This is just the start of this section that a lot of testers have asked me to add to the dox. It will get expanded as we go along, based on (answerable) questions I receive from you.

Q1. What's the best way of using MPGPC with Eudora for reading and replying to PGP ciphered mail?

• With other scripts, you probably were going through these steps:

a. Open a message.
b. Seeing that's PGP ciphered you call a Decrypt script of some sort.
c. This Decrypt script, will decrypt the message and copy it to a new message in your Out mailbox. The original cipher will usually be put in Eudora's Trash mailbox.
d. After reading the message you decide on replying to the sender (next steps e through g) or just forget about this message so you move it to the Trash and that's it.
e. You choose the Reply… menu item in Eudora and proceed to do so.
f. When you finish editing your message, you invoke an Encrypt script of some sort.
g. The Encrypt script, encrypts your message and copy it to a new message in your Out mailbox.

• With MPGPC, the most effective way to deal with this scenario is the following:

In Eudora:
1. Select or open the message.

In MPGPC:
2. Select Eudora from the Source popup menu.
3. Select Eudora from the Destination popup menu.
4. Click the Decrypt-Verify button.

• If once you see the message in clear (with the proper attribution and with its paragraphs quoted), you decide not to reply, just click the Cancel button of the Encrypt Message window, and that's that.

• If you decide to edit and reply to the sender, you can go ahead and do just that. You'll notice that MPGPC has put in the Recepients list in the Encrypt Message window, the email address of Eudora's From field. More information on editing this and other fields in this window are in the Sign-Encrypt Messages chapter of this documentation.

Notes

1. MPGPC does not change the original location of the source message. It's left where it is, and up to you if you want to trash it, save it, frame it or just move it to a special location.
2. Replies generated by MPGPC are always placed at the end of the Out mailbox: where they should be if you want to send them.
3. Generated replies are either Saved in the Out mailbox or Queued there. You control this with an option in MPGPC Preferences.

Q2. I received an application with a detached certificate claiming the authenticity of its origin. How do I make sure that what I received is what was really sent?

• When this is the case, you will receive –among other files and douments– two files: a Target file, and a Signature file. The Signature file contains a PGP signature certificate made by the author/publisher of the application, of the Target file. This is similar to the case when you PGP sign a message, with these two distinctions:

a. The signature is in a separate file, and
b. The signature applies to a Macintosh file, instead of an email message.

• Usually –but not always– the Signature file:

a. Is of MacPGP document kind (column Kind in the Finder View by Name),

b. Has the same name as the Target file it applies to, ended with a .asc suffix.

When this is not the case a ReadMe file or similar is usually included in the distribution that tells (a) which is the Signature file, and (b) which is the Target one.

• Launch MPGPC, if you haven't done that already and:

1. Select File from the Source popup menu.
2. Select Clipboard from the Destination popup menu. Effectively you will not make use of this option but it's here just in case.
3. Click the Decrypt-Verify button. A choose file dialog will appear with a Select a file to Decrypt/Verify prompt.
4. Select the Signature file.
5. MPGPC will recognize that the Signature file is a MacPGP one and will signal this in its feedback field with the following message: This is a MacPGP file. Will tell MacPGP to process it… It then sends an open AppleEvent to MacPGP designating the selected file.
6. MacPGP will display a choose file dialog asking you to specify the Target file with a File signature applies to? prompt.
7. Select the Target file.
8. Provided that you already have the public key of the signer of the certificate, MacPGP will announce, in its usual way, the result of the operation in its window; ie. Good signature from user etc…

Note
If the Signature file is not a MacPGP document, you can proceed as before. The difference will be that MPGPC not recoginizing the Signature file to be a MacPGP document (because it does not have the right Type and Creator codes) will attempt to decrypt it in its usual way, which works perfectly. Only in the case when you cancel MacPGP select Target file dialog, will MPGPC display a dialog claiming a 30: Signature check error. You can safely discard this error and clear it.

Q3. Where does MPGPC save the clear Eudora messages it decrypts?

Nowhere! MPGPC does not keep copies of the decrypted messages unless you tell it do so (Destination = User Input). This is in sharp contrast to the Kit and other Eudora scripts I've seen. And why should it? Any time you want to read a PGP message, you decrypt it. With MPGPC it's a matter of 5 clicks:

1. Select the appropriate source in the Source popup menu. I'll assume it's File; ie. the PGP cipher is in a file on one of your mounted disks.
2. Select Clipboard in the Destination popup menu.
3. Click Decrypt-Verify button.
4. Select the source file which contains the PGP cipher in the choose file dialog that will appear.
5. MPGPC will decrypt the message. and inform you –if the operation was successful– that the result is now in the clipboard.
6. Choose the Show Clipboard… menu item under the Edit menu or click the Command-T key combo.

Note
MacPGP always discard the text that it finds before and after the PGP headers (the famous -----BEGIN PGP etc… and -----END PGP etc…). MPGPC saves these text portions before passing the message to MacPGP, and restore them to the returned clear message.

Q4. How can I use MPGPC as a MIME helper application?

The following is a step-by-step cookbook for setting MPGPC as a MacWEB (ver. 1.x) helper application based on Chris Garrigues's suggestions.

1 Start up MacWEB.
2. Select Helpers… under the Edit menu.
3. Click on New.
4. Define a MIME Type of application/x-pgp and click on More Choices.
5. Click on the upper Select button and select any MacPGP Public Keyring file.
6. Click on the lower Select button and select MPGPC.
7. Clear the Don't Launch button.
8. Click on OK.
9. Repeat steps 3-8 with a MIME Type of text/x-pgp and using an existing *.asc file.
10. Click on OK again.
11. Selected Suffixes… from the Edit menu and define the obvious mappings from *.asc and *.pgp to text/x-pgp and application/x-pgp. (This would matter if you were pulling these off of an FTP site).
12. In MPGPC select the Decrypt/Verify behaviour by clicking on the area behind the Decrypt-Verify button.

From then on, if while browsing with MacWEB you click on the link to somebody's key, MPGPC is launched and it will ask you if you want to add the key to your public keyring; clicking on a public keyring URL allows you to browse its contents with MPGPC's keyring management window.

Similar thing can be done to Netscape and IC Config Preferences file. The following describes how it's done in IC Config, adapted from a post from Simon Saubern <s.saubern@chem.csiro.au>:

1. Launch IC Config. and push the File Mappings button.
2. Create 2 new Mapping Entries that look like the following:

his will map all received files ending with a .asc extension to MacPGP asciified text files. The next mapping, will

manage the 2 cases where the file with a .pgp extension is a keyring file OR consists of normal PGP cipher data. This is done by entering Cryp as the file type. MacPGP is robust enough to recognise, when processing the file, whether it's a keyring or not.

ote

If you wish to process, directly in MacPGP Control, keyring files you receive through Internet Clients that make use of the IC Preferences (Anarchie, Fetch, etc…), the previous mapping is insufficient. This is due to the fact that MacPGP Control decides on how to treat the file according to it's Macintosh type, contrary to MacPGP which scans the file and, based on its contents, decide what it is and what to do with it. If this is the case, replace the Cryp file type with PKey. MacPGP Control will then open a keyring management window for the downloaded file as soon as it's given control by the Internet Client application.

Once you OK the 2 file mappings described above, they will appear in the list (hereafter sorted by Application).

. Last, create a new entry in the Helpers list that will indicate where is MacPGP Control on your disks: