Enigmail Documentation Collection

Robert J. Hansen, The Enigmail Project

Subject to Change. This work documents an ongoing effort, and may be supplanted at any time without warning. Before relying on any data herein, please ensure the most recent edition is being used.

Table of Contents

Enigmail 0.95.3 Quick Start Guide

Robert J Hansen <rjh@sixdemonbag.org>

Enigmail 0.95.3 Quick Start Guide

by Robert J Hansen

Abstract

This document will give you a quick introduction to Enigmail 0.95.3. Downloading Enigmail, installing it, and using it for routine email tasks are all covered. It will not cover any of these subjects in great depth.

Legal Notice

Table of Contents

Preface

Subject To Change

This manual covers Enigmail 0.95.3, and may not match with your version. All official versions of the Quick Start Guide can be found at Enigmail's home page [http://enigmail.mozdev.org]. Please make sure you have the proper version before continuing.

Welcome to the Enigmail community! We're glad that you're here and we very much hope you'll find Enigmail to be a useful privacy tool.

This Quick Start guide will get you set up in a hurry. It won't do anything more than scratch the surface of the things you can do with Enigmail, but it should get you on your feet pretty quickly.

Chapter 1. Before You Begin

> There is nothing more difficult to plan, more doubtful of success, more dangerous to manage, than the creation of a new system.
>
> —Niccolo Machiavelli

Software hardly ever exists in isolation. Even something as simple as the solitaire game you got for free with your operating system depends on other pieces of software. In the case of your solitaire game, it depends on the operating system. In the case of Enigmail, it depends on a few pieces more than that. This chapter will help you make sure you have all the things Enigmail depends upon, and if not, where you can get them.

Please Read This Carefully

Please read this chapter carefully and *do not* skip steps. When people come on the mailing lists and say "Enigmail isn't working", the overwhelming majority of the time it's because they do not have Enigmail, Thunderbird and/or GnuPG properly installed.

This Quick Start Guide

Murphy's Law being what it is, a network will always die as soon as you need to look something up online. You can defend against Murphy by downloading this manual to your own local computer.

If you're reading this manual online, please visit the Enigmail Project's Documentation Page [http://enigmail.mozdev.org]. This manual is available in many different formats. Choose whichever one is most convenient for you. The content is the same regardless of which you choose.

The Enigmail Mailing List

This is only a Quick Start Guide. You will probably have questions that are not addressed here. You may want to join the mailing lists [http://www.mozdev.org/mailman/listinfo/enigmail/] or browse in the web forums [http://www.mozilla-enigmail.org/forum/]. If things go wrong, you can usually get answers very quickly from either place.

The GNU Privacy Guard

Enigmail uses the freely-available GNU Privacy Guard [http://www.gnupg.org] to do most of its work. The GNU Privacy Guard (usually abbreviated GnuPG) is available for many different operating systems, including Windows [http://www.microsoft.com], OS X [http://www.apple.com], UNIX, OS/2 [http://www.os2.org], OpenVMS and more.

Installing GnuPG on Unusual Systems

This manual only covers installing GnuPG for Windows and OS X, and provides some guidance for UNIX. Other, less-common operating systems will not be covered here. If you're using one of these rare operating systems, please ask for installation help on the mailing list or in the forum.

Installing GnuPG on Microsoft Windows

Downloading the Installer

As of this writing, there is a Windows installer of GnuPG 1.4.7 available directly from GnuPG [ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.7.exe]. If the preceding link is dead, as happens all too often on the web, then try visiting the home page [http://www.gnupg.org] of the GnuPG Project and see if you can't find it from there.

Some people prefer to use GPG4WIN, a sibling project to GnuPG. Enigmail can use GPG4WIN just as easily. However, we recommend people use the GnuPG 1.4.7 installer if feasible.

Installing GnuPG

Once you've downloaded the installer, just double-click it to begin the installation process. It's a very straightforward installer; you can literally just keep clicking "Next" until it's finished and you'll do just fine.

Installing GnuPG on Macintosh OS X

You have three basic ways to install GnuPG on OS X. Most users will choose the first option.

