



## CREATING AND MAINTAINING A GPG KEY FOR KMAIL



KMail's GPG integration is great, but you need a GPG key to use it. Here is the basic information necessary to create and maintain a GPG key. We can't provide an entire GPG tutorial here, but this introduction should be enough to get you started as a user who wants to correspond confidentially with a few people.

### Generating Your Key

The first time you run GNU Privacy Guard, by typing `gpg` on the command line, it will create a `.gnupg` directory and write a blank options file in your home directory, then exit.

Run `gpg` again with the `--gen-key` option, by typing `gpg --gen-key` on the command line, to generate a new key. GPG will prompt you for several options. The defaults are secure and convenient for almost any use.

The last step in the key generation process is selecting a passphrase. If someone steals your computer or gains access to a copy of your home directory, he or she will not be able to use your key to decrypt or sign anything without this passphrase.

However, if someone steals your computer or makes a copy of your home directory, he or she will be able to make an unlimited number of guesses at your passphrase very quickly. So pick a good one—not just a word, short sentence, or poem.

Your passphrase should be rude or embarrassing, and contain letters, numbers, and punctuation. Nobody will ever see it, so reveal your innermost thoughts or fantasies, which would be hard for others to guess. Using a naughty passphrase will remind you not to type it where others can see. If there are no numbers or punctuation in your naughty thoughts, add them in inappropriate but easy-to-remember places.

There are three more important steps to take when you first create a key. First, save the key ID and fingerprint, which you will need to prove to other people that the key is yours.

You can do this by cutting and pasting the last three lines of output from generating your key, which look something like this:

```
.....
pub 1024D/5BAD9DC9 2002-05-24 Joe Test (test key drivel do not use)
<joe@example.com>
  Key fingerprint = C321 0ACC 837E 3CCA 9EA1 0359 C9A8 2939 5BAD 9DC9
  sub 1024g/B5B76E08 2002-05-24
.....
```

Your key ID is the 8 hex digits after “pub”—in this case, 5BAD9DC9. If you need your key ID and fingerprint again, type `$ gpg --finger joe@example.com`.

And the last thing? Generate a revocation certificate. Don't worry, we aren't throwing away your hard work by revoking your key. We're making it possible for you to revoke your key if you need to do so but your computer is gone. (If someone sees you type your passphrase, then steals your computer, you will be happy you had this certificate.) To create the revocation certificate, type

```
.....
$ gpg --gen-revoke 5BAD9DC9 > gpg-emergency.txt
.....
```

Follow the prompts, then print the `gpg-emergency.txt` file, and keep it someplace safe, away from your computer.

## Posting Your Key to a Keyserver

Remember the `.gnupg` directory that GPG created the first time we ran it? Enter that directory, and edit the file options. Your system administrator should tell you what keyserver to use; otherwise, check <http://www.pgp.net/> for a server near you.

Let's say you have decided to <http://keyserver.example.com> as your keyserver. Add the line

```
.....
keyserver keyserver.example.com
.....
```

to your options file, save it, and quit your editor. (At *Linux Journal*, we use <http://wwwkeys.pgp.net.>)

Now you can post your key to the keyserver with the command

```
.....  
gpg --send-keys 5BAD9DC9  
.....
```

(use your own key ID).

## Signing Other People's Keys

KMail automatically tells GPG to get senders' keys from the keyserver when you get mail from them.

### ***Keysigning Events***

Some people hold keysigning events to sign each other's GPG keys. This helps people from around the world who don't know each other communicate. Don't worry about not knowing much GPG before you attend an event; the organizer will send you a step-by-step guide to follow.

## OpenPGP and GPG Documentation

Detailed documentation is available at <http://www.gnupg.org/docs.html>.

