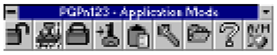
Table of Contents

Installation
Setup
Encrypting Messages
Decrypting/Signature Checking Messages
Clear Signing Messages
Key Management
File Processing



If you experience problems with the operation of this program or would just like to offer a suggestion, please write to alpha1@pobox.com.   All comments are welcome. When writing, for your own privacy, use our public key.

What is PGPn123?
In short, PGPn123 is yet another Windows shell for PGP. Yes, there are a few out there already, and more being written all the time. Some work good, others do not. Of those that work as advertised, they can be very cumbersome. PGPn123 is our vision of what a PGP shell should be, and nothing else. You may decide you like it, then again, you may not - if not, please write anyway to tell us how it can be made better.

What is Enhanced PGPn123?
Enhanced PGPn123 is the commercial release that replaces our popular freeware PGPn123 program. It has a number of additional features, and improved performance. So as to make the program as nag-free as possible, we have all but eliminated the nag screens except for those features that are considered part of the Enhanced package. If you are unregistered, use of those features will pop-up some windows asking for payment. We do rely on your contributions to continue development, so please pay the $15 personal use fee if you use PGPn123 on a regular basis.

Unique Features

Toolbar floats above linked application only - never obscures other windows. May be configured to float above all applications for clipboard-only operations. If linked, PGPn123 will start your application for you.

Multiple INI files allow you maintain a different toolbar for several applications at the same time.

Single-click message encryption, decryption and clear-signing from the floating toolbar.

File processing included for sending encrypted attachments with your messages.

Steganography can be applied to your encrypted messages to hide the fact that you have used PGP. Helps to prevent automatic logging of encrypted messages by mail servers and other interested individuals.

User-definable keystroke macros are sent to your application to automate the process of selecting and processing your message. In Eudora for example, all you need to do is place the cursor in the message body and click on the Encrypt button. A dialog box pops up where you select the encryption method, recipient key(s) and other options. After shelling to PGP, the result can be automatically pasted into your application.

Use an internal or external viewer. If you want to view the output before pasting the results into your application, there is an internal viewer, or you can configure an external program such as Notepad.

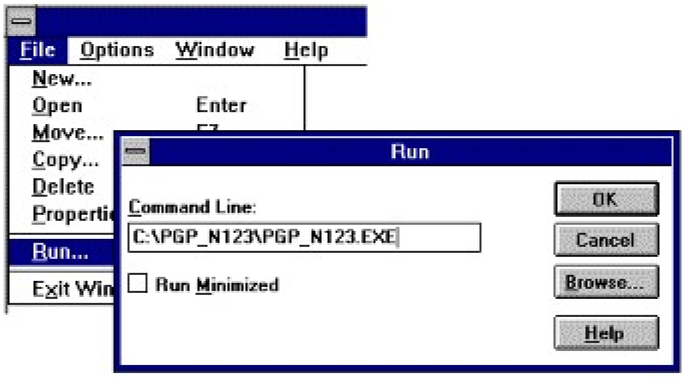
Separate key management module allows you generate your key pairs and manage the key rings. KeyOps can be launched from the toolbar.

Installation

What to do with the files

Copy everything into a separate directory, such as C:\PGPn123. You should have:

ORDER.TXT	When ordering, Please use this form.
PGP_N123.EXE	PGPn123 executable.
KEYOPS.EXE	Key operations module
BATCH.PIF	Used to run batch files created on the fly.
PGP_N123.HLP	This help file.
BRIGHT.EXE	Brightens the current DOS screen before running PGP. Can be deleted if desired.
README.TXT	PGPn123 description required by some archives
FILE_ID.DIZ	PGPn123 description required by some archives
CSCMD.VBX	Required Command Button control
QPRO200.DLL	Crescent Software's QuickPak Pro Toolkit
VBRUN300.DLL	Visual Basic's run time module.
CTL3D.DLL	Gives most message boxes the 3D look
NOUN.TXT, VERB.TXT, ADVERB.TXT, PROPER.TXT STRUCT.TXT	Steganography routines require a source of words and a structure file for forming words into sentences. These files serve that purpose.



Command Line:
C:\PGP_N123\PGP_N123.EXE

☐ Run Minimized

Running the first time

Run PGP_N123.EXE from the Program Manager Run dialog box. The first time PGPn123 is executed, a program group and icon will be created, so this is the only time you will need to perform this step.

Configuration

The default configuration is for a stand-alone "clipboard" mode. In this mode, there are no links other than the clipboard between applications, and the toolbar float over the desktop. Users upgrading from freeware PGPn123 will need to add a configuration entry for their linked application, whereas new users will have several default configurations to select from (they may have to be edited depending on your application directories).

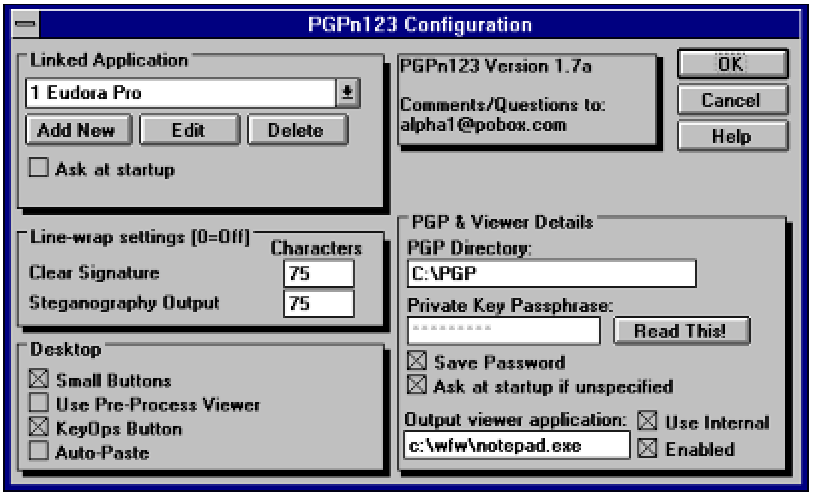
In the configuration window, you can define one or several applications, like Eudora, to load at startup. Once configured, it's best to use PGPn123 to start your e-mail or news-reader application, instead of loading PGPn123 afterwards. Not only is it more reliable, but since it saves a step, it's also faster and easier. If you frequently use PGPn123 with different applications, you may want to have it ask at startup for the desired program to launch, or create a separate INI file for each application configuration.

To run PGPn123 with a separate INI file, specify the -i option on the command line followed by a space and then the name of the INI file:

```
PGP_N123.EXE -i MYFILE.INI
```

Do not include drive or path information as part of the filename for your INI file. It will be created in the PGPn123 installation directory.

Configuration Window



Linked Application

1 Eudora Pro

☐ Ask at startup

PGPn123 Version 1.7a

Comments/Questions to:
alpha1@pobox.com

Line-wrap settings [0=Off]

	Characters
Clear Signature	75
Steganography Output	75

Desktop

☒ Small Buttons
☐ Use Pre-Process Viewer
☒ KeyOps Button
☐ Auto-Paste

PGP & Viewer Details

PGP Directory: C:\PGP

Private Key Passphrase: *********

☒ Save Password
☒ Ask at startup if unspecified

Output viewer application: c:\wfw\notepad.exe

☒ Use Internal
☒ Enabled

Linked Application: This is the e-mail program you will be linking with. See Application Setup for details..

To add entries, click the Add button. You will be presented with a blank entry which needs to be filled in.

To edit existing entries, select the desired entry then click on Edit.

To delete entries, highlight the desired entry then click on Delete.

The application showing in the window when you press OK will become the default application at startup.

Line-wrap settings: PGPn123 will word-wrap ling lines under cetain circumstances if you set the following values to a number greater than zero:

Clear-signature: PGPn123 will ensure that there are no lines longer than your specification sent to PGP during a clear-sign operation. This may be required depending on the application from which the message will be sent. Some applications (Agent is one) will wrap the text just prior to sending. If the text is wrapped after the signature is applied, the signature check will fail, because the message has been altered by the sending program. By setting this parameter to a number greater than zero, all lines of a length exceeding that value will be wrapped prior to being sent to PGP for signature application. We suggest setting this value to something slightly less than the wrap length setting of the application. Setting to zero disables this feature.

Steganography: When creating a steganographic message, PGPn123 creates paragraphs as a single, long line of text. Since the paragraphs can be quite long, some mailers are not able to properly line-wrap the message, and corruption can result. Setting this value to something less than your mailer's line-wrap setting will solve that problem by pre-wrapping the paragraphs.

