



Gpg4win for Novices

A publication of the Gpg4win project

based on original documents by

Manfred J. Heinze, Karl Bihlmeier, Isabel Kramer,

Dr. Francis Wray, Ute Bahn,

Werner Koch.

Translated from the German original by

Brigitte Hamilton

Version 1.0.0 as of Nov. 30, 2006

Imprint Gpg4win

Copyright © 2002 Bundesministerium für Wirtschaft und Technologie (German Federal Ministry of Economics & Technology)

Copyright © 2005 g10 Code GmbH

Copyright © 2006 Brigitte Hamilton

Permission is hereby granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 (or newer) published by the Free Software Foundation; with the Invariant Sections being "Impressum", no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Special Thanks to:

Bernhard Reiter for minor edits and coordination (2006, 2007).

Michael W. Lewis for proofreading (2007).

Andre Hosch for screenshots (2007)

<p>The statements on the next page are not anymore correct. Due to a wrong application of the terms of the GFDL, it is legally not possible to fix them. Please add new copyright notices only here.</p>

Impressum

Diese Seite darf nicht verändert werden.

Autor: Manfred J. Heinze, TextLab text+media
Beratung: Lutz Zolondz, G-N-U GmbH
Illustrationen: Karl Bihlmeier, Bihlmeier & Kramer GbR
Layout: Isabel Kramer, Bihlmeier & Kramer GbR
Fachtext: Dr. Francis Wray, e-mediate Ltd.
Redaktion: Ute Bahn, TextLab text+media
1. Auflage, März 2002

Copyright © Bundesministerium für Wirtschaft und Technologie

Dieses Buch unterliegt der "GNU Free Documentation License". Originaltext der Lizenz: <http://www.gnu.org/copyleft/fdl.html>. Deutsche Übersetzung <http://nautix.sourceforge.net/docs/fdl.de.html> sowie auf der beiliegenden CD-ROM. Es wird die Erlaubnis gegeben, dieses Dokument zu kopieren, zu verteilen und/oder zu verändern unter den Bedingungen der GNU Free Documentation License, Version 1.1 oder einer späteren, von der Free Software Foundation veröffentlichten Version. Diese Seite ("Impressum") darf nicht verändert werden und muss in allen Kopien und Bearbeitungen erhalten bleiben ("unveränderlicher Abschnitt" im Sinne der GNU Free Documentation License). Wenn dieses Dokument von Dritten kopiert, verteilt und/oder verändert wird, darf in keiner Form der Eindruck eines Zusammenhanges mit dem Bundesministerium für Wirtschaft und Technologie erweckt werden. Wie das OpenSource-Kryptografieprogramm GnuPP selbst wurden diese Texte nicht für Mathematiker, Geheimdienstler und Kryptografen geschrieben, sondern für jedermann.

Contents

1. About this manual	6
2. What is Gpg4win?	7
3. Installing Gpg4win	8
4. Creating a key pair	18
5. Publishing your key per email	25
6. Sending your key to a keyserver	31
7. Decrypting an email	32
8. Attaching a key to your key ring	38
9. Encrypting emails	43
10. How to archive/store encrypted emails	46
A. Suggestions regarding the Outlook plugin <i>GPGol</i>	49
A.1. Installation	49
A.2. Common Questions	50
B. Transferring from other GnuPG programs	52
C. History	53
D. GNU Free Documentation License	54

1. About this manual

The Gpg4win manual and exercise module consists of three parts:

- **an introductory guide called "Gpg4win for Novices"**, which you are reading right now,
- **the manual "Gpg4win for Advanced Users"** in PDF-Format, which can be found on your hard drive after you have installed Gpg4win,
- **the exercise robot Adele**, which allows you to practice the email en- and decryption process(an internet connection is required).

"Gpg4win for Novices" is a quick guide to the installation and everyday use of the Gpg4win software. You will need about half an hour to work through this manual, depending on your knowledge of computers and Windows.

"Gpg4win for Advanced Users" provides in-depth information about the basic principles and mechanisms used by Gpg4win, as well as its less commonly used capabilities.

Both manuals are available in PDF format; you can print your own manual if you did not receive a printed copy.

Each manual can be read independently. We suggest, however, that you read both manuals in order to get a better understanding of the software.

♠ This symbol references a link to the other manual.