MacGPG

The MacGPG [http://macgpg.sf.net] project provides pre-built Universal Binaries of GnuPG 1.4.7 for users running OS X 10.4 (also called "Tiger"). If you are running OS X 10.3 or earlier, you will not be able to use the MacGPG packages.[1]

Assuming you're running OS X 10.4 or later, just download the package and install it as you would any other piece of OS X software.

Fink

The Fink Project [http://fink.sf.net][2] keeps a very current version of GnuPG in their source tree. If you're using Fink, installing GnuPG is as simple as typing `fink install gnupg` into Terminal.app.

MacPorts

The MacPorts Project [http://www.macports.org], formerly called "DarwinPorts", keeps a current version of GnuPG in their source tree. If you're using MacPorts, open up Terminal.app and type `sudo port install gnupg`.

Installing GnuPG on UNIX

[1] This isn't quite true. They do have older versions of GnuPG packaged for older versions of OS X. However, since Enigmail depends on GnuPG 1.4.7 or later, older versions of GnuPG won't do you any good.

[2] "Fink" is German for "finch", as in the type of bird. The original developer of Fink was a German, and his name for it has stuck.

Unfortunately, here my remarks have to be very brief. Your best bet is to talk to your UNIX vendor and get a version of GnuPG that's already been compiled for your system. Compiling GnuPG from source is not advised for beginners.

Installing GnuPG on Linux

Most Linux distributions today include GnuPG by default. To find out if this is the case, get to a command prompt and type `gpg --version`. If it tells you that you've got GnuPG 1.4.7 (or some later version), then you don't need to do anything: it's already there.

Installing GnuPG on *BSD

The various flavors of BSD UNIX have a common way of installing software. Please see the instructions for MacPorts, above.

Thunderbird 2.0

Once GnuPG is installed on your system, the next order of business is to get Thunderbird 2.0 [http://www.getthunderbird.com]. Thunderbird is an email client; it allows you to talk to your mail server, allows you to read email, allows you to write it, allows you to filter it, all the things you expect an email client to do.

Thunderbird has excellent installation instructions. For that reason, we're just going to continue on with the last piece of software you need.

Thunderbird on Linux

Many Linux distributions ship with their own customized version of Thunderbird. If you use your distribution's version of Thunderbird, you must use your distribution's version of Enigmail. If you get Thunderbird from the official site [http://www.getthunderbird.com] and install it yourself, though, you can use the official Enigmail releases provided by the Enigmail Project.

Enigmail

Enigmail is a plug-in for Thunderbird that lets Thunderbird interface seamlessly with GnuPG. You can always find the latest version at Enigmail's downloads page [http://enigmail.mozdev.org/download.html]. As of this writing the latest version is 0.95.3.

Downloading Enigmail

Download the latest version of Enigmail for your operating system.

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...".

Installing Enigmail

Start Thunderbird. In the menu bar of the main window you will see "Tools". Select this, and then "Add-ons". This will bring up a new window listing all of your Thunderbird plug-ins. In the lower left-hand corner of this new window you'll see a button marked "Install". Click this button. Tell Thunderbird where you saved the Enigmail .XPI file.

Another window will pop open, warning that you're about to install a plug-in. You haven't done anything wrong. Thunderbird is just giving you the chance to back out before installing a plug-in. Confirm your decision.

Once installed, you will need to restart Thunderbird. Once you do that, Enigmail will be ready to go.

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" and then click "Uninstall".

Enigmail will be uninstalled once you close Thunderbird.

Chapter 2. Creating Your First Keypair

Public Key Cryptography

Enigmail uses public key cryptography to ensure privacy between you and your correspondents. In public key cryptography we use two different kinds of keys to give us confidentiality and assurance.

By "confidentiality" we mean that only the people you want to read a message will be able to read a message. By "assurance" we mean that people who read messages from you can be sure that it really came from you.

We're not going to explain all the mathematics that's involved. You don't need to have a Ph.D. in computer science to use Enigmail. All you need to understand is that you will be creating a *public key* and a *private key*. 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.

Using the Enigmail Key Wizard

By this time, you should have Thunderbird, Enigmail and GnuPG all installed. If you don't, go back and do those sections now.

You will need a piece of paper and something to write with.

1. **Start Thunderbird.** Due to the incredible number of different operating systems Thunderbird runs on, we're not going to try to tell you how to do this. If you need help finding Thunderbird, the Thunderbird site [http://www.getthunderbird.com] has excellent documentation.

