# Table of Contents

This is beta software - if you experience problems with operation or would just like to offer a suggestion, please write to alpha1@znet.com.   All comments are welcome. When writing, PLEASE 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, 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.

## Unique Features

- Loads the linked application automatically. For example, if you are a Eudora user, you will click on the PGPn123 icon instead of Eudora's. PGPn123 will load Eudora and then always sit on top of it.

  Once linked with an application, it stays with it. PGPn123 always 'floats' just above the linked application. It's always real handy, there when you need it (You can minimize it to a floating icon if it's in your way).

- Keystroke macros can be sent to your application to speed up the process even more. 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 recipient's key to use for encryption. After shelling to PGP, a viewer shows you what the output looks like, and lets you copy it to the clipboard. Back in Eudora, just paste it into the message body - you're finished!

- Use an internal or external viewer.

- Link to ANY Windows application. (though not on-the-fly, as yet anyway)

- Turn off keystroke macros for full control - Manual mode allows you to manually select and paste information to the clipboard, then process it with PGPn123. Use this when you don't want to process the entire message body or when you link to an application that doesn't respond well to the reception of foreign

keystrokes. (Microsoft Word is one that comes to mind).

# Installation

### What to do with the files
Copy everything into a separate directory, such as C:\PGPn123. You should have:

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.
DBTTIP.VBX            Freeware VBX adds "Tool Tips" to PGPn123
THREED.VBX            New button-bar requires this
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
CTL3D.DLL            Gives most message boxes the 3D look
VBRUN300.DLL         Visual Basic's run time module.



### 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. There are no links other than the clipboard between applications. PGPn123 always stays on top.

In the configuration window, you can specify a certain application, like Eudora, to load at startup. Once configured, it's best to use PGPn123 to start your e-mail application, instead of loading PGPn123 afterwards. Not only is it more reliable, but since it saves a step, it's also faster and easier.

# Configuration Window
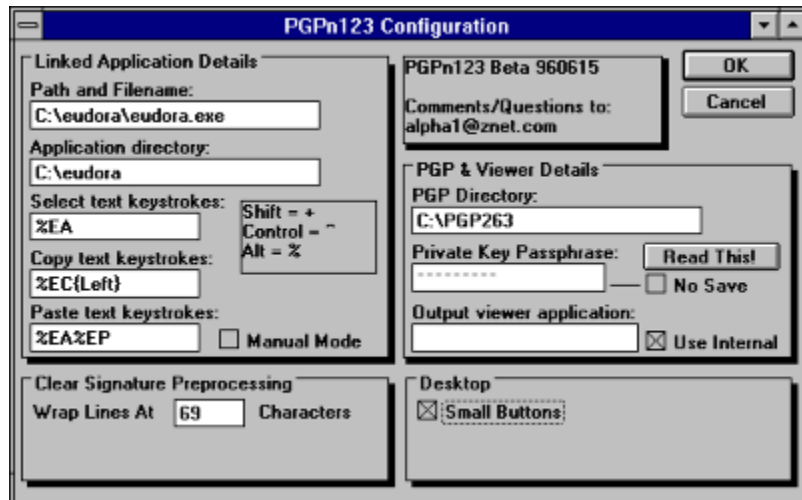


## Linked Application

Path and Filename: This is the e-mail program you will be linking with.

Application 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 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, 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 COPY keystrokes - 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.

The selected function is performed on the text currently in the clipboard by saving it the file PGP_N123.TXT in the PGP directory. All temporary files created and used by PGPn123 are wiped and deleted when the program exits.

If after viewing the output of the operation, 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) are pasted into the linked program.

Manual Mode: Manual mode essentially disables the keystroke macros. This may be a preferred setting for those who wish to do their own copy/paste operations. Simply put the subject text onto the clipboard, then click on the desired function. The Paste button is disabled while in manual mode.

When operating in stand-alone mode (without an attached application), manual mode is forced, since there is know way PGPn123 could know to which application the keystrokes should be sent. Without an attached application, you must operate from the clipboard.

Clear Signature Preprocessing - Word Wrap: 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.

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. It may as well read "Press Here If You're Not Too Smart", because that's probably the case if you actually use this "feature". If you put your private key password in here, PGPn123 will put it in it's PGP_N123.INI file, plain as day, for anyone to see if they choose to look (you can avoid this by checking the No Save box, but you will need to re-enter it next time you start PGPn123). The reason a person may want to do this is if they genuinely feel that their computer is inaccessible to others and dislike the hassle of entering their password for each and every operation requiring a private key.

PGP accepts passwords in two ways: manually from the keyboard; and in the form of an environment variable called PGPPASS. When you enter a passphrase in this field, the batch file that launches PGP is modified during creation to include two extra statements:

    SET PGPPASS=[Your Secret Key Passphrase]
    ...
    PGP .....
    ....
    SET PGPPASS=;

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.