KeyOps Button: If checked, the Help button is replaced with a KO (KeyOps) button. Clicking on this loads the included KeyOps module.

Auto Paste: Select this option if you want PGPn123 to automatically paste the results of operations.

Some mailers (Eudora for one) will not allow you to replace the contents of incoming messages. If you are decrypting a message, and you do not want PGPn123 to automatically paste the results, enter the following parameter into the PGP_N123.INI file under the [Application] section:

```
DecryptAutoPaste=0
```

Regardless of whether you use this or not, the contents of the clipboard can still be pasted by clicking on the paste button or using your application's paste command.

PGP Directory: The directory where PGP.EXE can be found.

Private Key Passphrase: There's a button next to this field that reads: "Read This!" You must to click on that button to gain access to this field. Unlike earlier versions, PGPn123 now scrambles your passphrase before placing into the INI file (if you choose to save it). Note however, that the method used to scramble the password could be reversed by a clever hacker and your secret key would be revealed. This is primarily done to prevent the casual snoop from acquiring your key. You can prevent PGPn123 from saving your pass phrase by unchecking the Save Password box, and you will need to re-enter it the next time you start PGPn123.

PGP accepts passwords in three ways: manually from the keyboard, in the form of an environment variable called PGPPASS, and on the command line. When you enter a passphrase in this field, the batch file that launches PGP is modified to include your password during assembly in on of two ways depending on your settings in the PGP_N123.INI file:

If you have PassCmd=1 under the [Application] section of the INI file, the batch file is modified like this:

```
        SET PGPPASS=[Your Secret Key Passphrase]
        ...
        PGP (usual commands)
        ....
        SET PGPPASS=;
```

Some people have reported that their environment is not large enough to accomodate this method, so the method below was added and set as the default. This method is also not without its problems, as DOS limits command lines to 128 charactors, so if you have a long passphrase, or encrypt to multiple recipients, DOS may truncate the command line passed to PGP, resulting in the incorrect passphrase being used. The worst-case here is that you will need to enter your passphrase manually if this happens.

If you have PassCmd=0 (or no entry) under the [Application] section of the INI file, the batch file is modified like this:

PGP (usual commands) -z [Your Secret Key Passphrase]

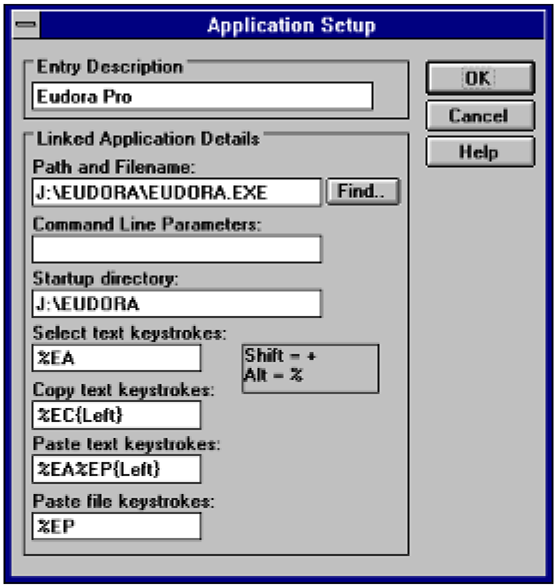
This allows PGP to perform any operation requiring your private key without prompting for it. For obvious reasons, this batch file (PGP_N123.BAT) is wiped after each use.

Viewer Application: If you would prefer to use an external viewer like Notepad, enter it here and uncheck the Use Internal box. If you want PGPn123 to automatically copy the result to the clipboard, Uncheck the Enabled box. The viewer will not show the result of PGP operations, and you can simply press the paste key to insert the result into your mailer.

Small Buttons: Check this box to change the visual appearance of PGPn123 on the desktop.

Use Pre-Process Viewer: Check this box if you want to show the viewer/editor before each operation. Doing so allows you to modify the message before sending it to PGP.   You may also invoke the Pre-Process Viewer/Editor by holding down the shift key when clicking the Sign, Decrypt, Encrypt or Add Key buttons.

