A REPORT FROM SOVEREIGNMAN.COM

EMAIL ENCRYPTION

HOW TO SECURE YOUR EMAILS **FOR FREE** WITH THE STRONGEST ENCRYPTION IN THE WORLD

A BLACK PAPER

SOVEREIGN MAN

Why You Should Encrypt Your Emails

Sending an unsecured email is like shouting something across a crowded room… if you expect the information to be kept private that is probably one of the worst methods available. You might as well rent a billboard so everyone can see.

And as the whole recent PRISM surveillance debacle has brought to light, if you suspected it was a bad idea to use Gmail or Hotmail(now Outlook), you've been proven correct!

So please don't use Gmail or any other common cloud based email service provider if you want to keep your communication and location private. All of these companies will bend over backwards to hand over your data as soon as a government agency knocks on their door.

Even Hushmail, a company that prides itself with offering "Free Email with Privacy", has been proven to be not so private, as in the cases where they have handed over cleartext copies of private e-mail messages at the request of law enforcement agencies. They also, just as the other big online email services, record your IP address (and thus location) every time you log in to check your email.

You see, the problem with the internet is that there are so many touch points. Email traffic is routed across a hierarchy of networks, and between the sender, the receiver, the various email hosts, internet service providers, etc., there are a number of nodes that have access to our data. Consequently, network transmissions are anything but private and secure.

Governments figured this out a long time ago. In the United States, for example, the government set up a series of special encrypted networks that function just like the internet. The Department of State and Department of Defense (ok, offense) uses a network called JWICS.

JWICS, pronounced Jay Wicks, stands for Joint Worldwide Intelligence Communication System– essentially; it is a secure version of the regular Internet. Special computers that sit in buildings with no windows communicate with each other through high level encryption algorithms.

Functionally, JWICS looks similar to the Internet that everyone else uses– there's email, web pages, etc. From a technical perspective, though, JWICS is highly secure, and the government uses it to transmit classified information up to the Top Secret level.

While you can't plug in to the government's classified networks, you can use free software to create your own secure environment, and this is exactly what you'll learn in this Black Paper.

One precaution I'd like to leave you with before we get started is that encryption is not some magic pill that will guarantee your privacy. You can have the strongest encryption in the world but if your password is weak, or someone steals your friends laptop and gains access to his email account, then encryption won't help you.

No matter how strong encryption you use the bottom line is that the safest way to communicate with someone in private is still to leave your phone and laptop at home and take a walk together.

Now let's get started.

Encrypting Your Emails With PGP:

The email encryption standard bar none is PGP, or its free cousin Gnu Privacy Guard. PGP is so good that when it was first invented, the US government considered it a military-grade weapon… and they spent years trying to pin criminal charges on its inventor Phil Zimmerman for violating the Arms Export Control Act.

PGP, which stands innocuously for "Pretty Good Privacy," is the closest you could possibly get to NSA level encryption. The algorithm uses a unique 'public key / private key' model that has confounded government authorities around the world.

HOW IT WORKS

It works something like this:

Everyone who uses PGP has two 'keys', a public key and a private key. For a physical example, imagine you literally have two physical keys and a lock box. The public key is appropriately named because you give it out to everyone… you go down to the locksmith and make hundreds of keys to hand out to your friends and business associates.

Anyone who wants to send you a secure message can write it on a piece of paper and put it in the lock box. Using their public key, they can lock the box, but they cannot unlock it. The only person who can unlock the box to read the message is you, using your private key. Naturally, you keep your private key secret.

In the email world, it essentially works the same. The sender will encrypt a message using your public key. Once this happens, the email message will look like a bunch of gibberish. This gibberish is what is sent across the network, so anyone who intercepts the message will only be able to see the gibberish, not the actual message.

Once you receive the message, you decrypt the gibberish with your private key, and voila, the original message is displayed in plain text.

So how secure is PGP? In a word, very. Nothing is unbreakable, but it would take teams of analysts and supercomputers quite a number of years to crack the code, if they could do it at all. Bottom line, governments will have to REALLY want your data to invest the time and money into cracking the code.

I'll skip the math, but the PGP algorithm is based on matching together incredibly large prime numbers– I'm talking millions of digits. Huge. Mathematicians occasionally 'discover' new prime numbers, and while most of the world laughs off these nerdy academics, each new prime number adds a whole new dimension to encryption technology.

THE SOFTWARE

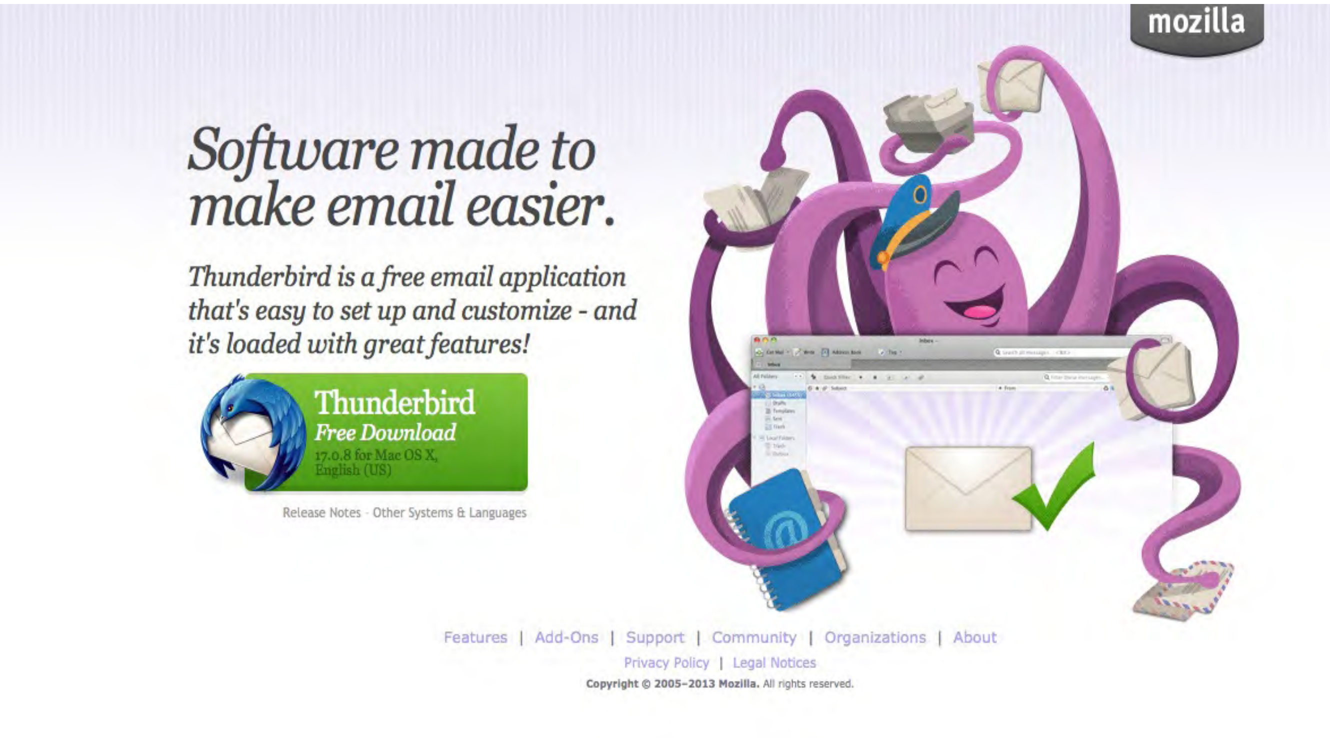
PGP/GnuPG can be configured to work with most major email clients, including Outlook, Mac Mail, and Mozilla Thunderbird.

