PowerPGP 1.2x

PGP Message Encryption Shell for Windows

Important!!!

Read this entire document before using to understand exactly what all the features do.

First - The Legal Stuff:

THIS SOFTWARE AND ACCOMPANYING MATERIALS ARE DISTRIBUTED "AS IS" WITHOUT WARRANTY, EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ANYONE INVOLVED WITH THE CREATION AND PRODUCTION OF THIS PRODUCT BE LIABLE FOR INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES, ARISING OUT OF ANY USE THEREOF OR BREACH OF ANY
WARRANTY. THIS SOFTWARE IS LICENSED NOT SOLD. YOU DO NOT OWN THE SOFTWARE AND YOU ARE NOT ALLOWED TO DECOMPILE OR DISASSEMBLE THIS SOFTWARE IN ANY WAY.

Requirements:

The DOS PGP program must be PROPERLY installed before PowerPGP!!!
Windows 95 or **Windows 3.1**X running enhanced mode
386DX+ CPU (486 or better recommended)
4 MB RAM (Required for Windows to Run Enhanced mode halfway efficiently)
8 MB RAM recommended

Required Files:

POWERPGP.EXE - The executable program itself. (Put in Any directory you like)

PGPUSR.EXE - A DOS executable creates a list of users in your Pubring.PGP file for PoerPGP to use. (**Put in the same directory as your PGP.EXE program**)

BIVBX11.DLL - A Dynamic Link Library used by the program. (copy into your C:\WINDOWS\SYSTEM Directory.)

POWERPGP.RTF - This document

FILE_ID.DIZ - BBS Description file

J_FEENIN.PGP - My Public Keys to import into your public keyring so you can encrypt mail to me.

What is PowerPGP? - PowerPGP is simply a shell program for the DOS based FREEWARE PGP Program. You must have the PGP program installed prior to running PowerPGP or it will do nothing. PowerPGP was designed to make writing and Encrypting E-mail messages E-mail messages simple and easy in Windows. It is designed mainly towards that end although it can also encrypt files as well. This file will cover the basics of PowerPGP operation, it will not go into detail on how to use PGP itself. PGP has it's own very well put together set of documentation that you should have already read and if you haven't go do it now. Also it should be noted that there are many more advanced options to PGP that are not supported in the shell. The idea was to keep it simple and easy to use so I did not put in options that I myself would not use on a regular basis. PowerPGP will encrypt and decrypt messages for any internet mail program or any Windows based BBS program because it uses the Windows Clipboard to cut and paste the info to and from the application.

Writing a message with PowerPGP. - To compose a message that you intend to encrypt with PowerPGP is simple. You simply type the message into the message window of PowerPGP and enter the Public Key name of the user you intend to send it to in the "Public Key To Use" box of PowerPGP. When you are done writing your message you select the encrypt option. PowerPGP will then write the file to a temp file and shell out to the DOS PGP program with the correct commands to encrypt it and then read the encrypted message back into the message window. PowerPGP will then automatically delete the temp files it wrote. You now have an encrypted version of your message in the message window. You can then click on the "Cut" button and it will cut the encrypted message to the clipboard. You then go to the message editor on your mail program and paste the encrypted message into your compose message window, It sounds a lot worse than it really is. Also it should be noted that you MUST have the public key to the person you are sending the message to on your public keyring already. Once you encrypt a message to someone with their public key not even you can decrypt it, only they and their secret key can decrypt it. For more information refer to the PGP documentation.

Decrypting a message with PowerPGP. - Similarly this is done with the clipboard. First make sure your message window in your mail reader is wide enough that none of the lines are word-wrapped where they are not supposed to be. You will be able to tell trust me. Making sure the lines are all even then select the entire message block including the BEGIN and END PGP message lines. PGP needs these to know when to start and stop decrypting, without them decryption will fail. After selecting the entire encrypted message copy it to the clipboard with whatever command your mail reader uses, usually Ctrl-C in windows programs. Then go to the PowerPGP program and select Paste. PowerPGP will automatically replace anything in your message window with the encrypted message. You can now decrypt the message with the decrypt key. If the message was properly encoded with your public key by the person who sent it you will be able to read it after decoding if you do not have the secret key required to decrypt the message decryption will fail. Once you read the message you can select the quote option and it will quote out all the text so you can reply to the original message and follow the encrypt message options to encrypt a reply back to them. Make sure you specify their public key for encrypting a message to them. You do not need to specify a public key for decryption, PGP will automatically search your Secret keyring for a valid secret key and prompt you for your pass phrase to decrypt. **Always be sure to protect your pass phrase and secret key DO NOT GIVE EITHER TO ANYONE!!!**

