GPG4WIN

GNU'S TOOLS FOR SECURE COMMUNICATION AND DATA STORAGE

USER'S GUIDE

Version Information

GPG4WIN User's Guide version 1.0 Released July 5, 2006

Copyright

Further Copyright Information

Limitations

We do not warrant that the information contained in this document meets your requirements or that the information is free of errors. The information may include technical inaccuracies or typographical errors.

Acknowledgement

We would like to thank the following people:

The GPG4Win Project Team for their effort in developing GPG4Win software

The developers and/or authors of the following software:
● *GnuPG* ● *WinPT* ● *GPA* ● *GPGol* ● *GPGee* ● *Sylpheed-Claws* ● *GPGME* ● *GLIB* ● *NSIS* ● *Pthreads-win32* ● *LIBGPG-ERROR* for making encryption, key management, and secure e-mail easier

CuteWriter and *Ghostscript* author for their Portable Document Format converter.

And all the others who made this work possible .

Table of Contents

1. Introduction

GPG4WIN is an installer package for Microsoft® Windows operating system (9x/ME/2000/XP/2003) that provides several modules. These modules are aimed in implementing OpenPGP Standard (RFC 2440[1]) for e-mail and file encryption.

It means two things:

1. everyone can use GPG4WIN and its modules to encrypt e-mails and files;
2. GPG4WIN is compatible with other software that conform with OpenPGP Standard.

The GPG4WIN modules are:

Module Name	*Description*
GnuPG[2]	Is a free software replacement for the PGP[3] suite of cryptographic software, released under the GNU General Public License. GnuPG is completely compliant with the IETF standard for OpenPGP. This module is the core module; this is the actual encryption tool.
WinPT	A key manager and helper for various encryption matters.
GPA	Another key manager.
GPGol	A plugin for Microsoft® Outlook 2003 (e-mail encryption).
GPGee	A plugin for Microsoft® Windows Explorer.
Sylpheed-Claws	A complete e-mail program with GnuPG plugin.

Depending on your requirement, you can install all or some of the modules, except for the GnuPG module. It is the core module that must be installed. If you are not sure which modules to choose, you can refer to the following tables:

If you ...	*install the following module(s)*
want to use the GnuPG command line tools only	GnuPG
have an e-mail program (Outlook, Thunderbird) and want to encrypt e-mail and files	GnuPG, WinPT or GPA

[1] Refer to http://tools.ietf.org/html/2440 for detailed information
[2] GnuPG is the GNU project's complete and free implementation of the OpenPGP standard. Visit http://www.gnupg.org for more information
[3] Pretty Good Privacy (PGP) is a computer program which provide cryptographic privacy and authentication. Visit http://www.pgp.com for more information

have an e-mail program (Outlook, Thunderbird), want to encrypt e-mail and files, and want a quick access to right-click context menu in Windows Explorer	GnuPG, WinPT or GPG, GPGee
use Microsoft Outlook 2003 and want to send e-mails using GnuPG plugin	GnuPG, WinPT or GPA, GPGol
want to use complete e-mail program with GnuPG plugin	GnuPG, Sylpheed-Claws
want to use all the GPG4WIN modules and features	All modules

Note : This document (version 1.0) will describe the third option, which provide a good compatibility for most of user's environment.

It is a good thing to understand some basic principles and concepts of Cryptography and Public Key Cryptography before using GPG4WIN (or other PGP/OpenPGP related products). You can find a good documentation here:

- *Applied Cryptography: Protocols, Algorithm, and Source Code in C, 2nd ed,* Bruce Schneier, John Wiley & Sons, 1996; ISBN 0471117099. If you are going to a remote island and could only pick one cryptography book, this is the one.
- *How PGP Works*, http://www.pgpi.org/doc/pgpintro/
- *Public-Key Cryptography – Wikipedia,* http://en.wikipedia.org/wiki/Public_key_cryptography

2. Obtaining GPG4WIN Installation Package

You can obtain the latest GPG4WIN Installation Package here:
http://www.gpg4win.org/download.html

If you want to verify the installation file integrity, you can use one of this small program to compute the installation file checksum[4] value:

- Microsoft FCIV, http://support.microsoft.com/?kbid=841290 or
- MD5sums, http://www.pc-tools.net/win32/md5sums/

and compare it with the checksum value posted on this site:
http://www.gpg4win.org/package-integrity.html

3. Installing GPG4WIN

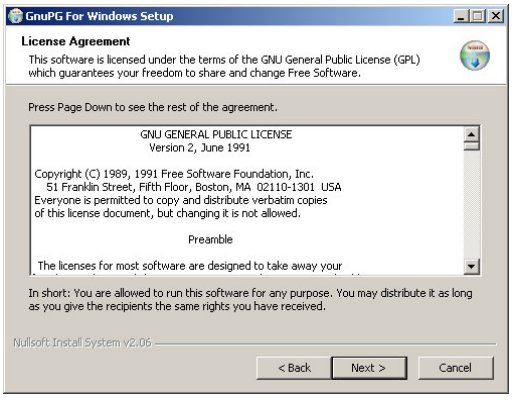
Before installing this program, please close all of other applications, especially Windows Explorer and Microsoft Outlook.

[4] Refer to http://en.wikipedia.org/wiki/Checksum for detailed information about checksum.

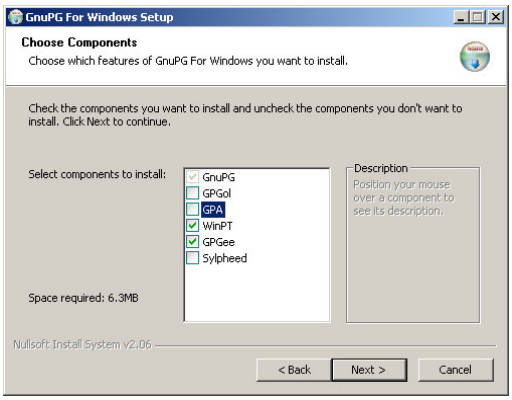
To install GPG4WIN, just double-click (or run) the Installation Package, and the installation process will start. You need, of course, administrator/power user privilege to install GPG4WIN.

Step 1:
The installation window will appear. Click '**Next >**' to proceed.

Step 2:
License Agreement window will appear. Click '**Next >**' to proceed.

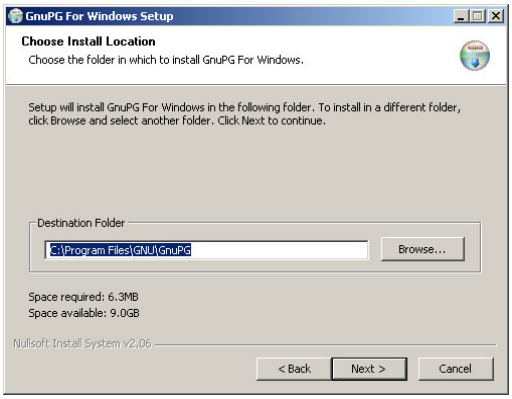


Step 3:
You may choose which components to install. In this document, we are going to use GnuPG, WinPT, and GPGee.

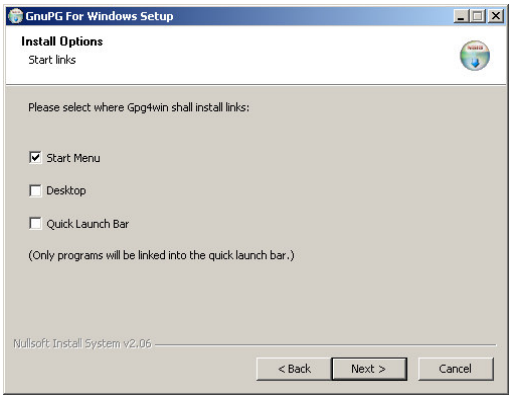


Step 4:

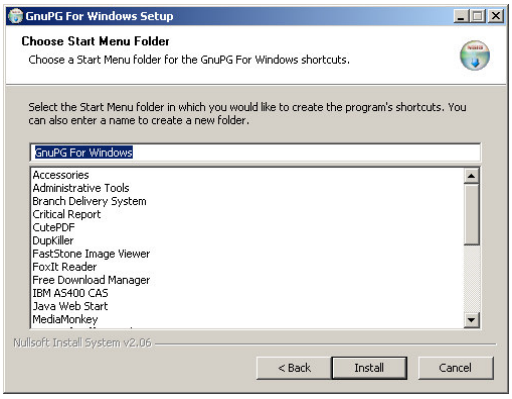
Pick the destination folder for the program. Click '**Next >**' to proceed.



