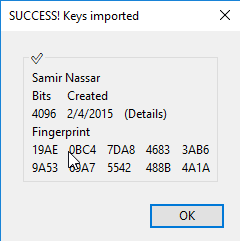
Open the Enigmail Key Manager and *click on the “File” menu. Select “Import Keys from File.”*



Select the public key, it might have very different file name endings such as .asc, .pgp, or .gpg. *Click the “Open” button.*



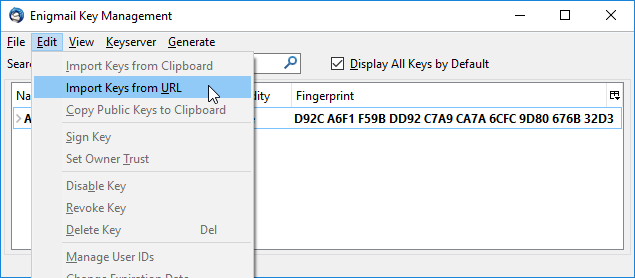
A small window will open asking you to confirm importing the PGP key. *Click the “Yes” button.*



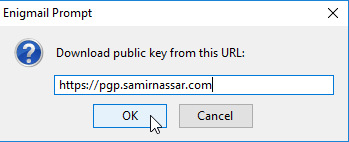
A new window will open with the results of the import.*Click the “OK” button.*

**Getting a Public Key From a URL**

It's possible to get a public key by downloading it directly from a URL

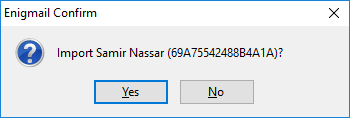


Open the Enigmail Key Manager and *click on the “Edit” menu. Select “Import Keys from URL.”*

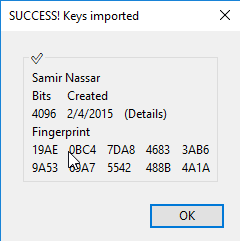


Enter the URL. The URL can have several forms. Most often it is likely a [domain name[](https://ssd.eff.org/en/glossary/domain-name)](https://ssd.eff.org/en/glossary/domain-name) ending in a file.

Once you have the right URL, *click the “OK” button.*



A small window will open asking you to confirm importing the PGP key. *Click the "Yes" button.*

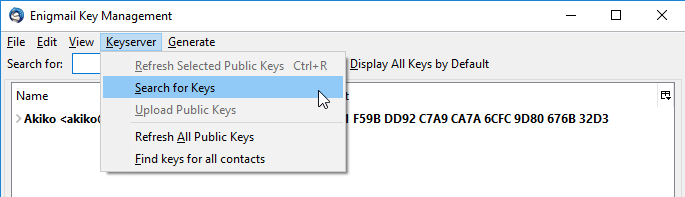


A new window will open with the results of the import. *Click the "OK" button.*

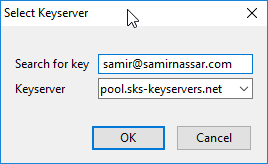
If you look at <https://www.eff.org/about/staff> you will notice a “PGP Key” link under the staff pictures. Danny O'Brien's PGP key, for example, can be found at: <https://www.eff.org/files/pubkeydanny.txt>.

**Getting a public key from a key server**

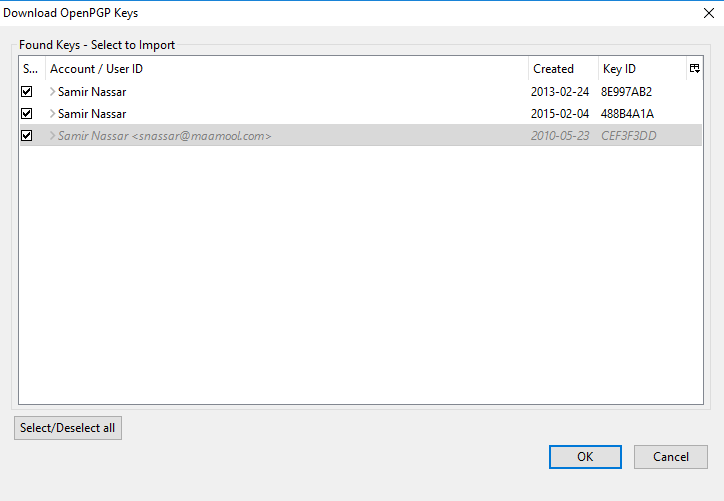
Keyservers can be a very useful way of getting public key. Try looking for a public key.