The practice robot Adele is available on the Internet. Adele receives, sends and decrypts encrypted emails. You can use it to practice a complete cryptographic exchange, as often as you need to be fully familiar with the software.

Adele was developed as part of the older GnuPP project, where it is still used. "Gpg4win for Novices" also uses this very reliable practice robot and hereby wishes to express its gratitude to the owners of gnupp.de for operating Adele.

2. What is Gpg4win?

Gpg4win (GNU Privacy Guard for Windows) is an email encryption software. It is the result of a project initiated by the Federal Office for Information Security, and includes the following components:

GnuPG: its key component, the encryption software

GPA: GNU Privacy Assistant, a key manager

WinPT: Key Manager, which also supports encryption via your Clipboard

GPGol: a plugin for Microsoft Outlook which integrates the operation of GnuPG

GPGee: a plugin for Windows Explorer which allows encryption of data by right-clicking on your mouse

Sylpheed-Claws: a complete email program with integrated GnuPG operation

The encryption program GnuPG (GNU Privacy Guard) provides you with a secure, simple and free method of email encryption. It can be used privately or commercially without restrictions. The encryption technology used by GnuPG is extremely secure and cannot be broken using current technology.

GnuPG is a free software¹. This means that anyone can use the software for private or commercial purposes, as well as analyze or change the source codes (ie. the actual programming commands), and distribute the same.²

The transparency of the source code forms an essential part of a security software, as it is the only way to verify the trustworthiness of the program.

GnuPG is based on the international standard OpenPGP (RFC 2440), is fully compatible with PGP and uses the same infrastructure (key server etc.).

PGP ("Pretty Good Privacy") is not free software; many years ago it was available on a temporary basis under similar conditions as GnuPG, but is no longer considered state-of-the-art.

Additional information regarding GnuPG and other projects undertaken by the German government in the area of Internet security can be found on the website of the Federal Office for Information Security www.bsi-fuer-buerger.de

¹sometimes incorrectly identified as Open Source Software

²However, keep in mind that a fair amount of technical knowledge is required to change the program, otherwise the program's security may be compromised.

3. Installing Gpg4win

If you already have a GnuPG-based application such as GnuPP, GnuPT, WinPT or GnuPG Basics installed on your system, we recommend that you read the Appendix B to find out how to migrate existing keys.

Installing Gpg4win from a CD-ROM:

Insert the CD-ROM in the CD-ROM drive of your computer and log in as Administrator. On the screen click on the CD-ROM icon titled 'Gpg4win'. Once the CD-ROM icon opens, click on the installation icon titled 'Gpg4win'.

Installing Gpg4win from the Internet:

If you have downloaded Gpg4win from the Internet, click on the new file (it should be named `gpg4win-1.1.0.exe` or a newer version). Please ensure that you have downloaded the file from a trustworthy site.

The following installation steps apply to all situations:

You will be asked if you want to install the program; click on [Yes].

The following screen will appear:

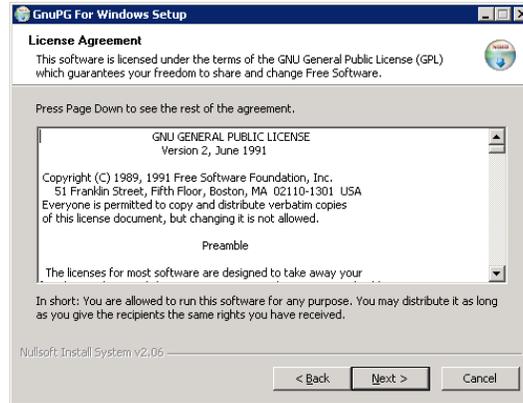


If you have other programs running on your computer, close them now and click on [Next].

The licencing page contains information regarding the licencing of this software.

If your sole intention is to install and use the software, you do not need to read this information.

However, if you plan to distribute and/or alter the software, you must familiarize yourself with the conditions contained in the licencing agreement.



Click on [Next].

On the components page you can select which features of GnuPG For Windows you want to install.

To assist you with your selection, a short description window appears when you move the mouse over a selected item. At this point, you may want to check the available free space on your hard drive as well.