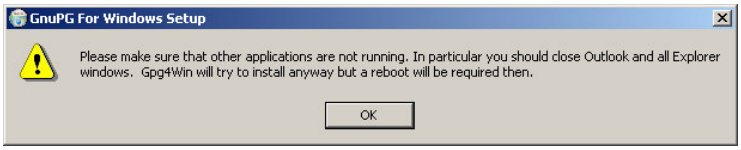
Step 5:
Pick your favourite link type. Click '**Next >**' to proceed.

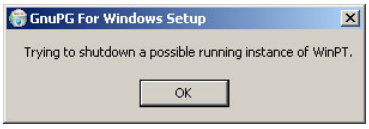


Step 6:
Pick the Start Menu folder if you choose Start Menu for your link type. Click '**Next >**' to proceed.

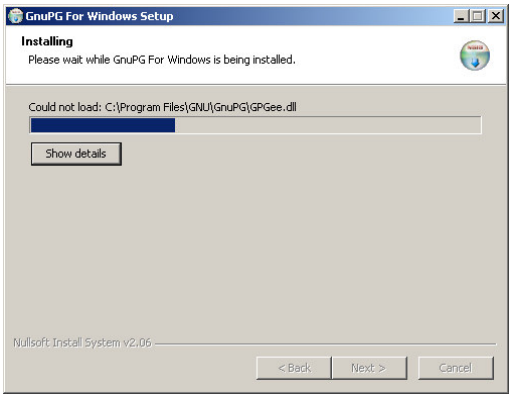


Step 7:
Some notification message might appear. Just click '**OK**'.

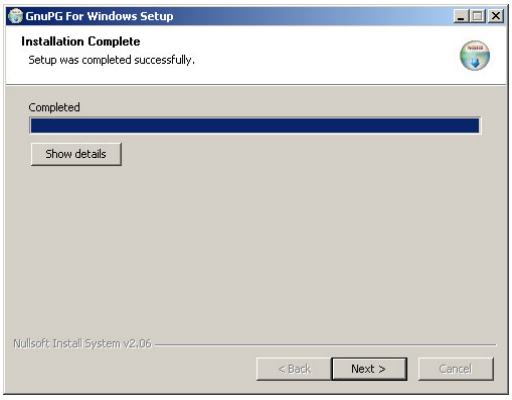




Step 8:
Now, GPG4WIN is being installed.



Step 9:
Click '**Next >**' after completed.



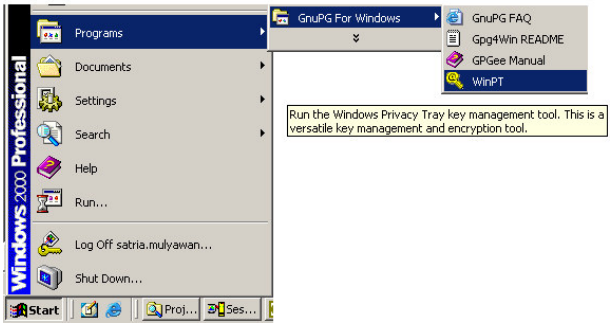
Step 10:
Installation is now complete. Click '**Finish**'.

4. Generating/Importing Your Keypair

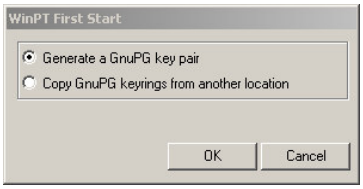
The very first step in using GPG4WIN is generating or importing your own keypair. Generate keypair if you do not have one. If you already have your own keypair, please jump to section "Importing Your Keypair".

4.1 Generating Your Keypair

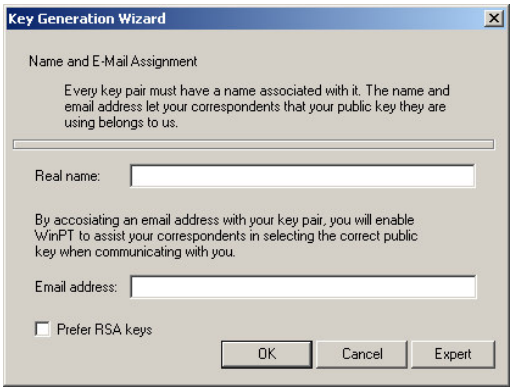
Step 1 :
You can start this process by selecting WinPT from the Windows Start Menu



Step 2:
Choose '**Generate a GnuPG key pair**'. Click '**OK'.**

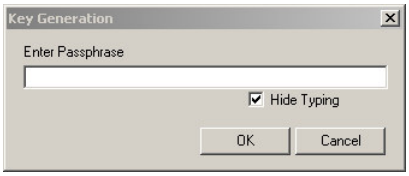


Step 3:
Enter your real name and your e-mail address. Unless you have specific need for RSA keys and other expert setting, leave the '**Prefer RSA keys**' empty[5]. Click '**OK**' to proceed.

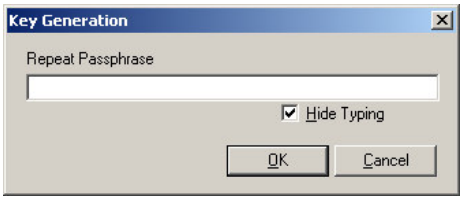


[5] For those who are curious enough, GnuPG use 2048-bit DSA and ElGamal algorithm, as specified in the OpenPGP standard as mandatory asymmetric algorithm.

Step 4:
Now you have to provide a passphrase[6] that will protect your secret key. Please note that there will be no way to retrieve or reset this passphrase if you forget it, so be very careful. And one more thing: pick a long phrase that hard-to-guess. Click '**OK**' to proceed.

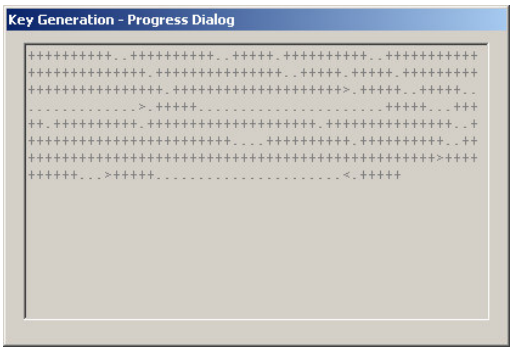


Step 5:
Re-type your passphrase for confimation. Click '**OK**' to proceed.



Step 6:
GnuPG will create your keypair by generating some random bits. To increase the randomness (and also increasing the keypair quality), you might want to try some of these:

- moving your mouse randomly
- typing random character using keyboard
- opening a large file
- running a resource-intensive program



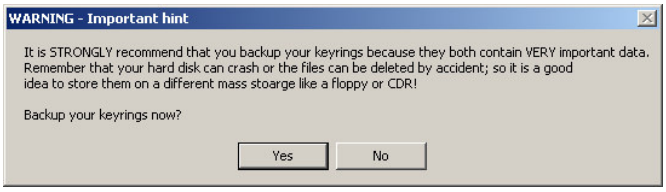
Step 7:
The key generation process is complete. Click '**OK**' to proceed.

