Legal

MailPGP is provided on an "AS IS" basis, without warranty of any kind. The author is not responsible for any possible damage that using this software might cause. Use at your own risk.

MailPGP is freeware and must be available to everyone without cost.

Files

Files included in archive:

MailPGP.exe	the program file
mailpgp.sig	an isolated signature certificate file for MailPGP.exe
mailpgp.hlp	help file
mailpgp.cnt	help contents file
mailhlp.sig	an isolated signature certificate file for mailpgp.hlp
samit.asc	my public key
setup.exe	install program
setup.sig	an isolated signature certificate file for setup.exe
unmailpg.exe	uninstall program
unmailpg.sig	an isolated signature certificate file for unmailpg.exe

If the archive does not contain all these files, please report me.

If you want to be sure that **MailPGP.exe**, **mailpgp.hlp**, **setup.exe** and **unmailpg.exe** have not been modified by anyone else but me, use PGP to verify the signature certificate files.

For **mailpgp.exe**:

Type ”`pgp mailpgp.sig mailpgp.exe`“ while in the DOS prompt. You should get a result similar to following:

```
File has signature.  Public key is required to check signature.

File 'mailpgp.sig' has signature, but with no text.
Text is assumed to be in file 'mailpgp.exe'.
.
Good signature from user "Sami Tolvanen <sami.tolvanen@iki.fi>".
```

Repeat the procedure for other files and their signature certificates.

If you get a bad signature, the file has been modified. After you have scanned the files for viruses, report me where you downloaded the archive (so that I can try it myself) and download the original archive at MailPGP Home page.

Introduction

MailPGP is an advanced, yet fast and easy-to-use Windows user interface for Philip Zimmermann's Pretty Good Privacy (PGP).

MailPGP conveniently integrates PGP with every program that uses the clipboard and does not require any space from the screen since the window can be minimized to the taskbar notification area. PGP is run on the background and the DOS window is shown only if necessary.

You can encrypt, decrypt and sign messages on the clipboard just by clicking the taskbar icon. The most important key management functions are located on a pop-up menu. You can also easily encrypt and decrypt files by choosing them from a file dialog, or just by dragging and dropping one to the program window.

New in this version

New features in MailPGP 1.3:

- Help file in Windows Help format
- Install & uninstall programs.
- Drag and drop files from explorer to MailPGP’s dialog
- Option to define a default directory for file operations
- Option to quote decrypted messages.
- Option to remove the signature from a signed message when checking it.
- Option to encrypt to multiple recipients
- Option to define a hot key for the default procedure (when the dialog is hidden)
- Now PGP can be set to use English, Spanish, French, German and Finnish and the user IDs will still be read properly.
- Option to use shorter DOS file names when encrypting a file.
- Option to remove all extra lines, e.g. "Charset:", from PGP signature when clear signing
- Option not to show the user ID menu on the main dialog
- Signature verifying results, key fingerprints and key signatures are shown on a dialog instead of showing them in a DOS window
- Option to copy key fingerprint to the clipboard
- Key management functions added to the taskbar pop-up menu
- Now you can choose multiple files in the “File Encrypt/Decrypt” and “File wipe and delete” dialog
- Larger text on toolbar buttons
- Option to manually add a public key from clipboard to key ring
- Several bug fixes

Configuring Pretty Good Privacy (PGP)

MailPGP requires PGP 2.6.x or newer properly installed to your system. You can obtain Pretty Good Privacy e.g. from the International PGP Home Page. If you live in the USA, you should use the version available from MIT.

Complete instructions are included with PGP.

Windows 95:

Add the following lines to your "autoexec.bat":

```
SET PGPPATH=C:\PGP
SET PATH=C:\PGP;%PATH%
```

(Replace "C:\PGP" with the directory where you copied the PGP files)

You also have to add time zone information to "autoexec.bat"; see instructions that are more precise from "setup.doc" that came with PGP.