Signing a message with PowerPGP. - This is exactly the same as encrypting except you use the Sign button instead of the encrypt and PGP will ask you for your pass phrase to verify it is really you signing the message. Note. PowerPGP automatically uses the CLEARSIG method for signatures. This method signs the message but leaves the message text readable. This is so the person you are sending the message to can verify that you are the one who actually send the message and that the message has not been altered. Anyone can read it and anyone with your public key can verify it. This is mostly an authentication method.

Signing & Encrypting a message with PowerPGP. - This is exactly the same as encrypting except you use the Sign/Encrypt button instead of the encrypt and PGP will ask you for your pass phrase to verify it is really you signing the message. This method does NOT use CLEARSIG, obviously since it is encrypting the message. Only the person you are sending it to can read it and verify you sent it, this is for both security and authentication.

I believe all the other features of PowerPGP are self-explanatory if you read the PGP documentation. It is really much simpler than it sounds. Yes it's a few extra steps to ensure your privacy but isn't it worth it? Would you send all you personal postal mail without an envelope? Of course not so why not put your e-mail in a digital envelope?

Technical information (READ THIS!!!)

Windows 95 users: Make sure that you have set the properties for the DOS PGP program in the explorer as follows. On the program tab of the properties box make sure that the window title is "**PGP**" without the quotes. On the same tab make sure the "Close on exit" box is checked. Now go to the Misc. tab and make sure the Background selection that says "always suspend" is not, I repeat is NOT checked. If these options are not set properly PowerPGP will not function properly.

Windows 3.1x Users: Windows 3.1x users should also make sure that the corresponding settings are properly set in their _default.pif file. Or in any PIF file they have associated with PGP because if their is a PIF windows will run it's parameters when it runs the EXE. If you do have a specific PIF file for PGP (you don't normally need one) make sure the Window Title is set to "PGP" without the quotes. Do not make this setting in your _default.pif, this is ONLY if you have a specific PIF file for PGP.

MSmail: Msmail has this nasty little habit of adding a space before the dashes "-" when displaying the PGP encrypted message. Why I don't know I guess they would rather show you their interpretation of the message rather than what was actually sent. Microsoft Exchange that ships with Windows 95 does not exhibit this problem even with mail sent from Msmail. When a message was copied to PowerPGP from Msmail you will need to remove that extra little space they added manually. Don't blame me I didn't write Msmail.

Why does the Window Title have to be **PGP** for both? Well the answer is quite simple... When encrypting a message PowerPGP shells to the DOS PGP program to do the real work, when it does it creates a windows that must be titled PGP because the PowerPGP program is looking for a window by that name to close so it knows PGP is done with it's work and PowerPGP can now import the results. If the window is not named properly then it will think the window is closed immediately and try to import the results since their are none yet it will fail. This may not be the best example of programming possible but what they hay, what do you expect for FREE.

Extremely Long Pass Phrases and Paths to the PGP file may cause problems with PowerPGP. This is because the maximum number of characters that can be sent directly to DOS form Windows is 128 whereas if you were at the DOS prompt you can use 256. When PowerPGP builds the command string to send to PGP if it excededs 128 Characters you will get some message saying something about unable to find a key for someone with their name chopped off and the PGP executable path attached to the end. If this happens you overran the 128 character limit. To help prevent this some things you can do are:

1. Keep the path to PGP a simple one such as C:\PGP rather than something like C:\WINDOWS\ENCRYPT\EMAIL\PGP this is an easy solution and present no security risk.

2. If your Pass Phrase is long it too can be a problem, the easiest solution to this is to tell PowerPGP you want to tell your pass phrase directly to PGP each time you decrypt a message. This will prevent your pass phrase from being included in the command line and thus shorten it quite a bit. This in fact is not only not a security risk but quite the opposite.

3. Long username keys can also be a cause to exceed the 128 character limit, however you will find that either one or both of the above fixes will allow almost any Public Key Name. The only fix if you have tried both of the above and this still happens it to use a shorter public key name. (Edit it yourself in the field). You can also edit the list of users yourself in the PowerPGP.USR file in your PGP directory so that you do not need to edit the name every time.

for the long ones you can edit the key and leave only the first and last name for that individual and it will work fine. This would be a last resort.

