Apple Menu

nly one menu item is relevant to the application. When invoked it displays the following dialog:

he About dialog, has a vertical scroll bar which you'll use to display the text.

File Menu

- Open…

Selecting this menu item invokes a standard choose file dialog. Depending on the Macintosh type of the file, MPGPC will execute a different action. Here is the list:

— If the file is a text clipping, the first TEXT resource is extracted and acted upon. The action depends on the Behaviour set in the main MPGPC panel being either To Encrypt or To Decrypt.

— If the file is a PGP public keyring file, then the keyring management environment is invoked and the file is opened. See the Keyring Management chapter.

— If the file is an MPGPC Addressbook, then the addressbook management environment is invoked and the file is opened. See the Addressbook Management chapter.

— If the file is a TEXT file, whether it was created by MacPGP or not, its contents are read and processed in the same way as text clipping files. In other words, it will be encrypted or decrypted depending on the behaviour status of MacPGP Control.

— If it's none of the above, the file is passed to MacPGP to open. What happens then depends on how MacPGP handles the file.

• Close…

By default this menu item is disabled. It becomes enabled when the active window is either a Keyring, an Addressbook or a Group nickname management window. Choosing this item when such a window is active, closes the window and activates the next one below it in the application's window layers.

Edit Menu

• Transliteration Table…

MPGPC uses one of two Transliteration Tables to convert non-ascii 8-bit characters into 7-bit USASCII characters. One referred to as a 1…1 table and the other is a 1…many.

The 1…1 (one-to-one) table as its name implies, translates each non-USASCII character into one USASCII character, while the one-to-many (1…many) table translates each non-USASCII character into a string (up to 256 chararcters) of USASCII characters.

Although not an ideal solution, the transliteration of your message into 7-bit USASCII characters is a secure way to prevent Internet transport programs from “misunderstanding/misinterpreting” the Macintosh character set and rendering the PGP clear signature into a bad one.

For the 1…1 table I used (with permission) the one that comes with Eudora Tables (id# 2002). You can not edit this table.

For the 1…many table, the transliteration process, as the name implies, looks for characters with code above 127 and replaces them with strings formed with 7-bit characters. The choice of replacement strings conform to Harald Tveit Alvestrand's <Harald.Alvestrand@uninett.no> Internet draft entitled Characters and character sets for various languages. I was not aware of the existence of this draft until Björn Andersson brought it to my attention. Thanks Björn :) For characters and symbols not defined in Harald's draft, I endeavoured to choose replacement strings that:

a. are common practice. Such as replacing single and double opening and closing quotes with straight ones,
b. are acceptable by usage. Such as replacing accented characters with their non-accented ancestor,
c. are visually close to their original. Such as '+' for the 'dagger', or '0/00' for the 'perthousand'.

When I ran out of imagination, I used the ISO name of the character or an abbreviation of the latter.

But, because your tastes might differ to mine, I allow you to edit these replacement strings, on the only condition that any replacement string has to be composed of 7-bit USASCIIs.

Choosing this menu item invokes a dialog similar to this:

he scrolling list contains all Macintosh characters with a code higher than 127. The code is shown in bold in the first column of the list. The second column is the Macintosh character used for this code. The last and most important column is the replacement string for this character.

To edit an entry, select it by clicking on it with your pointing device. The Macintosh character will be displayed in a large size within a non-editable region, and the current replacement string below it in an editable field.

dit the entry and press tab to exit editing. If the new replacement string is accepted, the new value will be displayed in the relevant line.

If you press the Cancel button, all your editing will be wasted. On the otherhand, when you press the OK button, I save this table to use for transliteration, until you change it again.

The Load… and Save… buttons allow you to store such tables and load them at will. This might prove to be helpful if and when you agree with your correspondents on a common table. Another by-product of this is a macro-like expansion of single character code into strings. An example might be to use the Paragraph sign (code 166) for your organisation name.

The Help icon/button -the one at the bottom left- toggles between the show/hide balloon help.

• Preferences…

When you invoke the Preferences… menu item, you will be presented with the following dialog:

•• General Settings

There are two parameters, you can set on this screen:

Your default user ID popup menu and field
This option contains a popup menu that lists your User ID values found in your secret keyring, in addition to an Other… field. If you select an entry different that the Other… one, it will be displayed in the field to the right of the popup menu button. If you intend on using a different user ID value than your MacPGP default ones, select the Other… entry and enter the new value for your user ID in the field which will become editable. This is an alternative to editing the (MYNAME option in MacPGP config.txt file).

Auto-decrypt source on open checkbox
Check this option to instruct MPGPC to decrypt PGP ciphered messages when bringing them into the Sign/Encrypt dialog.

If the decryption is successful, the deciphered message will be framed between a Header and Tail lines.

•• Eudora Settings

tart and Stop Notification

These two buttons will be enabled only when Eudora is running when the dialog is called or re-activated. As their names imply, they will allow Eudora to either start or stop notifying MPGPC of certain events.

Move received PGP mail to special mailbox

Check this option to instruct MPGPC to move newly received mail that looks like being PGP ciphered to a specially designated mailbox. This is a sort-of poor man's hard-wired filter for the freeware version of Eudora. If you are using the commercial version of Eudora, you will probably leave this option unchecked.

Save instead of Queue

Check this option if you want new mail generated by MPGPC to be saved in the Eudora Out mailbox instead of being queued. To know more about the differences between saving and queueing, read the Eudora documentation.

•• PGP Keyserver Settings

efault Keyserver popup menu and field

This is the mailing address of a PGP Keyserver. I have included a list of such servers from which you can select your preferred one. If you use different keyservers than the ones listed (under the pop menu to the left of this field), tell me about it so I can add it to the future versions.

This keyserver is assumed to respond to email messages sent to it as per BAL's keyserver email message formats.

I've already asked Peter N. Lewis to include in IC Config preferences file an option for the preferred PGP Keyserver. If the next version of IC Config indeed has this option, I will remove it from MPGPC preferences (as an “encouragement” for you to use IC Config ;-)

Use HTTP checkbox and HTTP Server Name field

Support for interaction with PGP Keyservers is being extended in MPGPC (Get keys in Addressbook management, and Update key info in Keyring management) with almost every release. If you want to use this feature, then check this box. Note however that if you're behind a firewall, MPGPC's requests using TCP/IP will not go through.

Also, I included as the default HTTP keyserver “www-swiss.ai.mit.edu.” I am not aware of any other server that accepts HTTP commands for key querries. If you know of any such servers, again tell me about it/them and I'll integrate it/them in the program.

•• MacPGP Settings

ain Public Keyring button

If you want to change your default main public keyring file, without going through MacPGP, then this is the place to do it. When you click the Set… button, a standard choose file dialog appears where you can select a PGP keyring.

Secondary Public Keyring button

Users of MacPGP2.6ui are not going to benefit from this, since this version of MacPGP, doesn't seem to make use of this secondary PGP public keyring file; On the other hand, users of the MIT and other versions, will.

Basically it's the same as the previous one, except it allows you to designate a secondary public keyring file that MacPGP is supposed to search for unknown keys/signatures.

Secret Keyring button

Same as the first option but for the secret keyring.

When you OK the dialog, I write this information in the PGP Preferences file that's supposed to be in your Preferences folder in your System Folder.

Note

With some strains of MacPGP, you will not be able to use the modified settings right away. To be on the safe side, I recommend you quit MacPGP after you alter its settings from MPGPC.   In the final version I might let MPGPC do that automatically.

- Show/Hide Clipboard

Selecting this menu item will display the clipboard if it is invisible, or hide it otherwise.

he bottom of the Clipboard window shows the character count of the textual contents of the clipboard at the time.

You can resize, move around the clipboard, and it will remember its own position and dimensions the next time you show it.

When the clipboard is visible on the desktop, the menu item reads Hide Clipboard.

The clipboard window now has a close box. When clicked, the clipboard is hidden. Alternatively you can use the shortcut Command-T (like in Alpha) to toggle between show and hide the clipboard window.

Service Menu

• Encrypt-Sign…

The Encrypt-Sign… menu item when selected invokes the same action as that of clicking on the Encrypt Sign button in the MacPGP Control window. In other words, the action will depend on the choices set for the Source and

Destination at the time.