For example,

Finland:	`SET TZ=EET-2DST`
Los Angeles:	`SET TZ=PST8PDT`
Denver:	`SET TZ=MST7MDT`
Arizona:	`SET TZ=MST7`
Chicago:	`SET TZ=CST6CDT`
New York:	`SET TZ=EST5EDT`
London:	`SET TZ=GMT0BST`
Amsterdam:	`SET TZ=MET-1DST`
Moscow:	`SET TZ=MSK-3MSD`
Aukland:	`SET TZ=NZT-12DST`

Windows NT 4.0:

Open "System" from the "Control Panel", select "Environment" and add the environment variables to the "System Variables" section.

Please notice that PGP language should be set to English, Spanish, French, German or Finnish (make sure that "config.txt" (came with PGP) contains the following setting: "`Language= [en|es|fr|de|fi]`". E.g. to set PGP to use English, use "`Language=en`"). Language modules are available at the International PGP Home Page.

Using MailPGP

Installation

All the installation needed is to configure PGP and run **setup.exe**. You can uninstall MailPGP normally via Control Panel|Add/remove programs.

Using MailPGP

Generating your own PGP key pair

If you are new to PGP and do not already have a key pair, you will have to create one. Start MailPGP, click the right mouse button, select "Key management|Generate a new key" from the pop-up menu and follow the instructions.

Notice! If you want MailPGP to use a specific user ID for signing messages (and extracting a public key) without you needing to select it every time, type in or select the desired user ID and select "Set default user ID" from the pop-up menu.

See the PGP documentation for more information on the other available key management functions.

Adding keys to your public key ring

To add your friends' public keys to your key ring, copy the key to the clipboard and select "Key management|Add public key" from the pop-up menu. If MailPGP finds a PGP key from the clipboard, it will add it to your key ring.

New! Now you can also drag and drop the key file to MailPGP's dialog and it will be automatically added to your key ring. The file extension must be '.asc', i.e. the file name could be e.g. **mykey.asc**. You can try this by adding my public key to your key ring, just drag and drop **samit.asc** to MailPGP's dialog.

Notice! MailPGP searches the clipboard for PGP keys every time you choose to "Encrypt", "Encrypt and sign", "Decrypt" or "Clear sign" a message. If it finds a key, you will be prompted for actions; click "Yes" if you want to add the key to your key ring, "No" if you want to continue with the selected procedure and "Cancel" to stop the procedure. This feature can be turned off by selecting "Ignore keys".

Extracting your public key to clipboard

To extract your public key from the key ring for sending it to your friends, select "Key management|Extract public key" from the pop-up menu. If you have not set a default user ID, you will have to select the user whose public key you want to extract to the clipboard. After MailPGP has finished, you can simply paste the key to your e-mail.

Encrypting and/or signing a message

If MailPGP is visible:

Copy the desired text to clipboard, choose the recipient from the user ID menu and click the "Encrypt" button. MailPGP runs PGP and copies the encrypted message to clipboard. If you also want to sign the message, click the "Encrypt and sign" button instead.

If you only want to sign a message, click the "Clear sign" button.

If MailPGP is hidden (i.e. minimized to the taskbar notification area):

Select the desired procedure from the pop-up menu. You can select a default procedure (performed when you left click the taskbar icon) from the options dialog. This allows you e.g. to clear sign a message just by clicking the taskbar icon.

Verifying a signature

If MailPGP is visible:

Copy the message to clipboard and click the "Clear sign / Check signature" button.

If MailPGP is hidden:

After you have copied the message to clipboard, select "Clear sign" from the pop-up menu. If you have set it as the default procedure, you will only have to left click the taskbar icon.

Decrypting a message

If MailPGP is visible:

Copy the encrypted message to clipboard and click the "Decrypt" button. The plain text message will be copied to clipboard.

If MailPGP is hidden:

After you have copied the encrypted text to clipboard, you can just left click the taskbar icon to decrypt it. MailPGP recognizes the message type and automatically decrypts it to the clipboard.

Encrypting and decrypting a file

To encrypt a file, click the “File Encrypt” button. A dialog will appear that allows you to choose a file. After you have chosen a file and clicked “OK”, you will be prompted for the recipient. If you have selected to use conventional encryption, user ID is not required. To decrypt a file, click “File Decrypt”. The original file will not be deleted.