The simplest way to get started with encrypting your emails with PGP is to download and install Mozilla Thunderbird **along with installing** GnuPGP **and the** Enigmail add-on, and this is what this Black Paper will show you how to do.

Step 1: Install Mozilla Thunderbird

1.1. DOWNLOAD THE INSTALLER

You will find Mozilla Thunderbird at this page, and it should detect whether you use Windows or Mac OS X and present the correct file for download. Click the green button to download Thunderbird.



Software made to make email easier.

Thunderbird is a free email application that's easy to set up and customize - and it's loaded with great features!

Copyright © 2005–2013 Mozilla. All rights reserved.

mozilla
Thunderbird
Free Download
17.0.8 for Mac OS X, English (US)
Release Notes · Other Systems & Languages
Features | Add-Ons | Support | Community | Organizations | About
Privacy Policy | Legal Notices

1.2. INSTALL MOZILLA THUNDERBIRD

Whether you use Windows or Mac OS X, click the installer and follow along with the instructions. Thunderbird has great installation instructions, so once you're done proceed to *Step 2: Install GnuPG*.

1.3. SET UP YOUR EMAIL ACCOUNT

If this is your first time using Thunderbird, you will have to set up your email account to send and receive email with Thunderbird. Gladly setting up a new account with Thunderbird is easy with their automatic configuration(guide). All you need to do is provide your user name and password for your email provider and your email address.

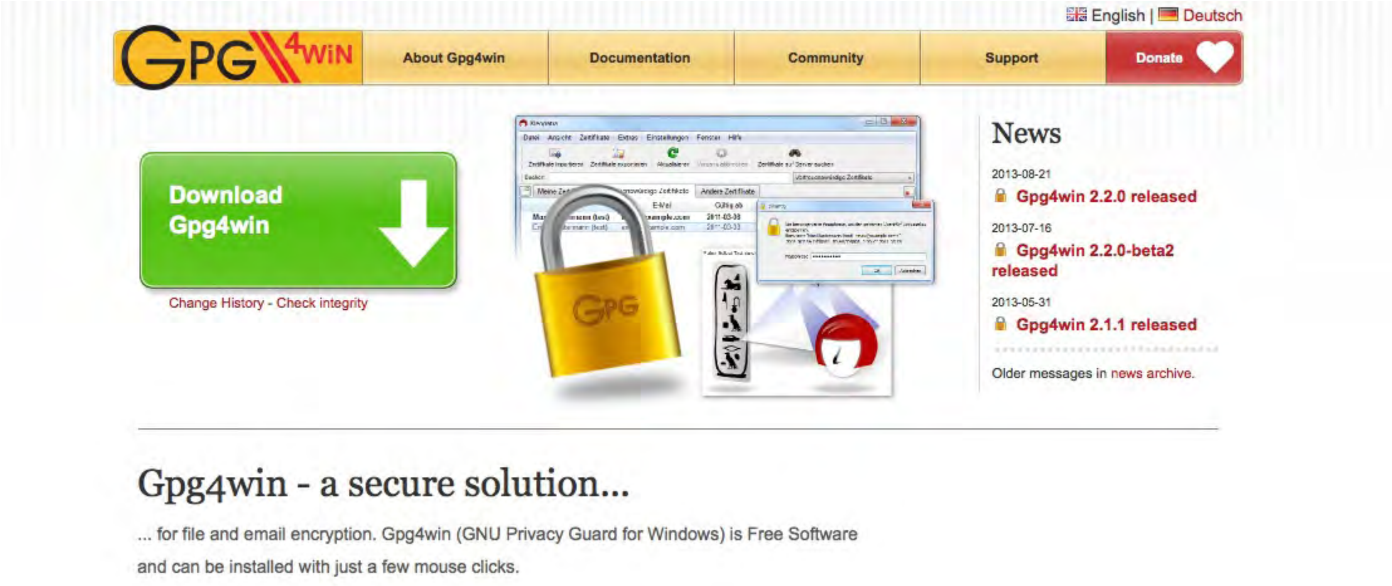
However, if your email provider is not listed in Thunderbird's automatic configuration database, or if you have a non-standard email configuration you will need to manually configure your account following their manual account configuration guide.

Once you've got your email account set up then proceed to *Step 2: Install GnuPG*.

Step 2: Install GnuPG

2.1. ...ON WINDOWS

2.1.1. Download the installer – GPG4WIN



News

2013-08-21
Gpg4win 2.2.0 released

2013-07-16
Gpg4win 2.2.0-beta2 released

2013-05-31
Gpg4win 2.1.1 released

Older messages in news archive.

Gpg4win - a secure solution...

... for file and email encryption. Gpg4win (GNU Privacy Guard for Windows) is Free Software and can be installed with just a few mouse clicks.