From the Key Management interface *click the “Keyserver”* menu and *select “Search for Keys.”*

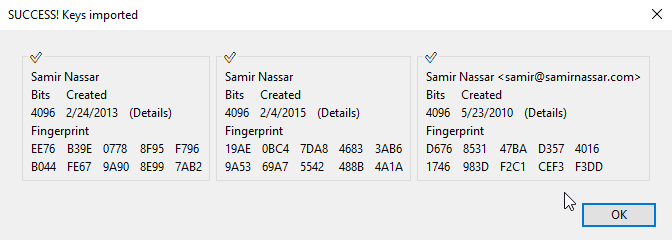


A small window will pop up with a search field. You can search by a complete email address, a partial email address, or a name. In this case, you will search for keys containing “[samir@samirnassar.com](mailto:samir@samirnassar.com)”. *Click the “OK” button.*



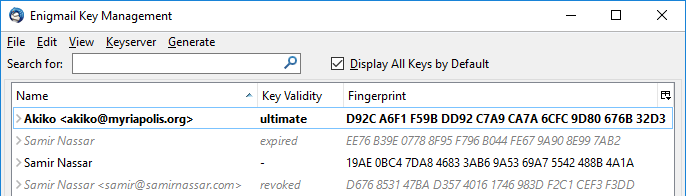
A larger window will pop up with many options. If you scroll down you'll notice some keys are italicized and grayed out. These are keys that have either been revoked or expired on their own.

We have several PGP keys for Samir Nassar and we don’t yet know which one to choose. One key is in grey italics which means that it has been revoked. Because we don’t know which one we want yet, we will import them all. *Select the keys by clicking the box on the left then press the “OK” button.*



A small notification window will pop up letting you know if you succeeded. *Click the “OK” button.*

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



Note that of the three imported keys, one is expired, one is revoked, and one is currently a valid key.

**Letting others know you are using PGP**[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#10)

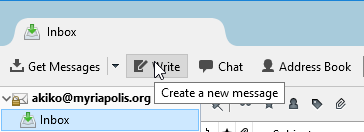
Now that you have PGP, you want to let others know that you are using it so they can also send you encrypted messages using PGP.

Using PGP doesn't completely [encrypt[](https://ssd.eff.org/en/glossary/encrypt)](https://ssd.eff.org/en/glossary/encrypt) your email: the sender and receiver information is unencrypted. Encrypting the sender and receiver information would break email. Using Thunderbird with the Enigmail [add-on[](https://ssd.eff.org/en/glossary/add)](https://ssd.eff.org/en/glossary/add) gives you an easy way to encrypt and [decrypt[](https://ssd.eff.org/en/glossary/decrypt)](https://ssd.eff.org/en/glossary/decrypt) the content of your email.

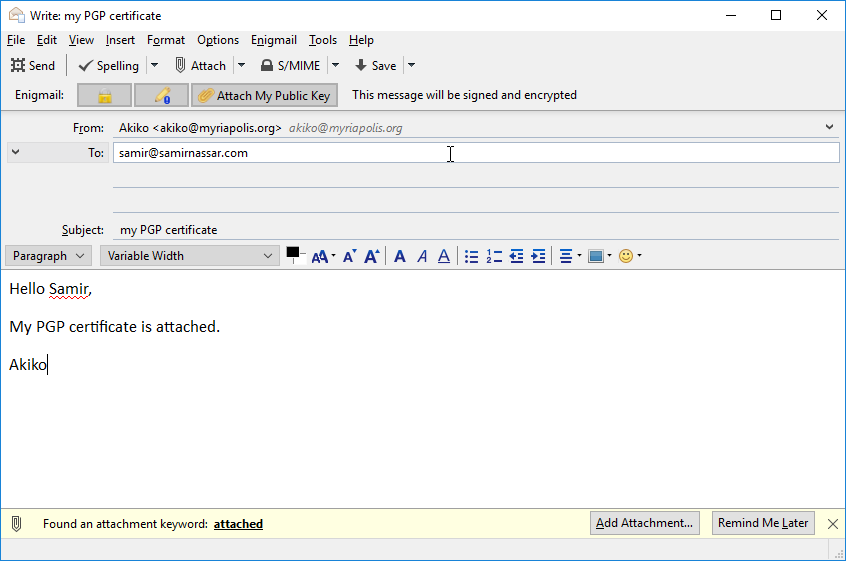
Let's look at three different ways you can let people know you are using PGP.