New! You can also drag and drop a file to MailPGP’s dialog to encrypt or decrypt it. If the file extension is ‘.pgp’ or ‘.asc’, it will be decrypted (’ .asc’ files will be also searched for keys), otherwise the file will be encrypted to a desired recipient.

Please notice that MailPGP wipes all the created files before deleting them.

"Wipe and delete a file” (on the pop-up menu) deletes a file securely.

Problems?

If you have a question regarding PGP or its functions, please read the PGP documentation at the International PGP Home Page before sending me e-mail. Also, be sure to check out the FAQ.

If you are having problems with MailPGP, feel free to e-mail me, I will help if I can.

The available functions

Pop-up menu	Description
Wipe and delete a file	Overwrites (three times) with pseudo-random data and removes a file leaving no trace of it on the disk. Please notice that the content of the wiped file cannot be restored. This function is similar to the one in PGP.
View clipboard	Executes **clipbrd.exe.**
Empty clipboard	Clears all clipboard data.
Key Management	
Extract public key	Extracts user's public key to clipboard. If you have not specified a default user ID, make sure you have selected a user ID.
Add public key	Adds public key to key ring from clipboard.
Generate a new key	Generates a new PGP public/secret key pair.
Remove key/user ID	Removes a public and/or secret key from key ring. If the selected key has multiple user IDs, you can also only remove one of them. Make sure you have selected a user ID.
Revoke/disable/enable key	Disables/enables a key from your key ring.
Sign a public key	Signs the selected user’s key.
Edit trust/pass phrase/user ID	Edits the trust parameters you have set to the selected user’s key or change the pass phrase for a secret key. You can also add another user ID to your keys with this command.
View key fingerprint	Shows the fingerprint of the selected key.
View key signatures	Shows signatures of the selected key.
Re-read user IDs	Reads your public key ring again. Available only if you have selected to read user IDs.
Set default user ID	Sets the default user ID. The default user ID will be used for signing messages and extracting a public key if no other user ID has been specified. Set your own user ID as the default user ID. If you want to use the user ID currently selected in the user ID menu, click “Yes”, if you want to select another user ID, click “No”.
About	Shows program information.

System menu (right click the toolbar icon)	
Help	Shows this file.
Reset Pass Phrase	Removes your pass phrase from the memory. (Available only if "Save Pass Phrase in memory" is selected and your pass phrase is saved)

Options dialog

Encryption

ASCII armor encrypted files	Uses ASCII (-a) switch when encrypting files. If you use this option, you can e.g. easily send an encrypted text or binary file via e-mail.
Use conventional encryption for files (only IDEA)	Uses only IDEA to encrypt a file. Requires that you set a password for a file.
Copy ASCII armored files to clipboard	If you select this option, all the files you encrypt using the ASCII option will be copied to clipboard. As default, this option is selected.
Use short file names (DOS)	Converts long file names to shorter DOS file names so that DOS PGP can handle them. E.g. "C:\Program Files\plaintext message.txt" to "C:\Progra~1\plaint~1.txt". If you are using the Win32 compilation of PGP, you do not have to use this option. As default, this option is selected.
Word wrap encrypted messages	Automatically word wraps messages at column 75.
Encrypt also to default user (if available)	If you have set a default user ID, by selecting this, MailPGP will encrypt all messages also to the default user.
Pause after encrypt	Pauses PGP screen after encrypting so that you can see what happened.

Decryption and keys

Restore original filename	Restores the original filename when decrypting a file. As default, this option is selected.
Quote decrypted text with	If you select this, the decrypted message will be quoted with the selected quotation mark.
Pause after decrypt	Pauses PGP screen after decrypting so that you can see what happened.
Ignore keys	Select this if you want MailPGP to ignore PGP public keys it finds from the clipboard.
Read user IDs	Reads your public key ring on startup. MailPGP saves the key ring contents to "pubring.txt" so that the next time you start MailPGP, it does not have to run PGP. If you want to update the user ID menu, select "Key management|Re-read user IDs" from the pop-up menu.
Only names	If you select this, only names will be shown in user ID menu.

