Encrypted form-mail and GnuPG (GPG)

Document revision: 2001-12-19 (JTS)

1. This document

This document was created with samples and screen shots using the GnuPG utility on Microsoft Windows 2000. Other Microsoft operating systems should be pretty similar, on Windows NT, 2000 and XP, *command prompt* is called *CMD, Shell,* or CMD.EXE. On Windows 9x/Me it is called *MS-Dos Prompt* or *Command.Com*. If you are using Linux/UNIX, the commands are similar but paths are different.
This document is written for those who have some knowledge of what files and folder are on a Windows system, and basic knowledge of HTML and HTML-Forms, as well as knowledge of how to upload files and scripts to your web page.
This document does not explain fully what is needed on the receivers e-mail client.

For a step-by-step instruction, start with chapter 2 and read page by page.

NOTE
This document does not cover all possibilities nor tell you the only way something can be done. In some cases, the way described here may not be the most efficient or recommended way.

1A. Table of contents

2. Download GnuPG binaries to your local computer

The first thing you need to do is to download the GnuPG in binary format (or you may download sources and compile yourself, but that is beyond the scope of this document).

Go to http://www.gnupg.org/download.html and scroll down to you find the binary download for your operating system, for Windows (Any version) us the one marked Windows 95,98,NT. This is a zip-file, so you need to unzip this using WinZip (WinZip.Com) or some other compression utility, uncompress to anywhere you want. Then copy gpg.exe to a system directory in path, C:\windows\ or C:\WINNT (depending on system) should be fine.
Create a directory; C:\gnupg\ (If you choose to use any other directory, please read the file README.W32 from the zip-fle for instructions). This is where your key rings will be stored.

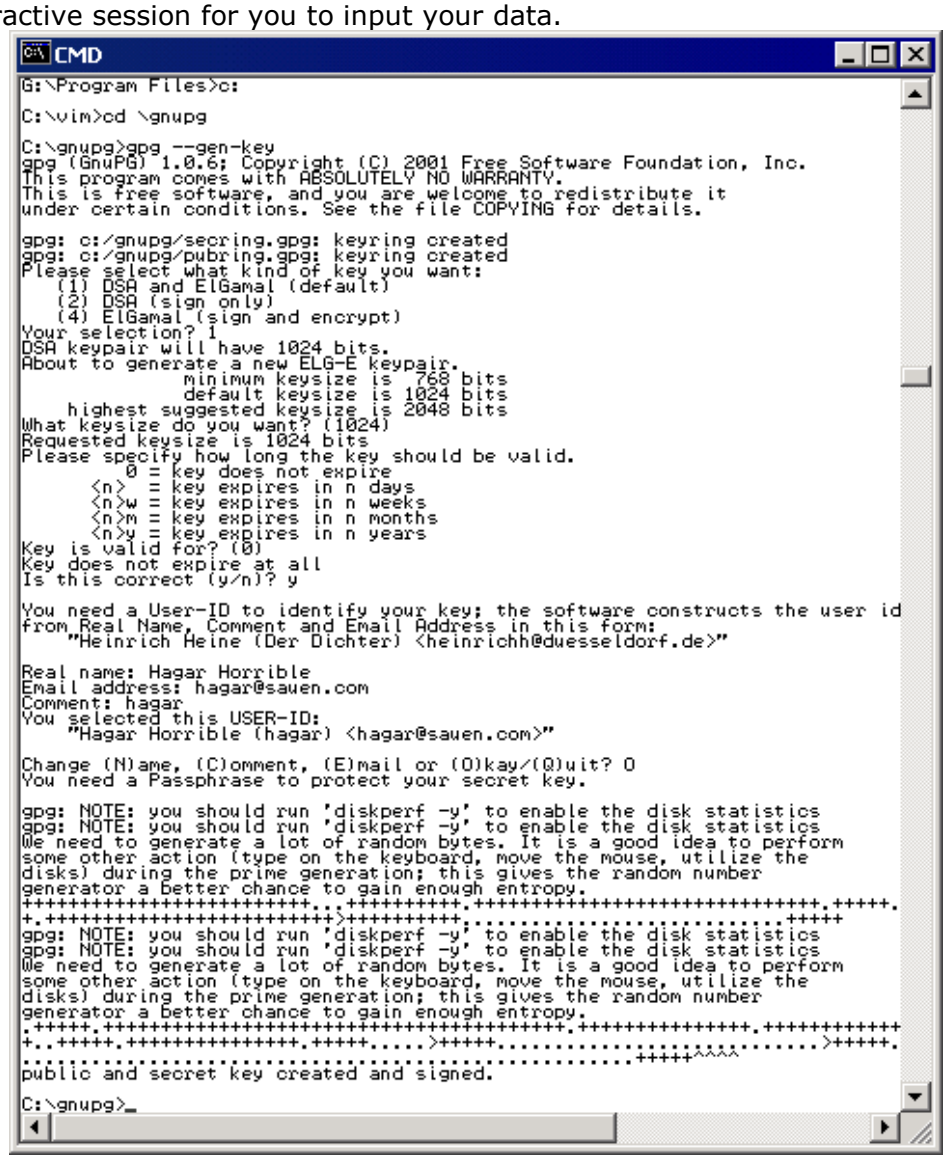
It is highly recommended that you read the README files (Using WordPad or similar) to get to know some of the basics and details about GnuPG.