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

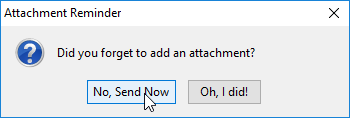
You can easily email your public [key[](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key) to another person by sending them a copy as an attachment.



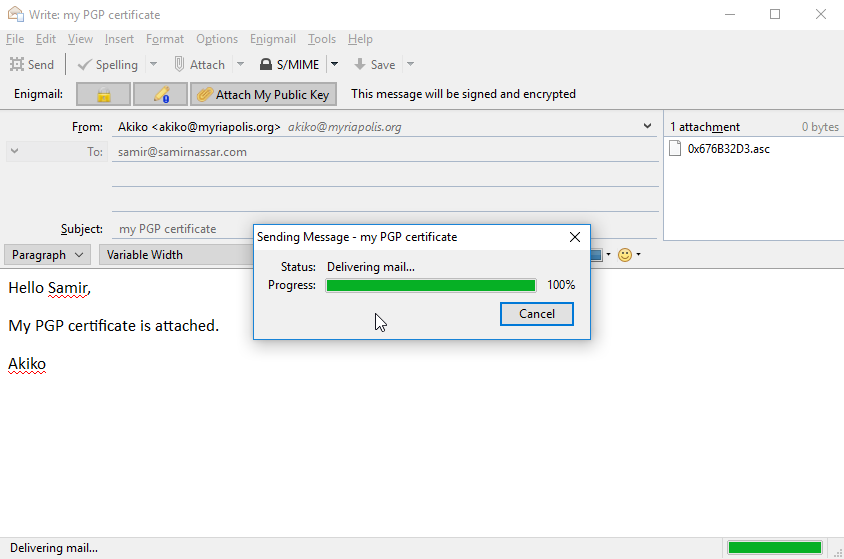
*Click the "Write" button in Mozilla Thunderbird.*



Fill in an address and a subject, perhaps something my “my public key,” click the “Attach My Public Key” button. If you have already imported a PGP key for the person you are sending the PGP key to, the Lock icon in the Enigmail bar will be highlighted. As an additional option, you can also click the Pencil icon to sign the email, giving the recipient a way to verify the authenticity of the email later.

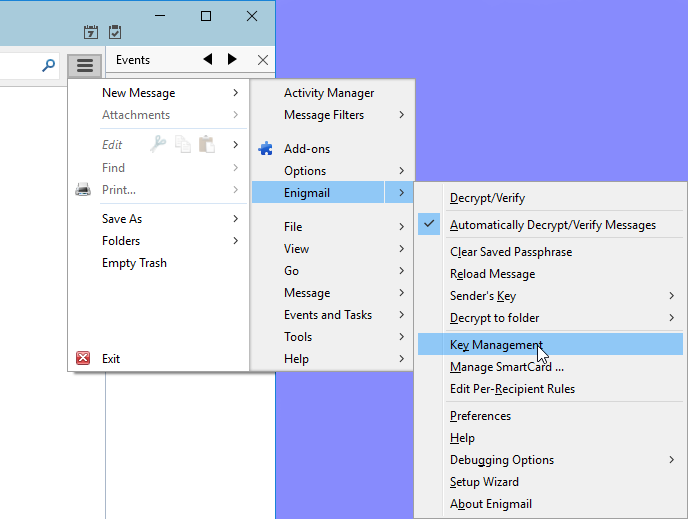


A window will pop open asking you if you forgot to add an attachment. This is a bug in the interaction between Enigmail and Mozilla Thunderbird, but don’t worry, your public key will be attached. *Click the “No, Send Now” button.*See below for proof:

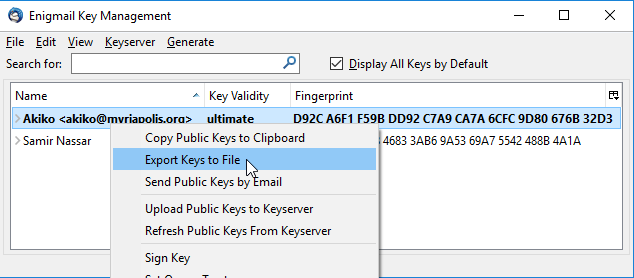


**Let people know you are using PGP on your website**

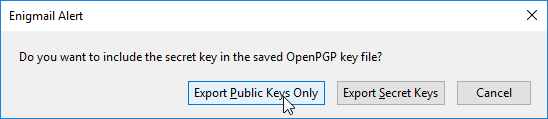
In addition to letting people know via email, you can post your public key on your website. The easiest way is to upload the file and link to it. This guide won't go into how to do those things, but you should know how to export the key as a file to use in the future.



