

How To Use GPG4Win (GNU Privacy Guard for Windows)

GnuPG is a completely free implementation of the Open PGP standard defined in RFC2440.txt. The folks at Gpg4win made an excellent Windows port that allows you to use the standard in almost any way imaginable. This document will explain how to use gpg4win with the intention of encrypting email communications and/or exchanging encrypted files.

This assumes you have a basic understanding of public/private key encryption. If not, don't panic. The principles of encryption are actually pretty simple. Unfortunately, even many IT personnel have been intimidated by "super secret ninja stuff" and have never really learned how it works. The following links will provide more than enough information for anyone to gain a good understanding of encryption.

[Wikipedia on Public Key Cryptography](#)

[About PGP \(Another Explanation\)](#)

[GRC Podcasts \(Start at Episode #30\)](#)

The good news is that the principles of cryptography are fairly easy to learn and understand. The bad news is that a lot of really, really bad mistakes have been made in the computer world by people using cryptography without understanding those principles. Keep in mind that cryptography is classified under munitions. Use it wisely! If you don't "get" public key encryption, avail yourself of the educational links above. For instance, the GRC podcasts will take a while if you listen to all of them, but they are very interesting. If you listen to and understand them, you will know more about encryption than the vast majority of people.

The steps mentioned here work with Microsoft's Office Outlook 2003 / 2007 in or out of an Exchange Server environment. If you have another e-mail client (like Groupwise), you may be limited to encrypting / decrypting files. Of course, you could use Outlook, Thunderbird, or another supported client just for encrypted e-mail. However, if you are not using encryption frequently, the resources required may not justify the added e-mail security.

If you use Outlook Express, search for and use GPGOe. Outlook and Outlook Express are significantly different, and I'm pretty sure GPG4Win will not work with Outlook Express, though I haven't tested it.

If you use Linux or a Mac, you're in luck. Encryption is far better integrated with those operating systems. Evolution e-mail integrates with the OS encryption components natively. For Thunderbird, you can add "enigmail" either through the add-on feature or by installing a package, whichever works best for you.

How To Use GPG4Win (GNU Privacy Guard for Windows)

Let's get started! Download Gpg4Win from www.gpg4win.org. The light version should be fine unless you want to read the complete documentation in German.

GPG4WIN EMail-Security using GnuPG for Windows

Version 1.1.3 (Change History) includes:
GnuPG 1.4.7
GnuPG2 2.0.7
WinPT 1.2.0
GPA 0.7.6
GPGol 0.9.92
GPGee 1.3.1
Claws Mail 3.0.0-rc2
Gpg4win for Novices 1.0.0
Gpg4win für Durchblicker 2.0.2

