

Main window

The operation of MPGPGC is simple. There is one main window which opens automatically at launch and remains on the desktop until you quit (the application).

here are three main sections in this window: Action & Behaviour, Target Selection and Feedback. Following is a detailed discussion of each.

• Action & Behaviour

This is the top left part of the screen consisting of two labelled icons, with a clickable background divided in two adjacent invisible squares, each surrounding one icon-button.

The two icons labelled *Encrypt Sign* and *Decrypt Verify* behave as normal Macintosh push buttons.

To start a PGP Encryption with or without your PGP signature, or to PGP Sign only, you press the first push button labelled *Encrypt Sign*. On the other hand, to start a PGP Decryption, or to authenticate a ciphered text, just press the other push button labelled "Decrypt/Verify."

Pressing the *Encrypt Sign* push button invokes the same action as selecting the *Encrypt-Sign* menu item from the *Services* menu. Similarly, pressing the *Decrypt Verify* push button invokes the same action as selecting the *Decrypt-Verify* menu item under the *Services* menu.

Note: These push buttons are droppable; ie. you can drag from the Finder desktop, or from any other drag-and-drop-aware application, objects –be it text files or text clippings– unto them to start execution.

Behind these two push buttons there is a background divided into two squares behaving as radio buttons (when the cursor is within their bounds, its shape becomes a pointing finger). When one is highlighted, its area is marked by a surrounding frame. The highlighted area (or radio button) indicates the default behaviour of the application. If the area around the *Encrypt Sign* push button is marked, then the behaviour of the application is *To Encrypt*. Alternatively if it's the area of the *Decrypt Verify* push button which is highlighted, then the application's behaviour is *To Decrypt*.

The state of these two areas (radio buttons), follows that of their corresponding icon/push buttons: As soon as you push the *Encrypt Sign* or *Decrypt Verify* button, the area around the pushed button becomes marked.

When the behaviour of the application is *To Encrypt*, then dropping a Finder object on the application's icon will initiate the *Encrypt-Sign* action. Similar thing happens but with *Decrypt-Verify* when the behaviour is *To Decrypt*.

Also opening a text file will automatically invoke the application's behaviour and apply the corresponding action to the selected file.

- Target Selection

This is the top right part of the screen consisting of two labelled popup menus, one called Source with: Eudora, Clipboard, Keyboard, File and Microphone as possible choices; and the other is labelled Destination with Eudora, Clipboard and File as possible choices.

The Encrypting and Decrypting actions will be performed on the contents of an object from the selected Source, and the result will be directed towards the selected Destination. The following two tables show the possible combinations of these parameters.

Source / Destination combinations for Encrypt Sign button

Source	Eudora	Clipboard	Keyboard	File	Microphone	
Destination						
Eudora	X	X		X	—	X
Clipboard	X	X		X	—	—
File	X	X		X	X	—

Source / Destination combinations for Decrypt Verify button

Source	Eudora	Clipboard	Keyboard	File	Microphone	
Destination						
Eudora	X	X		—	—	—
Clipboard	X	X		—	—	—
File	X	X		—	X	—

Note: When you select Eudora as either the Source or the Destination of MPGPC operations in the MacPGP Control window, I check if the Eudora application is actually running. If it is then I signal that MPGPC is Ready... Otherwise, I tell you that it's not and select another target (Keyboard for Source or Clipboard for Destination).

- Source = Eudora

When the source is Eudora, MPGPC goes through this algorithm:

```

if the Eudora application is running then
  if there is a selected message in Eudora (see Note-1 below) then
    choose this message.
  else
    if the Out mailbox of Eudora (see Note-2 below) is not empty then
      let the user choose a message (see Note-3 below).
    else
      Consider the Keyboard as the Source.
else
  Consider the Keyboard as the Source.
  
```

Few things to note here:

1. I don't do any checks on the properties of the Eudora message, whether it's sendable or not, when there is an already selected message if it's in the Trash, the In, the Out or any other mailbox. I chose not to include in MacPGP Control's job description any checks on the validity of the ciphered/clear text from the e-mail application's stand point.
2. When I say Out mailbox, I don't mean a mailbox named "Out", I mean the Out mailbox as specified by the user in a

Eudora Settings file (see description of the Preferences dialog later). This implies a more coherent integration with Eudora since the latter allows the user to specify any name for their Out mailbox and this name then appears in its menus and becomes the Out mailbox window name when this mailbox is opened.

Whatever the Out mailbox name is at the time, I work with it.

3. Choosing a Eudora message to work with, is done by invoking the following selection dialog:

he dialog shows the current name of the Out mailbox, its contents as a 2-column list with the first column displaying the recipient's address and the second the subject of the message.

Selecting a message is a matter of clicking on a line in this list and hitting the OK button, or alternatively double-clicking a line.