Step 8:

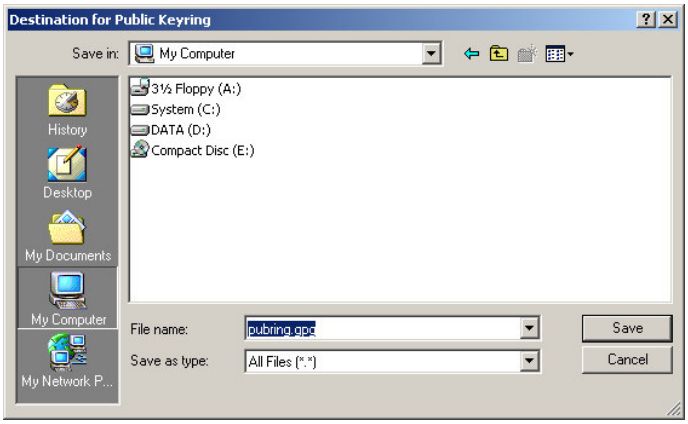
[6] Passphrase is similar to password, but (should) consists of two or more words. In means that passphrase should have more characters that ordinary password. You can read tips about passphrase at http://www.iusmentis.com/security/passphrasefaq/strength/#HowdoImakeastrongpassphrase

Since your keypair (and your keyring[7]) is an important part in public-key cryptography, we strongly recommend you to store your keyrings in a backup media (floppy disk, CDROM, or other removable media). Losing these keyrings means: (1) you cannot access your encrypted e-mails and files and (2) you need to re-distribute (or re-publish) your new public key. To back it up, choose '**Yes**'.

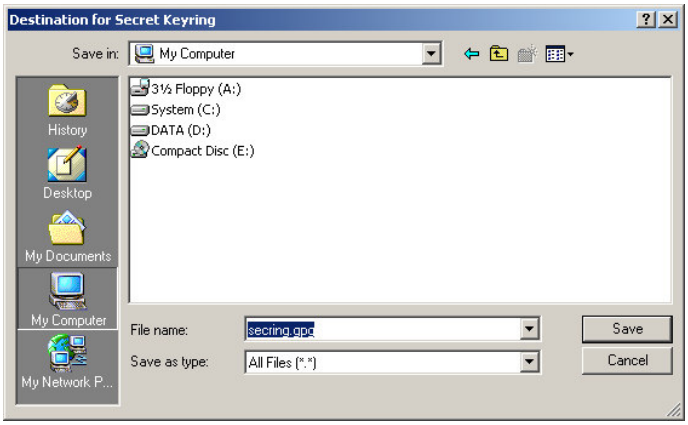
Please note that your private (secret) keyring is protected by your passphrase, so it would be safe enough to back it up in a common backup media (assuming you pick a good passphrase in previous step).



Step 9:
Now, you have two different keyring to backup: a public keyring and a private (secret) keyring. Choose your backup media to store your public keyring,



Step 10:
and your private (secret) keyring



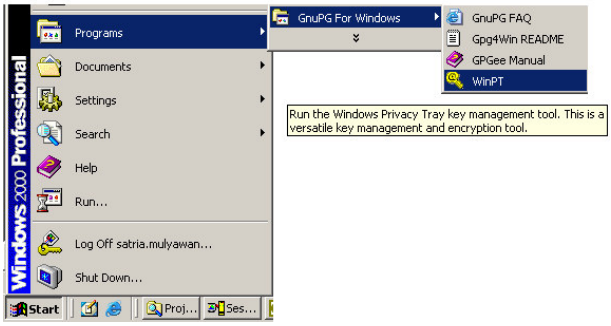
[7] A keyring is a collection of several keys

4.2 Importing Your Keypair

This section is only intended for those who already had their own keypair before WinPT installation. For example: veteran GnuPG command-line user or PGP Desktop[8].

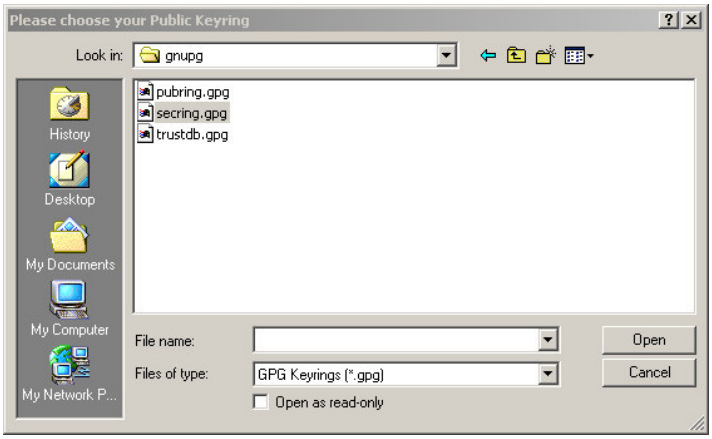
Tips for PGP Desktop user: You can import PGP Desktop keypair/keyring by simply renaming the **pubring.pkr** and **secring.skr** to **pubring.gpg** and **secring.gpg**. Then, you can import them using steps below.

Step 1:
Start the WinPT Program.



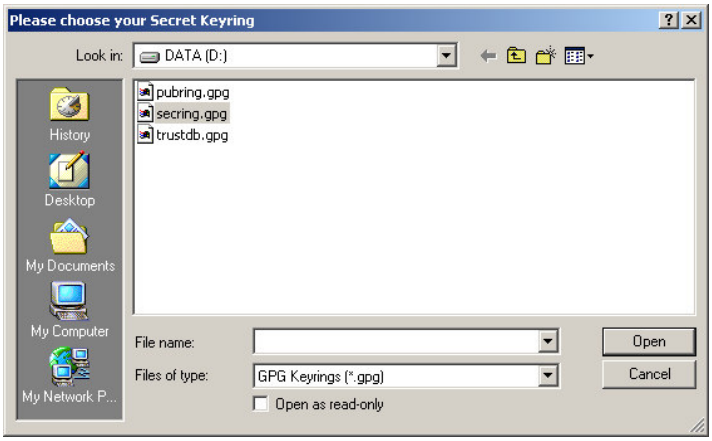
Step 2:
Choose '**Copy GnuPG keyrings from another location**' and click '**OK**'.

Step 3:
Browse to your public keyring location. Choose that keyring and click '**OK**'.

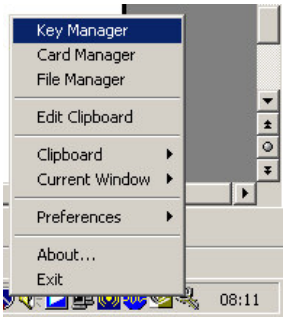


Step 4:
Browse to your private (secret) keyring location. Choose that keyring and click '**OK**'.

[8] © PGP Corporation. All rights reserved.

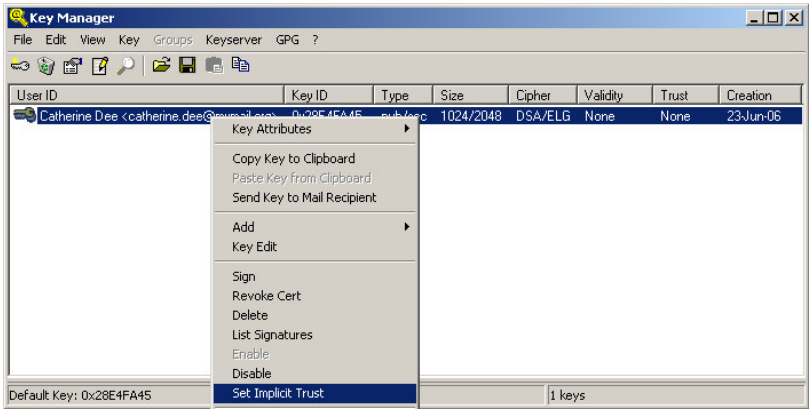


Step 5:
Right-click the WinPT System Tray icon and choose '**Key Manager**'.



Step 6:
You might encounter this message if WinPT cannot found ultimate trusted key in the current keyring. Just click '**OK**' for this message.

Step 7:
In the Key Manager, right-click on the key and choose '**Set Implicit Trust**'. This key will become valid and have ultimate trust properties.

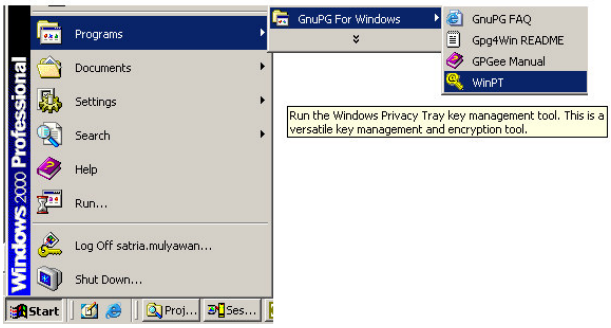


5. Exporting/Publishing Your Public Key

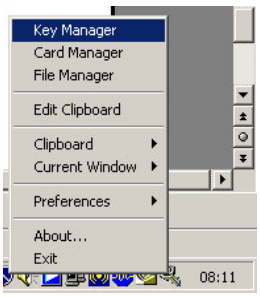
Now you have your own keypair: a public key and a private (secret) key. Bob, for example, will need your public key if he want to send encrypted e-mail to you. So the next logical step will be exporting/publishing your public key so that Bob and everyone else can send encrypted e-mail to you.