Application Setup Window



Entry Description: Eudora Pro

Path and Filename: J:\EUDORA\EUDORA.EXE

Command Line Parameters:

Startup directory: J:\EUDORA

Select text keystrokes: %EA

Copy text keystrokes: %EC{Left}

Paste text keystrokes: %EA%EP{Left}

Paste file keystrokes: %EP

Shift = +
Alt = %

Entry Description:
Assign a descriptive name based on the name of the application, such as "Eudora", or "Pegasus". If you use different INI files with your application, you might want to create an entry for each configuration. You might call one "Eudora - Personal" and the other "Eudora - Business". This field is has no bearing on the way PGPn123 functions, except that if you set PGPn123 to display a list of applications at startup, the entry will be displayed verbatim.

Path and Filename: This is the program to load for this entry. The entire drive, path and filename should be specified. Selecting Find will show a file dialog box for visually selecting the program. Do not enter command line parameters in this field. Enter them in the Command Line Parameters field below.

Command Line Parameters: If your application needs any switches or settings specified after the filename, enter them here.

Startup Directory: Some applications require that you change to their directory before launching them. For example, if you are linking with Agent .99 (and possible other flavors), you must specify your agent directory (e.g. C:\AGENT) or it will create a new AGENT.INI file in the current directory (which will typically be \PGPN123).

Macro Keystrokes: When you click on the Decrypt, Clear Sign, Add Key, or Encrypt buttons, PGPn123 does the following:

Select keystrokes are sent to the linked application. This is intended to select all text within the editing window of the application where the cursor is currently positioned. **Copy keystrokes** are sent immediately after the **select keystrokes**. This copies the selected text to the clipboard. See Key Commands for details on writing keystroke macros.

You may have noticed the {Left} command in the keystrokes macros - it simulates pressing the left arrow key to non-destructively deselect the text. If you would prefer to leave the text selected, take this out. Be aware that taking it out is somewhat dangerous, since if you hit a spacebar or any other key while that window has the focus, ALL selected text will be replaced with that accidental keystroke.

After your message is copied to the clipboard, it is saved to the file PGP_N123.TXT in the PGPn123 directory and processed by PGP as directed. All temporary files created and used by PGPn123 are wiped and deleted when the program exits.

If after viewing the output of the operation (if the viewer is enabled), you click on the Paste Results button, the **paste keystrokes** are sent to the application, where the contents of the clipboard (placed there during the viewing phase or automatically if the viewer is disabled) are pasted into the linked program.   If Auto-Paste is turned on in the configuration window, PGPn123 will automatically paste the results into your application.

The user-configurable menu may be used to paste text files into your message. The **paste file keystrokes** field contains the commands that PGPn123 sends to your application for this procedure.

Key Commands

NOTE: These specifications are derived from the Visual Basic SendKeys command reference.

We have been informed that SendKeys does not do well when you specify a Control sequence (e.g ^A for Control-A). It does however, seem to work very well with Alt and Shift sequences (% and + respectivly)

Key	Code	Key	Code
Backspace	{BACKSPACE} or {BS} or {BKSP}	Break	{BREAK}
Caps Lock	{CAPSLOCK}	Clear	{CLEAR}
Del	{DELETE} or {DEL}	Down Arrow	{DOWN}
End	{END}	Enter	{ENTER} or ~
Esc	{ESCAPE} or {ESC}	Help	{HELP}
Home	{HOME}	Ins	{INSERT}
Left Arrow	{LEFT}	Num Lock	{NUMLOCK}
Page Down	{PGDN}	Page Up	{PGUP}
Print Screen	{PRTSC}	Right Arrow	{RIGHT}
Scroll Lock	{SCROLLLOCK}	Tab	{TAB}
Up Arrow	{UP}	F1	{F1}
F2	{F2}	F3	{F3}
F4	{F4}	F5	{F5}
F6	{F6}	F7	{F7}
F8	{F8}	F9	{F9}
F10	{F10}	F11	{F11}
F12	{F12}	F13	{F13}
F14	{F14}	F15	{F15}
F16	{F16}		

To specify keys combined with any combination of Shift, Ctrl, and Alt keys, precede the regular key code with one or more of the following codes:

Key	Code
Shift	+
Control	^
Alt	%

To specify that Shift, Ctrl, and/or Alt should be held down while several other keys are pressed, enclose the keys' code in parentheses.   For example, to have the Shift key held down while E and C are pressed, use "+(EC)".   To have Shift held down while E is pressed, followed by C being pressed without Shift, use "+EC".
To specify repeating keys, use the form {key number};   you must put a space

between key and number. For example, {LEFT 42} means press the Left Arrow key 42 times; {h 10} means press h 10 times.

