

# Secure Your Email With GnuPG

Contributed by Doug Anger  
Wednesday, 25 April 2007  
Last Updated Thursday, 26 April 2007

Last week's article explained how to secure your email with X.509 certificates. The difficulty with X.509 is that proving a key belongs to who it says it belongs to can be difficult because only the issuer of the key (Thawte in last week's article) can verify the identity associated with the key. The process of verifying your identity usually involves time and money.

This week, we will introduce another way to secure your email: GnuPG. GnuPG (or the Gnu Privacy Guard) is an open source program for encryption and authentication that has a built in web-of-trust. If Alice &quot;trusts&quot; Bob's key and Bob &quot;trusts&quot; Carol's key, and Alice gets an email from Carol, she will be able to verify that Carol is indeed who she says she is, even if she has never met Alice. It is as if their mutual friend Bob had introduced them.

In addition to encrypted email, GnuPG allows other kinds of security to be implemented. GnuPG is compatible with the OpenPGP standard along with the popular commercial cryptographic software PGP.

It is assumed in this tutorial that you have a computer with an Internet connection and a working copy of Mozilla Thunderbird 2. You can download Thunderbird 2 (currently RC1) at <http://www.mozilla.org/projects/thunderbird/all-beta.html>.

## Getting GnuPG

The first step is to get GnuPG. The easiest way to do this is to download an installer. If you are using Windows, you can get the installer at <http://www.gpg4win.org/>. If you are using Mac OS X, you can get the installer at <http://macgpg.sourceforge.net/>. Most Linux users can install GnuPG through their default package manager.

The instructions in the installers vary by operating system, but are pretty straight-forward. (Note that Windows users need not install Sylpheed-Claws.)

The next thing you need to get running is Enigmail. Enigmail is a Thunderbird plugin available from <https://addons.mozilla.org/en-US/thunderbird/addon/71> that allows Thunderbird to use GnuPG to digitally sign and encrypt email. At the webpage above, right-click on the Install Now button and save the .xpi file to your desktop.

Now open Thunderbird and choose Tools > Add-ons. Click on the Install button. Browse to the .xpi file you just saved and click on Install. Then click on Restart Thunderbird.

## Setting Up GnuPG

In Thunderbird, choose OpenPGP > Key Management. Then choose Generate > New Keypair. Answer the questions in the wizard. These will include your name and email address. I suggest choosing 2048 when asked for a key size.

Your key consists of two parts: a public key and a private key. The public key will allow anyone who has it to encrypt messages that can only be decrypted with your private key. Your private key can decrypt these messages and sign messages that you send. Anyone who has your public key will be able to verify messages you have signed. Encrypted messages cannot be read by anyone without the private key. Signed messages cannot be changed in transit without alerting the recipient who has your private key.

## Using GnuPG

Now that you have GnuPG installed, you will be able to sign and encrypt messages with the OpenPGP toolbar whenever you compose a message. Signing a message proves to anyone who trusts your key that the message came from you. Encrypting it requires that you have the recipient's public key.

## Getting Email Timestamps With GnuPG

Have you ever sent an email and had the recipient claim he or she didn't get it? Did he or she perhaps say that you must not have sent it? Or did the email to your professor arrive late and result in you getting a lowered grade? There is a solution: timestamps. Using the PGP Digital Timestamping Service, you can prove that you sent that message when you did. While you don't have to have GPG to get a timestamp, you need it to verify one. Go to

<http://www.itconsult.co.uk/stamper/stampinf.htm> to learn more about digital timestamping and how you can get your email messages timestamped simply by bcc:ing them to the timestamping server's email address.

If you are a geek, check out [http://feraga.com/library/howto\\_use\\_a\\_type\\_i\\_anonymous\\_remailer\\_cyberpunk](http://feraga.com/library/howto_use_a_type_i_anonymous_remailer_cyberpunk) to learn how to send anonymous email with GnuPG.

Stay tuned for next week's article on securing your communications.