5.1 Exporting Your Public Key Into a File

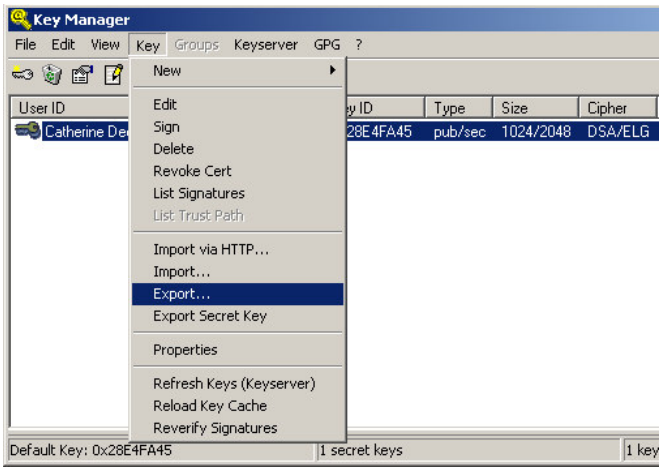
Step 1:
Start WinPT from the Start Menu.



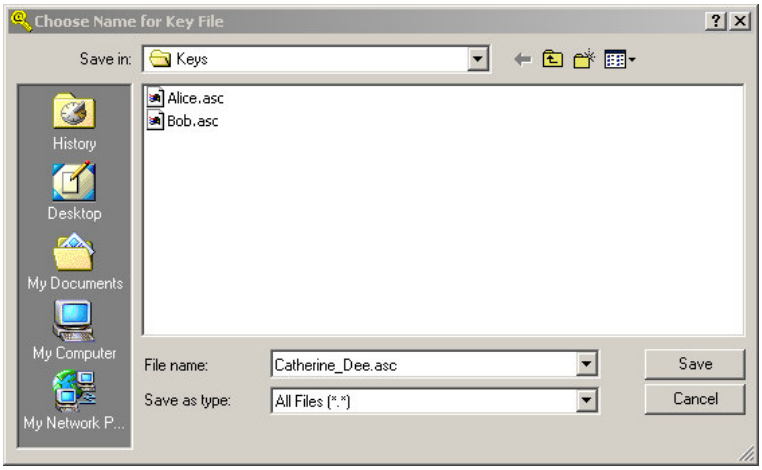
Step 2:
Activate the Key Manager by right-click on the WinPT system tray icon and choose '**Key Manager**'



Step 3:
Choose '**Key > Export...**' from the menu.



Step 4:
Name the key and save it.



Step 5:
Click '**OK**' when the notification box appears.

Now, you can send this file to anyone that need your public key. You can do it by:

- attach the file to your e-mail
- copy-paste its content (it's in ASCII format, just open it with notepad or other text editor) to your e-mail text
- put the file or its content in your website or weblog
- put it in removable media (floppy disk, USB flash, etc.) and circulating it

5.2 Publishing Your Public Key at Keyservers

If you want your public key to be recognized worldwide, you can publish your public key at some internet keyservers.

[this section is not complete yet]

6. Importing Others' Public Key

You will need Alice public key if you want to send encrypted e-mail/file to Alice. You can get her public key by asking her to send it to you by e-mail, or download it from keyservers or her website/weblog.

There are lot of methods to obtain Alice's public key. But whatever method you choose, make sure that the key is *really* Alice's, not key from someone else who pretends to be Alice.

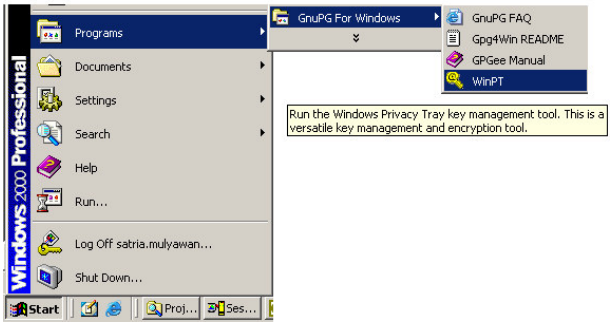
Usually, public keys are distributed in small file with **.asc** extension (e.g. charlie.asc for Charlie's public key). But if Alice sent you her public key embedded in her e-mail messages, for example :

```
From: Alice
Sent: Tuesday, 27 June, 2004 13:48
To: Catherine Dee
Subject: My public key

Hello,

I have already read your messages. I will send you the files as
soon as possible. Meanwhile, here is my public key:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.3 (MingW32)

mQGiBESbqegRBACUSFAyzJYpy/LlDNSkCyLO4/0afgifLwVt63Rd8BhPHMkI5GSZ
oh1EL9uCNKhSpRTmhWP3EzVHYsU3Vp1O7MNEcz2OAaUUDYtxpwKNrRFKPiR4M3/T
6O3xal3IXNlX3WRT/3szl2FKORqISQQYEQIACQUCRJup+wIbDAAKCRDmCGMQIAm5
KJorAKC57QqBqDeRQM9fzcGnwA2+hLBd1wCgrEXeqCr27ixJOWA+OOChi6tL84w=
=8R5H
-----END PGP PUBLIC KEY BLOCK-----

Allright, that's all for now.

Regards,

Alice
```

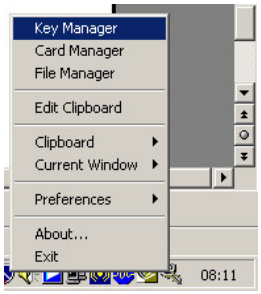
then all you have to do is copy the bold lines (from **--BEGIN PGP PUBLIC KEY BLOCK--** to **--END PGP PUBLIC KEY BLOCK--**), paste it to your favourite editor, and save it as **alice.asc** file.

After obtaining Alice's public key file, we need to import it to our public keyring

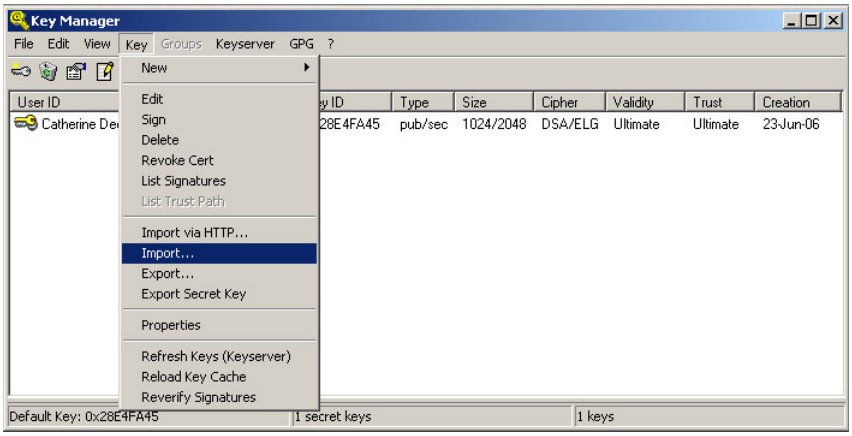
Step 1:
Start WinPT from the Start Menu.



