acPGP Control — MPGPC

version 1.0b3
Last updated: February-96

Author: Raïf S. Naffah <raif@FL.NET.AU>

Overview

MacPGP Control (or MPGPC for short) is an AppleScript® application that offers an easy-to-use, more Macintosh® friendly user interface to Philip Zimmermann's PGP software —MacPGP®.

MacPGP Control is cryptographically neutral. It relies on your AppleScript-aware version of MacPGP to perform encryption and decryption. It is thus perfectly legal to use inside, as well as outside, the USA. For information on how to obtain MacPGP in the USA or Canada, first refer to the file <ftp://ftp.netcom.com/pub/dd/ddt/crypto/crypto_info/where> using your FTP client (Anarchie, Fetch, etc…) or a World Wide Web browser (Netscape, MacWeb, etc…). For non-USA citizens, information on how to obtain MacPGP is available at Ståle Schumacher's International PGP Home Page <http://www.ifi.uio.no/~staalesc/PGP/>.

If you require human assistance on using the PGP software (not MacPGP Control), send e-mail to <mailto:pgp-help-humans@hks.net>. For MacPGP Control problems, questions, etc… send e-mail to me <mailto:raif@fl.net.au>.

The main features of MPGPC are:

• MacPGP related features

+ Compatible with all known scriptable versions of MacPGP including the MIT versions and the MacPGP 2.6.3i.
+ Keypair generation of any allowed (by MacPGP) length up to 2048-bit.
+ Update of PGP public key information of user keyring members through TCP/IP connection.
+ Definition and use of nicknames for Users and Groups recipients.
+ More user control for keyring related actions, through a true Macintosh Human Interface and —in some cases— direct manipulation of keyring file data, including: editing trust flag byte, enabling/disabling, extracting, checking, certifying, fingerprinting, and forcing Warn-Only bits.
+ More user control for PGP and conventionally encrypting text and binary files. When PGP encrypting file, users can designate more than one recipient.
+ Secure clean clear-signed PGP ciphers, through the implementation of features such as: expanding tabs, transliterating non-USASCII characters, and word-wrapping lines before processing and handing over to email application.
+ Viewing of PGP packets for educational and debugging purposes.
+ Opaque signing (asciified clear-signed text)
+ Transparent use of user's UserIDs found in his/her secret keyring file.
+ Encryption for multiple recipients.
+ Generates Key Revocation Certificates.

• Eudora™ related features

+ Allows working with more than one message at a time.
+ When replying, quotes initial message paragraphs using Eudora's quote string.
+ When replying, generates attribution message as defined in Eudora.
+ Supports Attachment(s) to message. Attachments are treated in the same way as the message; ie. PGP Encrypted, etc…
+ Supports drag-and-drop Finder files to Attachments listbox.
+ Supports latest Eudora versions (2.1.4 and 1.5.4).
+ Supports Eudora versions (2.1.3/1.5.3) known to break certain scripts.
+ User-configurable Auto Move PGP messages to designated mailbox.
+ User-configurable Auto Decrypt source data before processing.

• Macintosh related features

+ Encryption of voice messages recorded by Mac sound input devices.
+ Easy to use, point-and-click Macintosh User Interface.
+ Extensive support of drag-and-drop.
+ Documented handlers calls for use by other scriptors.

The latest version of MacPGP Control (MPGPC) can be found on:

1. <http://www.deepeddy.com/pgp/> thanks to the kind generousity of Chris Garrigues (DeepEddy)
2. <http://www.ifi.uio.no/~staalesc/PGP/utils.shtml>
   specifically at <ftp://ftp.ifi.uio.no/pub/pgp/mac/>
3. <ftp://ftp.dsi.unimi.it/pub/security/crypt/code/>
4. <ftp://gaea.scriptweb.com/pub/applescript/addons/>

Because I don't have full control on the final name of the distribution at the last three sites, you should always look for a file name that refers to MacPGP_Control, MacPGPControl, MacPGP-Control or MPGPC.

MPGPC assumes you are using Eudora –either the commercial Eudora Pro, or the freeware Eudora Light version– as your email application, that you have the public-domain Internet Config software installed on your system, and that you are connected to the Net through a TCP/IP connection with no firewalls. If any or all of these assumptions is false, MPGPC can still deliver an efficient, easy-to-use true Mac interface to MacPGP.

I chose to support Eudora because (a) I use it myself, (b) it's scriptable, and (c) Qualcom, Inc. (publishers of Eudora) promises to make available a freeware version of their product in addition to the commercial one. If in the future any ot the last two reasons ceases to be true, I will re-write MPGPC.

Eudora can be found on:

<ftp://ftp.qualcomm.com/quest/mac/eudora/>.

MPGPC's support for IC (Internet Config), although currently at a minimum level, is a strategic decision. I believe the concept of the IC Preferences file and shared management of Internet related settings among Mac applications will prevail. I also believe that the proposed scheme as implemented by Quinn (the eskimo) and Peter N. Lewis -authors of IC– is broad and comprehensive enough to enroll the active support of all major software publishers sooner or later. The facts that (a) IC was placed in the public domain, and (b) its authors are attentive enough to requests for inclusion of additional general preferences –as opposed to application specific which are already possible- in the structure of the Preferences file, add to the chances of success for the IC Preferences concept.