PGP_N123.INI Settings

These settings are not provided in any configuration window and must be set manually by editing the PGP_N123.INI file.

PassCmd

If set to 1, PGPn123 will pass your secret key passphrase to PGP via an environment variable, which is cleared upon termination of the batchfile. Also the batch file is wiped after use. The default for this value is 0, which causes PGPn123 to pass the passphrase as a command line parameter.

EXAMPLE:
[Application]
PassCmd=1

EndCmd

PGPn123 by default, adds this command to the end of its batch files, so it knows when PGP has finished processing:

ECHO Finished >PGP_N123.END

On some systems, and it is not yet known why, do not create the file as they should. This entry allows you to specify a different command which will more reliably create this file. You should not modify this setting unless instructed to do so by Alpha1. The example below is the alternative setting you might be instructed to try if default settings do not work for you.

EXAMPLE:
[Application]
EndCmd=COPY BATCH.PIF PGP_N123

ChkPGP

This command is related to EndCmd, and by default is disabled. It has been found on some systems that the PGP integrity check fails, even though PGP is working fine. In light of that knowledge, we have disabled the PGP integrity check. You may re-enable it by entering the following:

EXAMPLE:
[Application]
ChkPGP=1

AppLoadState

If you want your application to load in a certain state, use this parameter. By default, the value is Normal.

EXAMPLES:
[Application]
Normal (default):
AppLoadState=1
Minimized:

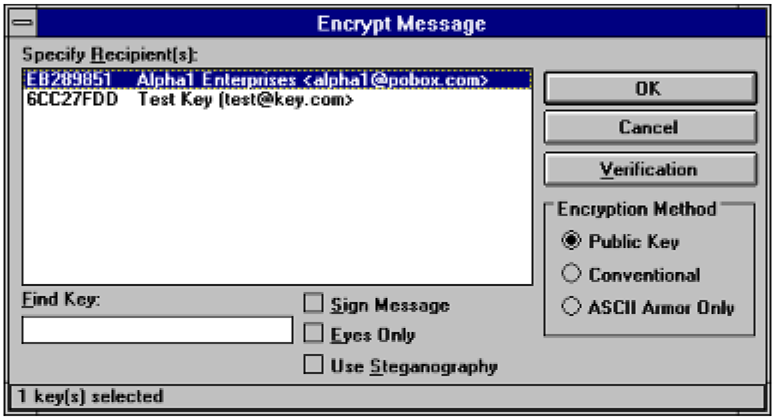
AppLoadState=2
Maximized:
AppLoadState=3

AppTimeout

If your application takes an unusually long time to load, PGPn123 may indicate that it could not be found, even though it has loaded. Increase this setting to allow more time for the program to load. Time is in seconds, 10 seconds is the default period to wait.

EXAMPLE:
```
[Application]
AppTimeout=10
```

Encrypting Messages



EB289851 Alpha1 Enterprises <alpha1@pobox.com>
6CC27FDD Test Key (test@key.com>

● Public Key
○ Conventional
○ ASCII Armor Only

□ Sign Message
□ Eyes Only
□ Use Steganography

1 key(s) selected

In the linked application, for example Eudora, type the body of the message. When finished, make certain the text cursor (as opposed to the mouse cursor) is placed in the message body. Click on PGPn123's Encrypt Message button. If you have properly configured PGPn123, the entire message body will be selected and copied to the clipboard.

If you pressed the shift key when you clicked on the Encrypt button, or if you have selected "Use Pre-Process Viewer" in the configuration window, the Pre-Process Viewer will pop up with the captured text. You can modify the text as needed in this window before sending to PGP by selecting Proceed.

A temporary file (which is later wiped) is created and PGPn123 will launch PGP in a minimized window to get a list of public keys available in your default public key ring. The list is placed into a list box, from which you may pick one, or several recipients for the message. Up to five recipients may be selected. You may also use conventional encryption (password protected encryption) or merely use PGP's ASCII-Armor (no encryption) feature to encode the plain-text for safe transport. *Hint: Click with the Control key depressed to make multiple selections in the public key list box.*

If you wish to add your signature to the file before it is encrypted, check the Sign Message box. If you have more than one secret key, your default key will be used to sign the message. See Key Operations for information on how to specify your default key.