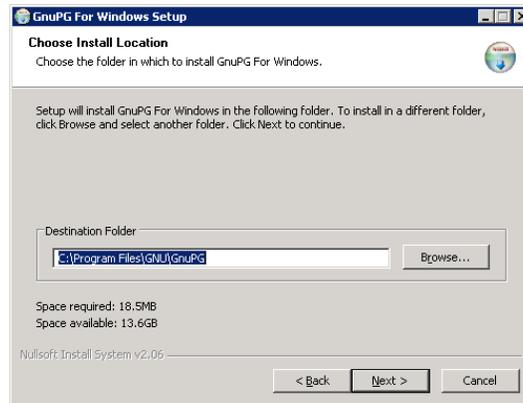


The recommended minimum installation consists of GnuPG, GPA, WinPT and the manuals. If required, the remaining programs can be installed later.

Click on [Next].

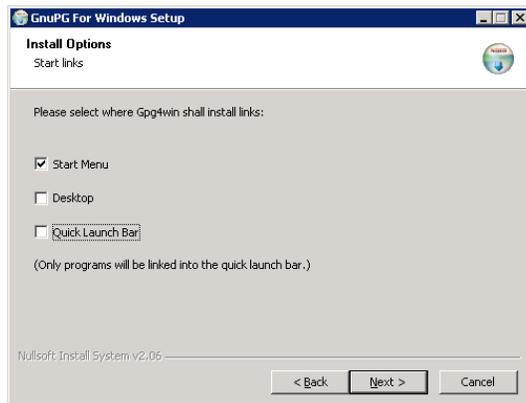
On this page you can choose the folder in which to install Gpg4win on your computer. If you do not enter a folder name, you should accept the default folder name, which is:

C:\Programme\GNU\GnuPG



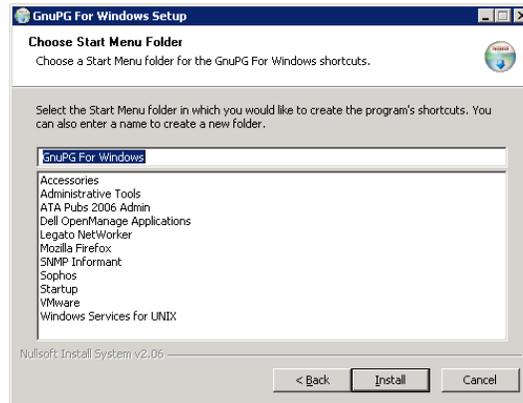
Click on [Next].

This page allows you to set start links for the program. The default setting adds Gpg4win to the start menu only. You can change these settings within Windows at anytime.



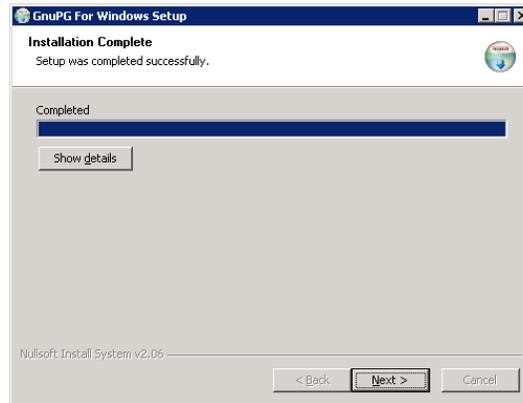
Click on [Next].

If you chose to add the program to the Start Menu (as per previous page), this page allows you to choose a Start Menu subfolder for the program.



For a standard installation, select the default setting and click on [Install].

During the installation a progress bar displays the file being installed. You can click on [Show details] to see a log of the installation.



Once the installation is complete, click on [Next].

The following page shows the last step of the installation process:



Click on [Finish].

You may need to restart Windows for the settings to take effect. In that case, instead of showing the installation completion page, the following page appears:



At this point you can choose to restart Windows automatically or restart later manually.

Click on [Finish].

And that's it!

You have now installed Gpg4win and are ready to use the program.

Prior to starting Gpg4win, we recommend reading Chapter 3 and 4 of the manual "Gpg4win for Advanced Users" (PDF-File). These chapters highlight the ingenious theory behind Gpg4win's ability to encrypt emails in a safe and user-friendly manner.

Of course you do not need to know all the technical details of Gpg4win to be able to use it. However, since you will use Gpg4win to handle your most sensitive correspondence and it probably is a good idea to understand the theory behind it.

...

The following section provides you with tips for creating a secure yet easy-to-remember passphrase.

♠ **At this point, please read Chapter 3 and 4 in the manual "Gpg4win for Advanced Users" before reading on.**

4. Creating a key pair

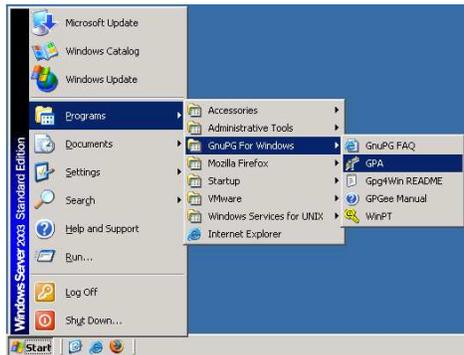
After reading the information explaining Gpg4win's security features and the creating of a good passphrase to protect your private key, this section shows you how to create a key pair.

The processes of creating a key, encryption and decryption are very important - so important that it should be possible to practice . . .

And this is what you actually can do: Run through the whole processes as often as you want. Those "dry-runs" help you gain confidence in using the program, so that some of the more intricate steps in creating keys will not pose any problems later on. You can use Adele to do this. It is a test server which was developed as part of the GnuPP project. Adele allows you to try and test several practice keys before creating your own set.

Let's get started!

Start the GPA program from your Windows Start menu:

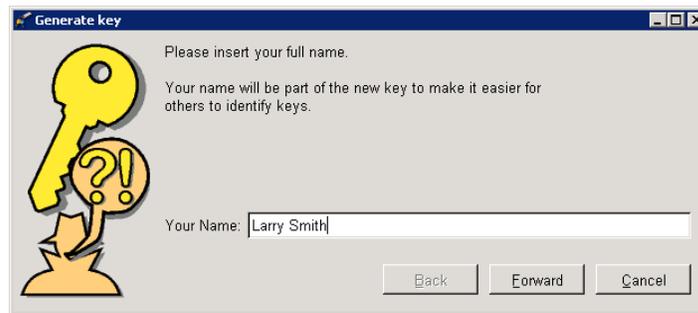


The following window appears:



Click on [Generate key now].

For practice purposes you can enter any name in the window for now, e.g. "Larry Smith".

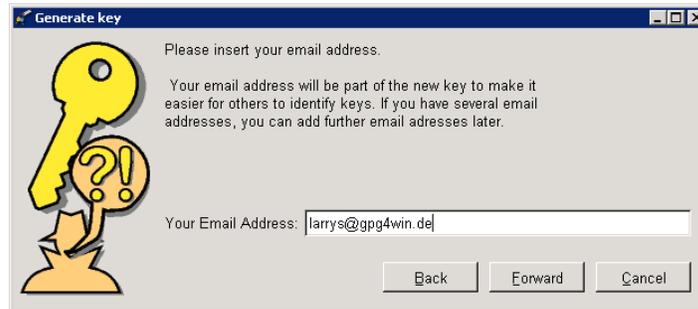


Or you can generate your 'real' key in which case you should enter your real name.

When you are done, click on [Forward].

Now enter your email address.

Again, if this is a test run, you can use an imaginary email address such as "larrys@gpg4win.de"



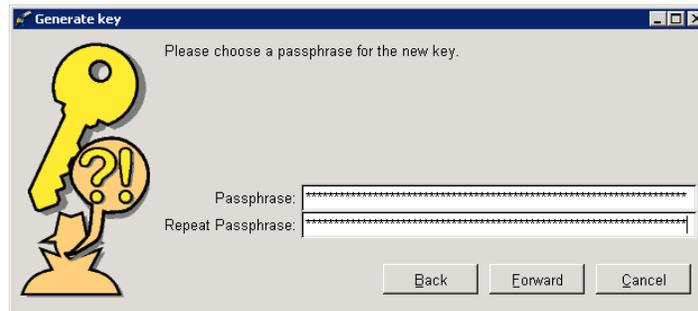
Or you can enter your real email address, and click on [Forward].

This option allows you to enter notes regarding your key. Usually this field is empty; however, if you are creating a test key, you should make a note, such as "test". The notes are a part of your User-ID and will be made public along with your name and email address. Now click on [Forward].