2. **Check your accounts.** If you don't have any email accounts set up yet, do that now. Again, see the Thunderbird site [http://www.getthunderbird.com] if you need help.

3. **Start the Enigmail Key Manager.** Click on "OpenPGP" in the menu bar of the Thunderbird main window. Select "Key Management".

4. **Start the New Key Wizard.** When the Enigmail Key Manager opens, click on "Generate" in the menu bar and select "New key pair".

   A new window will pop up. Take a deep breath: you are not expected to understand everything here. In fact, there are only a couple of things you need to worry about!

5. **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.)

6. **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. If at all possible, choose something that is easy to remember but very hard for someone to guess.

   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.

Danger!

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.

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

8. **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.

Next Steps

Your key ID

Now that you have your key, you should find your *key ID*. This is a sequence of letters and numbers eight long which is used to unambiguously identify your key.[1]

Go back to the Enigmail Key Manager and enter your email address in the search box. The key you just created should appear, and over at the right you'll see your key ID. Write this down; you'll need it.

Publishing your key

By far, the easiest way to share your key with the world is to publish it on the *keyserver network*, a global database of keys. Click on your key in the Key Manager. Then click "Keyserver" and select "Upload public keys".

Enigmail will ask where it should send your key. Generally speaking, `pool.sks-keyservers.net` is your best bet. That's the one Enigmail uses by default, so just click "OK".

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

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.

[1] In reality your fingerprint is forty long, but using the last eight is customary. You'd need to have over 65,000 keys before you'd have a good chance of two keys sharing the same shortened ID.

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.

Chapter 3. Hello, World!

Your first signature

Now that you have your key created, let's try writing a signed piece of email.

1. **Find a friendly face.** Not all people have Enigmail installed. In fact, very few people use email cryptography at all. It's probably a good idea to send your first test email to a mailing list that has a lot of GnuPG folk around, and that offers support to newcomers who are just starting out.

   Two of the best options are PGP-Basics [http://tech.groups.yahoo.com/group/PGP-Basics/] and Enigmail Users [http://www.mozdev.org/mailman/listinfo/enigmail/]. Both places are friendly and welcoming. If you make a mistake, no one will scream at you or call you names.

2. **Write a plain-text email.** 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 guide. 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.

   While your email can say anything you like, really, it is probably a good idea to give a little bit of an introduction. Tell us about yourself, and ask for people who are willing to help you test Enigmail's encryption features.

3. **Tell Enigmail to sign it.** At the top of your Compose window you will see a button reading "OpenPGP". Click on this. Make sure that the "Sign" option, *and only that,* is checked.

4. **Hit "Send".** You will be asked for your passphrase. Once you enter it, Enigmail will sign your email and send it off to the list.

Congratulations! You've just sent your first signed email.

Your first encrypted email

Before encrypting email to someone, please make sure that you can sign messages. The old adage of learning to crawl before learning to walk applies here.

You will need someone to help you with this. Learning how to get people's keys from a keyserver is an important skill to develop, and you won't do yourself any favors by just encrypting messages to yourself. You already have your public key, so you'll miss out on the entire process of finding keys.

Finding keys

Once you've found someone to help you, ask them for their key ID. This will be an eight-character sequence of letters and numbers. Write it down, and then open up the Enigmail Key Manager ("OpenPGP --> Key Management" from the main window).

From the Key Manager, click on "Keyserver --> Search for keys". Enter the person's key ID in the search box, prefixing it with "0x", if necessary. For instance, if someone were to tell you their key ID was "DECAFBAD", you'd enter it as "0xDECAFBAD". But if someone were to tell you their key ID was "0xDEADBEEF", you'd enter it exactly as-is, "0xDEADBEEF".

Make sure your internet connection is active and click "OK". Enigmail will begin searching through the keyserver looking for the key you want. If Enigmail finds it there, it will be added to your own local copy of keys.

Encrypting email

Once you've obtained a copy of your correspondent's key, you're set to send encrypted email. Write an email to them just as you normally would, but before sending, click on the OpenPGP button and select "Encrypt". Once that's done, click "Send".

There are two options here. If the email address of your message matches an address on your keyring, there's nothing more to do; your message will be encrypted and sent on to your correspondent. 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.

Index