Tick the Use Steganography box to have PGPn123 turn the PGP output into English sentences. This option is designed to prevent the automatic detection of PGP messages by mail filtering and logging systems. Steganograpic processing results in a file that is no less than eight times the size of the original PGP message. It is very easy to exceed the 30KB limit of PGPn123's message handling routines, so you will not be allowed to use this feature on large messages. For a recipient to decrypt your message with this option enabled, they too, will need to be using your same version of PGPn123.

To verify that you are encrypting the right information, you can click on the Verification button. A message box with the first 512 characters of your message will appear for your examination. If the wrong information is displayed, it means that your message did not get copied to the clipboard properly.

Click on OK to have PGP encrypt your plaintext. The output will loaded into the viewer. You must manually copy the text from the viewer (internal or external) to get it onto the clipboard. The Express button will copy the contents of the viewer to the clipboard and close the viewer in one step .

At this point, your plaintext message is still present in the message body. Use your mouse to select the entire body, or choose Edit|Select All from the application's menu. Click on PGPn123's Paste Results button or choose Paste from your application's Edit menu.. The selected message body will be entirely replaced with the PGP's output (or your selection from it).   It is possible to do this automatically, by adding to the Paste Macro for this application:

> With Eudora for example, instead of %EP for the paste macro, use %EA %EP{Left} . This will select all of the message for you and paste the results in place of the message.

Keep in mind however, that if you have chosen to work in manual mode, you will first need to select and copy the message body to the clipboard, do the encryption, then manually place it back into the body of the message, replacing the plaintext.

Clear Signing Messages

In the linked application, for example Eudora, type the body of the message. When finished, make certain the text cursor (as opposed to the mouse cursor) is placed in the message body. Click on PGPn123's Clear Sign Message button. If you have properly configured PGPn123, the entire message body will be selected and copied to the clipboard.

If you pressed the shift key when you clicked on the Sign button, or if you have selected "Use Pre-Process Viewer" in the configuration window, the Pre-Process Viewer will pop up with the captured text. You can modify the text as needed in this window before sending to PGP by selecting Proceed.

You will be prompted by PGP for your passphrase to unlock your secret key. The signed message output will loaded into the viewer. You must manually copy the text from the viewer (internal or external) to get it onto the clipboard. The Express button will copy the contents of the viewer to the clipboard and close the viewer in one step .

At this point, your plaintext message is still present in the message body. Use your mouse to select the entire body, or choose Edit|Select All from the application's menu. Click on PGPn123's Paste Results button or choose Paste from your application's Edit menu.. The selected message body will be entirely replaced with the PGP's output (or your selection from it). It is possible to do this automatically, by adding to the Paste Macro for this application:

> With Eudora for example, instead of %EP for the paste macro, use %EA %EP{Left} . This will select all of the message for you and paste the results in place of the message.

Keep in mind however, that if you have chosen to work in manual mode, you will first need to select and copy the message body to the clipboard, sign the message, then manually place it back into the body of the message, replacing the plaintext.

Decrypting Messages and Checking Signatures

PGP handles encrypted and signed messages in the same way. If it is encrypted with your public key, PGP uses your private key to decrypt it. If it is a signed message, PGP checks the signature against the signers public key on your public key ring. PGP itself will tell you whether there was a signature, and if so, whether it checked-out as good. Make sure you pay attention to the PGP messages, as the output is the same regardless of signature integrity.

In the linked application, for example Eudora, open a window with the signed and/or encrypted message. Move the text cursor to the body of the message by clicking in the message body. Click on PGPn123's Decrypt Message button. If you have properly configured PGPn123, the entire message body will be selected and copied to the clipboard

If you pressed the shift key when you clicked on the Decrypt button, or if you have selected "Use Pre-Process Viewer" in the configuration window, the Pre-Process Viewer will pop up with the captured text. You can modify the text as needed in this window before sending to PGP by selecting Proceed.

If the message was encrypted with you as the recipient, PGP will prompt you for your secret key passphrase. The plain-text output will loaded into the viewer. You must manually copy the text from the viewer (internal or external) to get it onto the clipboard. The Express button will copy the contents of the viewer to the clipboard and close the viewer in one step .