Entering a passphrase is one of the most important steps in the program, as the program is only as good (and as secure) as your passphrase!

Chapter 4 ("The Passphrase") from the manual "Gpg4win for Advanced Users" already provided you with suggestions on creating a secure passphrase. So, at this point you should have come up with your own passphrase - one that is private, easy to remember, and difficult to crack.

Enter your passphrase now.



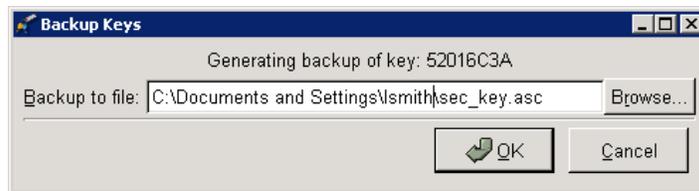
If the passphrase you entered is not very secure, a warning will be displayed, allowing you to enter a more secure passphrase.

Again, you can enter a test passphrase for practice purposes, or your real passphrase.

Once you have entered your passphrase twice, click on [Next].

This starts the creation of your key pair, which can take a few minutes. In the meantime, you can continue to work with other programs on your computer which will slightly increase the quality of the key being generated.

Once the key is generated, the following window appears:



This window asks you to create a back-up copy of your key. Please do this now, even if this is just a test run.

If the default file name is acceptable, click on [OK]. If you would like to store the back-up in a different location, please select a different file name now.

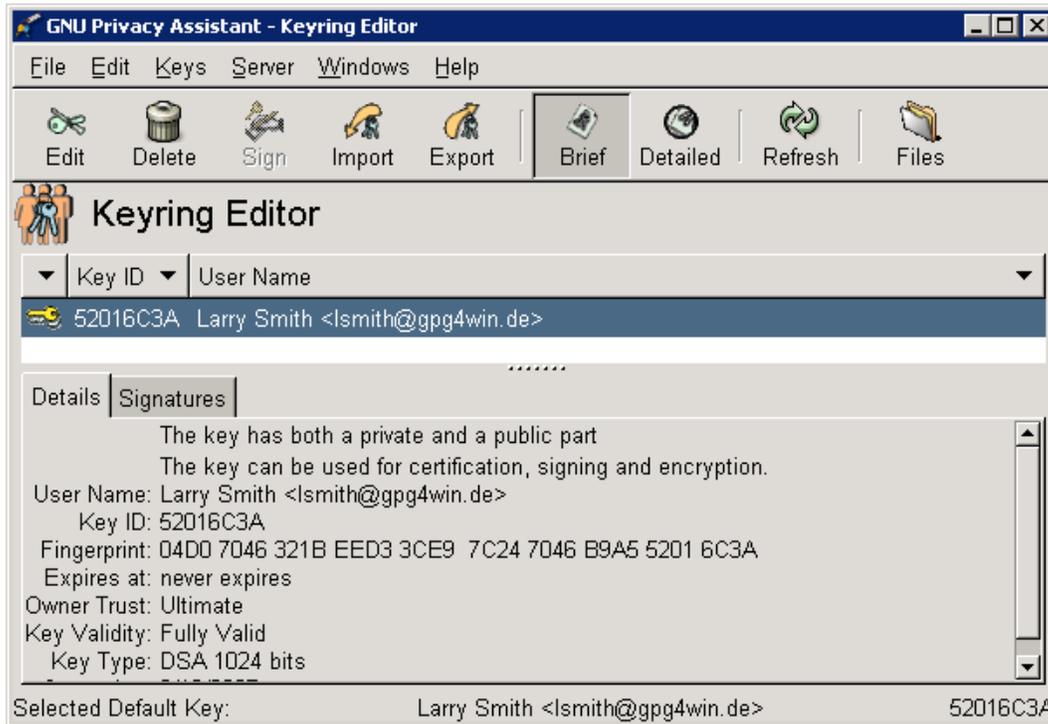
Important: Once the the back-up file is saved onto your hard drive, you should save this file onto a removable storage device (e.g. USB stick, diskette or CD-ROM), and subsequently delete the original file. Be sure to keep the storage device in a secure place.

Please note that you can create back-up copies at any time by selecting the following option from the main menu: *Key*→*Backup*.

This concludes the installation of Gpg4win and the generation of your key pair. You are now the owner of a unique and secure digital key.