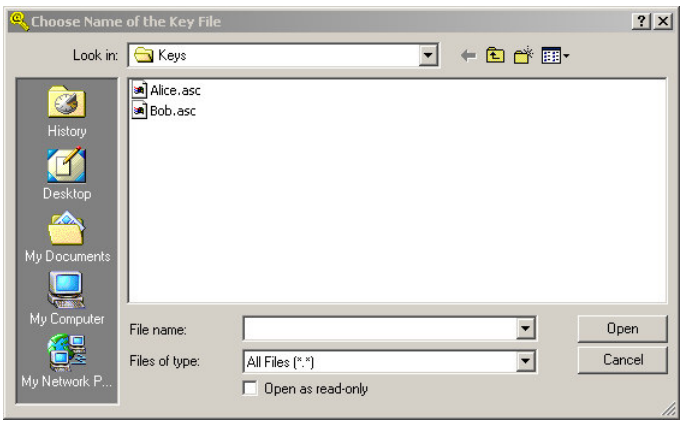
Step 2:
A WinPT System Tray icon will appear in the bottom left corner. Activate the Key Manager by right-click on the icon and choose '**Key Manager**'



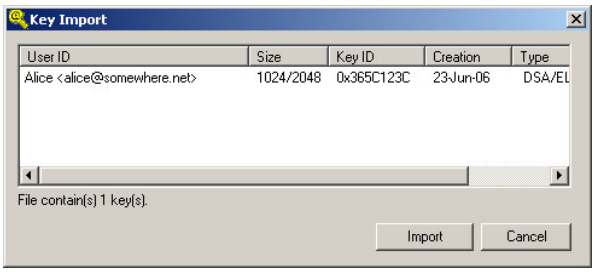
Step 3:
From the Key Manager menu, pick '**Key > Import...**'



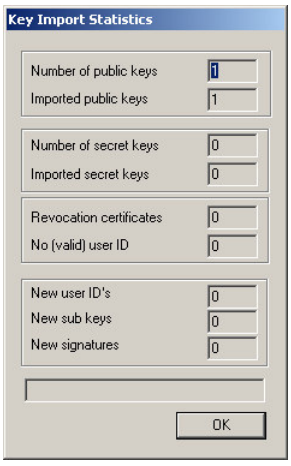
Step 4:
Browse to the public key file, click the file, and click '**OK**'



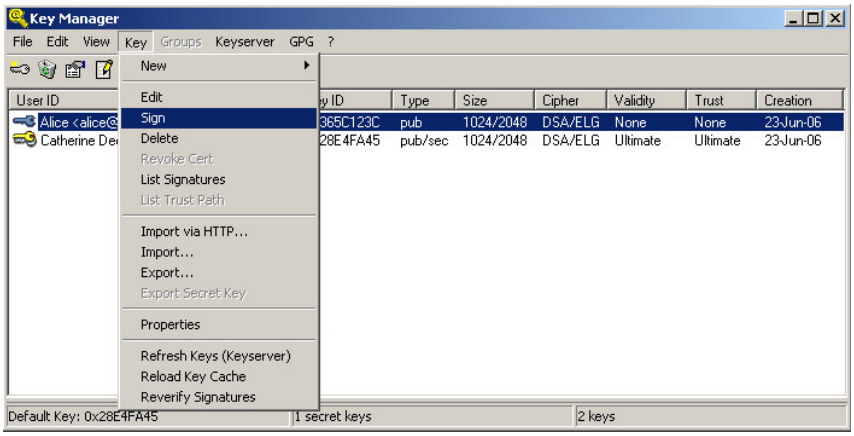
Step 5:
Information about the public key will be displayed. Click '**Import**' to proceed.



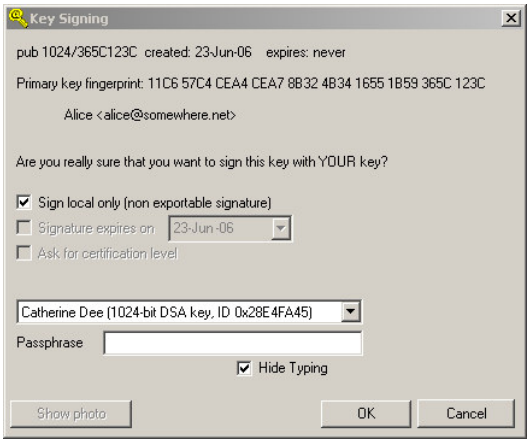
Step 6:
Key import statistic will be displayed. Click '**OK**' to proceed.



Step 7:
Now, we have to sign this public key to validate that this key is truly Alice's public key. At the Key Manager, click the Alice's key. Choose menu '**Key > Sign**'.

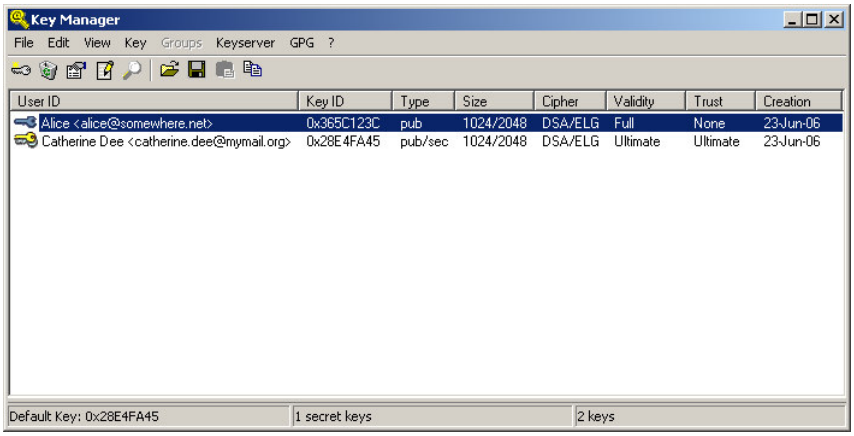


Step 8:
At the Key Signing dialog box, choose your key (it might have been chosen by default) and type your passphrase. Click '**OK**'.



Step 9:
An information box will be displayed. Click '**OK**'.

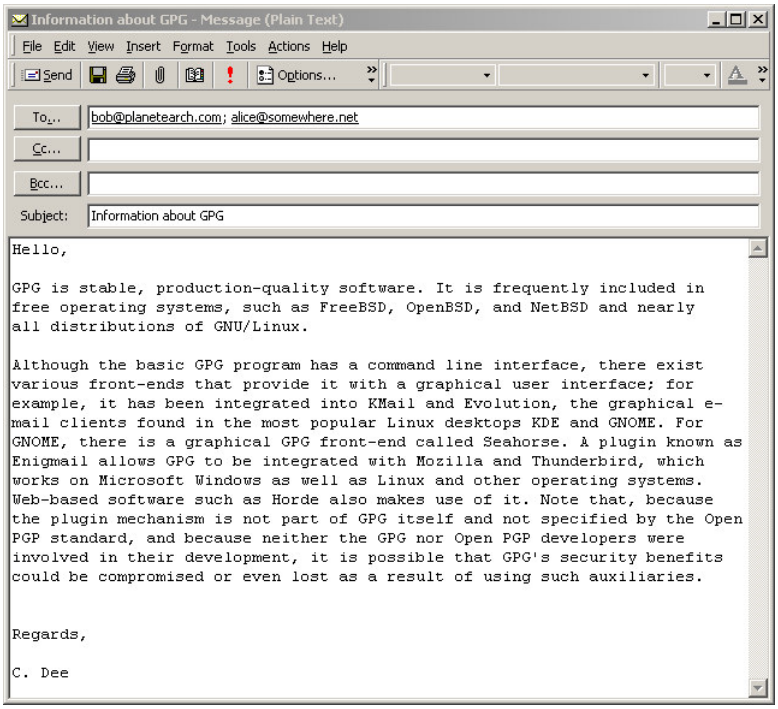
Step 10:
Alice's key will now have full validity (see Validity column).



7. Sending Encrypted E-mail

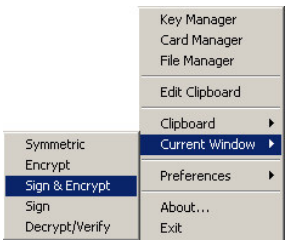
Let us assume that Alice and Bob have received our public key, and we also have import their public keys into our keyring. Now, we can send encrypted[9] e-mail to them.