At this point, your encrypted and/or signed message is still present in the message body. In Eudora, it is not possible to replace the message body of a received message without creating a reply, as to what you do with the plaintext - that's up to you. You might very well want to create a reply, pasting the plaintext into the reply's message body. If so, just click your mouse in the new message body, then click on PGPn123's Paste Results button. The plaintext result will be pasted into the message body, ready for quoting or whatever.

Keep in mind however, that if you have chosen to work in manual mode, you will first need to select and copy the message body to the clipboard, decrypt the message, then manually place it into a new message or reply.

Alpha1's Public Key

Click here to copy our key to the clipboard.   Start the PGPn123 KeyOps module. Select Add Public Key.

```
Type Bits/KeyID    Date       User ID
pub  1024/EB289851 1996/05/02 Alpha1 Enterprises <alpha1@pobox.com>
```

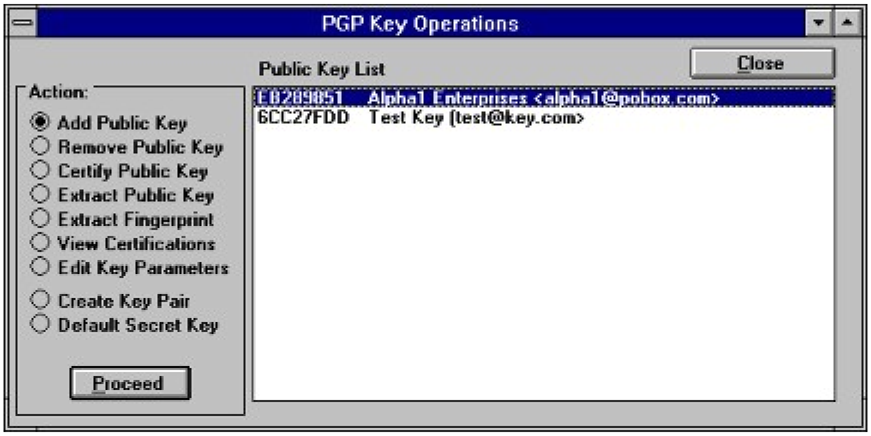
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3a

mQCNAzGI+awAAAEEALRA45WJJ2NFUjVoYzKCc/cRs5bwK4o8Hiyo4vuMA6n1pYSQ
s6PQvI++PwxedI6gG2YTbpl65w0OtIZmzz9GuW+QwowdVViWgPM5KJumBMK9fWkp
lZldCrlc3tNOoovXZbS2kCMxn9LKytiYapdiNR4PMHRm7XD6EEDlIgTrKJhRAAUT
tCVBbHBoYTEgRW50ZXJwcmlzZXMgPGFscGhhMUBwb2JveC5jb20+iQCVAwUQMers
2UDlIgTrKJhRAQGeBgP+P45/etDhZwnKEZhgKPsivKN5cUVhlObS1Mv1C5t9yDZm
ONuS8ENICTWKl7n70eFq5VvkZKgti+MDlzIN3DN5vvNSmGURqVy38dUWDtM/LWsg
jAqGR5Du7HVhdagoaN0yYBXhMAnN+Xd07NVmbX/oANzoW5NGKwGGNsptQlSx+es=
=jQ2+
-----END PGP PUBLIC KEY BLOCK-----
```

Wiping Files

As you probably know, DOS does not actually delete files, but simply marks the space they once occupied as now available. This makes it possible to undelete files containing possibly sensitive information.   A common practice to get around this, is to overwrite the file with random garbage before deleting it, rendering it's recovery irrelevant.

Worthy of note however, is that whether it's PGP's internal wiping procedure, or PGPn123's procedure, a file may never be touched if it resides on a drive that is cached by a memory caching utility such as Smartdrive, or a hardware caching device. For this reason, we once again warn against using PGPn123's features to automate the entry of your secret key. Even if you check the No Save box, the password is written to a batch file during the next operation (for the purpose of passing it to PGP). Due to the drive caching issue, this file, though wiped after use, may indeed still contain your passphrase if the cache did not see fit to write to the hard drive before the file was deleted.

Key Operations



Action:
● Add Public Key
○ Remove Public Key
○ Certify Public Key
○ Extract Public Key
○ Extract Fingerprint
○ View Certifications
○ Edit Key Parameters
○ Create Key Pair
○ Default Secret Key

Public Key List