Download
Gpg4win 1.1.3 (2007-09-17)
SHA1MD5/OpenPGP-Sig

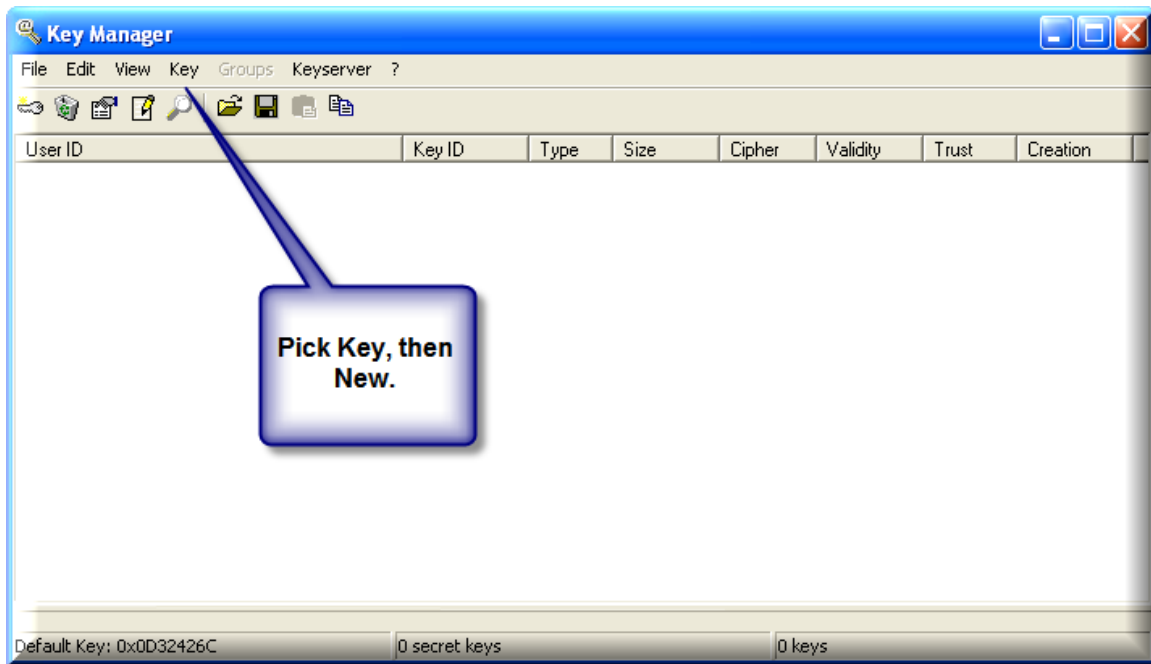
Download
Gpg4win 1.1.3
You can download the full version (including the German manuals) of Gpg4win 1.1.3 here:
gpg4win 1.1.3
Size: 9.3 MByte

Install gpg4win with all the available components except Claws Mail, unless you want to install an email client. It is a good idea to close Outlook first, if it is running.

If you are using Outlook, you will notice new tools for encryption and you will be prompted upon first usage to create a key. If you are not using Outlook just run WinPT manually (typically located at: C:\Program Files\GNU\GnuPG\WinPT.exe). A new key-shaped icon will appear in your system tray. Double-click on that icon to open WinPT, select "Key" and "New" to generate a new key pair.

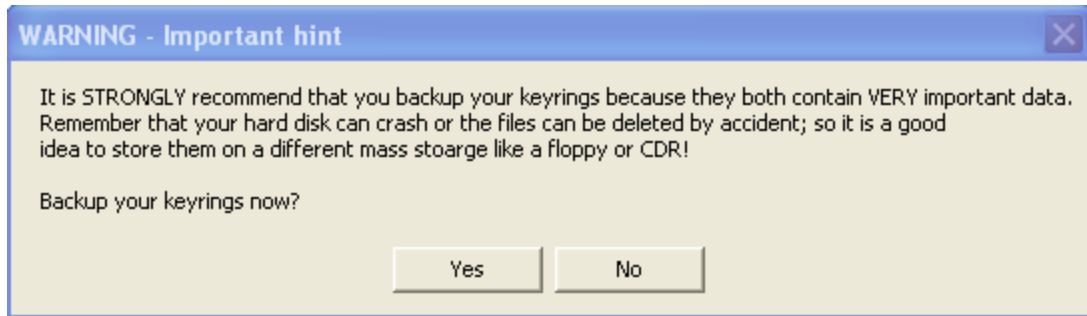
Supply the information requested (name, email, key password, etc). Hint: A passphrase is similar to a password, but generally is a phrase with mixed case, punctuation, and numbers. For instance: "My dog's license # is: 1832." might be a good passphrase. Make it something only you would know, but record it in a secure location, just in case.

How To Use GPG4Win (GNU Privacy Guard for Windows)