Step 1:
Compose your e-mail as usual, using your favourite e-mail client. In this example we are going to use Microsoft® Outlook 2000. We are going to send it to Alice and Bob

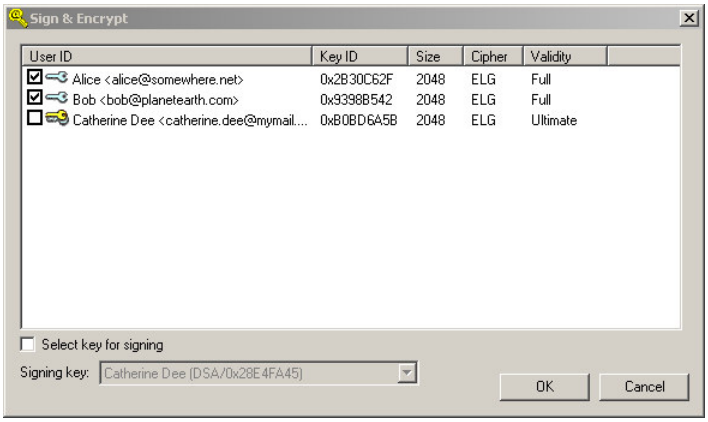


Step 2:
Right-click the WinPT sytem tray icon. Choose '**Current Window > Sign & Encrypt**'.

[9] GPG4WIN/GnuPG use Blowfish as default symmetric algorithm. Visit http://www.schneier.com/blowfish.html for more information about this algorithm.



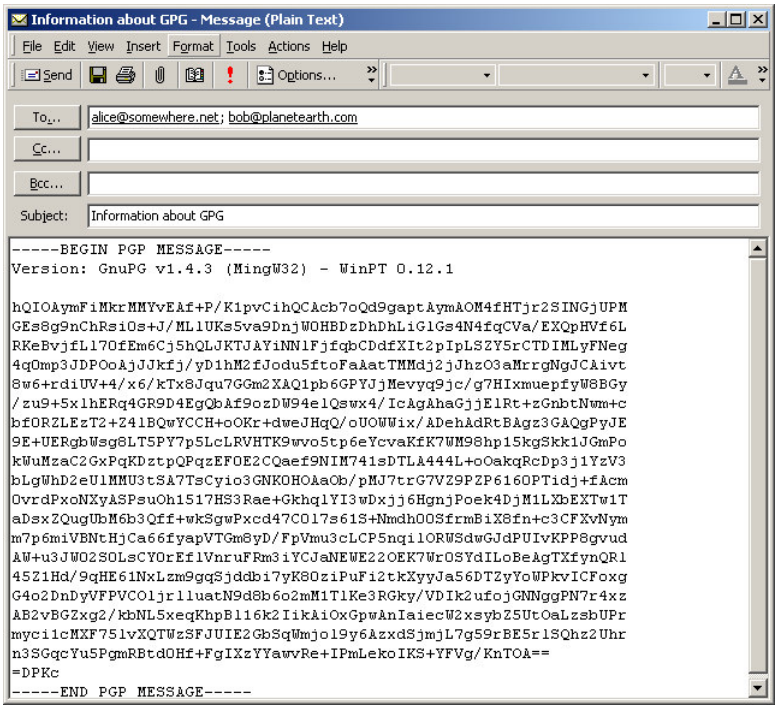
Step 3:
Put check marks on Alice and Bob keys. Click '**OK**'.



Step 4:
WinPT will ask for your passphrase. Enter your passphrase and click '**OK**'.

Step 5:
WinPT wil automatically replace your e-mail message with encrypted messages. Then, you can send this e-mail by clicking '**Send**' button.

If WinPT does not automatically replace your e-mail messages with encrypted one, you can manually replace it. This could be done easily by using **Ctrl-A** (select all) and then **Ctrl-V** (paste) combination at the e-mail client window.



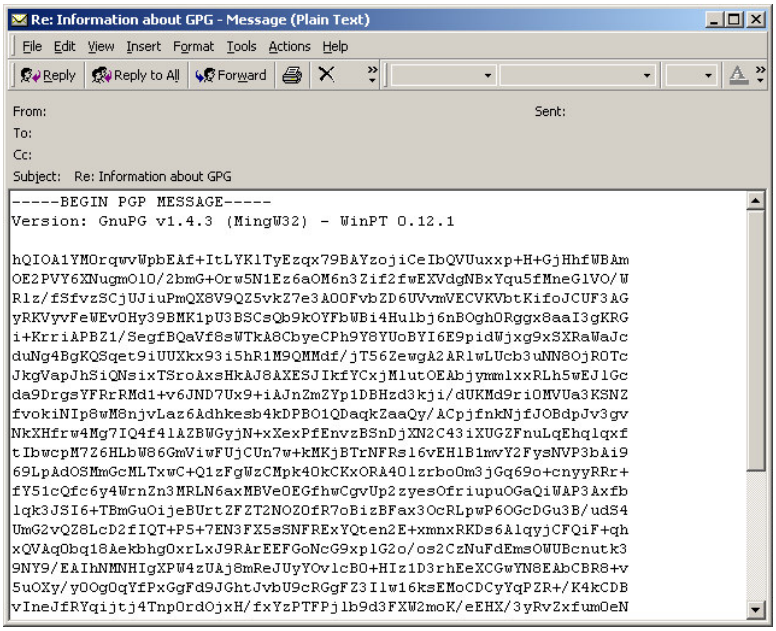
Alice and Bob will received this encrypted message and decrypt it using their own private (secret) key. They will also (automatically, by their software) verify your signature in the message to prove that it was sent by you.

If you are going to attach files in your encrypted e-mail message, you will need to encrypt the files first. Please refer to '**Encrypting Files**' section in this manual.

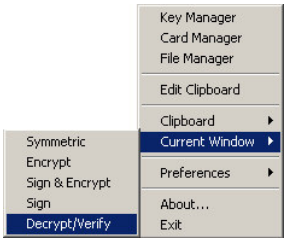
8. Receiving Encrypted E-mail

Allright, you have successfully sent encrypted e-mail now. One day later, Alice replied your e-mail using encrypted messages. Now, we are going to decrypt her message.

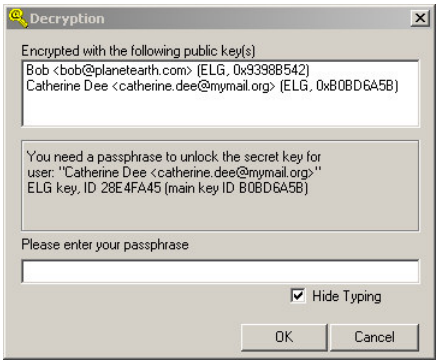
Step 1:
Open the e-mail as usual.



Step 2:
Right-click WinPT system tray icon. Choose '**Current Window > Decrypt/Verify**'.

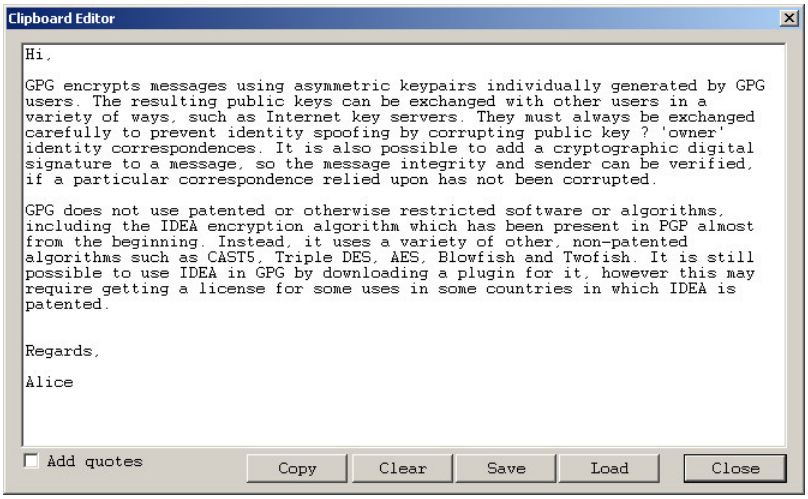


Step 3:
You need to enter your passphrase to decrypt/verify the message. Click '**OK**' to proceed. Sometimes, you will see other people names in the list (Bob, in this example). It means that Alice is also encrypt the messages with Bob's public key.



Step 4:
WinPT will decrypt the message and verify its signature. Click '**OK**' to proceed.

Step 5:
WinPT will display the plaintext message in the Clipboard Editor



You can read the message in the Clipboard Editor and then click '**Clear**' to ensure that the plaintext message will remain secret. But, of course, you can save this plaintext message into an ordinary text file by clicking '**Save**'. Click '**Close**' to end Clipboard Editor.

