Overview

Warning
Although care has been taken in coding the functionalities offered by MacPGP Control with regard to keyring manipulation, User is strongly recommended to keep up-to-date backup copies of his/her public and secret keyring files. Please report any anomalies you find while using this code to the author. TIA.

The Keyring management is invoked when a PGP public keyring file is opened by selecting it from the Open… dialog. A window similar to the following will be displayed:

ote: Depending on the available RAM you have, you can open more than one Keyring file at a time.

The window is divided into two main areas separated by a 3D-look line. The top area deals with the keyring as a whole, while the bottom one addresses User ID and key owner issues. The bulk of the second area is occupied by the Keys Table with four labelled columns: Key ID, V, T, and User ID.

Before going through the action of each button, I should explain the conventions used to display the Keys Table (the scrollable area in the centre).

First of all, the table will display information on the keys found in the selected keyring file. The User ID string itself being that of the first one (primary) that comes after a Public Key Certificate in a Public Key Packet, will be shown in the column labelled User ID.

The first column in the table, labelled Key ID will display the 8-character code that PGP assigns to the key.

The second column labelled V (for Validity) will indicate whether the key is Enabled (valid) or Disabled (invalid). According to the MacPGP documentation, it's Bit 5 of the Trust Flag Byte of the Keyring Trust Packet following a key packet which will tell us that. When a • appears in this column, the key is Disabled. Otherwise, when the key is valid, the column is left blank.

The third column labelled T will visually indicate the Trust value we (proprietor of the keyring) associate to the owner of the key with all of its User IDs. The MacPGP documentation calls this information OWNERTRUST Bits and defines six valid possibilities for their values. Here is how MacPGP Control interprets them:

1. "Undefined, or unintialized trust (000)" is displayed as a blank,
2. "Unknown, we don't know the owner of this key (001)" is displayed as "?"
3. "We usually do not trust this key owner to sign other keys (010)" is displayed as "X"
4. "We usually do trust this key owner to sign other keys (101)" is displayed as "√"
5. "We always trust this key owner to sign other keys (110)" is displayed as "•"
6. "This key is also present in the secret keyring (111)" is displayed as "U" for ultimate.

Keyring file related actions

• Make @Book…

When you press this button, a new Addressbook file will be created and its contents built by default from those of the current Keyring file. For more information on Addressbooks refer to the next chapter Addressbook Management.

This is currently the only way you can create new Addressbooks.

Note: Once you select a public keyring file and MacPGP Control is going through its contents, you can halt the operation by pressing the Command-period key combination.

• More…

Pressing this button invokes the PGP® Dataskope environment. For more detail on what this environment does read • PGP® Dataskope in the chapter entitled Application Menus.

• Warn Only checkbox

Check this box to force MPGPC into setting the WARNONLY bit of all user IDs in this keyring file. When this bit is set, you will not be asked whether or not you want to use this key, when it's not fully certified.

• Add multi-choice button

The Add button allows you to add keys to the selected keyring. You can add these keys from data either present in the clipboard, or saved in a text file. You specify the source with the popup menu that will appear when you press the button.

If you select Add from File, a standard choose file (similar to the following) allows to specify the source.

- Clean Up button

This button forces MacPGP to execute a maintenance path. Basically a maintenance pass is a Check key and signature certificates for all the keys in the keyring file. I suggest you use it before exiting if you have added, removed and/or edited keys.

Key and User ID related actions

Once you make a selection inside the Keys Table, all the buttons become enabled.

he Help icon/button shows/hides the balloon helps while the Trash icon/button is used as either a Remove button, or a drag-drop destination for User IDs removal from the table.

• Edit… button

This button will allow you to edit the Trust value you have in the key owner of the key associated with the selected User ID (see earlier in this chapter about the meaning of the Trust value).

The action that follows pushing this key depends on whether you are selecting one of your user IDs or not. If the selected user ID is the keyring owner (you), I call directly MacPGP to handle the editing. This is so because in such case you can edit your own pass phrase and there is no way I can (or want to) do that.

On the other hand, if the selected User ID is not one of the keyring owner, you will be presented with the following dialog:

f you cancel the dialog, all is well; nothing happens. But if you press the OK button, I take whatever is selected in the popup menu and use it as the new Trust value.

The popup menu offers you four choices:

1. I don't know the owner of this key, equivalent to a (001) OWNERTRUST bits,
2. I usually don't trust this key owner to sign other leys, equivalent to a (010) OWNERTRUST bits,
3. I usually trust this key owner to sign other keys, equivalent to a (101) OWNERTRUST bits, and
4. I always trust this key owner to sign other keys, equivalent to a (110) OWNERTRUST bits.

Also, when you OK this dialog, the keyring file is updated and the table will show the –eventually– new value of the Trust factor.

Note: Because MacPGP Control edits the Trust byte in the keyring file directly without any call to MacPGP, before returning control to you, a Check is forced by an "execute pgp -kc …" Apple Event on the selected User ID to ensure the sanity of the operation.

• Enable/Disable button

This button will be titled Enable if the key associated to the selected User ID is disabled (has a • displayed in the second column), and Disable otherwise. All it does is that it toggles the value of Bit 5 of the keyring trust packet of the key packet associated with the selected User ID.

Again, the action carried out by MacPGP Control is direct on the keyring file.

• Extract… button

This button allows you to export a key packet to an ascii armored text file. When pushed, you will be presented with a standard new file dialog with a default name. The default name is the first word of the selected User ID followed by the suffix .kc You are at liberty to change the name of this file but…

ote: The final name of the output file, will have the suffix .asc appended to it, and its Finder icon changed to that of a MacPGP TEXT file.

• Check button

The Check button allows you to PGP check a key and its certifying signatures.

• Certify button

The Certify button allows you to certify a key with your own secret key. You specify your own user ID to use for certification in the popup menu that will appear when you press the button.

• Fingerprint button

Pushing this button instructs MacPGP to report the key fingerprint for the public key associated with the selected Key. Because I use the Key ID itself, I always get a fingerprint, if there is one valid…

The key fingerprint, when one is found, is returned in the field to the right of the button.

Note: Although it looks like you can edit the fingerprint field, you'll soon discover that it's not allowed. The field can only be copied (to the clipboard) for pasting in other applications.

- Update button

Pushing this button will instruct MPGPC to start a TCP/IP connection to a BAL-lookup-command-conformant keyserver and download the extracted key data and then proceed to adding this key to the keyring displayed in this window. This insures that the latest copy of the requested key is included in the keyring file, provided of course that the key owner has already uploaded his/her key to a PGP keyserver.

- Trash-icon button

This button allows you to remove a whole key with all of its associated User IDs, signatures and other from the keyring. Press it when a User ID line is selected in the table or drag the table line and drop it on the icon to delete this User ID from the keyring file.