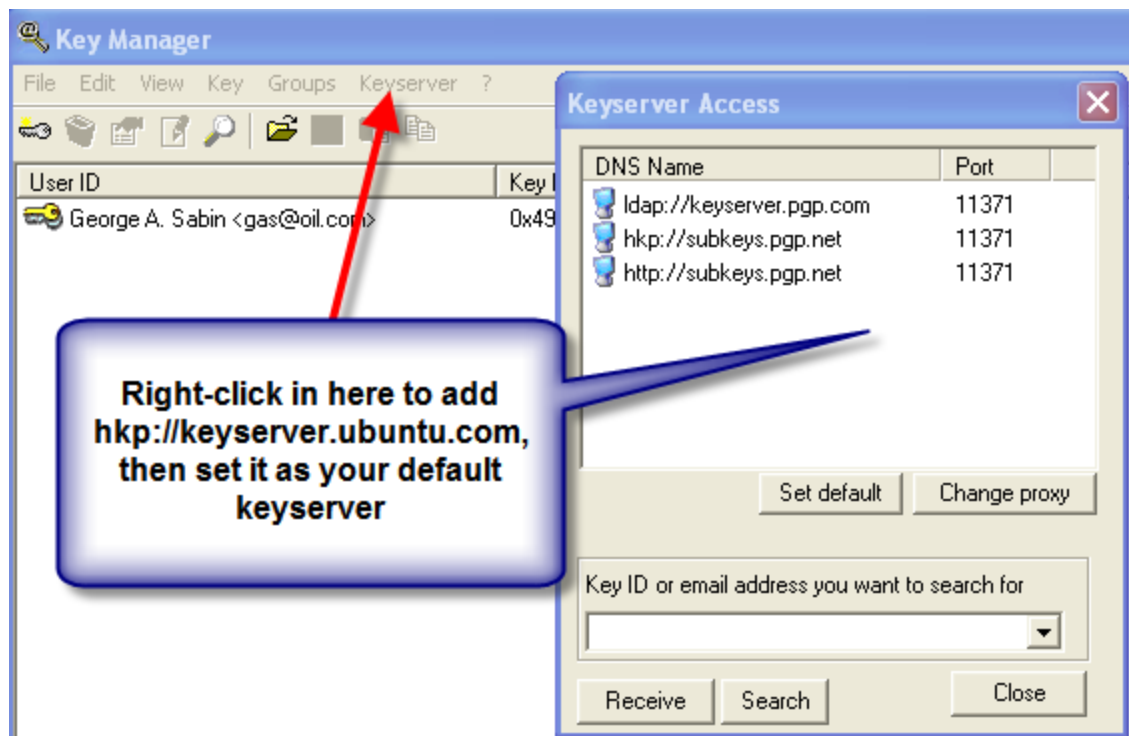


How To Use GPG4Win (GNU Privacy Guard for Windows)

WinPT will begin generating a random key which you'll use to decrypt incoming encrypted messages. Create a backup of this key and keep it in a safe place to prevent losing encrypted information in the event of hardware/software failure. It is also a good idea to immediately generate a revocation certificate and store that with the backup certificate. This way, even if you forget your password, you can still revoke your certificate on the keyserver.



It is far easier to use a public keyserver for key exchange since it makes key management easier. A preferred server is `hkp://keyserver.ubuntu.com`. (Yes, that is "hkp", not "http".) You will need to manually add this keyserver and make it the default.



How To Use GPG4Win (GNU Privacy Guard for Windows)

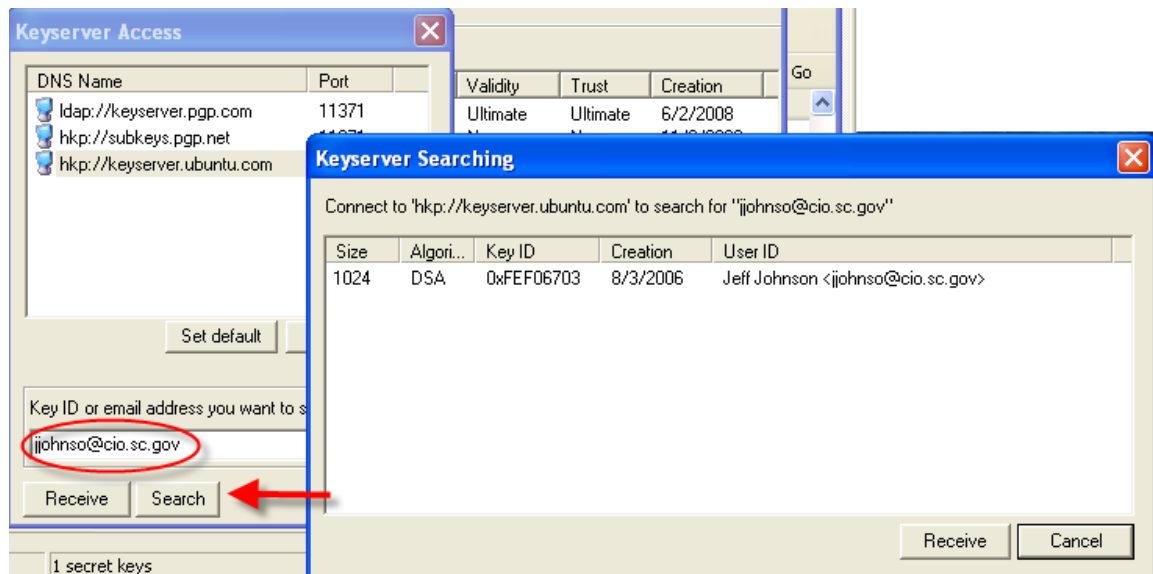
To export your public key, right-click on it and choose "Send to keyserver".