While a line is selected, the Status field, displays a clear text of the message's status.

When you press the Encrypt Sign button, I bring the Eudora message and do the following:

1. If you checked the Auto decrypt source before processing option in the Preferences dialog, then the body of the message is decrypted.
2. The message is then opened in the Sign / Encrypt dialog, with the other Eudora header fields (except for Attachments) copied to their corresponding places in the said dialog. The interaction in the Sign / Encrypt dialog is explained in the Sign-Encrypt Messages chapter.

When you press the Decrypt Verify button, I bring the Eudora message and check if its body consists of a PGP cipher (with the right headers). If it doesn't, I signal that and return. Otherwise, I decrypt the body of the message and continue processing depending on the Destination. There is however a special case, when the Source = Destination = Eudora and you press the Decrypt Verify button. More details on what MPGPGC does in this case is given in the Note in the following section.

•• Destination = Eudora

When the Destination is Eudora, I attempt to create a new message in the Eudora –if it's running– Out mailbox, and either queue or save it (depending on a set value in the Preferences dialog) for transmission.

Note

There is a special case when Source = Destination = Eudora and you press the Decrypt Verify button. In this case, after the body of the Eudora message is decrypted (provided of course it is a PGP cipher), I do the additional following steps:

1. I quote the paragraphs of the message using the same Eudora's quote character,
2. I check with Eudora if you have an Attribution line defined in the current Eudora Preferences file. If such setting is defined then I make an attribution line, similar to Eudora's and add it to the beginning of the message preceded with a "**** " string.
3. I check if the subject line contains a "Re: " string, if it doesn't, I add one.
4. Hand over the lot to the Sign / Encrypt dialog.

•• Source = Clipboard

When the source is the clipboard, then I check to see if the clipboard, at the time an action is initiated, contains textual non-empty information. If it does, this is then used, otherwise I signal that it's empty and go to sleep.

•• Destination = Clipboard

When the Destination is the Clipboard, then I copy the processed message to the clipboard.

•• Source = Keyboard

When the Source is Keyboard and the action required is to Encrypt-Sign (the only one available), an Encrypt Message window is opened (see the discussion in the Sign-Encrypt Messages chapter).

Note: If MacPGP comes back with an error, I still offer you the chance to continue working with your message. This becomes useful when MacPGP returned an error because it didn't find a proper User ID for a recipient of your message. In these cases you don't want to lose the message you already edited and/or worked with, rather continue processing it and try to eliminate the causes of the error later.

•• Source = File

When the Source is File then the File Encrypt dialog is launched. See the File Encrypt section in the Application Menus chapter.

•• Destination = File

When the Destination is File then I ask you to supply me with a text file –through a standard Finder dialog– to save the processed message in. If you cancel the dialog, I do the same with your request.

•• Source = Microphone

This launches the Voice Encrypt dialog.

he To... button (disabled in this picture) allows you to specify the recipient(s) of the voice message —See Specifying Recipients later in this chapter. The voice message itself will be saved in a Macintosh file and PGP Encrypted using the PGP public key(s) of the recipient(s). Furthermore, the file can also be PGP Signed by yourself using a User ID you select from the popup menu of all your User IDs found in your secret keyring file.

The Voice Encrypt offers three voice qualities depending on whether or not you will use a Sound Encoder. If you don't use any Sound Encoder, the sound file will be a standard MacOS sound file. Such file can/will be played by the

recipient by double-clicking it (System 7.5 and later) or opening it with the SimpleSound application (System 7.5.2 and later).

The other options of the Sound Encoder, will only work with a Best voice quality. These encoders are those offered by the freeware RealAudio Encoder 2.0 <<http://www.realaudio.com/>>.

Once you select at least one recipient for the voice message, the Continue button will be enabled. Press it and the voice recording tool will activate.

When you finish recording your message, and pressing the Save button, MacPGP Control, will compress the sound file if you have specified a sound encoder, PGP Encrypt it with the recipient(s) public key, and finally open a Message Encrypt window and load the voice message file as an attachment.

Note: If you use one of the Real Audio Sound Encoders (Real Audio 14.4 or Real Audio 28.8) make sure that the recipient(s) of your voice message have the Real Audio Player 1.0 or 2.0. Here is a table that summarises all that:

If you use this Sound Encoder / Your recipient should have this software
None / No additional software required
Real Audio 14.4 / Real Audio Player 1.0 or Real Audio Player 2.0
Real Audio 28.8 / Real Audio Player 2.0

Both the Real Audio Encoder and Player are available as freeware (for the time being;-)

• Feedback


This is the bottom part of the screen consisting of one “diode,” a feedback zone that displays a message on:

1. state of readiness of the application,
2. current execution phase, or
3. result of the last requested action;

and an Iconify icon button (at the bottom rightmost part of the window).

ote: The diode will turn red when an error occurs during the execution of a command and no new messages will be displayed until (a) you clear the error, or (b) the window is re-activated. To activate the window just press your pointing device either on the window title bar or in any point within the window boundaries.