```
EB289851    Alpha1 Enterprises <alpha1@pobox.com>
6CC27FDD    Test Key (test@key.com>
```

Add Public Key_

To add a public key in the Key Operations window, select Add Public Key, then click on Proceed. This option takes the data in the clipboard and sends it to PGP. Because of this technique, if you have not previously copied the public key block to the clipboard, PGP will not find a key and will give you an error message.

Remove Public Key

Select Remove Public Key, then highlight the public key you wish to remove. Click on Proceed. PGP will prompt you for confirmation before removing the key.

Certify Public Key

Select Certify Public Key, then highlight the public key you wish to sign. By signing a public key, you are certifying that it does in fact belong to the listed owner. As a general rule, the more signatures present on a key, the more certain you can be of it's ownership. Click on Proceed. PGP will ask for confirmation before proceeding.

View Certicifications

Select View Certifications, then highlight the public key you wish to examine. Click on proceed. PGP will extract the key ID and references to any attached signatures for you to review.

Edit Key Parameters

Select Edit Key Parameters, highlight the key to edit, then click on Proceed. PGP will walk you through this process .

Extract Public Key

Select Extract Public Key, then highlight the key you wish to extract. Click on Proceed. PGP will create and ASCII armored copy of the key, and PGPn123 will place it into the viewer. From there, you can copy and paste it anywhere you wish. The key itself is not removed - this only makes a copy of the key.

Extract Public Key Fingerprint

Select Extract Fingerprint, then highlight the key you wish to fingerprint. Click on

Proceed. PGP will create a file with the key fingerprint, and PGPn123 will place it into the viewer. From there, you can copy and paste it anywhere you wish. The key itself is not removed - this only extracts a fingerprint of the key for easy verification of its authenticity.

Create Key Pair

Select Create Key Pair. Click on   Proceed. PGP will prompt you for the length of key you wish to create. After making a selection, a pair of complementary keys will be created, one secret key and one public key.

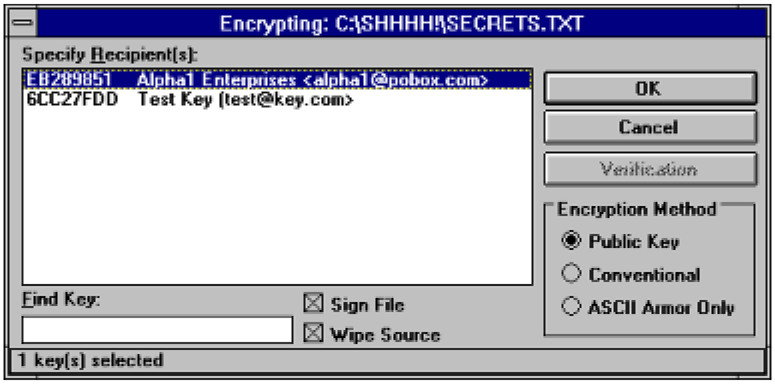
Default Secret Key

Select Default Secret Key. The list box with be loaded with your secret key ring. If there are two or more secret keys, select the one you wish to use. Click on Assign, to mark that key as the default. From this point forward, when you sign a message, it is this default key which will be used to make the signature. It is not necessary to set a default key if there is only one secret key. PGPn123 uses the PGPPATH environment variable to determine the location of your secret keyring.

File Operations

PGPn123 allows you to process files as well as messages. To process a file, click on the File Services button. A dialog box will appear allowing you to select a file to work with.

To encrypt a file, click on Encrypt. After PGPn123 obtains the list of public keys, the following window will pop up:



Encrypting: C:\SHHHH!\SECRETS.TXT

Specify Recipient(s):

```
EB289851   Alpha1 Enterprises <alpha1@pobox.com>
6CC27FDD   Test Key (test@key.com>
```

Encryption Method

● Public Key
○ Conventional
○ ASCII Armor Only

Find Key:

☒ Sign File
☒ Wipe Source

1 key(s) selected

Choose the encryption method, signature and wipe options, then click on OK.   The encrypted file will be placed into the same directory as the source file.

To decrypt a file, click on Decrypt. PGPn123 will prompt you for the output directory, which by default is the same as the source directory. Click on OK.

To delete a file, Click on Delete. You will be prompted for confirmation before the file is deleted.