

PGP5GUI

Stefan Zakarias <stef@amitar.com.au>

COLLABORATORS

	<i>TITLE :</i> PGP5GUI		
<i>ACTION</i>	<i>NAME</i>	<i>DATE</i>	<i>SIGNATURE</i>
WRITTEN BY	Stefan Zakarias <stef@amitar.com.au>	August 22, 2024	

REVISION HISTORY

NUMBER	DATE	DESCRIPTION	NAME

Contents

1	PGP5GUI	1
1.1	PGP5GUI Documentation	1
1.2	Description	1
1.3	Installing	2
1.4	Usage	3
1.5	Notes	3
1.6	Bugs	4
1.7	License	4
1.8	Credits	5
1.9	Status Bar	5
1.10	Encrypt Page	6
1.11	Encryption Modes	6
1.12	File To Encrypt	7
1.13	Encrypt The File	7
1.14	Decrypt Page	7
1.15	Decrypted File Output	8
1.16	File To Decrypt or Verify	8
1.17	Decrypt The File	8
1.18	Signing Page	9
1.19	Detached Signature	9
1.20	File To Sign	10
1.21	Sign The File	10
1.22	ASCII Armoring Mode	10
1.23	Text Compatibility Mode	11
1.24	Pop-File Requester	11
1.25	Key Management Pages	11
1.26	Keys - Add Page	12
1.27	Add Key(s) From Input File	12
1.28	Add Key(s) In File To Keyring	12
1.29	Keys - Edit Page	12

1.30	Check Key(s)	13
1.31	(En/Dis)able Key	13
1.32	Remove Signature	14
1.33	Sign A Key	14
1.34	Remove A Key	14
1.35	Edit A Key	14
1.36	Keys - Miscellaneous Page	15
1.37	Generate Key Pair	15
1.38	Extract Key(s) To File	15
1.39	List Key(s)	16
1.40	MUI Information	16

Chapter 1

PGP5GUI

1.1 PGP5GUI Documentation

PGP5GUI - An MUI Graphic User Interface for AmigaPGP 5.

(c) Copyright by Stefan Zakarias, 30/MARCH/1998
All Rights Reserved World-Wide, 30/MARCH/1998

My EMAIL address is: <stef@amitar.com.au>

This application uses
~MUI~ - MagicUserInterface
(c) Copyright 1992-98 by Stefan Stuntz

~~~~~DESCRIPTION~~~What~it's~all~about~~~~~

~~~~~INSTALLING~~~Where~to~put~it~~~~~

~~USAGE~~~How~to~start~PGP5GUI~and~use~it~~

~NOTES~~~A~few~thoughts~while~I~wrote~this~

~~BUGS~~~My~mistakes~(or~someone~else's;)~~

~~~~~LICENSE~~~What~you~can/cannot~do~~~~~

CREDITS - Thanks to all those...

### 1.2 Description

#### DESCRIPTION

PGP5GUI provides an MUI Graphic User Interface to ease the use of PGP 5

---

on the AMIGA platform. Specifically, it is a collection of buttons and gadgets you can manipulate to do almost all functions related to PGP 5.

PGP5GUI can be used with an 68020 or better CPU.

PGP5GUI is currently FREEWARE.

## 1.3 Installing

### INSTALLING

1. You can put PGP5GUI anywhere you like.

The important thing to remember is that PGPE , PGPS , PGPV and PGPK must be accessible to PGP5GUI.

The best place to have PGPE, PGPS, PGPV and PGPK, is in your "C:" drawer... Most programs look for other programs in the "C:" drawer so it's probably the best place for PGP5GUI too.

2. You should also put this AmigaGuide file (you are reading) in your assigned "PGP:" directory.

PGP5GUI will look for this AmigaGuide file if you press the [Help] key on any of the 'hotspots'.

These 'hotspots' are:

- on a button or gadget for information about the button or gadget.
- just outside of a button or gadget for information about a page.

PGP5GUI has links to this AmigaGuide document and uses it to display 'Help' information about a page/button/gadget.

3. If you have it, you should also put PGP5.guide into your assigned "PGP:" directory. The PGP5.guide is available from my web-site at:

<http://www.amitar.com.au/~stef/DownloadsPGP5.html>

look for the archive pgp5guides.lha on that page.

The PGP5GUI.guide (you are reading) has links to PGP5.guide.

If you have correctly installed PGP5.guide, then if you

click this button

the next document you see should be the main page of PGP5.guide.

## 1.4 Usage

### USAGE

From Workbench: Double-click the icon.

From Shell/CLI: PGP5GUI

See Notes for more information about this program.

You MUST have Magic User Interface V3.8 installed and operational on your system before attempting to use PGP5GUI.

When PGP5GUI starts, you will be presented with a GUI that has four "Pages" on it. The "pages" are:

~Encrypt~~~For~Encrypting~a~file~

~Decrypt~~~For~Decrypting~a~file~