The main window also has a zoom box. When the zoom box is clicked the size shrinks to a more compact area thus using a minimal space for small screen users.

hen you press the Iconify button, the application window is reduced to just a titled icon which you can drag anywhere on your desktop. When MacPGP Control is iconified, all menus and menu items are disabled except: About MacPGP Control... under the  menu and Quit... under the File menu.

hen you click on the application icon in this iconified window, the application expands again to the last saved view of the main window and all menus and menu items become enabled again.

Specifying Recipients

Throughout MacPGP Control you will be asked to designate one or more recipient to carry out an operation. An example of such case is the Voice Encrypt dialog described above. Some other times, some options will only be enabled if there is one or more recipient selected. An example of this is the Encrypt button in the Sign / Encrypt dialog (Sign-Encrypt Messages chapter). In all these instances there will be a button –usually labelled To...– that will invoke the following dialog.

he dialog will show in the top left area, the name of the currently active keyring or addressbook at the time (see Addressbook Management chapter for what Addressbooks are). The picture above shows an Addressbook file. The scrollable area below this field lists the contents of selectable keys/recipients you will choose from. If the recipient is not available in the displayed list, you can choose another keyring or addressbook to lookup.

- [PGP Keys... button](#)

Pressing this button allows you to import information from either a PGP public keyring or an Addressbook file into the Keys listbox (the top scrollable area) for use as a source of possible recipients of your message. For details on what Addressbooks are, see the Addressbook Management chapter.

Note: MPGPC will always keep a list of the contents of the last selected file. When the dialog is invoked, MPGPC will check to see if the file has been modified since it was last scanned. If it was modified, then its name is displayed in Italics, otherwise it's in Plain. This is to visually alert you to the synchronisation-state between what you will see displayed in the Keys area and the actual contents of the file.

When you press the button you are asked to select a file through a standard choose file dialog. The choose file dialog used has a filter that will only show keyring and addressbook files, in addition of course to folders and volumes.

If you choose a PGP public keyring file, the Keys area will show the primary user-ids of valid (non-disabled) key certificates in the selected keyring file. A valid public key certificate is a PGP key packet followed by a Keyring Trust Packet whose bit #5 is not set. For more about this refer to the File Formats Used by PGP document included in the distribution of MacPGP.

The name of the keyring file you select, as well as its full pathname are then displayed in the file pathname non-editable field to the left of the button.

Note: You can halt this operation at any time by pressing the Command-period key combination.

If you select an Addressbook file, each line in the Keys area will show different information, depending on whether the line refers to a User or a Group nickname. For a User, the line will show:

1. The nickname you specified for the entry, followed by a colon and a space,
2. The PGP Key ID for this User, and
3. His/her email address.

For a Group nickname, the line will show:

1. The nickname you gave to the Group, followed by the colon and the space, and
2. A comma-separated list of the Users nicknames belonging to the Group.

- [Move button](#)

You move one or more keys from the top scrollable area to the lower one by: (a) selecting the entries and pressing the Move button, (b) drag and dropping the entries unto the lower scrollable area, or (c) double-clicking an entry in the top scrollable area.

When no entry is selected in the top area, the Move button is disabled.

- [Recipients area](#)

This is the lower scrollable listbox that will contain the list of the recipients for the message you are currently processing. If selected, a black 2-pixel frame is displayed around the box.

When selected, you can drag any line and move it to a new position in the box, thus modifying the order of the recipients. Also when a recipient's data is dragged into this box, a solid black line will be displayed showing you where the lines you are dragging will eventually be inserted.

To delete a recipient from the list of selected ones, either (a) select it and push the Trash icon button, (b) select it and drag it into the Trash icon, or (c) double-click it.

- [Manual entry field](#)

The editable field below the scrollable areas is there for manual entry of recipient key and email address. Using the right format is your responsibility; ie. MPGPC doesn't do any checks at this time on the syntax of your entry. Use the following syntax:

```
recipient-hex-key <recipient-email>
```

An example is:

```
0xE611BE29 <raif@FL.NET.AU>
```

As soon as you tab out of this field, its contents are added -if they are not already there- to the lower scrollable area, ie. the Recipients area.

- [Trash icon button](#)

The Trash icon is effectively a droppable button. In plain English this means that you can push the icon as you do with a normal push button when it's enabled, or you can drag and drop objects into it to delete them. The Trash icon in this dialog window becomes enabled when there is at least one entry selected in the lower scrollable area.

- [Help button](#)

The lower left icon toggles between showing and hiding balloon help. It's present in all MPGPC windows.