You should now see the GPA's main window. The key pair you just created will be shown in the middle of the window, beside the key pair symbol.

Clicking on the key pair symbol will provide details about your key pair, which are discussed in more detail below.



What is the significance of the notes regarding your key? Your key has no built-in expiry date and is, therefore, valid indefinitely. You can, however, change the key's validity period - more about this later.

A key consisting of 1024 bits is considered very secure, without creating undue strain on your computer's capacity.

♠ **More information on this topic can be found in Chapter 5 "More about keys" in the manual "Gpg4win for Advanced Users".**

5. Publishing your key per email

One of the more practical aspects of Gpg4win is its ability to use a "non-secret" public key for the encryption and decryption of data. As long as your key and its corresponding passphrase are secure, you have gone a long way towards keeping your information confidential.

Everyone can and should have your public key, just as you can and should have the public keys of the people you correspond with.

Because:

In order to exchange secure emails, each party must have access to the public key of the other party.

In order to send someone encrypted emails, you must have their public key in order to encrypt the emails to send to them.

Similarly, someone wanting to send you encrypted emails must have your public key in order to encrypt the email being sent to you.

This is the reason that your public key should be made widely available. Depending on the number of correspondence partners, can do this in two ways:

- **directly sending an email** to selected recipients
- **or publishing the key on a key server** — making it available to anyone

The first way to distribute your public key is to send it by email to one or more selected recipients. Alternatively you can make your email address available to anyone in the Internet. The second option is somewhat risky, as it can result in considerable SPAM activity on your email account. Therefore it is a good idea to only use an address with a good SPAM filter.

You can use Adele to practice the following steps:

Adele is a very good email robot for practicing secure correspondence. Because most people prefer to correspond with a real person rather than with a piece of software (which is what Adele is, after all), we developed the following scenario:



You first send Adele your public key. Once Adele has received your key, she uses it to encrypt an email which she sends to you along with her own public key. You can now decrypt Adele's email using your own private key, and you can also respond to Adele by encrypting your email with her public key.

You can now export your public key, copy it into an email and send it to Adele.

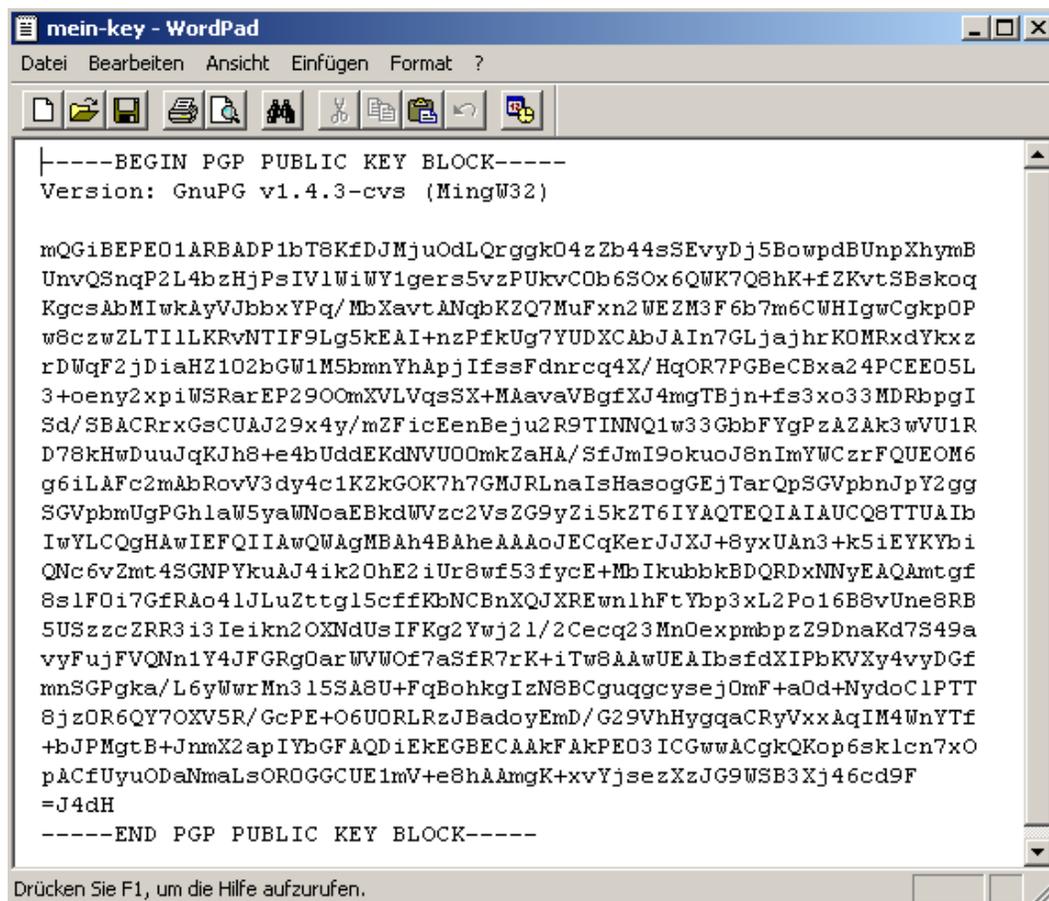
Here is one possible way of doing just that, a method which works even if your email service does not allow attachments. This procedure also gives you a first in-depth look at your key and its components.