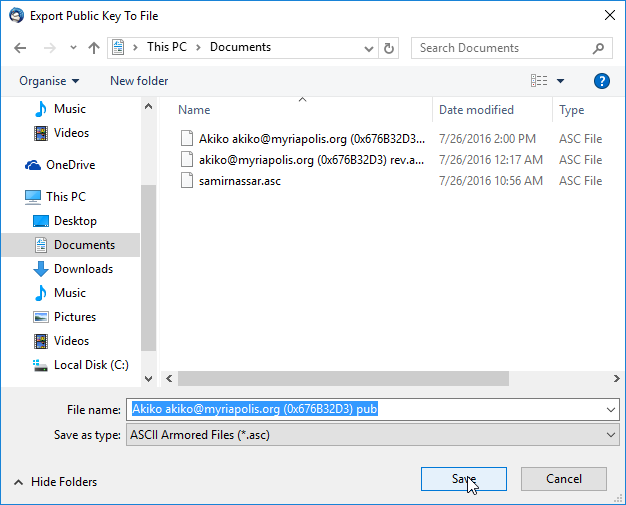
*Click the configuration button, then the Enigmail option, then Key Management.*



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

****[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#10)

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



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.

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[](https://ssd.eff.org/en/glossary/password)](https://ssd.eff.org/en/glossary/password).

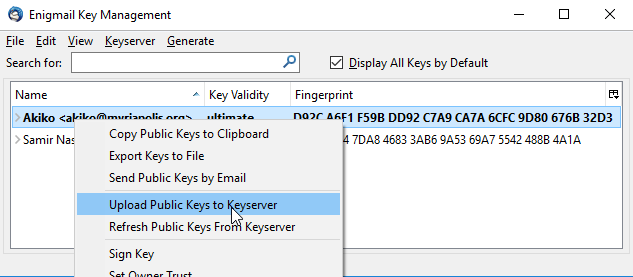
**Uploading to a keyserver**

Keyservers make it easier to search for and download public keys of others. 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.

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 certificate without the ability to remove this information at a later time.

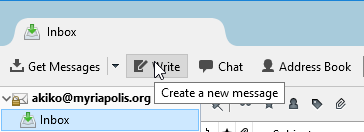
If you choose to upload your public key to keyservers, you will go back to the Enigmail Key Management window.



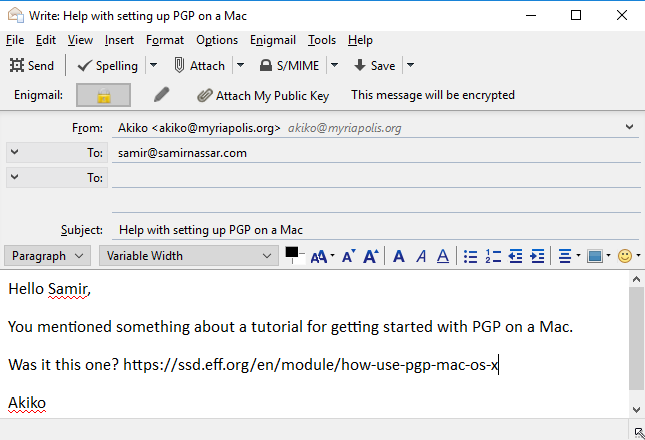
Right-click your PGP key and select the Upload Public Keys to Keyserver option.

**Sending PGP Encrypted Mail**[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#10)

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.

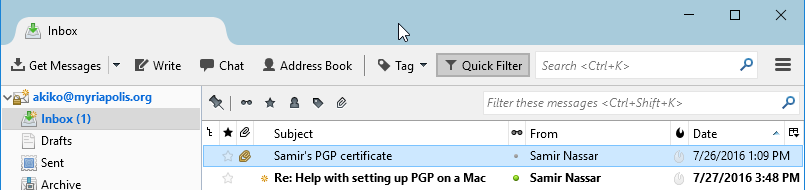
The subject line won't be encrypted, so choose something innocuous, like "hello."