To receive other keys, you may search for and download keys from the keyserver: *Please exercise caution when downloading keys.*

You may have noticed that there was nothing preventing you from spoofing someone else's e-mail address when creating a key. This is a known weakness of this type of key management, but it is easily mitigated if you simply check with the individual and get their key ID and "fingerprint" before downloading their key. You should also test the key by sending them a message encrypted with that public key. If they can't decrypt it, they don't have the private key. (This could still be circumvented with a "man-in-middle" attack if the attacker could intercept the mail, decrypt it with the false private key, then re-encrypt it with the real public key. But it is has a lot of dependencies and would be very difficult to perform.)

Check the fingerprint against the downloaded key and you will have a high degree of certainty that you have the correct key. (Besides, if you don't, the first mail you send encrypted to the real recipient will not work for that recipient.)

Open the keyserver dialog and type in the e-mail address you want to search for, then click Search. In general, if more than one key with the same address exists, choose the newest one. If there is any doubt, double-check the Key ID and/or check with the person before trusting a key.



If you are using a supported e-mail client, it is a good idea to import the public keys of anyone with whom you want to exchange encrypted e-mail. For instance, my key is whinsch@bellsouth.net

How To Use GPG4Win (GNU Privacy Guard for Windows)

If you are not using Outlook, there are still ways to use GPG. For instance, you may encrypt files with symmetric key encryption (where you supply a password that both you and the recipient will know). Or, if the sender has your public key, they may encrypt a file with your public key and send it to you. Only you will be able to decrypt it with your private key. Finally, if you have a recipient's public key, you may likewise encrypt a file with their public key and send it to them.

For those not using Outlook, there are still alternatives. If you use the Mozilla Thunderbird client, install the "enigmail" add-on for GPG integration into that client. Evolution (Linux) integrates encryption if you have GPG installed.

If you are using a mail client that GPG4Win does not directly integrate with, you can still use GPG for exchanging files. Essentially, what you will need to do is encrypt and decrypt files from the command line, then send/receive those files using your regular e-mail client.

Another tip: To send your public key to someone who cannot get to a keyserver for any reason, just right-click on your key and pick on the option to e-mail it. The public key will be extracted and attached to a new mail in your default mail client.

For those comfortable with the command line, you can change to the "Files\GNU\GnuPG" directory and run: `gpg --help`

Some quick-start command line tools are:

`gpg --gen-key` # This will walk you through key generation

`gpg --armor --export-key <key>` # Export a public key in a format that can be e-mailed

`gpg --list-keys` # List keys in your key ring

`gpg -r <key> -e <file>` # Encrypt a file.

`gpg -d <file>` # Decrypt a file

If `gpg` is not in your path for the above commands, you may have to supply full paths. For example, to decrypt a file you have saved to the [c:\temp](#) directory and save it to a file in that same directory without the `.gpg` extension...

```
"c:\Program Files\GNU\GnuPG\gpg.exe" -d c:\temp\MyFile.html.gpg > c:\temp\MyFile.html
```

Hopefully this document answered some of your questions. If you are still confused, There are many places where you can find more information about public encryption, PGP, GPG, and any other information you need. Feel free to ask a club member as well.