We also recommend that you download the Gnu privacy handbook, it can be found at http://www.gnupg.org/gph/en/manual.pdf, It contains a lot of useful information about crypto technologies and how to use GnuPG.

A 1024 bit RSA key, which is default and very common, is considered to be secure enough for most applications, the amount of possible combinations for decryption is a large number with 155 digits.

3. Generate a new key-pair

Now start a command prompt window, go to C:\gnupg\, and type `gpg --gen-key`, this will start an interactive session for you to input your data.



Just follow it step by step, the first 3 steps you can just hit enter for default. Then you hit Y for accepting the settings. Then you enter your full name, then your e-mail address, then a comment. We recommend putting a short nickname as comment.

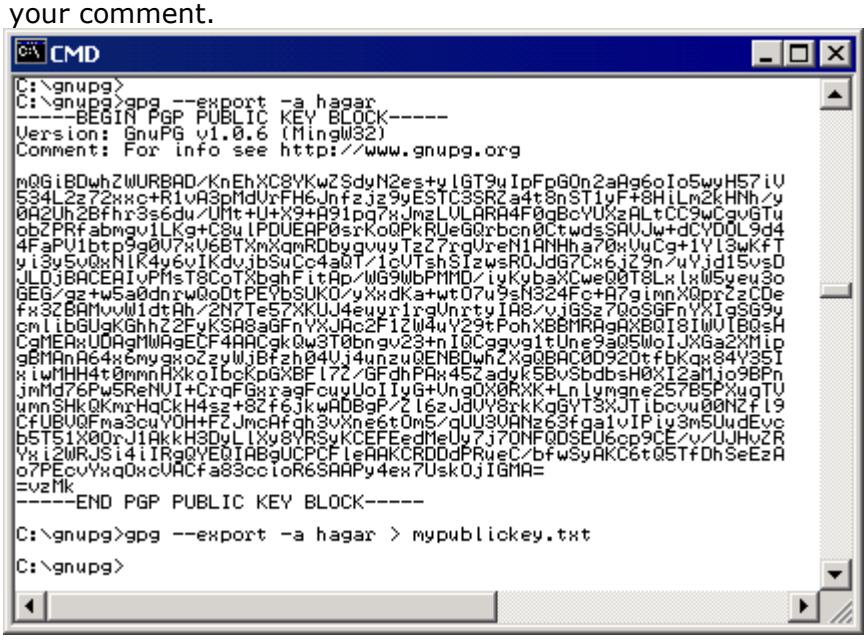
If you typed everything correctly you hit O for Okay. The you are prompted for a secret pass-phrase. Make it long and very difficult, but DO NOT FORGET it. You will be asked to enter it again for verification. Then the keys will be created.

4. View your keys

To verify that the key rings where created, type `dir`, to list the pubic keys on your public ring type `gpg --list-keys`.

5. Export the public key in ASCII format

Most likely you want to use ASCII (Text) format when moving and sending your keys around, the format is supported by most types of electronic transfers and messaging, such as email.
To View the key in ASCII format, type `gpg --export –a user`, where user should be your name or your email or your comment.



Your public key will now be printed on your screen, you can now copy and paste it elsewhere if you like. To save it to a file you can type `gpg --export –a user > filename.txt`, this will put your public key in filename.txt.
Save this key so that you don't loose it, perhaps make several copies. This public key is not a secret, you should share it with anyone who whish to send you encrypted messages.

When handling keys in ASCII format they always begin and end with a dashed line, make sure you always get all of those lines and everything in between when you copy and paste or move these keys around.

6. Private Keys and Secrets – The 'Key' to security

You don't have to export your secret key, but it might be a good idea to store it in on a disk for storage in a safe place. In many cases (in most cases for windows users), you do want to export the secret key, store it somewhere safe, and then delete the key ring from your machine.