I could write a batch file and execute it like other programs do then there is only the 256 character limit of DOS, however, this leaves a little to be desired if you want to use the option of sending the pass phrase to PGP. Obviously you would not want to write your pass phraseinto a batch file even if it was deleted when it was done being used, this would be a huge security breach. I cannot stress enough that for most people none of these options will be required and if any the first will solve almost all problems.

NOTE: These same symptoms can happen with encrypting (ASCII ARMORing) a file, the simplest solution in that case is to move the file to a directory right off the root such as C:\TEMP and try encrypting it again, files are easy to do this with since you can typically move them at will.

New Features Since 1.00 (1.00 to 1.20)

AutoSave: PowerPGP will autosave the message you are working on once a minute in the background. If you are working on a message when you exit PowerPGP it will automatically reload that message when PowerPGP is restarted. Some people may consider this a security breach while other will like the feature so for those that want to disable the feature run PowerPGP with the d switch as so "PowePGP.EXE d" without the quotes of course.

Save Message: PowerPGP will now save a message to a file if you wish. This is so you can write several encrypted messages off-line and then log on and send them. If you want to come back to the message and read it yourself later it is recommended that you encrypt it with your own public key before you save it then when you reload it you will be able to decrypt it and edit it then re-encrypt it with the recipients key and send it. Of course you can save a message that isn't encrypted but that is most definitely NOT recommended.

Resizability: The Form is now resizable so you can change the size of your message editor to your liking. There is a minimum size however the form will not get smaller than a certain amount.

Fonts: There have been problems with certain keyboard sets with the built in fonts of the previous version so now you can pick your own from your favorite from your own system. Keep in mind that the message is encrypted as text the recipient will not see the font you used to enter the message with it is simply for you to be able to pick the font you find the most readable. I recommend Terminal, MS Sans Serif, or Arial but the choice is yours.

Pull Down list of PUBRING.PGP names: Instead of manually typing in the name of every person you send mail to there is now the option to run the DOS Program PGPUSR.EXE in your PGP directory. This program will make a list of the names in your Public Key file for PowerPGP to use. This way you can just scroll down to who you want to encrypt mail to rather than doing all the typing and worrying about misspellings. There is also the option under the Key Management menu to "Update Public Keyring List" this will run PGPUSR for you but the changes will not take effect until you close PowerPGP and rerun it. You should update this list everytime you add or remove a key from your Public Keyring. PowerPGP will also automatically run PGPUSR when you add or remove keys from your public keyring from within PowerPGP.

New Quoting Method: Instead of using the ">" method of quoting PowerPGP now places the message below the current message and places the text "-------- REPLY, Original message follows --------" before the quoted text and "-------- REPLY, End of original message --------" after. This method was necessary since the for is now resizable and there will be a different number of characters in different peoples editors. The only other option was to impose a line character limit but I would rather leave that up to individual taste and individual mailers. If they didn't match the result would be a mess so this was the only logical method for me to use.

Printing: You can now print out your messages.

New Features Since 1.00 (1.20 to 1.23)

Remember Pass Phrase: PowerPGP will now remember your pass phrase if you choose. Unless you tell it other wise PowerPGP will only ask you for your pass phrase once per session (each time you run it) after that it will remember it and send the pass phrase to PGP automatically. This is much more convenient when reading and signing many mail messages, however it does represent some potential for a security breach since an experienced attacker "might" be able to analyze your swap file and find your key. It is a minimal risk in most cases but nonetheless it is a risk. It is for that reason you will also see a checkbox when the program asks for your passphrase where you can choose to tell your pass phrase directly to PowerPGP each time, the choice is yours.

Signature: PowerPGP will now allow for a text signature much like the signature most mail clients automatically add to your E-mail. This is handy if you want your signature to be added BEFORE your message is encrypted also it is a good place to put your public key so anyone you send mail to automatically gets your Public Key. If you leave the signature blank PowerPGP adds nothing, the self promotional tags it used to add are gone.

Contacting the Author:

If you have read this and the PGP manual and would like more help on PowerPGP or you have a bug report you can contact me at:

Internet:

joe@feenin.roc.servtech.com
joe@servtech.com

BBS:

The Fruitcake Sanitarium BBS (716) 647-6030 and leave a comment to the SysOp-me.

Or via snail mail to:

Joe Feenin
236 Flower City Park
Rochester, New York 14615

There usenet newsgroups on the subject of PGP and many fine articles about it I recommend reading a few.