~~~~Sign~~~For~Signing~a~file~~~~

~~~~Keys~~~PGP~Key~management~~~~

## 1.5 Notes

### NOTES

When a requester pops up asking you for a key, or keys to select, pressing [Ok] will begin the operation on the SELECTED key(s) in most cases. If no keys are selected, then it is assumed that you wish to abort the operation.

There is one exception to the above mentioned rule - ~Check~Key(s)~ will check ALL keys if [Ok] is selected.

Pressing [Cancel] or the [Close Window] gadget will abort the operation before you begin and take you back to the main GUI window.

The default "UserID" used for Encrypting/Signing/Key operations is the one PGP 5 considers the default UserID. This is the one you have specified in the MyName= line of pgp.cfg. If no key is specified as the default, then PGP 5 will use the first usable key found on your secret keyring.

You will notice that I have omitted the 'Key Revocation' functions. I have done this for a reason. They are not commonly used and are NOT functions to be casually messed around with on PGP5. If you want to do a key revocation function, then read the PGPK document carefully and do it from a CLI shell.

All of the 'cycle' gadgets will have their settings saved to:

ENVARC:mui/PGP5GUI.1.cfg

---

when you exit PGP5GUI. Also, the 'AmigaPGP5 Output Window...' and the ASL File Requesters will have their positions and dimensions saved to a file called:

ENVARC:PGP5GUI.wcfg

when you exit PGP5GUI. The next time you run PGP5GUI, these settings will be reloaded and used. See BUGS for a problem I found with the ASL File Requester.

If you have any ideas, suggestions, or want something changed/added, then, please, feel free to EMAIL me:

Stefan Zakarias <stef@amitar.com.au>

## 1.6 Bugs

### BUGS

Yep, there's got to be some hiding in there for sure...  
Tell ME if you find them!

1. MUI causes a lot of 'Mungwall' hits. It's not my fault!

This happens on almost ALL MUI based programs I've tested. If the program tends to crash erratically, then increasing the stack may help!

2. To properly save the last used dimension and position of the ASL File Requester, you might have to open a File Requester, with the new dimension and position, TWICE in the program! This is a bug in the "asl.library".

## 1.7 License

### LICENSE

The program, "PGP5GUI", and it's documentation, "PGP5GUI.guide" are

(c) Copyright by Stefan Zakarias, 30/MARCH/1998.  
All Rights Reserved World-Wide, 30/MARCH/1998.

PGP5GUI is currently FREeware.

You must NOT sell - either in original or modified form - the program, "PGP5GUI", or it's documentation, "PGP5GUI.guide".

You may use and distribute ONLY the COMPLETE, UNMODIFIED, PGP5GUI distribution as long as NO credit, reward or financial profit is gained by you, or anyone else, for such use or distribution.

---



All the files that come with the PGP5GUI archive are provided "AS-IS". No warranties, liabilities or responsibilities, either expressly or implied, are to be made regarding the use of this distribution or it's contents.

All use is at your own risk.

You have received the program, PGP5GUI, and it's documentation, in good faith, on the assumption that you will use and test them and report any bugs or errors that you may find directly to the author:

Stefan Zakarias <stef@amitar.com.au>

## 1.8 Credits

### Credits And Thanks...

Thanks go to these 'beta' testers...

Shane Cracknell: <shane@amitar.com.au>  
Domenic Gebauer: <campino@gmx.net>  
Paul Gooch: <PGooch@cableinet.co.uk>  
Chris Page: <dasoft@zetnet.co.uk>  
Dwayne Rideout: <dwayne@rideout.u-net.com>

Thanks go to...

Chris Page for converting the PGP5 documents into the AmigaGuide files, PGP5.guide and pgp-intro.guide.

Domenic Gebauer for creating a new Amiga PGP mailing list...  
For information on how to subscribe to his mailing list, see the page on my web-site at:

<http://www.amitar.com.au/~stef/AmiPGP5Links.html>

Eric Totel for MUIBuilder v2.2b. I used MUIBuilder to (easily) create the GUI for PGP5GUI and from it I learned a little about MUI programming techniques.

Stefan Stuntz for MUI

## 1.9 Status Bar

### Status

This tells you what processing state PGP5GUI is currently in.  
The possible messages are:

Initializing - PGP5GUI start up.  
Processing - Executing a PGP5 program.

---

Getting key list - Updating key list.  
Generating key list - Generating list for PGP5GUI.  
Waiting for key choice - Waiting for your key selection.  
Waiting for file choice - Waiting for your file selection.  
Ready! - Ready to perform a function.

## 1.10 Encrypt Page

### Encrypt

PURPOSE - File encryption.

#### DESCRIPTION

This page is where file Encrypting operations are performed.

On this page you will find:

- 3 cycle gadgets for selecting the options you wish to use for encrypting an input file.

These are (from the top):

~Encryption~Mode~~

~Use~ASCII~Armor~~

~Text~Mode~ON/OFF~

- A ~File~To~Encrypt~ text string and pop-File gadget used for selecting the file you wish to encrypt.
- An ~Encrypt~The~File!~ button to begin the encryption process.

## 1.11 Encryption Modes

### Encrypt Mode

PURPOSE - Select method of Encryption.

#### DESCRIPTION

#### Public Key Encrypt

This is the default method for encrypting a file. This mode encrypts the file using the recipient's key you specify after you press ~Encrypt~The~File!~

#### Public Key Encrypt And Sign

This mode encrypts the file using the recipient's key you specify after

---

you press ~Encrypt~The~File!~ It also signs the file as well, using the default signing key specified in the MyName= line of ~pgp.cfg~, or the first secret key found on your secret keyring.

### Conventional Encrypt (IDEA)

Conventional encryption mode. This uses a symmetric cipher called "IDEA" to encrypt your message. No public-key related information is used in this method. This method depends on a mutual pass-phrase to be shared between the author and the recipient(s).

## 1.12 File To Encrypt

### File To Encrypt

PURPOSE - Name of the file to encrypt.

#### DESCRIPTION

This is where you enter the name of the file you wish to encrypt. To make it easier to select a file, there is a pop-file gadget next to the file name entry box.

## 1.13 Encrypt The File

### Encrypt The File

PURPOSE - Begin the encryption process.

#### DESCRIPTION

This starts the encryption process on the file using the settings you have specified.

## 1.14 Decrypt Page

### Decrypt

PURPOSE - Decrypt or verify a file.

#### DESCRIPTION

This is the page where Decrypting or Verifying an input file is done.

On it you will find:

- An ~Output~To...~ cycle gadget for selecting the option you wish to use when decrypting an input file.

- A ~File~To~Decrypt~ text string and pop-file gadget used for selecting the file you wish to decrypt.
- An ~Decrypt~The~File!~ button to begin the decryption process.

When verifying an input file, the cycle gadget will have no effect on the result of the operation.

## 1.15 Decrypted File Output

### File Output Mode

PURPOSE - Select output method used for decryption.

DESCRIPTION

#### Output To File Only

This mode decrypts to a file using the name of the input file minus any filename extension after the last period - "." - in the filename. PGP5 normally encrypts a file using either a ".asc" or ".pgp" extension after the input filename so that when the recipient decrypts the file, they don't have to worry about what to name the file as.

#### Output To Internal Pager

This mode displays the decrypted file using the internal pager of PGP5. If the file is binary, it will not be displayed!

## 1.16 File To Decrypt or Verify

### File To Decrypt Or Verify

PURPOSE - Name of the file to decrypt or verify.

DESCRIPTION

This is where you enter the name of the file you wish to decrypt or verify. To make it easier to select a file, there is a pop-file gadget next to the file name entry box.

## 1.17 Decrypt The File

### Decrypt/Verify The File

PURPOSE - Begin the decryption/verifying process.

DESCRIPTION

---

This starts the decryption/verifying process on the file. The decrypting process will send the resulting output to either PGP5's internal pager or a file. The verifying process ignores the output settings button.

## 1.18 Signing Page

### Sign

PURPOSE - File signing.

#### DESCRIPTION

This page is where you can Sign an input file.

Here you will find:

- 3 cycle gadgets for selecting the options you wish to use for signing an input file.

These are (from the top):

~Detached~signature~ON/OFF~