Make sure the secret key is stored VERY VERY safe; if anyone ever gets your private key, your security is gone. Well, all that is left is the protection with your key pass phrase, but this last defense is not considered as great as the key encryption itself. (So never write this pass phrase down with your key or anywhere else)

NOTE: If you are on a Windows computer, the security of your private key ring file is very limited (NOT VERY SECURE STORED ON A HARDDISK IN A PC CONNECTED TO ANY NETWORK OR IN ANY TYPE OF MULTIUSER ENVIRONMENT!)
Windows NT/2000/XP has the possibility of using the NTFS file system, which is somewhat secure if you set the appropriate permissions to your file. The FAT/FAT32/VFAT file systems used in other windows versions and sometimes for NT/2000/XP are not secure at all. Using Encrypted file systems with Windows 2000 or XP offers a lot better security to stored files. Linux/UNIX offers a greater file system security, and by default gpg will set the right permissions on your files.

GNU recommends: Store your private key on a floppy or CD and nowhere else. And when it is time to decrypt a message, you download the message to your computer, then disconnect your computer physically from any network and/or phone line, reboot, and then you can insert the disk with your key, import it and decode your message(s). After decryption is done, make sure no sensitive data is stored in your computer in clear text and remove your private key rings and the key-disk before re-attaching any network connection.

It is highly recommended to NEVER store your private key on a server connected to the internet without any form of protection.

Please read the GNU privacy handbook, as mentioned in section 1.

7. Exporting the private key

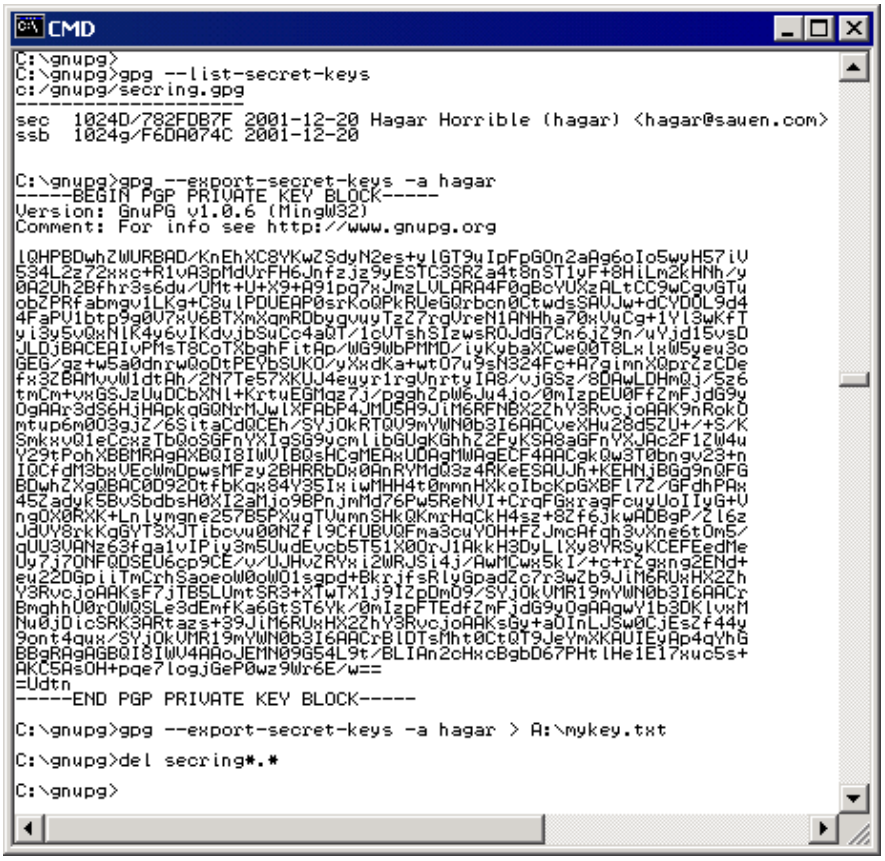
By default gpg will not do anything with your secret keys without explicit telling it to. Please read section 6 above before doing anything to your secret keys.

You can list the secret key with `gpg --list-secret-keys`

To export your secret key to a file mykey.txt to a floppy in you A: drive, type

```
gpg --export-secret-key –a user > A:\mykey.txt
```

And you can delete your secret key ring with `del secring*.*` in the gnupg directory. You may want to make an extra security copy or two before deleting it.



If you did as the example was written, you should now have your secret key on a floppy, make sure you store it in a very safe place. Please read section 6 about securing this key, as well as the GNU privacy handbook mentioned in section 1.

So by now, you should have both your secret key and your public key on file in ASCII format.

More to come… the script and so on..