How it works:

Select the key you want to export by clicking on the corresponding key on your list, and then clicking on the [Export] icon of the main GPA menu. Choose a file to export your key to, e.g.

`my-key.asc`. A popup window will let you know whether the operation was successful. Then click on [OK].

You can access the file through Windows Explorer; make sure you choose the same folder you chose when exporting the key. You can open the file with a text editor (ex. WordPad), which will show your public key as a series of blocks containing text and numbers.



```

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.3-cvs (MingW32)

mQGibEPEO1ARBADP1bT8KfDJMjuOdLQrggk04zZb44sSEvyDj5BowpdBUnpXhymB
UnvQSnqP2L4bzHjPsIV1WiWY1gers5vzPUkvCOB6SOx6QWK7Q8hK+fZKvtSBskoq
KgcsAbMIwkAyVJbbxYPq/MbXavtANqbKZQ7MuFxn2WEZM3F6b7m6CWHIgwCgkpOP
w8czwZLTI1LKrvNTIF9Lg5kEAI+nzPfkUg7YUDXCAbJAIn7GLjaJhrKOMRxdYkxz
rDWqF2jDiaHZ102bGW1M5bmnYhApjIffsFdnrcq4X/HqOR7PGBeCBxa24PCEE05L
3+oeny2xpiWSRarEP290OmXVLVqsSX+MAavaVBgfXJ4mgTBjn+fs3xo33MDRbpgI
Sd/SBACRrxGsCUAJ29x4y/mZFicEenBeju2R9TINNQ1w33GbbFYgPzAZAk3wVU1R
D78kHwDuuJqKJh8+e4bUddEKdNVU00mkZaHA/SfJmI9okuoJ8nImYWCzrFQUEOM6
g6iLAFc2mAbRovV3dy4c1KZkGOK7h7GMJRLnaIsHasogGEjTarQpSGVpbnJpY2gg
SGVpbmUgPGhlaW5yaWNoaEBkdWVzc2VsZG9yZi5kZT6IYAQTEQIAIAUCQ8TTUAib
IwYLCQgHAwIEFQIIAwQWAgMBAh4BAheAAoJECqKerJJXJ+8yxUAN3+k5iEYKYbi
QNC6vZmt4SGNPYkuAJ4ik2OhE2iUr8wf53fycE+MbIkubbkBDQRdxNNyEAQamtgf
8s1FOi7GfRao41JLuZttg15cfffKbNCBnXQJXREwnlhFtYbp3xL2Po16B8vUne8RB
5USzccZRR3i3Ieikn2OXNdUsIFKg2Ywj21/2Cecq23MnOexpmbpzZ9DnaKd7S49a
vyFujFVQNn1Y4JFGRgOarWVWOf7aSfr7rK+iTw8AAwUEAIbsfdXIPbKVXy4vyDGf
mnSGPgka/L6yWwrMn315SASU+FqBohkgIzN8BCguqgcysejOmF+aOd+NydoCLPTT
8jzOR6QY7OXV5R/GcPE+O6UORLRzJBadoyEmD/G29VhHygqaCRyVxxAqIM4WnYTF
+bJPMgtB+JnmX2apIYbGFaQDiEkEGBECAAkFAkPEO3ICGwwACgkQKop6sklcn7xO
pACfUyuOdaNmaLSOROGGCUE1mV+e8hAAmgK+xvYjsezXzJG9WSB3Xj46cd9F
=J4dH
-----END PGP PUBLIC KEY BLOCK-----

```

Drücken Sie F1, um die Hilfe aufzurufen.