~~~~~Use~ASCII~Armor~~~~~

~~~~~Text~Mode~ON/OFF~~~~~

- A ~File~To~Sign~ text string and pop-file gadget used for selecting the input file you wish to sign.
- A ~Sign~The~File!~ button to begin the signing function.

## 1.19 Detached Signature

### Signature Output Method

PURPOSE - Select the method of signing a file.

#### DESCRIPTION

##### Detached Signature ON

Creates a detached signature file using the input file's name with a ".sig" extension attached. This mode is useful for signing binary files like, for example, executable files.

##### Detached Signature OFF

Combines the signature with the input file. In other words, the signature becomes part of the file. This mode is mainly used for

---

signing documents like, for example, Email. This mode should NOT be used on binary files.

## 1.20 File To Sign

### File To Sign

PURPOSE - Name of the file to sign.

#### DESCRIPTION

This is where you enter the name of the file you wish to sign. To make it easier to select a file, there is a pop-file gadget next to the file name entry box.

## 1.21 Sign The File

### Sign The File

PURPOSE - Begin the file signing process.

#### DESCRIPTION

This starts the signing process on the file using the settings you have specified.

## 1.22 ASCII Armoring Mode

### ASCII Armoring

PURPOSE - Toggle "ASCII Armoring" ON or OFF.

#### DESCRIPTION

With ASCII Armoring ON, PGP5 creates a "text-only" version of the file being processed. This makes the file safe for electronic mailing because most Email programs and servers are expecting text only when dealing with mail. The downside of this is that the resulting file is about 30% larger than with ASCII Armoring turned off.

This mode is also useful to create a message suitable for paper mailing or hard-copying. The message can be printed to paper and later retrieved using a hand or page scanner with character recognition software.

With ASCII Armoring OFF, PGP5 creates a binary output file.

---

## 1.23 Text Compatibility Mode

### Text Mode

PURPOSE - Toggles "Text Mode" ON or OFF.

#### DESCRIPTION

This deals with the carriage-return/line-feed sequence differences between the major operating systems.

With Text Mode ON, PGP5 converts your input message to a platform independent form. It's primary use is for when you expect or don't know that the recipient of the file may have a different operating system to the one you are using. E.G: AMIGA -> MAC/IBM.

With Text Mode OFF, PGP5 leaves the message untouched.

## 1.24 Pop-File Requester

### Pop-File Requester

PURPOSE - Pops up a standard ASL File Requester.

#### DESCRIPTION

Clicking the left mouse button on this gadget will pop up a standard ASL file requester from which you can select the file you want to perform a specific function on.

## 1.25 Key Management Pages

### Key Management Functions

PURPOSE - Pages with functions for managing your PGP keys.

#### DESCRIPTION

On this page you will find 3 more pages with functions to use for managing your PGP keys.

The pages are:

~~~~Add~~Add~a~key,~or~keys~to~your~PGP~keyring~~~~

~Edit~~~Edit~details~about~PGP~keys~on~your~keyring~

~~Misc~~~Miscellaneous~functions~for~your~keyring~~~

1.26 Keys - Add Page

Keys - Add

PURPOSE - Add key(s) from an input file.

DESCRIPTION

Provides you with gadgets used for adding a key to your keyring.

The first is a file name input gadget where you can enter the name of the "keyfile" that contains a PGP key or keys.

The other gadget is a button called ~Add~Key(s)~In~File~To~Keyring~. You press this button to begin the operation after you have selected a file.

1.27 Add Key(s) From Input File

File To Read A Key Or Keys From

PURPOSE - Name of the file to get a key or keys from.

DESCRIPTION

This is where you enter the name of the file that contains a key or keys that you want added to your keyring. To make it easier to select a file, there is a pop-file gadget next to the file name entry box.

1.28 Add Key(s) In File To Keyring

Add Key(s) In File To Keyring

PURPOSE - Begins the process to add key(s) from a file.

DESCRIPTION

This begins the process to read an input file you have specified. If any keys were found in the file, they will be added to your keyring.

1.29 Keys - Edit Page

Keys - Edit

PURPOSE - Key management functions.

