

An Unauthorised Guide to PGP Cryptography

[PDF version](#)

Introduction

Pretty Good Privacy by Phil Zimmermann is the industry standard in public-key cryptography. Public key cryptography uses a pair of keys: a public key, which encrypts data, and a corresponding private key, for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt data that only you can read. Conversely you can send anyone an encrypted message with their public key which only they can read.

PGP is useful for encrypting messages, files and folders, although Secure Multipurpose Internet Mail Extensions are becoming more popular, which integrate PGP into email. However not all email clients support S/MIME and it requires an X.509 Certificate issued by a Certificate Authority (CA).

It is essential that the PGP software is open source to ensure that there is no hidden "back door key" which might enable state agencies or others to decrypt it.

Which PGP Version?

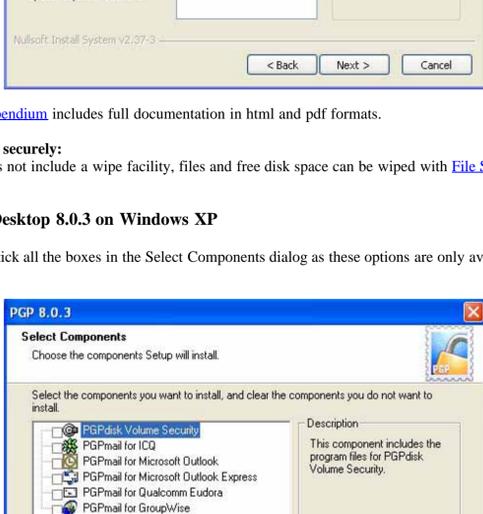
PGP Desktop 9 and later versions can only be used for a limited period before online registration is required. Some earlier versions of PGP are available at [The International PGP Home Page](#).

PGP Desktop 8.03 is available free for unlimited use from [PGPDesktop803.zip](#)
Note: PGP Desktop 803 cannot be installed on Vista or Windows 7
See [Installing PGP Desktop 8.0.3 on Windows XP](#)

[PortablePGP](#) is available in a free USB memory stick version which can be used anywhere without installation on Windows and some GNU/Linux.

Text messages are encrypted and decrypted simply by copying and pasting.
See [Using PortablePGP](#)

[GNU Privacy Guard](#) or GPG is the premiere open source implementation of OpenPGP encryption. GNUPG is available free from [Gpg4win](#) (Windows), [Mac GPG](#) (Mac) and is available in some GNU/Linux flavours. Note: The right click shell extension (GpgEX) component is not currently available for 64-bit Windows versions, although the optional GNU Privacy Assistant (GPA) component has the same functionality.



[The Gpg4win Compendium](#) includes full documentation in html and pdf formats.

To delete messages securely:

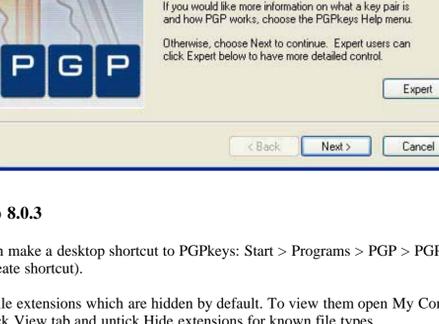
Since Gpg4win does not include a wipe facility, files and free disk space can be wiped with [File Shredder](#).

Installing PGP Desktop 8.0.3 on Windows XP

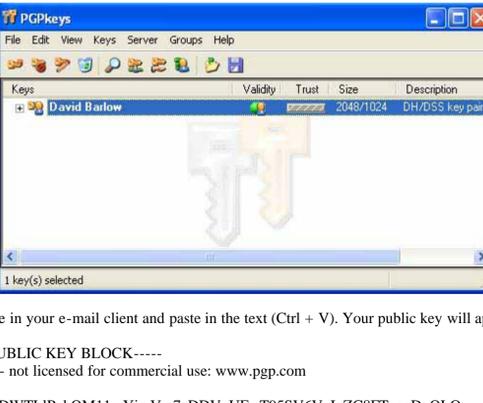
When installing, untick all the boxes in the Select Components dialog as these options are only available for the licenced version:



After rebooting, the PGP License Authorization dialog appears - select Later:



Follow the Key Generation Wizard to generate a key pair:



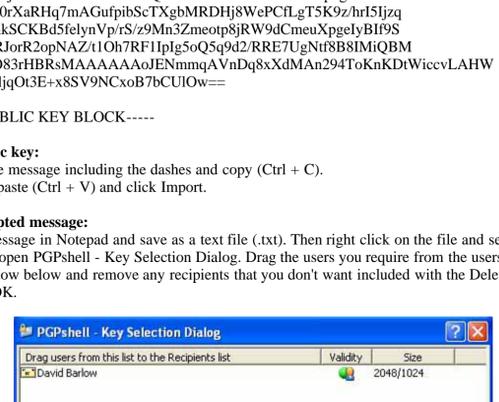
Using PGP Desktop 8.0.3

For convenience we can make a desktop shortcut to PGPKeys: Start > Programs > PGP > PGPKeys > right click > Send To > Desktop (create shortcut).

We will need to view file extensions which are hidden by default. To view them open My Computer and select Tools > Folder Options..., click View tab and untick Hide extensions for known file types.

To export your public key:

Click on your name in PGPkeys and copy (Ctrl + C).



Open a new message in your e-mail client and paste in the text (Ctrl + V). Your public key will appear as below:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.0.3 - not licensed for commercial use: www.pgp.com

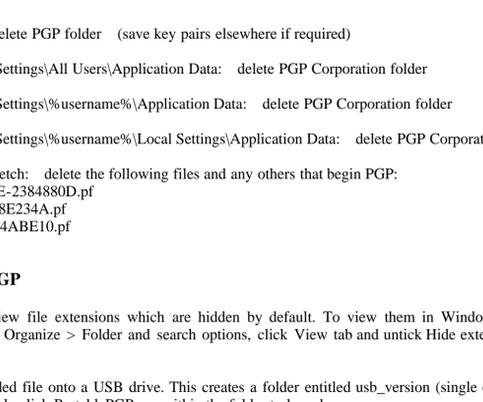
mQGiBE7zescRBADWTLIPxkQM11mYjmVm7aDDV0UfW9T5SV6VlgZC8FTzooDgQLO
SABHY9uPpNioidVbAOllZSn5b9qaJt+cKfOGj+Dab0bEiYx+tmcUYgGs5bST1oCP
QgYIH3e+CX+4VNgPaIJG1Vz6R0YeEDFQ6lFvXbW6DUq9YBPxs7eDxTrQCg/145
uuYCV1Ay+u824/Ab1zAU3MD/3+qnAXrYwIkdIb/K080orzpXULqoh3CH8Y4iCj
WlPzLN2fC88e2aEnUcPQ5nwUnVGvYxYmfelaykFstfId56ba2TonY9Ps2caCm/7z
sLClcZP0/mYK7/03ej7esFK+pwtvJP3Jfj9OrzoT6GCxrGPguhSlcLw/HF+1Dp
v8RLBACmGnNH/PzMTfTdkckCYn0f5qPU16Zf0amwijeWpmp/igpvvc+iXtWes5
JxyYovEvqZGu4Dv7hbPm8HQwaLT7Izqt8300w5GnWdzJeywetgZqV9VHk27Te
7z9vYQqBXTw37Xoqke08YS+3vJmoNkkBfP0CITVj0qteZ7QMRF2aWQgQmFy
bG93iQBxBBARAgAXBQJO83rHBwJcAcDAgoCQEFwMAAAACgkQ2naoBwCOrZF9
AwCgnQTW50JGqcw9JLm3oFvYWYUauFMAoK38UyOZbV9v97T0J/mr4zsPhxq3uQIN
BE7zescQCAD2Qle3CH8IF3KiutapQvMF6PITETiPvFuuUs4JInoBp1ajFomPQFXz
0AfGy0OpK33TGSgSfgMg71l6RfUodNQ+PVZX9y2Ukq8L9GAFg5fSI/VhOSdVn
Rf2vIPFRzBhznzJZr8V+bv9Kv7H7AarT56NoKX9yOtQa8L9GAFg5fSI/VhOSdVn
IL5d5JEHNmszbDgNRR0PflzHHxblY7288kjwEPwpVsYjY67VY4XTJTNTN8F1dD
ox0YbN4zIsY1Kv884bEPQBgRjXyEppwY1obEaxnIByl6ypUM2Zaf94AKUJsCRIMI
PwAKXGfnHy9iUsiGSa6q6lEw1XpMg57AAICADnHeDkQyidSo8YTeaCR458Ua
2oRxSgF4VjDIY1viL9vFdxsbEmblYZ5W/hhPhfANuOmq0CIEglay03RySbjZO1
J82lbgk8HuDjAFesjzbiCIX1POB2vftISSiQvW90H9mO3kivkEFdRlPngE3DFW
CF2KosJgOhl48X0rXaRHq7mAGufpbScTXgBMRDHj8W9PClGt5K9z/hr151jzq
/MGmJClac5iHmkSCKBd5felyNvpr/rs/z9Mn3Zmeot8p8WRRE7UgNtr8B8IMiQBM
571KUX6fW148RjorR2opNAZt1h0H7RF1Pljg5oQ5q9d2RRRE7UgNtr8B8IMiQBM
BBwRAgAMBQO83rHBrsMAAAAAA0JENmmqAVnD8q8xXdM294ToKnKDtWiccvLAHW
skuQ+DFAAJ43HjqO3E+x8SV9NCx0B7bCUiOw==
=SM7B
-----END PGP PUBLIC KEY BLOCK-----
```

To import a public key:

Highlight the entire message including the dashes and copy (Ctrl + C). Launch PGPkeys, paste (Ctrl + V) and click Import.

To send an encrypted message:

First write your message in Notepad and save as a text file (.txt). Then right click on the file and select Notepad > Encrypt. This will open PGPShell - Key Selection Dialog. Drag the users you require from the users window above to the recipients window below and remove any recipients that you don't want included with the Delete key. Tick Text Output and click OK.



This includes a .txt.asc file. Open this file in Notepad (right click, Open With..., select Notepad), highlight the entire message including the dashes (Ctrl + A) and copy (Ctrl + C). Open a new message in your e-mail client and paste in the text (Ctrl + V). Your message will appear as below. (Leave the message subject blank to maintain confidentiality.)