Signing

Word wrap signed messages	Automatically wraps signed messages at defined length to prevent other people from getting bad signatures when reading e.g. with a newsreader that wraps long lines. As default, this option is selected and length is set to 65 characters.
When checking a signed message, ... the signature	When checking a signature, you can choose whether you want MailPGP to leave it to the signed message or to remove it.
Ignore signatures	If you select this, MailPGP clear signs a signed message instead of verifying its signature.
Use comment	If you select this, MailPGP will add a comment to your clear-signed messages (CS). You can type in the desired comment to the text field. If you select this option but leave the text field empty, MailPGP

		uses "MailPGP 1.3" as comment text.
		Do not use quotation marks in the comment text.
		Notice! Because DOS limits command line length to 128 characters, comments that are over 100 characters long usually do not work.
	Remove extra lines from signature	Removes all extra lines from PGP signature when clear signing. Leaves only "Version:" and "Comment:" (if selected).
Display		
	Start MailPGP on Windows startup	If you select this, MailPGP will be run every time you start Windows.
	Hide MailPGP on startup (only taskbar icon)	If you select this, MailPGP will start minimized to the taskbar notification area.
	Show user ID menu	If you select this, the user ID menu will be shown on the main dialog. If you prefer smaller dialog, do not select this option.
		As default, this option is selected.
	Show DOS window	If you select this, the DOS window will be shown every time MailPGP runs PGP. Otherwise PGP will be run as a background process and DOS window will be shown only when necessary.
		Notice! If you hear a beep while PGP is running in the background, it means that an error has occurred. MailPGP will automatically terminate PGP if it does not finish in 25 seconds. If this is the case, select "Show DOS window" and repeat the procedure.
	Remember window position	If you select this, MailPGP dialog will be opened to the same position it was when you last time exited the program.
	Keep MailPGP always on top	Keeps MailPGP window visible even if it is not active.
Other		
	Default procedure for plain text	You can choose whether you want MailPGP to "Encrypt", "Encrypt and sign" or "Clear sign" when you left click the taskbar icon, MailPGP dialog is hidden and there is plain text on clipboard.
	Hot key	You can define a hot key for the default procedure. E.g. if you define CTRL-D as the hot key, every time you press CTRL-D, MailPGP will perform the default procedure.
		Notice that the hot key will work only when MailPGP is hidden.
	Use a default folder for file operations	Select this to enable the default folder option. You can type in the desired directory to the text field or select it from the dialog.
		MailPGP will use the defined directory as the initial file directory when encrypting, decrypting or wiping files.
	Leave temporary files	If you want the files that PGP creates not to be removed after use, select this option. This option is not recommend because it might leave some sensitive data to your disk.
	Save pass phrase in memory	Saves your pass phrase in memory so that you have to type it only once. Pass phrase will stay in memory until you quit MailPGP or choose to reset the pass phrase. Notice that your pass phrase will not be saved to disk.
	Save settings on exit	Saves the current settings when exiting MailPGP. If you want to remove all the registry keys created

	by MailPGP, deselect this option. As default this options is selected.
User interface objects	
EN (Encrypt)	Encrypt a message from the clipboard.
ES (Encrypt and Sign)	Encrypt and sign a message from the clipboard. MailPGP will use the default user ID if it is defined. If not, PGP uses the secret key that is most recently added to your secret key ring.
DE (Decrypt)	Decrypt a message from the clipboard.
CS (Clear Sign or Check Signature)	Clear sign message. If you have not set a default user ID, you have to type in or select a user ID. PGP will use the defined user's secret key to sign the message. If a signed message is found on clipboard and Ignore signatures is not selected, checks the signature.
FE (File Encrypt)	Encrypt a file.
FD (File Decrypt)	Decrypt a file
O (MailPGP Options)	Shows the program options.
User ID menu	Type in or select the user ID for encryption or extracting a public key, or the sender for signing. If you leave this field empty when signing or extracting a public key, MailPGP will use the default used ID if it has been defined.
Taskbar notification area	
Left click the MailPGP icon while MailPGP is VISIBLE	Hides MailPGP window. You can also hide the window by clicking the minimize button.
Left click the MailPGP icon while MailPGP is HIDDEN	Performs encryption, decryption, clear signs or checks the signature depending on the clipboard contents.
Right click the MailPGP icon while MailPGP is HIDDEN	Shows a pop-up menu that contains the available options. The default option (performed on left click) is displayed in bold.
Drag and drop files	You can drag and drop files from explorer to MailPGP's dialog. The procedure depends on the file type.
.pgp-files	If you drag and drop a file with a '.pgp' extension to MailPGP dialog, it will be decrypted.
.asc-files	If you drag and drop a file with an '.asc' extension to MailPGP dialog and it contains a PGP public key, the key will be added to your public key ring. If the file does not contain a key, it will be decrypted.
Other files	Files that have other extensions will be encrypted to a desired recipient.