DESCRIPTION

On this page you will find 6 functions commonly used with managing your

PGP keys:

```

~~Check~Key(s)~~~Check~all~details~about~keys(s)~~
~~~(En/Dis)able~Key~~~Toggle~the~usage~of~a~key~~~
~Remove~Signature~~~Remove~a~signature~from~a~key~
~~~~~Sign~A~Key~~~Sign~a~key~with~YOUR~key~~~~~
~Remove~A~Key~~~Remove~a~key~from~your~keyring(s)~
~~~~~Edit~A~Key~~~Edit~the~details~about~a~key~~~~~

```

1.30 Check Key(s)

Check Key(s)

PURPOSE - Check details of a key or keys.

DESCRIPTION

*** A very slow operation ***

This button allows you to check the details of keys on your public keyring. When you click this button, a 'keylister' will be presented to you.

If you select a key, PGPK will check/display only the details for that particular key.

If no keys are selected, then ALL keys will be checked and displayed.

When you click [Ok] in the keylister, the operation is begun.

1.31 (En/Dis)able Key

(En/Dis)able Key

PURPOSE - Toggle the ability of PGP5 to use a key.

DESCRIPTION

This function toggles enabling/disabling of a selected key on your keyring. When you click this button, a 'keylister' will be presented to you.

Selecting a key and clicking [Ok] in the keylister will begin the operation.

1.32 Remove Signature

Remove Signature

PURPOSE - Remove a signature from a key.

DESCRIPTION

Removes a signature from a key. When you click this button, a 'keylister' will be presented to you.

Selecting a key and clicking [Ok] in the keylister will begin the operation.

1.33 Sign A Key

Sign A Key

PURPOSE - Sign a key with your key.

DESCRIPTION

Signs a selected key with your DEFAULT signing key. The default signing key is the key you have specified in the MyName= line of pgp.cfg . If no key is specified as the default, then PGPK will use the first key found on your keyring.

When you click this button, a 'keylister' will be presented to you.

Selecting a key and clicking [Ok] in the keylister will begin the operation.

1.34 Remove A Key

Remove A Key

PURPOSE - Remove a key from your keyring(s).

DESCRIPTION

Removes the key from your public keyring, and your secret keyring as well, if it is there. When you click this button, a 'keylister' will be presented to you.

Selecting a key and clicking [Ok] in the keylister will begin the operation.

1.35 Edit A Key

Edit A Key

PURPOSE - Edit details of a PGP key.

DESCRIPTION

Edits the selected key. If this is YOUR key, it allows you to edit your userid and passphrase. If the key belongs to someone else, it allows you to edit the trust you have in that person as an introducer of new keys.

When you click this button, a 'keylister' will be presented to you.

Selecting a key and clicking [Ok] in the keylister will begin the operation.

1.36 Keys - Miscellaneous Page

Keys - Misc

PURPOSE - Miscellaneous key functions.

DESCRIPTION

On this page you will find 3 utility functions commonly used with managing your PGP keys:

~~~Generate~Key~Pair~~~

~Extract~Key(s)~To~File~

~~~~~List~Key(s)~~~~~

1.37 Generate Key Pair

Generate Key Pair

PURPOSE - Generate a Secret/Public keypair.

DESCRIPTION

This button begins the operation to generate a public/secret key pair for yourself.

When you click this button, the operation is begun.

1.38 Extract Key(s) To File

Extract Key(s) To File

PURPOSE - Extract selected keys to a file.

DESCRIPTION

Extracts the selected key(s) in ASCII-armored form and saves it to a file specified by you via an ASL File Requester that will pop-up.

When you click this button, a 'keylister' will be presented to you.

Selecting a key, or keys, and clicking [Ok] in the keylister will begin the operation.

1.39 List Key(s)

List Key(s)

PURPOSE - Show general information about keys.

DESCRIPTION

Shows a list of keys you have on your public keyring. If any keys are selected, then PGP5 will show more information about those keys.

When you click this button, a 'keylister' will be presented to you.

When you click [Ok] in the keylister, with NO keys selected, the operation is aborted.

Selecting a key, or keys, and clicking [Ok] in the keylister will begin the operation.

1.40 MUI Information

This application uses

MUI - MagicUserInterface

(c) Copyright 1992-98 by Stefan Stuntz

MUI is a system to generate and maintain graphical user interfaces. With the aid of a preferences program, the user of an application has the ability to customize the outfit according to his personal taste.

MUI is distributed as shareware. To obtain a complete package containing lots of examples and more information about registration please look for a file called "muiXXusr.lha" (XX means the latest version number) on your local bulletin boards or on public domain disks.

If you want to register directly, feel free to send

DM 30.- or US\$ 20.-

to

Stefan Stuntz
Eduard-Spranger-Straße 7
80935 München
GERMANY

Support and online registration is available at

<http://www.sasg.com/>