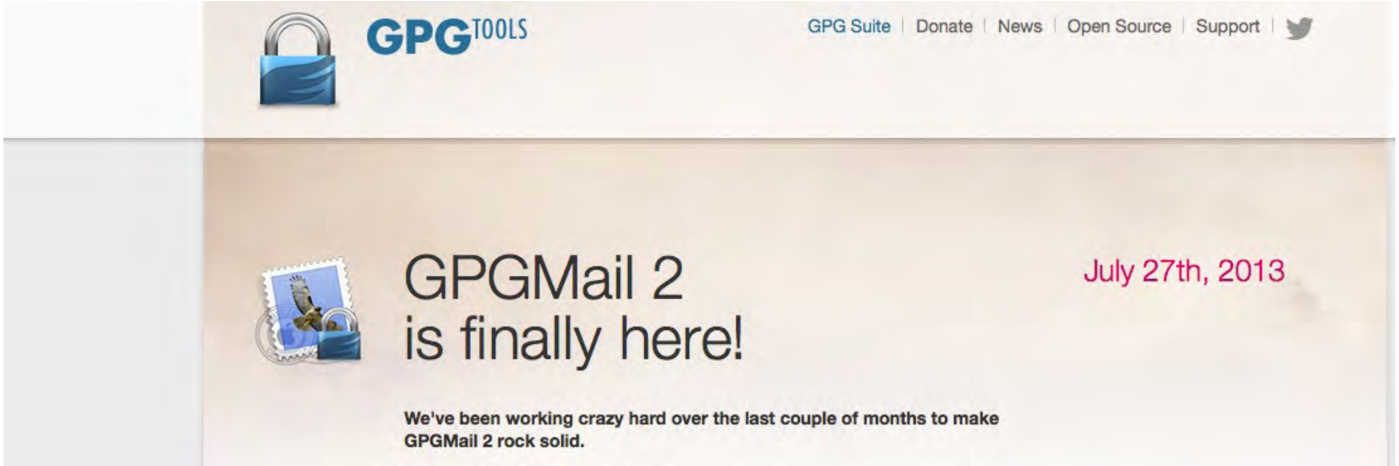
GPG4WIN (GNU Privacy Guard for Windows) is a sibling project to GnuPG and provides an installer for Windows, plus it has support for Enigmail which is what we need.

2.1.2. Install GPG4WIN

Download the newest version of GPG4WIN here(currently 2.2.0), and once you've downloaded the installer, double-click it to begin the very straightforward installation process. Once the installation of GPG4WIN is done continue to *Step 3: Install Enigmail*.

2.2. ...ON MAC OS X

2.2.1. Download the installer - GPGTools



GPGMail 2 is finally here!

July 27th, 2013

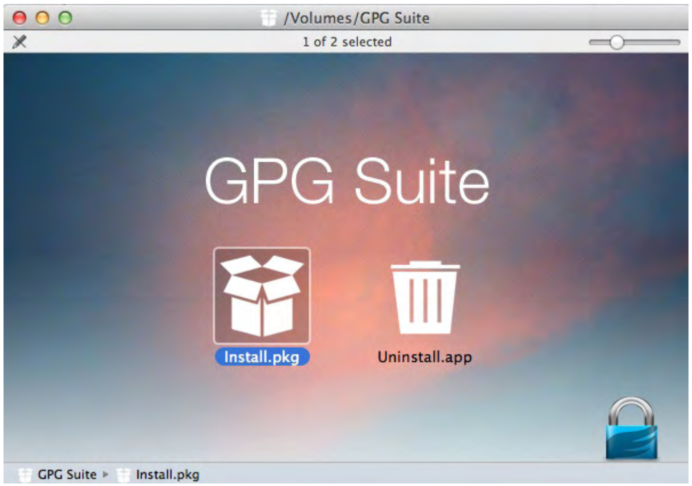
We've been working crazy hard over the last couple of months to make GPGMail 2 rock solid.

Head over to the GPGTools.org website and download the free GPG Suite, that include four components:

“**GPG for Mail** is an open source plugin for Apple Mail. Encrypt, decrypt, sign and verify mails using OpenPGP with a few simple clicks.
GPG Keychain is an open source application for Mac OS X. It allows you to manage your OpenPGP keys. Create and modify your keys and import the keys of your friends from a key server.
GPG Services is a plugin that brings GPG power to almost any application.
It allows you to encrypt/decrypt, sign/verify and import keys from text selections, files, folders and much more.
MacGPG is the underlying power engine of our GPG Suite. If you're familiar with the command line use the raw power of it. Based on gnupg 2.0.20.”

2.2.2. Install GPGTools

Double-click the .dmg file which you've now downloaded. This will open up an installation window as you can see below. Now double-click the Install.pkg icon and follow along with the instructions. Once the installation of GPGTools is done continue to *Step 3: Install Enigmail*.



Step 3: Install Enigmail

Enigmail is a plug-in for Thunderbird that lets it interface seamlessly with GnuPG and enables you to write and receive email messages signed and/or encrypted with the OpenPGP standard.

3.1. DOWNLOAD ENIGMAIL

Download the latest version of Enigmail for your operating system. You can always find the latest version at Enigmail's downloads page. As of this writing the latest version is 1.5.2.

Firefox Users:

Thunderbird and Firefox both use the .XPI extension for their plug-ins. If you click on the download link, Firefox will think you're asking it to install Enigmail as a Firefox plug-in. This will not work. Instead, right-click on the link and choose "Save link as...".

3.2. INSTALL ENIGMAIL

Start Thunderbird. In the menu bar of the main window you will see "Tools". Select this, and then "Add-ons".