```
-----BEGIN PGP MESSAGE-----
Version: PGP 8.0.3 - not licensed for commercial use: www.pgp.com

qANQR1DBW4U4Acfrj5EABKKB/4p9aH09qb1JRM3/cEdpgeKic/zF9PLyQLTceHww
csHsJqX4RlyeDt3QQWV2mPSvniJlBpWC8n5QCqLqDbDQjWlAjA6Dq4+rjF5
UG+/UzwlrEc5HyM06RtqDOSc0gNmmfBaLSiSE0mrIz3JqU0J3qFKGUnQNC
akq/Dru8aB4xvZ6Va4NLkN0qnUhxNMmPJoTEmoDhhHzj1Wj/OvMhC/218YkaLBV1
ruHsMkcp6fimbZ5DyMm4/YyhXpF7+naWl.m59w8yxLqWJbFN83KpY0C2IKxi6wzF
w7E46N8n5hhvyX8RactEN2Y/uk+6sWzEtK8SAKJEDXnoB3B/GIZVgOEQMSV+S
s13td/OTRbTZygm67zgPsV1ghQWfzNq35vPnGscWrlMZLXjr448rJFz5VGFki
RDMfghRWO5ahYyR8XNyhakKsLN3homjPMYGDfV1Xu47EJrsUVQM/3e9VA
M+BiSMmdu9KV5XkMLuPdXQsiDiDkE8Jb8D0h0ScGcZ7u6fYGseqmQNiCYq
7xPKF0poP8+87Sv0AK+8UZWcYHARLpdmrJR5uG6bnjuss58Tqik1xJoNu9
S3QM13FK0kcBADMQRk7WQY3wxzNRuGib+XB08TZ+gI5SS9bSaA49/2e7u09BDLrG
B6h/JaAFEmq+BoYDcowJTZVAZTPxvcoMqSKOeyTEMg==
=beEb
-----END PGP MESSAGE-----
```

To read an encrypted message:

Highlight the entire message including dashes and copy (Ctrl + V). Open Notepad, paste (Ctrl + V) and save as Message.txt.asc in the File name box. Then right click on the file and select PGP > Decrypt & Verify. Enter the passphrase for your private key and click OK. The decrypted message will be saved as a text file. However, if the message was sent from a different encryption application, the decrypted message may be saved with an asc extension which can be opened in Notepad (right click, Open With..., select Notepad).

To delete messages securely:

Right click the message and select PGP > Wipe. The number of passes can be selected in PGPkeys > Edit > Options... If another encryption application is used without a wipe facility, files and free disk space can be wiped with [File Shredder](#).

Problems with File Attachments

If you do not select text output when encrypting, the file created will have a .pgp extension which can be sent as an email attachment. However, if the person receiving the message is not using the same encryption application, they may not be able to open the file. Similarly, if the message is written with a word processor and encrypted (e.g. doc.pgp), the message receiver will not be able to read it unless they have the same one installed. So writing messages in Notepad and sending them as text is more reliable.

Uninstalling PGP Desktop 8.0.3 from Windows XP

Use Add or Remove Programs in Control Panel or launch PGPDesktop.exe to remove PGP 8.0.3. In addition certain folders and files need to be removed before a clean installation can be made.

To view them open My Computer and select Tools > Folder Options..., click View tab and select Show hidden files and folders.

My Documents: delete PGP folder (save key pairs elsewhere if required)

C:\Documents and Settings\All Users\Application Data: delete PGP Corporation folder

C:\Documents and Settings\%username%\Application Data: delete PGP Corporation folder

C:\Documents and Settings\%username%\Local Settings\Application Data: delete PGP Corporation folder