If Alice attach encrypted files in her e-mail, you should save the attachments in a folder and decrypt it. Please refer to '**Decrypting Files**' section for more information.

9. Encrypting Files

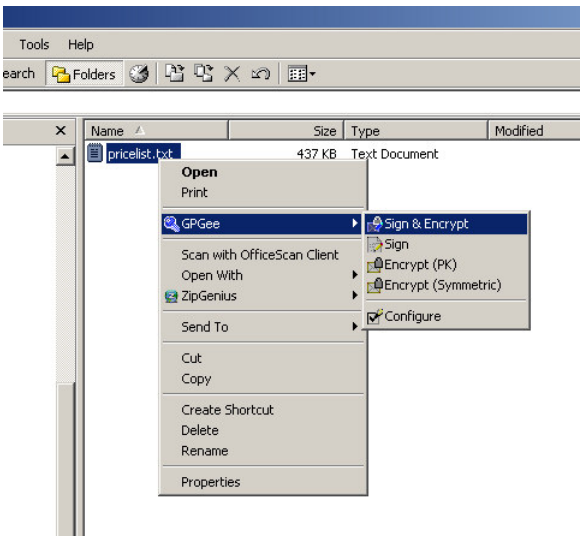
GPG4WIN, through its GPGee modules, provide encrypting/decrypting files feature thorugh it context menu. You can use this feature to protect your confidential file, either in your harddisk or in e-mail attachments.

If you are going to compress the files to reduce their size and then encrypt them, your should know two things:

1. You might want compress the files first and then encrypt them. It is almost useless to compress encrypted files because encryption algorithm will reduce (or eliminate) redundancy in digital data for –of course—security reason.
2. GPG core modules has bulit-in compression library (zlib). It means that whenever you encrypt files, GPG will automatically compress them using that library. In most cases, you do not need to compress them using seperate compression tools.

Allright, let's encrypt a file.

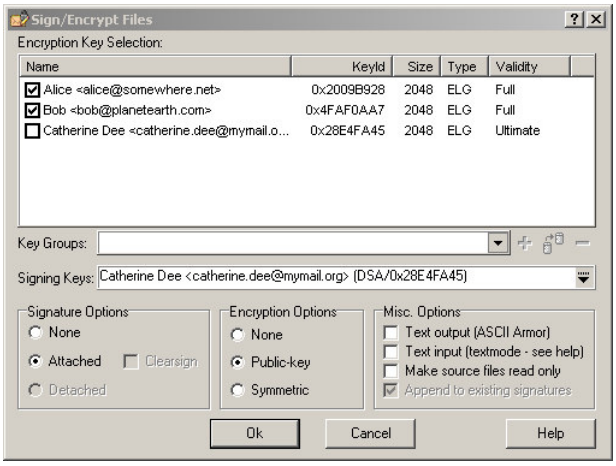
Step 1:
Right-click on the file. Choose '**GPGee > Sign & Encrypt**'



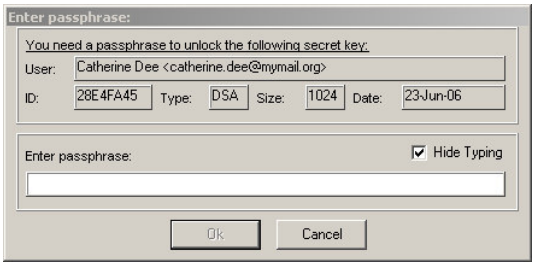
Step 2:
Now, depending on your objective, you may choose which key(s) you are going to use. If:

1. you are going to send this file to Alice and Bob as an e-mail attachment, you should encrypt it using their public keys.
2. you are going to encrypt the file to protect it from everybody but you, you should encrypt it using your key and wipe the original (plaintext) file. Refer to '**Wiping Files**' section for detailed information about wiping files.

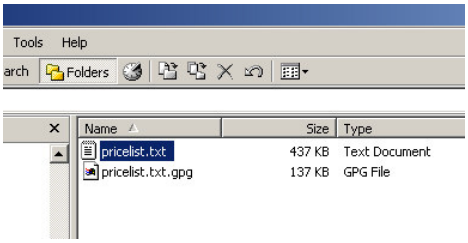
For this example, we are going to send that file to Alice and Bob as e-mail attachments. Put check marks on Alice's and Bob's key, and click '**OK**'.



Step 3:
Enter the passphrase and click '**OK**'.



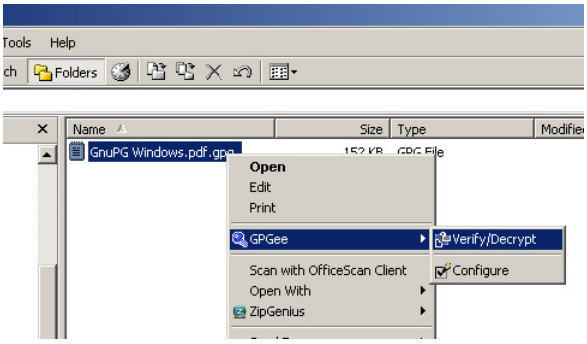
Step 4:
The new encrypted file (with .gpg extension) will be placed in the same folder. Note that the encrypted file (usually) has smaller size than the plaintext file. You can attach this encrypted file to your encrypted e-mail message to Alice and Bob.



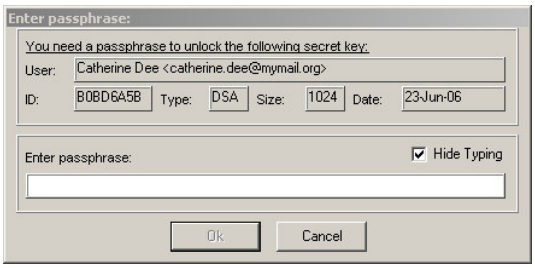
10. Decrypting Files

GPGee context menu will automatically detect .gpg, .pgp, .asc, .sig extension file as encrypted file. This is how to decrypt it:

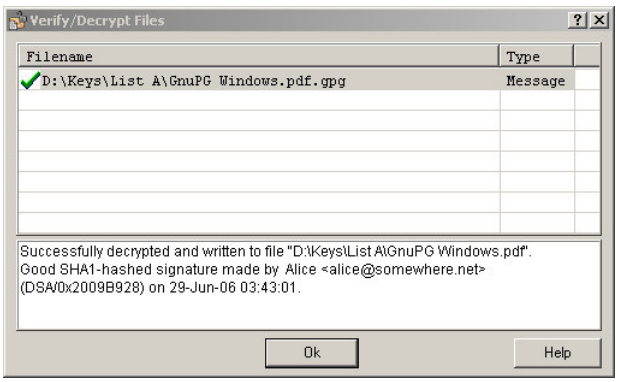
Step 1:
Right-click on the encrypted file and choose '**GPGee > Verify/Decrypt**'



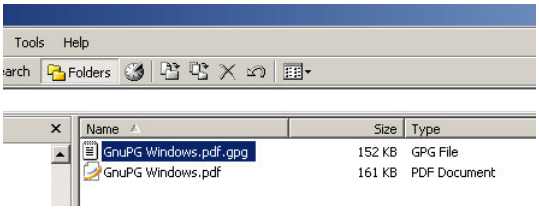
Step 2:
Enter your passphrase and click '**OK**'.



Step 3:
The report window will be displayed, click '**OK**'.



Step 4:
The decrypted file will be put in the same folder.



11. Wiping

If you delete files using **Del** or **Shift-Del** key or emptying Recycle Bin, the files will leave 'traces' in the storage media (harddisk, USB flash disk, or other storage media). Eve, for example, could use file recovery tool to recover the original files by analyzing this 'trace'. This process is called 'file/data recovery' or 'undelete'.

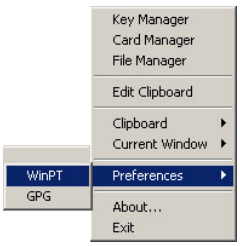
You can sweep these 'traces' away and truly erase files by overwriting it several times using some defined binary pattern. This is called wipe (or shred or purging) process. WinPT provide several pattern mode in wiping[10].