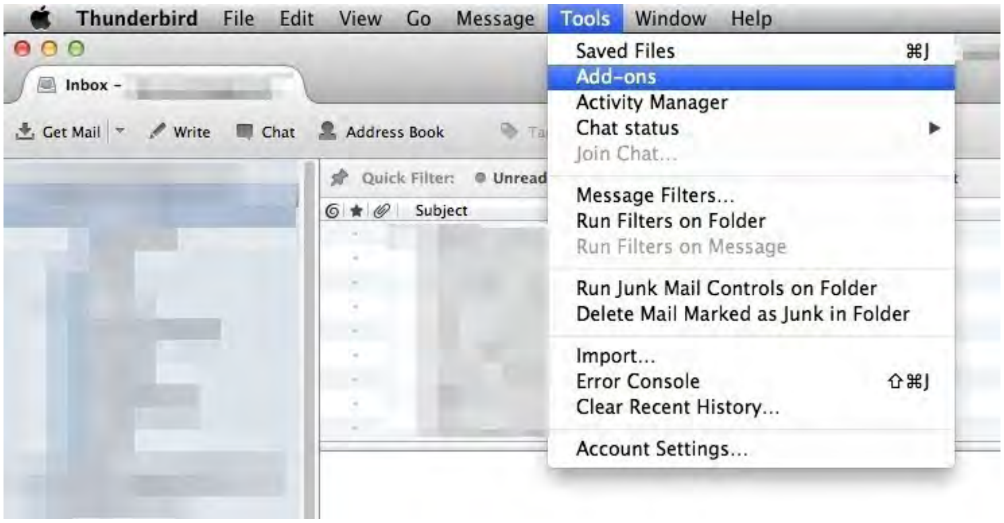
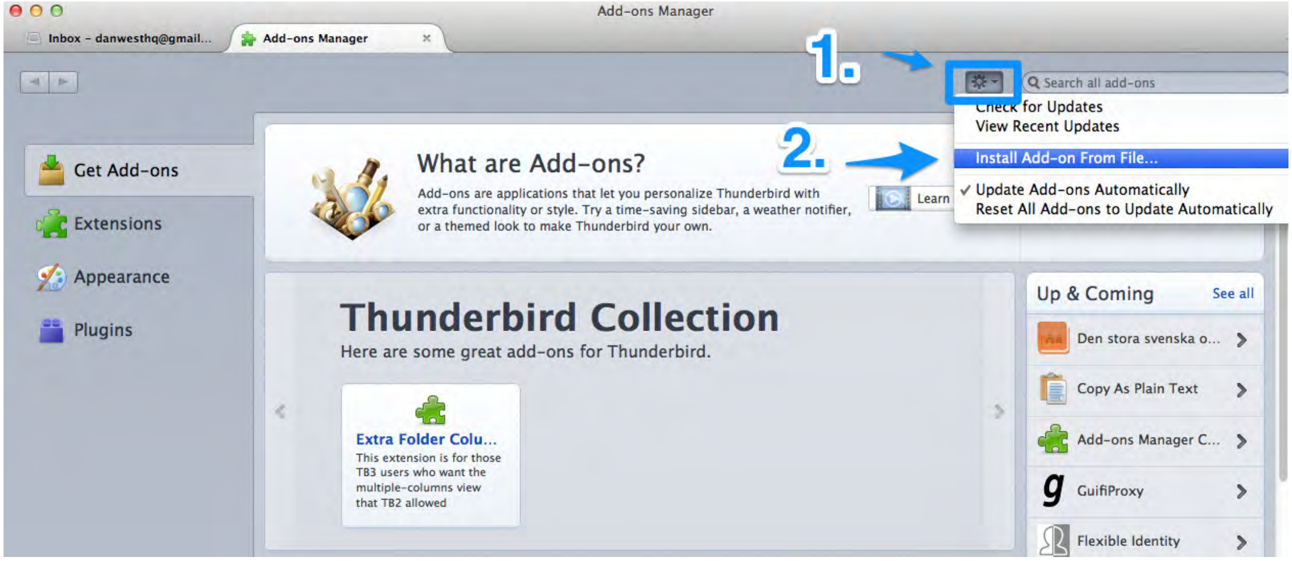


Image 3.2.1.

This will bring up a new window listing all of your Thunderbird plug-ins, or if you don't have any you will land on the Add-on homescreen.

To install the Enigmail plugin click on the cog-wheel in the upper-right corner as shown in step 1 in *image 3.2.2.* below, and then choose "Install Add-on From File..." and tell Thunderbird where you saved the Enigmail .XPI file.



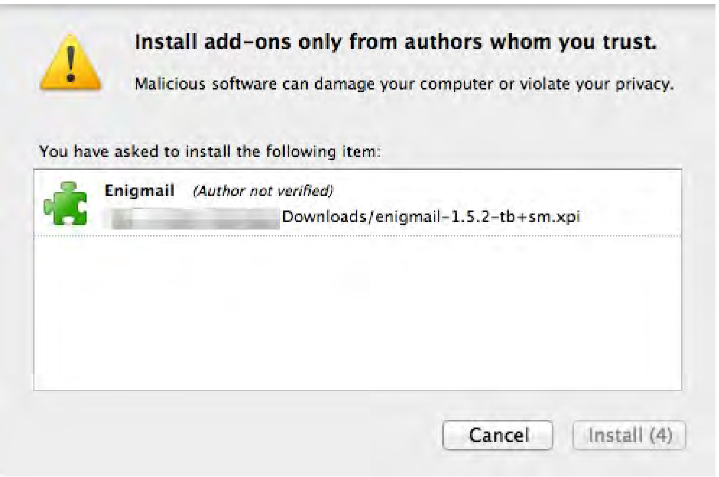
Add-ons are applications that let you personalize Thunderbird with extra functionality or style. Try a time-saving sidebar, a weather notifier, or a themed look to make Thunderbird your own.

Here are some great add-ons for Thunderbird.

This extension is for those TB3 users who want the multiple-columns view that TB2 allowed

Image 3.2.2.

Another window will pop open(*image 3.2.3.*), warning that you're about to install a plug-in. This is just an extra precaution where Thunderbird makes you think twice about installing plugins from unknown sources. Don't worry too much about this now.



Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:

Enigmail *(Author not verified)*
Downloads/enigmail-1.5.2-tb+sm.xpi

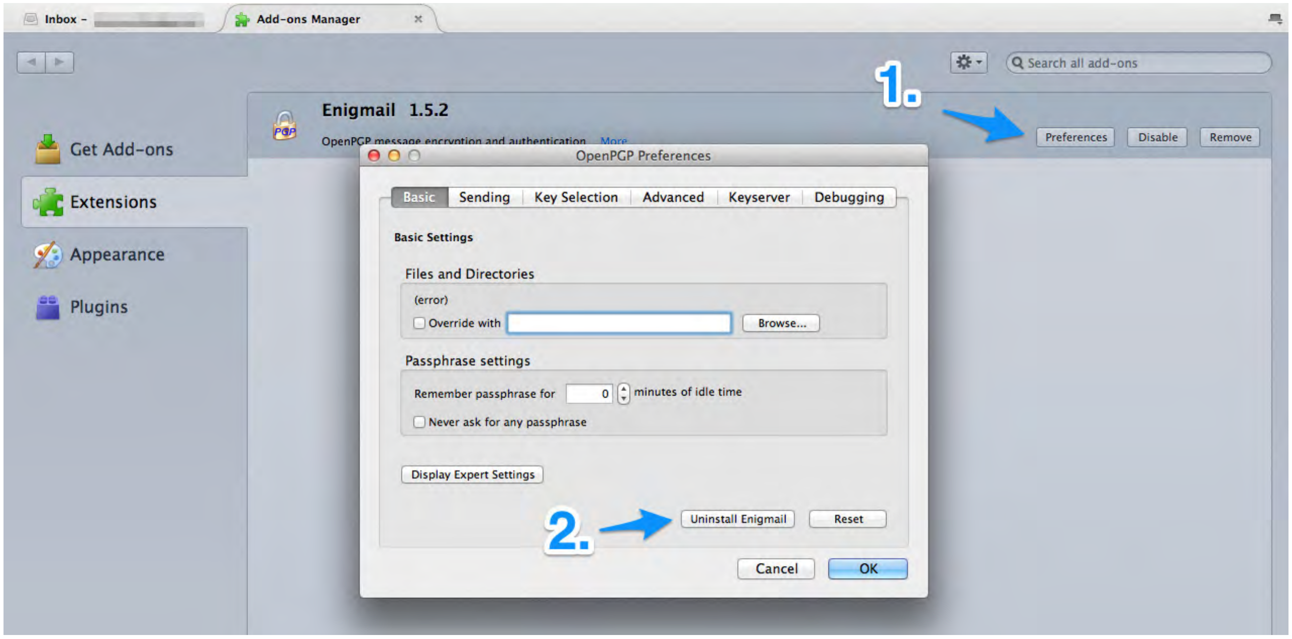
Image 3.2.3.

Confirm your decision by clicking the "Install" button.

Once installed, you will need to restart Thunderbird, and after that Enigmail will be ready to go. Now proceed to *Step 4 – How To Manage Encryption Keys.*

3.3. UNINSTALLING ENIGMAIL

If for some reason you ever need to uninstall Enigmail, begin by starting Thunderbird. Select "Tools", then "Add-ons". A new window will appear showing all of your Thunderbird plug-ins. Click on Enigmail "Preferences" (step 1 in I*mage 3.3.*) and then click "Uninstall Enigmail" (step 2 in I*mage 3.3.*).



Enigmail 1.5.2
OpenPGP message encryption and authentication More

Basic Settings

Files and Directories
(error)
☐ Override with

Passphrase settings
Remember passphrase for 0 minutes of idle time
☐ Never ask for any passphrase

Image 3.3

Enigmail will be uninstalled once you close Thunderbird.

Step 4: How To Manage Encryption Keys

Before proceedin with this step you should have Thunderbird, GnuPG and Enigmail installed, and your email account set up.

As I mentioned earlier in the introduction everyone who uses PGP has two 'keys', a public key and a private key. But again, I'll skip the math. All you need to understand is that you will be creating a public key and a private key. As Enigmail states:

> *"The public key can be shared with the whole world--friends, neighbors, relatives, enemies, even intelligence agencies. But you need to guard the private key very, very carefully."*

4.1. HOW TO GENERATE A NEW KEYPAIR

To generate your public and private key, click on the **OpenPGP** menu inside Thunderbird(*Image 4.1.1.*)

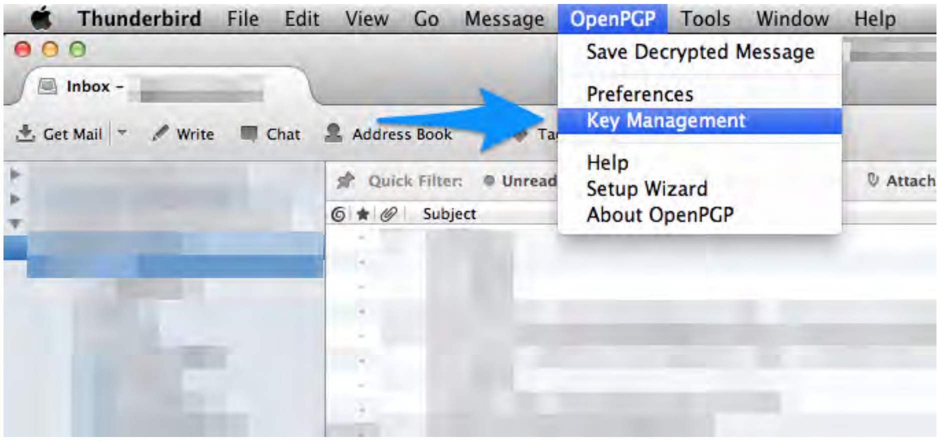


Image 4.1.1.

A new navigation menu will appear, in which you should click **Generate** and then New Key Pair.(*Image 4.1.2.*)

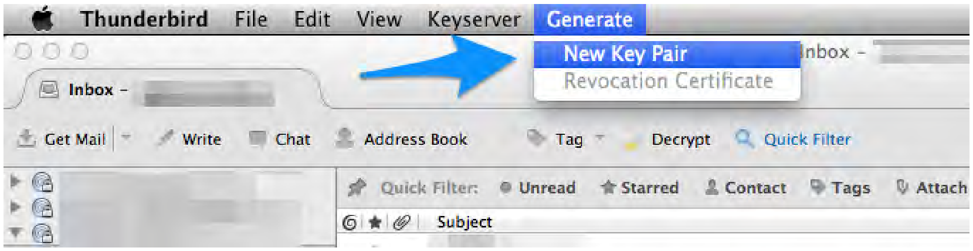
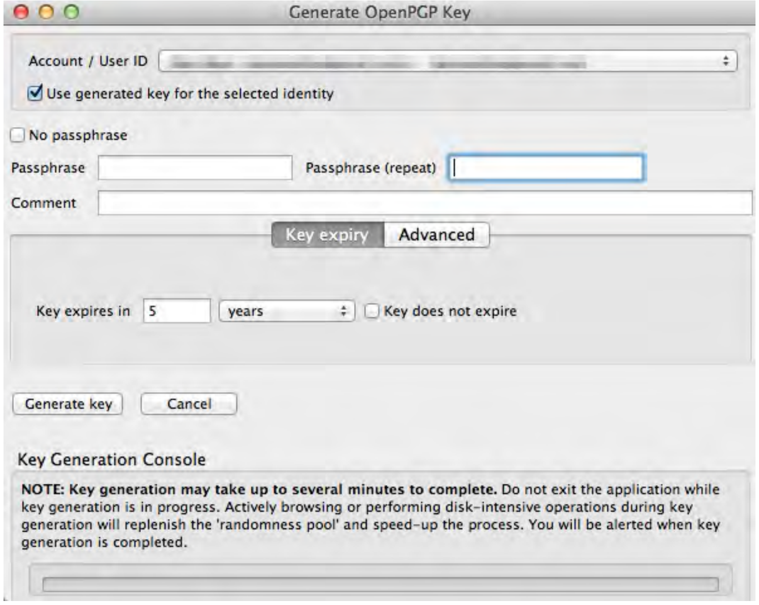


Image 4.1.2.