• Decrypt-Verify…

The Decrypt-Verify… menu item when selected invokes the same action as that of clicking on the Decrypt Verify button in the MacPGP Control window. In other words, the action will depend on the choices set for the Source and Destination at the time, just like Encrypt-Sign…

The only thing to note here is that if the file creator of the file you specify in the choose dialog is MacPGP (signature is "MPGP") I pass the file as is to MacPGP to open and process it, otherwise I decrypt it. This is because with such files, MacPGP behaves in a way that usually confuses MPGPC, which is understanble since MacPGP scans the file contents and conducts different actions depending on the semantics of the data. A good example is when decrypting a message/file that contains one or more public keys: MacPGP not only decrypts and verifies the data, but also adds the key(s) and their related signatures to the main public keyring!

If everything goes OK, an appropriate message is signalled in the feedback zone.

Note: MacPGP always discards any text outside the ciphered text block which is delimited by special strings. I don't! I scan the text, save the before and after ciphered text, and restore them BUT only in the clipboard and not in the text file. So if say you're decypting something that looks like this:

he clipboard will contain something that looks like this:

did this because I got fed up with loosing people's clear signature that usually contains their address, phone and fax number which they forget to include in their ciphered text.

- File Encrypt…

MacPGP allows you to conventionally encrypt files. These are usually files you want to archive either on- or off-line for later use. MacPGP when conventionally encrypting such files, does not use any recipient public key.

But MacPGP also allows you to PGP encrypt files with one or more recipient public keys! You would use this feature to send files, either text or binaries, intended for specific persons.

MacPGP Control implements the interface to these MacPGP features through the File Encrypt… menu item under the Service menu. Detailed explanation about the difference between the two types of encryption is given in the MacPGP documentation.

When you select this menu item, or press its shortcut key combination (Command-I), the following dialog appears on your screen:

•• File… button

Press this button to select a file to encrypt. When you do a standard Finder find file dialog appears and you will be able to browse through your disks and folders to designate the file.

•• To… button

This button when pressed will allow you specification of the recipient(s) of the encrypted file. The dialog that will appear when you push this button is the same as the one you'll see and use throughout MacPGP Control anywhere you have to specify a list of recipients to process an action. See Specifying Recipients in User Interface chapter for the details of this dialog.

Once the file is specified, depending on its type and on whether there is or not a list of designated recipients, some options and buttons will become enabled.

•• Asciify output checkbox

This option is always enabled. It allows specification of wether or not to asciify the output or in other words encode it with Base-64. It's always a good idea to do that if you're unsure about how the encrypted file will travel on the Net.

•• Wipe out source file checkbox

When checked, it instructs MPGPC to shred the source file after encrypting it.

•• MacBinarise output checkbox

When checked, MacOS related information, such as the file type and creator type are saved. This is a good option to use if you plan on sending the encrypted file to another Mac user.

This option is enabled for text files. For non-textual files, MPGPC always MacBinarise the input before encrypting.

•• View by recipient(s) only checkbox

When checked (text files only), the encrypted file will only be displayed by the MacPGP Pager on the receiving machine (which can also be yours if you included yourself as one of the recipients of the encryption process).

s soon as you select a file, the Conventional button becomes enabled. The PGP Encrypt button will only become enabled if you have specified at least one recipient and of course selected a file.

The other options in the dialog are self-explanatory. If you check the PGP Sign icon checkbox which, you mean to tell MPGPC to (a) you want to sign the file and (b) you will use the selected User ID currently showing in the popup menu. When you check this option a popup menu showing all your User IDs found in your secret keyring is enabled. Your default user ID, which you specify in the Preferences dialog is selected by default. Choose another user ID if you wish to do so.

Note
When you choose Conventional Encryption, MacPGP will ask you to enter a pass-phrase. THIS DOES NOT NEED TO BE YOUR SECRET KEY PASS-PHRASE. In fact the MacPGP documentation strongly recommends not to use your secret key pass-phrase for conventional encryption pass-phrases.

The result file will have the extension .asc or .pgp appended to its name depending on whether the Asciify output option was checked or not respectively, and will be placed in the same folder as the source file.

• Make Certificate…

This menu item allows you to select a file and create a detached/separate PGP signature certificate of it.

• Asciify…

This menu item allows you to select a file, and asciify its contents. the resulting file will be located in the same folder as the specified input file, and its name will be the same as that of the input except there will be a .asc suffix appended to it.

• Generate Keypair…

When selected, you will be presented with a dialog similar to the following that will allow you to generate a new public/secret keypair.

ou specify the key grade you want to generate in the top popup menu and your user ID in the following one.

