Getting Started with PGP
By Mark Kaprielian
2005-11-21

I. Focus of this Document

PGP will let you send and receive secure and or signed messages or Files. At first, PGP is a little confusing but it will soon seem quite simple.

Most of the guides I have come across are pretty out of date or are at too high a level for the beginner. This guide should help you get started without actually reading the manual.

If you come across better instructions somewhere on doing the basic operations, please let me know.

This guide was written against **version 8.0** but is probably very similar for Version 7.x.

II. An overview of what has to happen to use PGP

The following is a bullet list of items that have to be done to use PGP. In the sections that follow, these steps will be explained.

- Install the program
- Create your own key and publish it to a Public Key Server
- Send your Public key to the person to whom you want to be able to decrypt your message or help them find your Public Key (tell them which server).
- Find or get the key of whom you want to encrypt a message to
- Encrypt your message using the Public Keys of yourself and your recipient.

III. Where to Get PGP

Currently the only place to get the PGP is from the manufacturer – PGP corporation

http://www.pgp.com/

In the past it has often been available from authorized re-distributors.

It is initially a 30 trial with full (advanced) functionality. After that it reverts to just the "free" functionality, which is all you need for basic securing of files. The link below, if it does not change, will take you directly to the page to download it from.

http://www.pgp.com/downloads/desktoptrial.html

IV. Installation Notes

When you run the installation program I will at some point ask you if you already have a Key pair or something like that. You answer no and create your Keys.

You will need a password phrase that you won't forget. You should not write this one down, this identifies you to the world as you.

V. Dealing with Keys

Immediately after installing the program, the only key you need or have should be your own. If there are other keys, feel free to delete them. Be careful to **not delete your own**.

A. Set your own Key to be the Default Key.

1. Launch PGPKeys by clicking on the PGP Icon in the tool tray and selecting PGPKeys
2. Right click on your key and select "Set as Default"

B. Publishing your Key so others can search for it

There are Servers (computers) out on the Internet set up to serve as a common repository for PGP Keys. This is an essential element to how PGP works. To allow someone to find your key without them having to contact you first to get it, you need to publish your key to a Key Server. The idea is to publish your key to servers you think people are most likely to check. One good selection is the PGP Corporation's server.

1. Launch PGPKeys by clicking on the PGP Icon in the tool tray and selecting PGPKeys
2. Click on the menu items Server, Send To, ldap://keyserver.pgp.com
3. You can now verify and get some practice by doing a Search for your own key.
   a) Click on the menu items Server, Search and enter your own name. The options on the left should say User ID contains

C. Finding or Getting someone's Key

To send an encrypted message or to decode a message, you must first have the other persons Public Key. You can get someone's Public Key by several means. I will cover some of these below.

1. Searching for someone's Public Key
   a) Go to PGPKeys window, click on the menu items Server, Search and do a search using their name or possibly email. Pay attention to the options on the left when deciding how to search.
   b) Assuming for the moment that you get more than one Key found, you must decide which of found Keys is that of the person you are looking for. This can be done several ways.
      (1) You recognize the email associated with the name and are positive that is the person you were looking for.
      (2) You click on the plus sign next to the persons Key symbol to expand the view and there, see other peoples keys that you recognize who are vouching for that person. Basically, that person knows people you know so hence it must be the right person.
   c) If you've decided you believe you have found the right key, you now need to add it to your Key Ring. You can do this one of several ways:
      (1) Drag and drop it into your list of keys in the PGP keys window or
      (2) Right Click it and then select Import to Local Key Ring
2. Someone has sent you an Email attachment that is their Public Key

There are several ways you can get the Public Key you were sent onto your Key Ring.

   a) Drag the Attachment from your email and drop it into the PGPKeys window
   b) Click on the menu items Keys, Import then navigate to where you saved the attachment and then click Open.
3. They point you to their Public Key on their Web site.
   a) Find the key on the persons site as they directed you
      (1) If the Key is available as a download

      (a) Download the file to your machine

      (b) Click on the menu items Keys, Import then navigate to where you saved the attachment and then click Open.

4. They copy their public key into their email or let you copy it from their web site as text
   a) (to be filled in later)

D. Sending Someone your Key

You can save someone the trouble of searching for you key by sending it to him or her directly.

1. Go to PGPKeys window, Right click on your own Public Key and select Send to Mail Recipient
2. You can also export your key to a file and then send it to someone or perhaps post it on a web site. Go to PGPKeys window, Right click on your own Public Key and select Export. Pick a location to save the file, which will have a file extension of .asc and then send or post that file.

VI. Sending an Encrypted Message

A. Encrypting the text of an email

1. Type your email as you would normally do
2. Clicking on the PGP Icon in the tool tray and select Current Window, Encrypt and Sign
3. A window titled **PGPtray - Key Selection Dialog** should open up
4. Double Click on all the people’s keys that you want to be able to decrypt the message to add it to the collection at the bottom of the window. You can also drag and drop them. I strongly suggest you always make sure your key is there so that you can decrypt the message you sent in case you need to read it sometime later.
5. You should then be prompted to enter your password. Enter it. This is to ensure that you and only you can create the encrypted message that everyone will believe is coming from you.
6. You should now see the encrypted message in your email window. You may want to write some greeting in front of it or perhaps give other directions such as where to find your key.

VII. Opening an Encrypted Message

A. Decrypting the text of an email

1. Clicking on the PGP Icon in the tool tray and select Current Window, Decrypt and Verify
2. You may be prompted for your password. If so, provide it.

VIII. Signing other peoples keys

One of the central ideas behind PGP and other schemes is knowing whom you can trust. By signing someone’s key or having them sign yours, you are adding weight to probablility that the key belongs to whom they think it does. If all the other signers are people you already know or trust, having their signatures on the key will give you greater confidence in the integrity of that key.

A. Signing someone’s key

1. Go to PGPKeys window, Right click on the Public Key you want to sign and select Sign.

2. Check the box that says you will allow your signature to be exported (if you wish).
3. You now need to let the world know that you signed this Public Key. Click on the menu items Server, Send To, ldap://keyserver.pgp.com or whatever servers you generally use. It will merge your information with what is already up there.

IX. Other Things you can do

There are a number of other things that you could choose to do with PGP. Some of these things depend on the version and if you have a licenced or Free version. Somethings you may choose to do are

- Sign a message but not encrypt it
- Encrypt a file
- Encrypt your drive (useful for notebooks if your concerned about keeping its contents secret should it be stolen)
- Encrypt parts of messages.
- Use the clipboard in the encrypting and decrypting process

X. Maintainence

Absolutely make sure you back up your key rings. You should put your key ring on floppy so you never lose your own key pair.

The two files to back up are: **pubring.pkr** and **secring.skr**

The default location of where these files were put when they were first created can be found by way of

PGPKeys window, Edit Options, Preferences, Files Tab

Since I keep all my data, regardless of application, inside a top level folder on a different drive, I created my own folder to hold my keys and copied my keys there so that I would be sure to back them up every time my other data is backed up. Then, from the same window as detailed above, I select the keys from my own folder.