Internet Config (or IC Config) can be found on all major archives. Here are two URLs for it:

(Australia) <ftp://redback.cs.uwa.edu.au/Others/Quinn/Config/>,
(USA) <ftp://ftp.share.com/pub/internet-configuration/>.

MacPGP Control was developed in AppleScript English dialect, with FaceSpan® 2.0.1. It is packaged as a mini-application and hence requires that you have the FaceSpan Extension 2.0.1 in your Extensions folder. You can download the FaceSpan extension from SDU site. The URLs are:

<http://facespan.sdu.com/FaceSpanDemo/FaceSpanExtension_sea.hqx>
<ftp://duke.bwh.harvard.edu//pub/adam/mcip/FS201Ext.hqx> or
<http://www.deepeddy.com/pgp/FS201.sit>

Because MPGPC was written in AppleScript using FaceSpan as the interface builder, it is itself scriptable. A detailed list of calls and parameters available for scriptors is detailed in the chapter: Technical Aspects.

Starting from version B3, MacPGP Control now supports voice mesage handling as either standalone files or as attachments to messages to be sent with Eudora. Voice encoding into data files is done with:

1. The standard built-in Macintosh MACE encoder, or
2. Real Audio Encoder 2.0 (freeware available from <http://www.realaudio.com/>) that seems to use a variation of the GSM voice encoding technology. More on that in the next chapter: First Time Users.

Acknowledgements

First of all I'd like to express my acknowledgements to Gregory S. Combs who encouraged me to publish this software. I wish him courage to finish the MacPGP Kit 2.0 as soon as he is able to.

Big thanks for Adam Shostack for offering his ftp site as the MacPGP Control distribution home, while he was able to. Thanks to Chris Garrigues whose WWW site now hosts the MPGPC distribution and its Web Page. My thanks go to the following MCIP mailing list members and others who helped shape this code and its manual into something reliable and useful, with their relentless testing, positive critiques and helpful suggestions:

• Jack Repenning <jackr@dblues.engr.sgi.com>,
• Björn E. Andersson <bea@algonet.se>,
• Michel Eytan <eytan@dpt-info.u-strasbg.fr>,
• Amos Elberg <aelberg@MAIL.WESLEYAN.EDU>,
• Kristopher K. Barrett <kbarrett@teleport.com>,
• Michael R. Schuppenhauer <schuppenhauer@tech.chem.ethz.ch>,
• Carl B. Constantine <cconstan@PINC.COM>,
• Andrew Poulos <nextinln@mpx.com.au> and Wayne K. Walrath <Acme@kagi.com> for their suggestions on the user interface,
• Brian A. LaMacchia <bal@martigny.ai.mit.edu> for help on implementing the HTTP interaction with his (BAL) keyserver.

My gratitude goes also to the following generous developers and copyright owners. Without their excellent osaxen, this software wouldn't have seen the light in such a short time:

• Gregory T. Quinn, for his Add Resource, Extract Resource, Object Database and Record Sound To osaxen (part of the GTQ Scripting Library 1.2. Note #1),
• Wayne K. Walrath, for his Balloon Help osax (part of ACME Script Widgets 2.5. Note #2),
• Atul Butte, for his TCP/IP Scripting Addition (note #3).

Thanks also to Steve Dorner (author of Eudora) and Qualcom, Inc. (publishers of Eudora) for allowing me to include the 1…1 Transliteration Table data, and to use similar icons to Eudora's in MPGPC message encrypt windows.

Finally, thanks to Toni Childs, Peter Gabriel, Pink Floyd, Supertramp, Jean Michel Jarre and Mozart. Their Art soothed the long white solitary nights I spent putting together this tool.

Notes

1. GTQ Scripting Library: The Add Resource, Extract Resource, Object Database and Record Sound To are part of the v. 1.2 GTQScriptingLibrary1.2 copyright 1994 Gregory T. Quinn. The latest and full set of the library can be found on all major archives.

2. ACME Script Widgets: The Balloon Help Scripting Addition copyright 1994-95 Wayne K. Walrath included in MPGPC is a demo version. The latest commercial and indeed the full set of the ACME Script Widgets can be ordered by email to: <Acme@kagi.com (Wayne K. Walrath)>

3. Mango Tree Software: The TCP/IP Scripting Addition osax included in MPGPC is the unregistered 1.1.2 version. The full commercial version and information on how to order it can be obtained by: <mailto:atul@netcom.com (Atul Butte)> or <http://www.mangotree.com/biz/mango>.

How to Use this Manual

This manual is prepared with the Manual Maker freeware software copyright James W. Walker <JWWalker@aol.com>.

To view the manual contents on your screen as the author intended, you need to have the Geneva font installed. Colour is a plus albeit not necessary.