You will now see the following window:



Account / User ID

☑ Use generated key for the selected identity

□ No passphrase

Passphrase | Passphrase (repeat)

Comment

Key expires in 5 years □ Key does not expire

Key Generation Console

NOTE: Key generation may take up to several minutes to complete. Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.

Don't be alarmed if you don't understand everything. There are only four things you need to worry about.

Tell Enigmail which account to use. At the very top of the window you will see a combobox showing all of your email addresses. GnuPG will associate your new key with an email address. Enigmail is just asking you which address you want to use for this key. Select whichever account will be receiving encrypted mail.

(If you decide later that you want to use the same key for multiple accounts, that can be done, too, but it's beyond the scope of this Quick Start Document.)

Choose a passphrase. Private keys are so important that GnuPG will not use them unless you know the secret phrase. You're being asked here what the secret phrase should be for your new keypair, and it should *not* be the same password that you use for your email account.

If at all possible, choose something that is easy to remember but very hard for someone to guess, or use a website such as strongpasswordgenerator.com to generate a strong password and keep it somewhere safe.

Enter your passphrase in the "Passphrase" box. Then repeat it again in the "Passphrase (repeat)" box. By entering it twice, Enigmail is protecting you from accidentally mis-entering your passphrase.

As a security feature, Enigmail will not display your passphrase as you type it.

Warning! If you forget your passphrase, there is absolutely nothing anyone can do to help you. This is a security feature of GnuPG. There is no way around the passphrase.

Click "Generate Key". That's it! That's all you have to do. Everything else is handled for you automatically.

Generate a revocation certificate. Hard drive failures happen to us all. So do house fires and theft and other things that might separate us from our keys. When this happens, it's a good idea to send out a revocation notice. You can think of this as a message from your key saying "please don't use me any more".

Using the magic of assurance, people who see your revocation certificate can be confident that your key really is no more. Having a revocation certificate tucked away in a safe place is a very good idea.

When you finish creating your new key, Enigmail will give you the chance to create a revocation certificate. If you want one, click "Yes". You will be asked to enter your passphrase. Enter it, and you'll be finished.

4.2. HOW TO SHARE YOUR PUBLIC KEY WITH YOUR CONTACTS

For people to be able to read your encrypted emails you need to exchange public keys with them. There are four ways to do this, and you will find all of them by going to the **Key Management** window under the **OpenPGP** menu in Thunderbird and right-clicking on the email account that you want to share the public key for. You will then see the menu in *Image 4.2.1*.

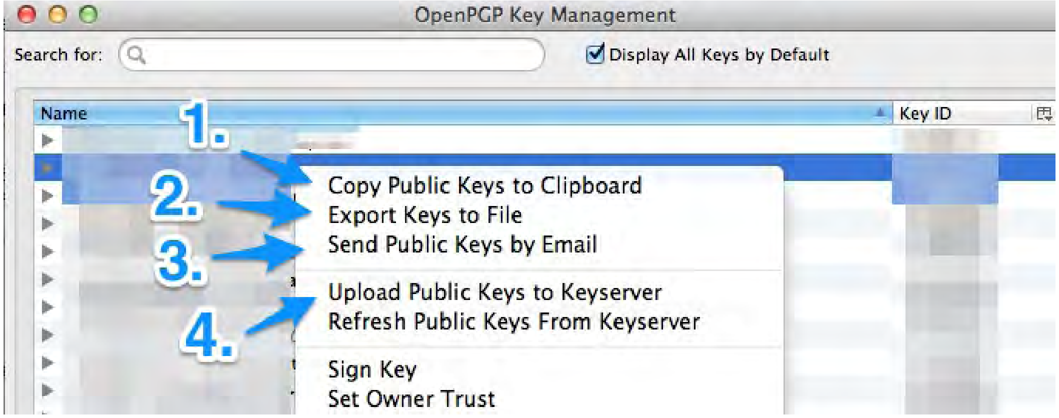

OpenPGP Key Management
Search for:
☑ Display All Keys by Default
Name
Key ID
1.
2.
3.
4.
Copy Public Keys to Clipboard
Export Keys to File
Send Public Keys by Email
Upload Public Keys to Keyserver
Refresh Public Keys From Keyserver
Sign Key
Set Owner Trust

Image 4.2.1.

The four ways are:

Share your public key on your website. When you copy your public key to the clipboard you will be able something similar to what you see below on your website:

-----BEGIN PGP PUBLIC KEY BLOCK-----

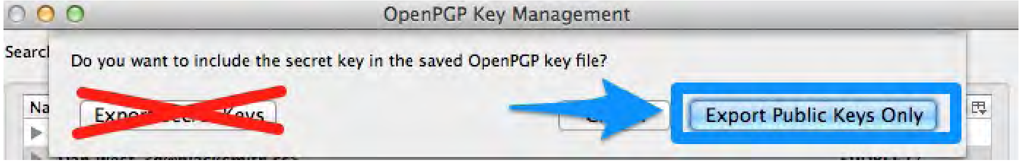
Version: GnuPG/MacGPG2 v2.0.18 (Darwin)
Comment: GPGTools - http://gpgtools.org

mQENBFECu7UBCACkuFbAjZZY+JWxa6F7FmKSHZiPVmAbw6m3CXs5b5s687sIIHJ00MQC
PrDaewrvdqVVQiWKVWuuAlQBEcUxg/u4E7+nyLVVrPRs5DPaFKIaex7zdRwgBa2t5MA5PPoMPGBv/

-----END PGP PUBLIC KEY BLOCK-----

This is your public key. By sharing it on your website people will be able to import it into GnuPG.

Export your public key to a file. This option is good if you would like to carry your public key around on a USB-stick or your smartphone. *However*, make sure that when you export you only export your public key and NOT your secret key. See *Image 4.2.2.* below.

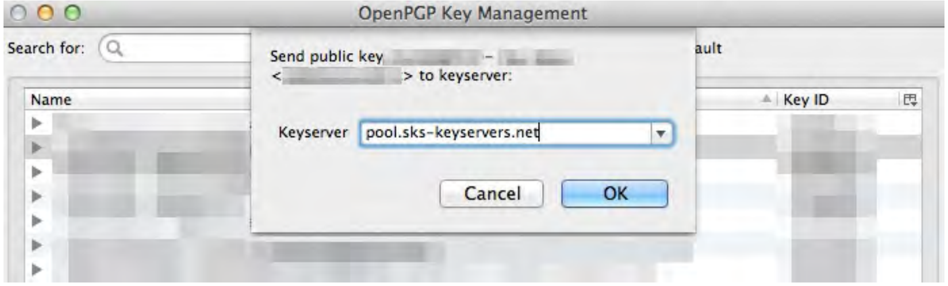


Do you want to include the secret key in the saved OpenPGP key file?

Image 4.2.2.

Email your public key as an attachment. When you choose this option, a new "Compose Email" window will pop up where your public key will already be attached to the email. So just enter your friend's email, a subject line, maybe a greeting to let them know this is your public PGP key, and click send!

Upload your public key to the *keyserver network*. This is a global database of public keys and it's by far the easiest way to share your key. When you click this option you will be asked to select a keyserver. Enigmail recommends pool.sks-keyservers.net, so select that from the list or enter it as you can see below in *Image 4.2.3*.



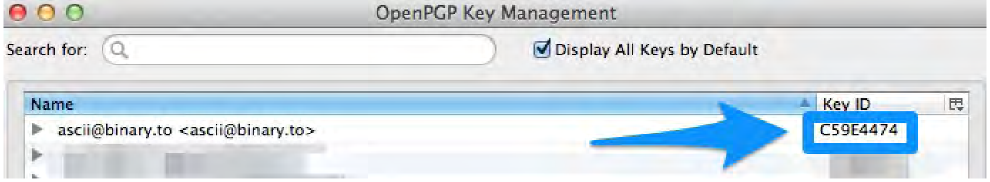
Send public key – < > to keyserver:

Keyserver: pool.sks-keyservers.net

Image 4.2.3.

Your public key is now published on the internet for anyone to find!

If your friend want to find your key then they need to know your *Key ID*, which is a sequence of letters and numbers eight long. You will find your Key ID to the right in the Key Management window next to your email address, as you can see in the example in *Image 4.2.4.* below.



☑ Display All Keys by Default

ascii@binary.to <ascii@binary.to> — Key ID: C59E4474

Image 4.2.4.

However, as you will see in the next chapter on finding keys they will need to prefix your key with "0x" when searching for it, but more on that in the next chapter.

A word of precaution from Enigmail regarding spam

"Some people will tell you never to use a keyserver at all, because spammers search them for email addresses. While this is true, this kind of misses the point.

There is nothing you can do to prevent spam from littering your inbox. Trying to stop it is like King Canute marching into the sea, commanding the rising tide to turn back. It didn't work for King Canute and it won't work for you.

There are excellent ways to stop spam. Blacklists, whitelists, Bayesian filtering, ISP-level solutions and more. Some of those options work better than others. All of them work better than the naive "if I don't publish my key on the keyservers, then I won't get spammed" strategy."

4.3. HOW TO FIND AND IMPORT OTHER PEOPLE'S ENCRYPTION KEYS

Now that your friends have your public key, you will need their public key as well. For all four ways to share a public key above there are corresponding ways to import the key, and we review them below.

Import a public key from the clipboard. When you have found a public key on someone's website and want to import it, select all the text from and including -----BEGIN PGP PUBLIC KEY BLOCK----- to -----END PGP PUBLIC KEY BLOCK----- and copy it to the clipboard with **ctrl + C** on Windows or **command + c** on Mac OS X.

To import it, go to **Key Management** under the **OpenPGP** menu in Thunderbird, and under the **Edit** menu click on **Import Keys from Clipboard** as seen in *Image 4.3.1.* You will then be asked to confirm by clicking **Import**, and then you're done!

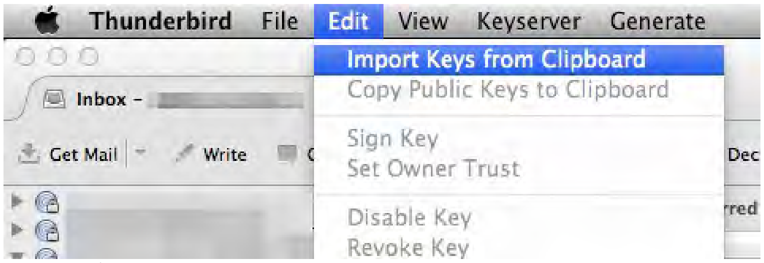


Image 4.3.1.

Import a key file. You might have received the keyfile as an attachment or through an USB-stick. Either way, you import the key by clicking on the **File** tab in the Key Management navigation menu, and then click on **Import Keys from File** as seen in *Image 4.3.2.* and select the key file on your harddrive and click the open/import button. It will then be added to your list of public keys.

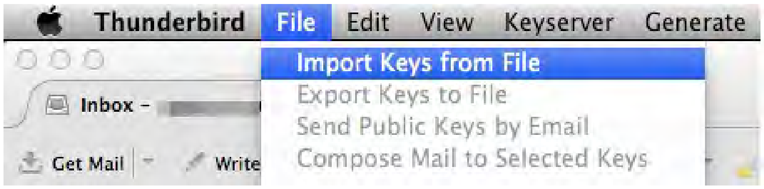


Image 4.3.2.