Errors

MailPGP Errors

Error	Description
001	“At least one user ID is required for this procedure.” **Solution:** Type in or select a user ID from the menu.
002	"No text available on clipboard." MailPGP could not find text from the clipboard. **Solution:** Copy a message to the clipboard.
003	"No encrypted text was found on clipboard." MailPGP could not find an encrypted message. **Solution:** Copy an encrypted message to the clipboard.
004	"File couldn’t be opened." MailPGP tried to open or create a file, but failed. The code at the end of the error message (E1-E15) specifies the exact event that caused the error. **E1:** Failed to create temporary file when encrypting a message. **E2:** Failed to create temporary file when encrypting and signing a message. **E3:** Failed to open the file that contains the encrypted message. **E4:** Failed to create temporary file when decrypting a message. **E5:** Failed to open the file that contains the decrypted plain text message. **E6:** Failed to create temporary file when clear signing a message. **E7:** Failed to create temporary file when verifying a signature. **E8:** Failed to open the file that contains the signed message. **E9:** Failed to open the file that contains the extracted PGP public key. **E10:** Failed to create temporary file when adding a key to key ring. **E11:** Failed to open the file that contains signature verification of a clear signed message. **E12:** Failed to create temporary file when viewing key fingerprint. **E13:** Failed to create temporary file when viewing key signatures. **E14:** Failed to open the file that contains signature verification of an encrypted and signed message. **E15:** Failed to open the file that contains the plain text message when checking a signature.
005	"File couldn't be deleted." MailPGP could not remove a file.
006	"Couldn't execute command."

	MailPGP could not find “pgp.exe” from your system. **Solution:** See how to configure PGP properly.
007	"Memory allocation error." Not enough memory.
008	"Couldn't open clipboard." MailPGP could not open clipboard because some other application has not closed it or is currently using it.

Contacting the author

You can contact me via Internet e-mail using the PGP public key included.

E-mail: <sami.tolvanen@iki.fi>

If you have any comments at all concerning MailPGP or if there are any features you would like me to add to the future versions, please let me know.

Reporting bugs

If you find any bugs or annoying features from MailPGP, it really would be helpful if you reported them to me. The best way is to e-mail me a description of the bug you found. I will try to fix it as soon as I can.

Obtaining the latest version

You can get the newest version of MailPGP at the MailPGP home page <http://www.iki.fi/st/mailpgp/>. Beta versions are available at <http://www.iki.fi/st/mailpgp/beta.html>.

MailPGP Newsletter

If you would like to receive e-mail when a new version of MailPGP is released, send e-mail to `<st@iki.fi>` and use `"subscribe MailPGP Newsletter"` as subject.

The International PGP Home Page

<http://www.ifi.uio.no/pgp/>

PGP at the Massachusetts Institute of Technology, MIT

<http://web.mit.edu/network/pgp.html>

MailPGP Home page

<http://www.iki.fi/st/mailpgp/>

My PGP key's fingerprint

```
67 EB 0B 88 7F 01 C5 62
ED CC C4 AE C9 7A 2A E8
```

MailPGP status

Visible = the dialog is visible on the screen.

Hidden = the dialog is minimized to the taskbar notification area.