Wiping utility is a complement for encryption utility. Imagine this situation: Alice sent some encrypted secret documents to Bob. Eve, Bob's adversary, has access to his computer harddisk. Eve wants to recover the plaintext secret documents so that she can sell it to the higest bidder, but all she gets are the encrypted files. Does it means Bob's and Alice's secrets are safe? Maybe not. If Bob decrypt the files, read them, and then delete the plaintext files using Shift-Del combo, Eve could simply use file recovery tool to recover the plaintext files. And then, the encryption is futile.

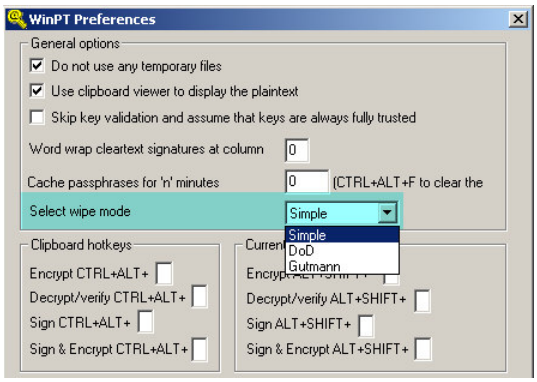
11.1 Selecting Wipe Mode

Step 1:
Right-click on WinPT system tray icon. Choose '**Preference > WinPT**'.

[10] For detailed information: http://en.wikipedia.org/wiki/Data_remanence#Standard_patterns_for_purging



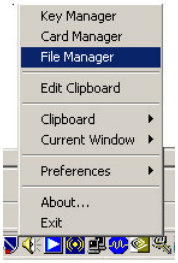
Step 2:
Pick wipe mode (method) on **'Select wipe mode**' dropdown list. The '**Simple**' mode is the quickest mode, but the least secure. The '**Gutmann**' mode is the slowest mode, but the most secure.



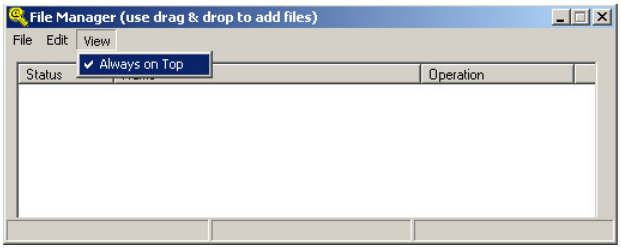
11.2 Wiping Files

You can wipe several files at once. Be very careful: it is very hard (if not impossible) to recover wiped files.

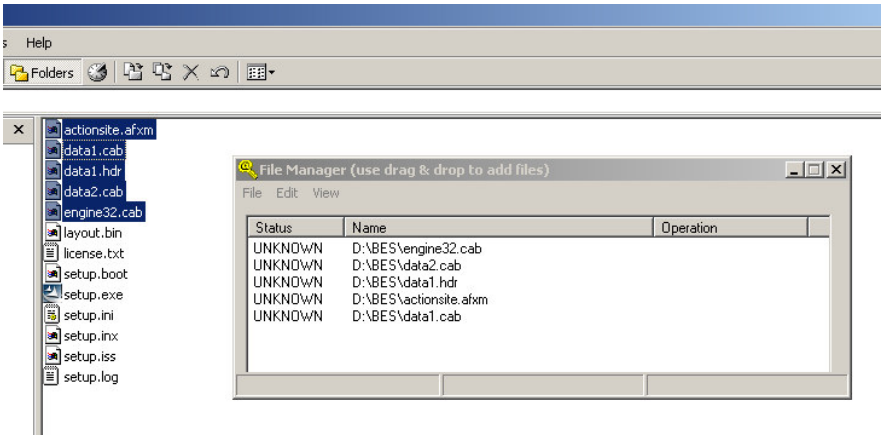
Step 1:
Right-click on WinPT system tray icon. Choose '**File Manager**'.



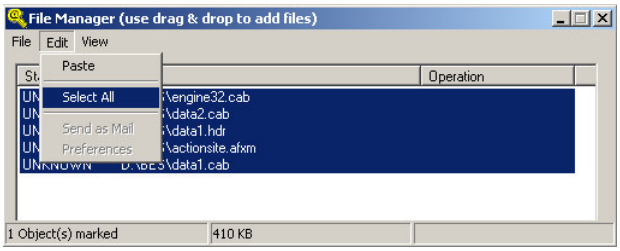
Step 2:
From File Manager menu, choose '**Always on Top**', This is not mandatory step, but it would be much easier to drag-n-drop files from Windows Explorer to the File Manager if the File Manager always on top.



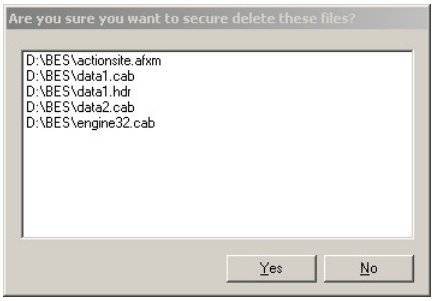
Step 3:
Drag-n-drop the files from Windows Explorer to the File Manager windows.



Step 4:
Choose '**Edit > Select All**' at File Manager window.



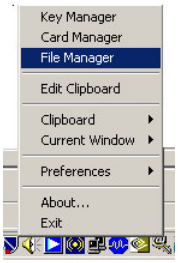
Step 5:
The confirmation dialog box will appear. Click '**Yes**' to wipe these files.



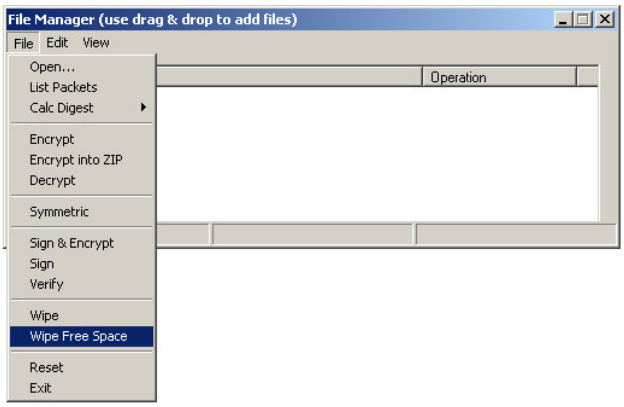
11.3 Wiping Free Space

Instead of wiping files, you can wipe the storage media's free space. This is very useful to sweep 'traces' of previously deleted files. Alice could reformatted her old harddisk and use this feature to ensure that nobody could retreive her secret documents when she dumped her old harddisk in trashcan (or gave it away to someone else).

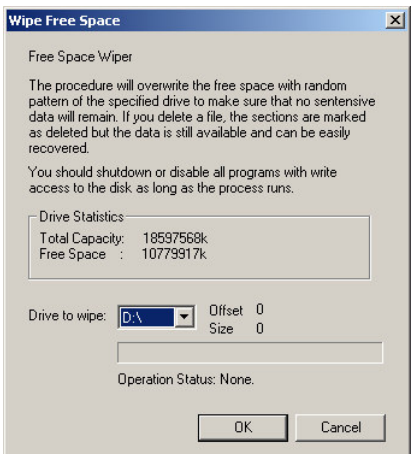
Step 1:
Right-click on WinPT system tray icon. Choose '**File Manager**'.



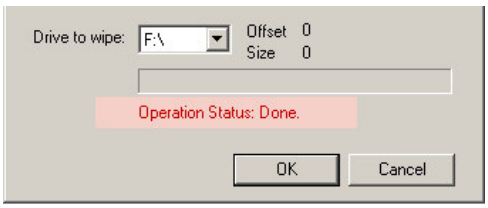
Step 2:
Choose '**File > Wipe Free Space**'



Step 3:
The Wipe Free Space dialog box will appear. Choose drive to wipe. Click '**OK**' to proceed.



Step 4:
A status message will appear after the wiping process complete.


Drive to wipe:
F:\
Offset 0
Size 0
Operation Status: Done.
OK
Cancel

12. Appendix A: GNU Free Documentation License

Version 1.2, November 2002

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

* A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
* B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
* C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
* D. Preserve all the copyright notices of the Document.
* E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
* F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
* G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
* H. Include an unaltered copy of this License.
* I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
* J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

* K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
* L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
* M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
* N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
* O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements."

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.