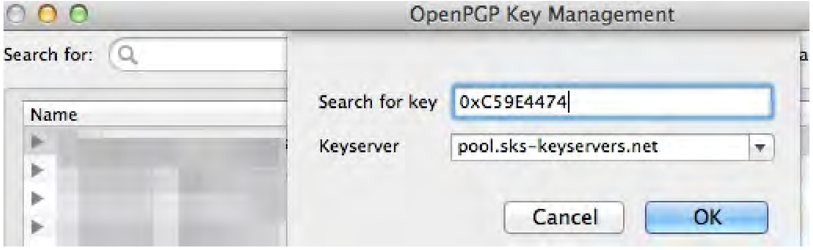
Find and import a key from the *keyserver network*. To do this you will need to know your friend's Key Id, as mentioned in the previous chapter.

Continuing with the example Key ID in *Image 4.2.4.*, let's search for the Key ID C59E4474.

To do this, when you are inside the Key Management window click on **Keyserver** in the navigation menu and then on **Search for Keys**. You will then see the window in Image *4.3.3.* below where you can enter a Key ID and a Keyserver.

As I mentioned though, you will have to prefix the key with "0x" if it isn't already, i.e. Instead of searching for C59E4474 you will search for **0x**C59E4474, as illustrated in the image.

As for the keyserver we are searching on pool.sks-keyservers.net, the same keyserver that we uploaded your key to in the previous chapter.

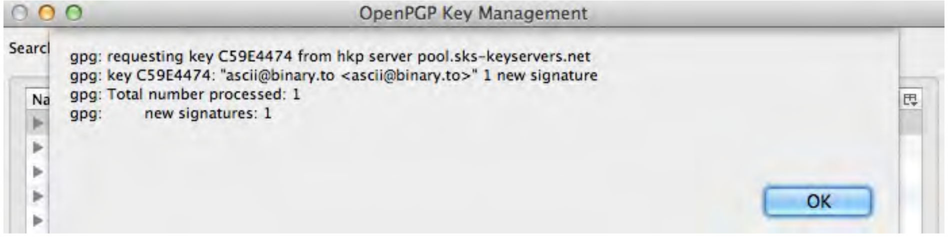


Search for key: 0xC59E4474

Keyserver: pool.sks-keyservers.net

Image 4.3.3.

If you are successful with finding the key, then you will see the message below (*Image 4.3.4.*) saying it has found 1 new signature, meaning it has successfully imported the key.



```
gpg: requesting key C59E4474 from hkp server pool.sks-keyservers.net
gpg: key C59E4474: "ascii@binary.to <ascii@binary.to>" 1 new signature
gpg: Total number processed: 1
gpg:        new signatures: 1
```

Image 4.3.4.

However if you did NOT find a key, then contact your friend and make sure the key was uploaded correctly, and that you are searching on the right keyserver.

Once your friend has your public key, and you've got his, then you are both ready to send and receive encrypted emails. Proceed to *Step 5* to get started.

Step 5: Sending Your First Signed And Encrypted Email

Congratulations! This is the final step where you will actually send an encrypted email.

I highly recommend that you send plain text emails when you wish to encrypt them, because Enigmail does not work very well with HTML email. While it can be made to work, it's pretty far beyond the scope of this black paper.

If you normally compose your email in plain text, then you're just fine. If you normally use HTML, then hold down the shift key as you click on "Write" in the Thunderbird window.

Whether you choose to encrypt your message or not, it is always a good idea to sign your message. This means that you include something similar to a hand-written signature, except by signing it cryptographically:

It can be used to validate that the message came from who it claims to come from.

It can be used to prove that the message wasn't tampered with.

For this validation to work your recipient needs to have imported your public key into Enigmail, as shown in *Step 4*.

Now, to send a signed and/or encrypted email, write an email to your friend just as you normally would, but before sending, click on the OpenPGP button as shown in *Image 5.1.* and select "Sign Message" and/or "Encrypt Message". Once that's done, click "Send".

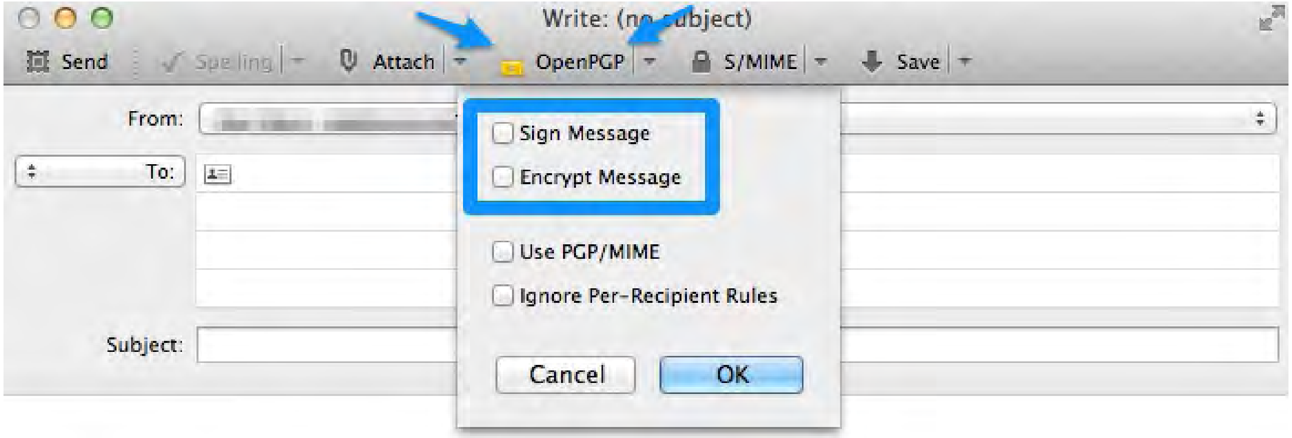


Image 5.1.

Two things can happen here.

If the email address of your message matches an address on your keyring, then you're done; your message will be encrypted and sent to your recipient.

If there's a problem with the matching, you will be asked to manually select a key from your keyring. If you see this menu, then simply select the proper keys and you're done.

The Bottom Line

If you've followed all five steps in this black paper you will now have Thunderbird, GnuPG and Enigmail set up on your Windows or Mac OS X computer, and you will have the most powerful email encryption in the world at your fingertips.

The truth though is that PGP encryption is only as powerful as the number of people using it.

You need to use it, and your friends need to use it.

To that end, feel free to share this black paper with your closest circle of friends, family and business partners.

To your freedom,

Simon Black

Simon Black
Sovereign Man