The body of the email was encrypted and transformed. For example the text above will be transformed into something like this:

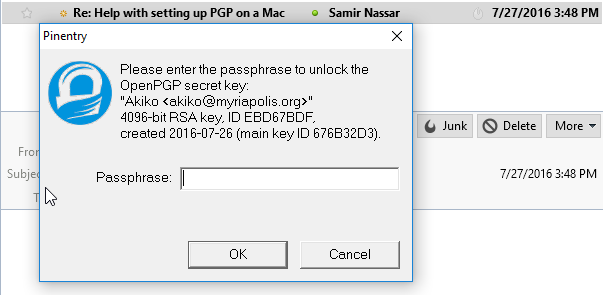


**Receiving PGP Encrypted Mail**[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#11)

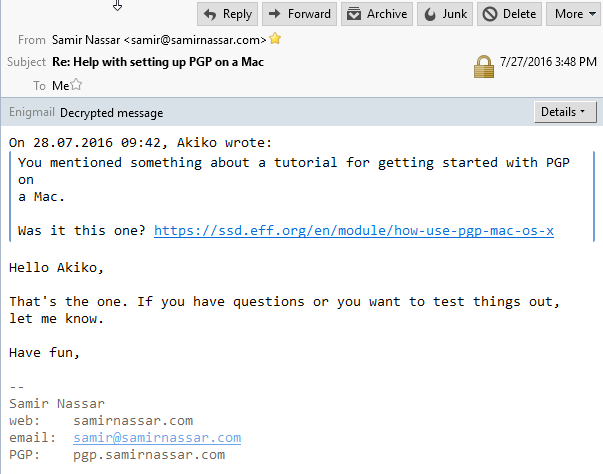
Let's go through what happens when you receive encrypted email.



Notice that Mozilla Thunderbird is letting you know you have new mail. *Click on the message.*



A small window opens asking you for the [password[](https://ssd.eff.org/en/glossary/password)](https://ssd.eff.org/en/glossary/password) to the PGP [key[](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key). Remember: Don't enter your email password. *Click the "OK" button.*



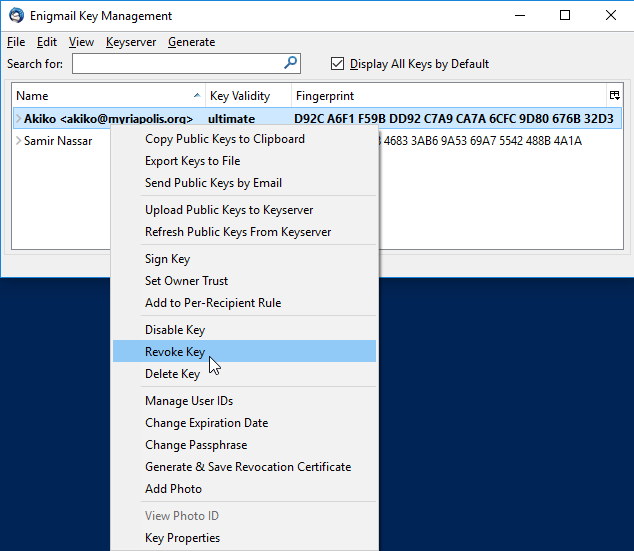
Now the message will show up decrypted.

**Revoking the PGP Key**[**Anchor link**](https://ssd.eff.org/en/module/how-use-pgp-windows#12)

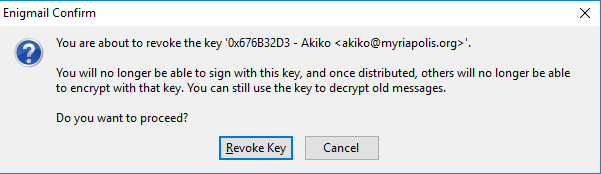
**Revoking Your PGP Key Through the Enigmail Interface**

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.

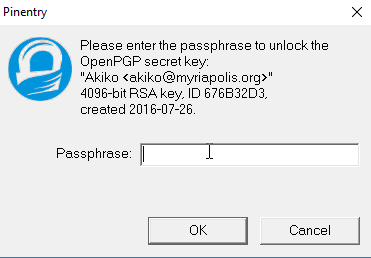
You might have a good reason to disable the PGP key before it expires. Perhaps you want to generate a new, stronger PGP key. The easiest way to revoke your own PGP key in Enigmail is through the Enigmail Key Manager.