C:\WINDOWS\Prefetch: delete the following files and any others that begin PGP:

PGPDESKTOP.EXE-2384880D.pf

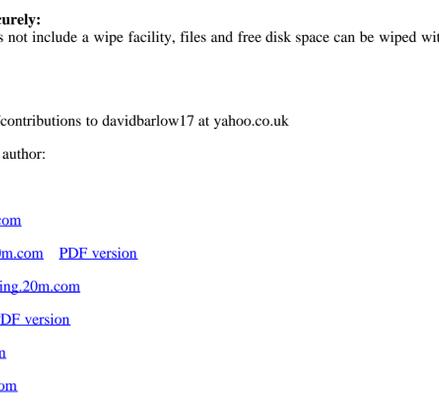
PGPKEYS.EXE-078E234A.pf

PGPMAIL.EXE-0B4ABE10.pf

Using PortablePGP

We will need to view file extensions which are hidden by default. To view them in Windows 7 open Windows Explorer and select Organize > Folder and search options, click View tab and untick Hide extensions for known file types.

Unzip the downloaded file onto a USB drive. This creates a folder entitled usb_version (single click on the folder or F2 to rename). Double click PortablePGP.exe within the folder to launch:



Type in a name.txt and save to the Desktop (it doesn't make a text file by default). Open the file and select it all including the dashes (Ctrl + A), copy (Ctrl + C) and paste into your e-mail client (Ctrl + V). Alternatively the text file can be attached to an email.

To import a public key:

Highlight the key including the dashes and copy (Ctrl + C). Open Notepad (All Programs, Accessories), paste it in (Ctrl + V) and save as a text file on the Desktop. Ensure that there are no spaces or blank lines before -----BEGIN PGP PUBLIC KEY BLOCK----- . Click Keyring on the PortablePGP menu and then click the down arrow after Public Keys to import from a file.

To send an encrypted message:

Click Encrypt on the PortablePGP menu and select the Encrypt Text radio button. Type your message, select the Target recipient and click Encrypt. The Text Editor will open - click Copy to clipboard and paste into your e-mail client (Ctrl + V). Alternatively the encrypted message can be saved as a text file and attached to an email. (Leave the message subject blank to maintain confidentiality.)

To read an encrypted message:

To read a message select Decrypt on the PortablePGP menu and the Decrypt ASCII-Armored Text radio button. Highlight the message including dashes and copy (Ctrl + C), then paste it into the box (Ctrl + V) and click Decrypt. You will be prompted to enter your passphrase and the Text Editor will then open with the message. Alternatively the encrypted message can be saved as a text file and decrypted using the Decrypt a file radio button.

To delete messages securely:

Since PortablePGP does not include a wipe facility, files and free disk space can be wiped with [File Shredder](#).

David Barlow

Comments/suggestions/contributions to davidbarlow17 at yahoo.co.uk

Other sites by the same author:

[www.asthma.20m.com](#)

[www.colourcasts.20m.com](#)

[www.customsrogues.20m.com](#) [PDF version](#)

[www.difficultyswallowing.20m.com](#)

[www.dmt.20m.com](#) [PDF version](#)

[www.eugenics.20m.com](#)

[www.euthanasia.20m.com](#)

[www.guitarscores.20m.com](#)

[www.lsd25.20m.com](#)

[www.mescaline.20m.com](#) [PDF version](#)

[www.mushrooms.20m.com](#) [PDF versions](#)

[www.nasalpolyps.20m.com](#)

[www.nuclearfusion.20m.com](#)