The MPGPC Manual is divided into 11 chapters:

- Introduction (this one),
- First Time Users,
- User Interface,
- Application Menus,
- Sign-Encrypt Messages,
- Keyring Management,
- Addressbook Management,
- Legal Aspects,
- Version History,
- Technical aspects, and
- Tips and How To?

You can print the manual by first saving its chapters to SimpleText™ and printing them from there.

The headers and subheaders in this manual follow these rules:

1. A chapter name is accessible from the Chapter menu of the MPGPC Manual application.
2. Main Sections in each chapter are in Green Geneva-10 Bold.
3. First level sub-sections have their text preceded by one bullet sign (•) and are in Blue Geneva-9 Bold.
4. Second level sub-sections have their text preceded by two bullet signs (••) and are in Cyan Geneva-9 Bold.
5. Sections and both levels sub-sections appear under the Section menu of the MPGPC manual application.
6. Notes have a header that is in Red Geneva-9 Bold.
7. Keywords, screen areas, and graphical elements when referenced are in either Black or Gray Geneva-9 Bold.
8. The body of the text is in Black Geneva-9 Plain.

Conventions Used in the Software

- Cursors

n addition to the standard Macintosh cursors (pointing arrow and I-beam), MacPGP Control uses the following cursors in special circumstances:

•• Pointing Finger

When a background area is clickable the cursor becomes a Pointing Finger when within the bounds of the area. It reverts to its standard shape when it moves outside these bounds.

•• Magnifying Glass

When an area beneath the cursor is clickable and clicking it will reveal other information in another area, the cursor becomes a magnifying glass when it's located within the bounds of such area. It reverts to its standard shape when it leaves these bounds.

•• Multi-choice Button

MacPGP Control uses a new type of push buttons. These buttons have multiple choices that are revealed –in a popup menu– when you press the button. The action the button will execute will be the selection you make in the revealed popup menu. Externally these buttons have a right hand pointing gray arrow similar to what the Mac uses for hierarchical menus.

When the cursor is positioned above a multi-choice button, the cursor changes to a Multi-choice Button cursor, and reverts to its standard shape elsewhere.

•• Cross

In a multi-line table, the cursor changes to a Cross. When a selection is made inside a table and the table is draggable, the cursor changes to an Arrow when positioned above the selection. Otherwise, it remains as a Cross until it exits the table area.

•• Spinning Ball

Also called the Beach Ball cursor. When MacPGP Control is busy waiting for an internal operation to conclude, it displays the Spinning Ball cursor. As soon as user interaction is active again, the cursor reverts to its standard shape.

•• Watch

Also called the Busy cursor. When MacPGP Control is waiting for a reply from another application it told to execute an AppleEvent, the cursor changes to a Watch. When control is given back to MacPGP Control, the cursor reverts to its standard shape.

• Icon Buttons

MacPGP Control uses buttons that sometimes do not look like the normal or 3D-look buttons. These icon buttons are used in a consistent fashion throughout MacPGP Control to allow specific actions.

ome of these buttons are also droppable, that is you can drag objects and drop them onto their graphical representation. If the object is of a class the button is supposed to operate on, then the same action as clicking them will occur.

•• Encrypt Sign button

When pressed, invokes the Sign-Encrypt menu item under the Service menu. This button is droppable.

•• Decrypt Verify button

When pressed, invokes the Decrypt-Verify menu item under the Service menu. This button is droppable.

•• Trash icon button

It becomes enabled only when an object it can operate on is selected. When pressed, it deletes/removes the selected object(s). This button is droppable.

•• Trash full icon

This is not really a button. It's in fact the same previous button but it changes to this shape while you're dragging an object over it. It switches back to the Trash icon shape when you're outside the icon's bounds or when you release the object(s) you were dragging.

•• Balloon On/Off button

This button when pressed toggles between showing and hiding the balloon help associated with MacPGP Control window items. It's often referred to in the documentation as the Help button.

•• Record Voice icon button

Pressing this button will invoke the Voice Encrypt dialog.

• Icon Checkboxes

MacPGP Control uses some checkboxes that do not look like the normal or 3D-look checkboxes. Again these elements are used in a consistent fashion throughout MacPGP Control and indicate specific states. All of these icon checkboxes reflect the status of global properties used throughout MacPGP Control.

•• PGP Sign checkbox

When checked indicates that the information (message, attachments) should be PGP Signed. As a matter of course, a popup menu to the right of this checkbox will become visible and/or enabled to allow you selection of a User-ID to use.

•• Expand Tabs checkbox

When checked indicates that any Tab character in the message being processed for output should have all its tab characters replaced with spaces. A popup menu to the right of this checkbox when and where it's present in a window, allows you to specify how many space characters should be substituted for each Tab.

•• Transliterate checkbox

When checked indicates that non-USASCII characters found in the message to process should be replaced by USASCII ones. A popup menu which becomes enabled when and where this checkbox is present and checked, allows you to select which transliteration table to use.

•• Word Wrap checkbox

When checked indicates that the message will be word-wrapped before processing.

•• Include Clear Signature checkbox

When checked indicates that MacPGP Control is to include your clear signature from the IC Config Preferences file, if such file is present.