WinPGP™ Version 3.1

By: Christopher W. Geib
Geib Enterprises Network©

Table of Contents:

Overview of WinPGP™ 3.1

Thank you for using WinPGP™. This is version 3.1, still the best **author supported** full-featured Windows shell for the popular DOS program, PGP™, created by Phil Zimmermann. WinPGP™ version 3.1 has many new features over previous versions of the program. Some of these features are:

Windows-style Help
Added parameters, -b, -m, -d, -u, -p and -o
Preferences radiobuttons highlighted for current defaults
ListNames feature to aid in Receive User ID
New Main Menu with Toolbuttons
Launch Button **now** with multi-drive support
Bulk file Encryption

In addition, WinPGP™ is still fully compatible with all versions of PGP™, including the US versions 2.6.1 and 2.7(commercial) as well as the European versions 2.6ui and 326ui. Also, the pre- and post- 1 September features are included.

WinPGP™ 3.1 is shareware and the cost to register the program is **still only** $29 US dollars (direct registration with me). If you register with me directly, you can also take advantage of the latest book on PGP™ by Mr. Bill Stallings titled, Protect Your Privacy: The PGP User's Guide. This book is available at many bookstores for $19.95. It ***is*** the definitive text on PGP™. Please read the text file, **READ_1ST.WRI** for details on a special offer.

This help file is organized into several topics. If you are setting up this program, please take time to read the section on setting up WinPGP™. If you ever need help or assistance with the program, or have comments and suggestions, please contact me via email at the following:

72144,1426 on Compuserve,
and
72144.1426@compuserve.com
on the Internet

Setting Up WinPGP™

By now, you have read the file, **READ_1ST.WRI**. This file simply describes how to install the program on your hard drive. What I would like to cover now is the specifics of preparing your copy of WinPGP™ for correct use with your copy of PGP™.

US versions 2.3a, 2.6, 2.6.1, 2.6.2, 2.7 If you are using these versions of PGP™, then you will want to leave the file, **PGP30UI.~NF**, just as it is. This will disable the parameters, **version_byte** and **armor_version**. These two parameters are unique to the European versions of PGP™ and allow setting the Version tagline and the Version_Byte for pre- and post- Sept. 1994 versions of PGP™. See the feature topic on Preferences for details on additional setup.

European versions 2.6ui, 326ui, and 2.6.i If you are using these versions, then you should rename the file, **PGP30UI.~NF** to **PGP30UI.INF**. This enables both the **version_byte** and **armor_version** parameters. Read the documentation in either Bill Stallings book or the documentation that comes with versions 2.6ui, 326ui, or 2.6.i, for details on the function of these parameters.

All versions With version 3.1 of WinPGP™, you can install the program files into their own separate directory. Please ensure that the directory containing **PGP.EXE** is in your **AUTOEXEC.BAT Path** statement.

Launching telcomm products If you want to use the Launch button (the one with the rocket on it), you can now modify the file, **winpgp30.ini from the Preferences dialog box**. Simply press the Configure button, and enter the path and program name. I use WinCIM as an example. Also note that with version 3.1, the Launch feature works on programs in other drives (i.e. E:\).

LaunchPath C:\CSERVE\WINCIM
Launch Program WINCIM.EXE

Note that different programs like Procomm+ and CsNAV may be located in different directories/drives and have different names. WinPGP™ will start your telcomm product (or any other program you want) once these are set. Note also that the default setting for this Launch button is a Message Box saying that the button is **not** configured.

Debugging Feature WinPGP™ 3.1 now deletes the **.BAT** file when the program exits. It also runs the batch only in the WinPGP™ directory. However, if you check the Debug Status On in the Preferences dialog box, you can retain the **.BAT** file at program exit.

Using the Windows Editors

On the Main Screen for WinPGP™ 3.1, you are shown a toolbar with toolbuttons. The editors, MS-Write, is displayed as a bitmapped button with a pen,

and the Notepad editor is displayed as a bitmapped button with a notepad,

Clicking on either button will start these editors. Also, you can still start the editors by using the drop down menu bar.

Using Preferences in WinPGP™

When you select this button on the Main window of WinPGP™ with the letters Prefs, you will be presented with the Preferences Dialog Box. If you have previously set preferences, the current settings will be checked. When you change them and click just the **OK** button, the changes will be effective for the current session only. If you click the Save bar at the bottom, you will update the **WINPGP30.INI** If you are using one of the European versions of PGP™, ***and*** you have changed the file, **pgp30ui.~nf** to **pgp30ui.inf,** then the next screen below will come up when the button marked 2.6ui+ is pressed. **NOTE: If none of the boxes are checked or some are unchecked, PGP™ WILL use the default settings in the file CONFIG.TXT that came with PGP™. To avoid strange results, it is highly recommended that you set this file back to its AS-DELIVERED state. These checkboxes simply modify the default behavior of PGP™.**

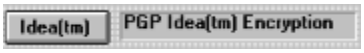
Pressing this button sends you to the 2.6ui (European) options dialog. This screen allows the user to set the European versions to version_byte=2 (PGP™ 2.3a, pre-9/1/94) or version_byte=3, (PGP™ 2.5 and up, US versions). Additionally, the tagline in ASCII armored messages will show one of the four sets of numbers listed for selections. Pressing **OK** will return you to the first screen and pressing the **Update bar** will record your Preferences in the **WINPGP30.INI** file for future use.