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

# Key Commands

| 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.

# Encrypting 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 Encrypt Message button. If you have properly configured PGPn123, the entire message body will be selected, copied to the clipboard, then saved to a temporary file (which is later wiped). 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. *Hint: Click with the Control key depressed to make multiple selections.*
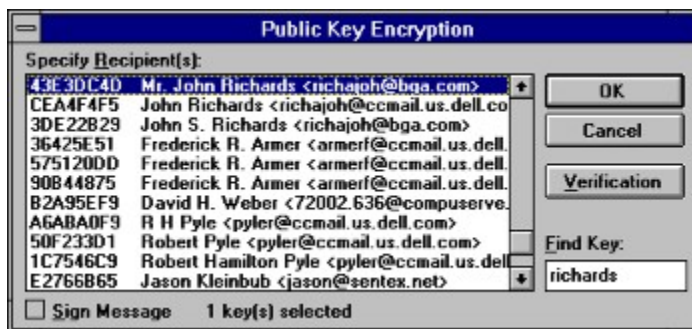


If you wish to add your signature to the file before it is encrypted, check the Sign Message box. If you have more than one secret key, your default key will be used to sign the message. See Key Operations for information on how to specify your default key.

To verify that you are encrypting the right information, you can click on the Verification button. A message box with the first 512 bytes 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 simultaneously be placed onto the clipboard and loaded into the viewer. You need not manually copy the text from the viewer (internal or external) to get it onto the clipboard - it's already there. The only time you would do this is if for some reason you didn't want to paste the entire output. Just manually select what you want, then copy it to the clipboard - the current contents will be replaced with your selection.

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. The selected message body will be entirely replaced with the PGP's output (or your selection from it).

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, copied to the clipboard, then saved to a temporary file.

You will be prompted by PGP for your passphrase to unlock your secret key. The signed message output will simultaneously be placed onto the clipboard and loaded into the viewer. You need not manually copy the text from the viewer (internal or external) to get it onto the clipboard - it's already there. The only time you would do this is if for some reason you didn't want to paste the entire output. Just manually select what you want, then copy it to the clipboard - the current contents will be replaced with your selection.

At this point, your unsigned 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. The selected message body will be entirely replaced with the PGP's signed message output (or your selection from it).

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, copied to the clipboard, then saved to a temporary file.

If the message was encrypted with you as the recipient, PGP will prompt you for your secret key passphrase. The plaintext message output will simultaneously be placed onto the clipboard and loaded into the viewer. You need not manually copy the text from the viewer (internal or external) to get it onto the clipboard - it's already there. The only time you would do this is if for some reason you didn't want to paste the entire output. Just manually select what you want, then copy it to the clipboard - the current contents will be replaced with your selection.

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.

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.

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

mQCNAzGI+awAAAEEALRA45WJJ2NFUjVoYzKCc/cRs5bwK4o8Hiyo4vuMA6n1pYSQ
s6PQvI++PwxedI6gG2YTbp165w0OtIZmzz9GuW+QwowdVViWgPM5KJumBMK9fWkp
lZldCrlc3tNOoovXZbS2kCMxn9LKytiYapdiNR4PMHRm7XD6EEDlIgTrKJhRAAUT
tCRBbHBoYTEgRW50ZXJwcmlzZXMgPGFscGhhMUB6bmV0LmNvbT4=
=4xO1
-----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 it 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
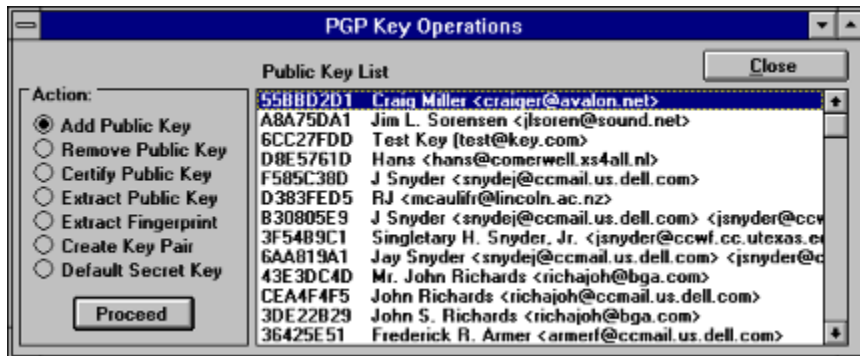


## Add Public Key
To add a public key in the Key Operations window, select Add Public Key, then click on Proceed. This option takes the data in the clipboard and sends it to PGP. Because of this technique, if you have not previously copied the public key block to the clipboard, PGP will not find a key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

## 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.

NOTE: Some users have reported problems with this feature. If the list box fails to display your secret keyring, please notify us. We are still trying to track down the source of this problem. Please supply your PGP version number (eg: PGP 2.6.2i).