•• Key grade

The popup menu for the key grade has 4 options: Casual, Commercial, Military and Other. The first three correspond respectively to key lengths of 512, 768 and 1024 bits. As soon as you select one of them, the corresponding key length is displayed to the right, but you can not modify this value. If you want to designate another key length, choose the fourth option: Other. When you do so, the field to the right becomes enabled and you can then enter an integer value in the range [384…2048] inclusive. If you enter a value outside this range or if you enter a non-numerical value, MacPGP Control, will signal this in its feedback area (in the main window) and the cursor will remain in this field until you enter a valid value.

Notes

1. Beware that I don't use the NOMANUAL switch for this command and hence I honour Philip Zimmermann's request that the PGP documentation be present in the same folder where MacPGP is.

2. All keypairs generated by MacPGP Control have a 17-bit exponent. If you want to use other exponent lengths you should use the Generate Key… menu item under Key menu in MacPGP.

•• User ID

The user ID popup has Other… as its first option. If you choose this option, the field that usually displays the current user ID, becomes editable and you can enter manually your new user ID to associate with the new key.

• Revoke Key…

The dialog that will be displayed when you select this item, will allow you to generate a Key Compromise Certificate in an ascii armored file. This file/certificate contains a copy of your REVOKED key associated with a designated user ID. Usually, you would send this file to a PGP Keyserver to broadcast your dissociation with this key.

ecause revoking a key is not -or shouldn't be- an every-day operation, I took care of forcing you to press the OK button in the top part of the dialog, before effectively carrying on with the operation.

• PGP® Dataskope…

The Dataskope is invoked either from the respective menu item under the Service menu, or when pressing the More… button in a Keyring Management window (see Keyring Management chapter).

The windoid that appears, looks like this:

f you click on the zoom box, the windoid shrinks to look like this:

•• Analyze… button

When you press this button, you will be presented with a standard choose file dialog to select a file that will be analyzed. The file is assumed to contain plain PGP packets. Examples of such files are: Public and Secret keyring files. In fact when this windoid is invoked by pressing the More… button from a Keyring Management window, the PGP packets of this keyring file will be displayed. Something similar to the following:

he table will show a letter for each PGP packet it finds inside the file whose name will be shown at the top of the windoid. Use the Help button to get a grip of what each letter refers to.

When your cursor is positioned inside the table area, its shape changes to that of a magnifying glass.

When you click on a letter, more detailed explanation on the PGP packet contents are displayed in the bottom area of the dialog.

•• De-Asciify… button

Asciified files, might also contain PGP packets. Such files are Public keys you receive, extract or send, or even messages you encrypt with the “-a” option in a PGP command.

This button when pressed, will allow you to select a text file that will be de-asciified, and an attempt to analyze its contents will be made. If the result is meaningful, then the window will show the same sort of info as when you press the previous button.

Window Menu

his menu will keep track of all opened major windows belonging to MPGPC. The first one with a Command-1 shortcut activates the main MPGPC window. The second one with a Command-2 shortcut, will bring this manual on-screen.

The rest of the menu will contain eventually two sub-lists for all Public keyring files being edited at the time, and all Addressbook files being edited at the time also. Grey lines will separate these sub-lists from each other and from the MacPGP Control and Help entries.

To activate any of these windows, you can, in addition to clicking inside them, select their name from this menu.

Keyring Menu

his menu will appear when at least one Keyring Management window is opened. The menu items found in this menu relate to buttons found in a Keyring Management window. For more details on what each menu item does see the chapter entitled Keyring Management.

There are two hierarchical menus attached respectively to Add Keys and Certify Key With… menu items. The first one has two menu items: from Clipboard and from File…. Their selection ignites the action relevant to the same options in the multi-choice button Add in the Keyring Management window. The second hierarchical window will display the list of all your User-IDs, similar to the list related to the multi-choice button labelled Certify… in the Keyring Management window.

Addressbook Menu

his menu will appear when at least one Addressbook Management window is opened. The menu items found in this menu relate to buttons found in an Addressbook Management window. For more details on what each menu item does see the chapter entitled Addressbook Management.

Group Menu

his menu will appear when at least one Group nickname window is opened. The menu items found in this menu relate to buttons found in a Group nickname window. For more details on what each menu item does see the chapter entitled Addressbook Management.