Encrypting Files Using WinPGP™

 When the **Locked** padlock button on the Main menu toolbar is clicked, the user sees a dialog box with several buttons. There are four choices**,** Signed Encryption (pgp.exe -es), Unsigned Encryption (pgp.exe -e), Idea® Encryption (pgp.exe -c), and Plaintext Signature (pgp.exe -s) . Selecting one of these will bring you to the next series of dialogs.

Pressing this button gets you to the Signed Encryption Dialog. Use the **Browse...** button to select the file you want to Encrypt. With WinPGP™ 3.1 you now have the choice here of filtering files for ***.txt**, ***.wri**, and ***.***. When the user selects the **OK** in the File dialog, the choice is placed in the Edit control on the Signed Encryption dialog. Press the ListNames button, and the dialog opens where the user selects from a table of public keys, the receiving user. At the **OK**, WinPGP™ returns a parsed form of the key ID number and places that in the Edit control.

Pressing this button gets you to the Unsigned Encryption Dialog box. The button functions, **Browse...** and **ListNames** function the same as in the Signed Encryption Dialog. Again note that WinPGP™ passes the first six hex digits to PGP™ for user ID.



Pressing this button activates the Idea® Encryption Dialog box. Because this method simply encrypts a file, no **ListNames** button is necessary. The **Browse...** however works the same as it does in the previous boxes.

Finally, this button gets you to the Plaintext Dialog box. **Browse...** for the file of choice and then press the dialog box OK button to create the clearsig ASCII file. **NOTE: if you want to clearsign a file, make sure that the Text Mode checkbox is checked. A Message box will remind you.**

Decrypting Files With WinPGP™

 Pressing this button in the Main Menu of WinPGP™ activates the Decrypt Files Dialog. By pressing the **Browse...** button, a selection of files are presented. In WinPGP™ 3.1, you are able to choose, *.pgp (pgp binary files), *.asc (ASCII armored files), and *.sig (Sig files). Additionally, the user has the option of putting in an output filename. The **-o** parameter is automatically set if a filename is entered. When the user selects the **OK** in the File dialog, the choice is placed in the Edit control in the dialog box. Press the **OK** button to start PGP™ and decrypt the file.

Key Management Functions With WinPGP™

 Pressing this button in the Main Menu of WinPGP™ activates the Key Management Dialog. There are a wide selection of choices here to choose from. Each of the key management functions are described in detail in the PGP™ documentation. In WinPGP™ 3.1, when the user is completed with Key management activities, pressing the **Cancel** button will cause the program to update the file, **pgpkeys.tab**, which is the file containing a listing of users in your public keyring.

The file, **pgpkeys.tab** is created the very first time you run WinPGP™ and every time you add or delete a key from your keyring. It is recommended that you edit this file with an editor like Write or Notepad after you update it. The reason to do this is to keep your table file neat.

There have been several dialog boxes modified in this section. These options allow the user to use all the options available in key management.

Registering WinPGP™

WinPGP™ is a "shareware program" and is provided at no charge to the user for evaluation. Feel free to share it with your friends, but please do not give it away altered or as part of another system. The essence of "user-supported" software is to provide personal computer users with quality software without high prices, and yet to provide incentive for programmers to continue to develop new products. If you find this program useful and find that you are using WinPGP™ and continue to use WinPGP™ after a reasonable 30 day trial period, you must make a registration payment of $29 US by check or money order to me, or if you register via Compuserve, the registration cost is $34.50 US. The $29 US registration fee will license one copy for use on any one computer at any one time.

The cost for registering WinPGP™ 3.1 has gone down over previous versions. The new lower pricing is as follows:

WinPGP™ register direct to author:	$29.00 US
WinPGP™ registered via Compuserve:	$34.50 US
WinPGP™ + Bill Stallings book:	$45.00 US

You can register the software via Compuserve by doing a **GO SWREG**. Or you can register with me directly. To do so, send a check or money order with a note telling me if you want the book, to the address below:

Christopher W. Geib
c/o Geib Enterprises Network
7605 Mt. Hood
Dayton, OH 45424
USA

Remember, updates and revisions are always free. Simply download them and enjoy.

Legal Issues and WinPGP™

DISCLAIMER - AGREEMENT

Users of WinPGP™ must accept this disclaimer of warranty: **"WinPGP™ is supplied as is. The author disclaims all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The author assumes no liability for damages, direct or consequential, which may result from the use of WinPGP™."**

PGP™ is a copyrighted program utilizing patented modules from PK Partners, Inc., RSA Data Security, Inc. and Ascom-Tech AG. Each of these organizations carry various trademarks and copyrights for their respective companies and software products See the MIT and RSA licenses for additional details.

WinPGP™ is a copyrighted program from Christopher W. Geib, D.B.A. Geib Enterprises Network. Trademark registration for the name WinPGP™ has been obtained.

WinPGP™ contains **none** of the PGP™ executables and incorporates **none** of the PGP™ source code in any way or form. This program simply provides the user with a convenient Windows interface.

Windows© is copyrighted to the Microsoft Corporation.

Turbo C++© is a product of Borland International.

BWCC.DLL is a product of Borland International and is available for use free with developed applications.

Protoview Development Co. is the copyright holder of WNCTL.DLL and PVPLUS.DLL. Both libraries are lisenced for free distribution with developed applications.

WinFront© is a copyrighted program of Mr. Ross Barclay.

Final Note from the Author

The name WinPGP™ is being illegally used by a pair of rogue programmers at the University of Southern California. These programmers contacted me early this year to see if they or I were the first to use the name WinPGP. As it turned out, my use was first and an email reply so stating that, and a polite request to cease using my trademark was sent. To date, these rogues have chosen to ignore that request. This is a Windows shell that is similar to the ***real*** WinPGP™. Caution should be exercised by users of this illegal program. I cannot, nor will I support or be able to support any problems associated with the fake version. Please do not contact me if you are using it. I have been asked at some expense to help users who have been using the illegal version for assistance. I simply cannot help them.

If there are questions of credibility between my WinPGP™ and the illegal version, consider this, the illegal version **did not** even get an honorable mention in Bill Stallings new book. The book whose Forward is by Phil Zimmermann himself, who is well aware of the ***real*** WinPGP™ and Mr. Ross Barclays WinFront©.

The Clipboard Style En/Decryption Dialog

New with this version is a new button to allow Internet users and others who frequently send and receive short ASCII armored messages to cut and paste plaintext and cipher. The button opens a document editor with the default filename of, winpgpg1.txt. The following instructions outline how to use this powerful new feature.

Encryption

The first method is to type your message directly into the editor.

Once your message is typed as you want it, do a **File | Save Exit** and the action dialog appears. Set the radiobutton for the option you want, -sta clearsig, -ea, -esa. Select additional controls, -b, -m.

Click the **GetNames** button (if selecting one name only). Select the name for encryption. Press **Encrypt.** PGP™ will be invoked, and you should answer the questions it asks. Also, if you are encrypting to multiple users, enter the names at the prompt by PGP™. When PGP™ is satisfied, it will encrypt the message.

When PGP™ closes, you no longer have to click a View button. The encrypted result, is now automatically displayed. Do a **Edit | Select All**, then a **Copy** (or **Cut**), and then paste the message into the document or email.

The second method is to get a previously written file, open it and select the text for encryption, do your **Edit | Copy**, then after opening the Clipboard dialog, press **Edit | Paste**.

Make your selections as outlined above and then encrypt. **Cut** it and paste it wherever. Thats all there is to it!

Decryption

Decryption is just as simple. Youve received your encrypted email, you select the encrypted text (or all text in the message because PGP™ could care less) do an **Edit | Copy**, and then open the Clipboard editor, click **Edit | Paste**. Do a **File | Save Exit**.

Select the **Decrypt** radiobutton. And if you choose, the -p option.

Click the **Decrypt** button. PGP™ is invoked and the file is decrypted. Use the **View** button to pick up the decrypted text. **Cut**, **Paste**, or **Save** to another filename are all available from the editor.

Bulk File Encryption

Version 3.1 adds multi-file encryption to WinPGP™s list of capabilities. By clicking this toolbar button, the user can select a directory to encrypt, plus enters a passphrase for the session twice. This feature uses **Idea©** encryption and wipes the plaintext files with the PGP™ wipe feature. For security, the character arrays and the batch file both in memory as well as on the disk is re-written with the bytes, 0xFF (eight ones), then 0xAA (10101010), then a final 0x55 (01010101). This ensures that the passphrase has been destroyed and is unrecoverable (even in the Windows swap file). As an aide to the user, the passphrase used for encrypting the directory is saved in a Signed Encrypted message. The user should utilize his own name to encrypt to self. Message boxes are displayed at various points in the process to notify the user of status.

Because this feature encrypts **ALL** files in the selected directory, I suggest you use this feature **only** to archive plaintext files. Then copy these encrypted files to a floppy for storage. If you intend to use selected files later, re-encrypt these separately to avoid double or triple encrypting the same file.

If archiving files, put them all in a directory of your choice. I personally use a sub directory to the WinPGP™ main directory. I then multi-file encrypt. After the process completes, I copy the directory contents to a floppy for safe storage. I then simply delete the contents of the directory. If an attacker does an Undelete, all he has is the encrypted **.pgp** file.