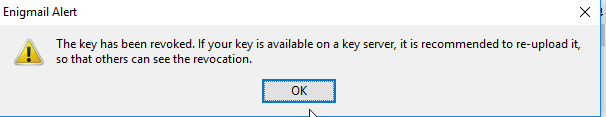
Right click on your PGP key, it's in bold, and *select the "Revoke Key" option.*



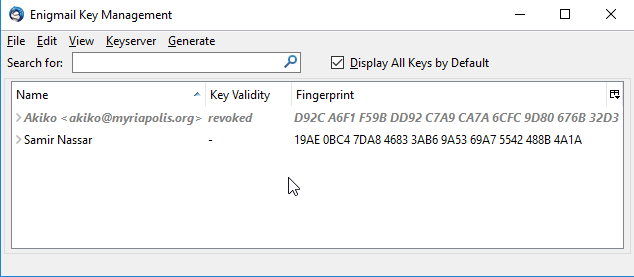
A window will pop up letting you know what happens and asking for your confirmation. *Click the “Revoke Key” button.*



The [password[](https://ssd.eff.org/en/glossary/password)](https://ssd.eff.org/en/glossary/password) window opens, enter your password for the PGP key and *click to "OK" button.*



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

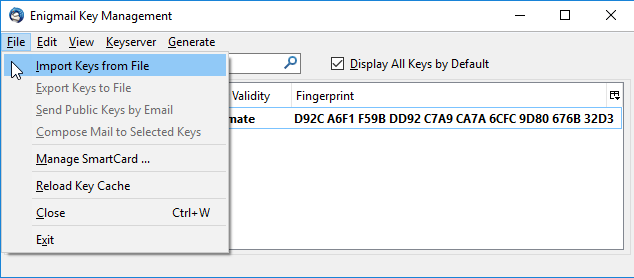


When you go back to the Enigmail Key Management window you'll notice a change to your PGP key. It is now grayed out and italicized.

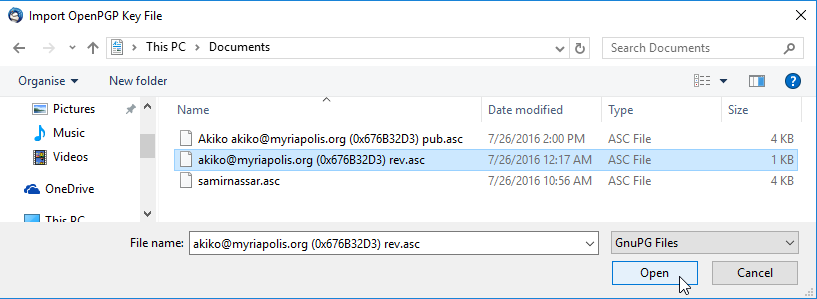
**Revoking a PGP Key with a**[**Revocation Certificate[](https://ssd.eff.org/en/glossary/revocation-certificate)**](https://ssd.eff.org/en/glossary/revocation-certificate)

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. 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.

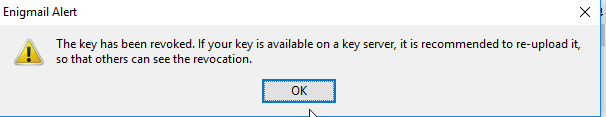
You might get sent revocation certificates from friends as a notice that they want to revoke their key. Since you already have a revocation certificate, you will use the one you generated earlier to revoke your own key.



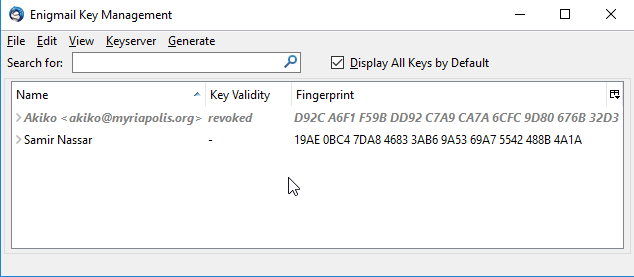
Start with the Enigmail Key Manager and *click the “File” menu and select “Import Keys from File.”*



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.*



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.

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