Highlight the whole key portion from

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

to

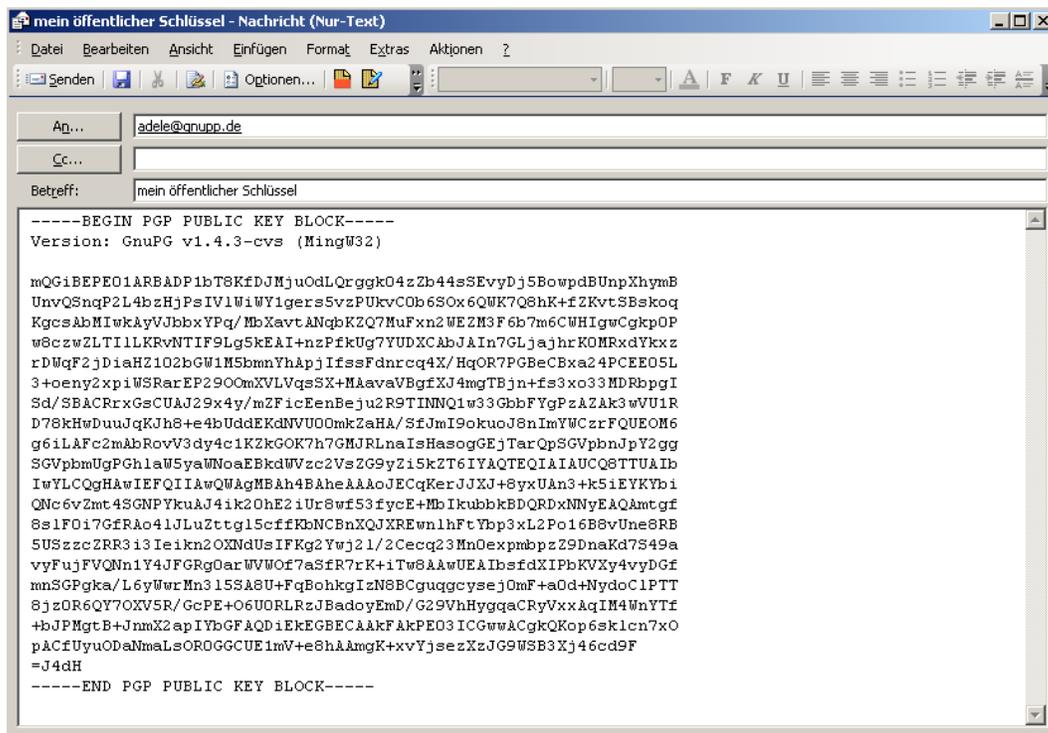
```
-----END PGP PUBLIC KEY BLOCK-----
```

and copy it using the copy function on your toolbar or a keyboard shortcut such as Ctrl-C. This saves your key on the clipboard until you are ready to paste it, as described below.

Start your email program. Open a new email message and paste your public key (Windows users may use a shortcut key such as Ctrl-V). Before doing this, you should configure your email program to send messages in text-only format rather than HTML.

Put `adele@gnupp.de` into the address line of the email, and **my public key** on the subject line.

Your email should look like this:



Now send this email to Adele. Make sure that you include your proper email address as sender rather than your practice address, otherwise you will never get a response from Adele!

This process works exactly the same way if you send your key to a real email address. You can add other text, just like in any other email. Obviously, this is not required for emails addressed to Adele, as the robot's only purpose is to help you with the technical aspects of this process.

Summary: You have now sent your public key by email to someone else (e.g. Adele).

♠ **The "Copy & Paste" method shown in this example is easily understood by beginners. Chapter 7 of the manual "Gpg4win for Advanced Users" describes how to send your key as a file attachment, which is a more commonly used method.**

6. Sending your key to a keyserver

You can use this option even if you are exchanging encrypted emails with only a few people. By making your key available on a keyserver, it is always accessible to you and/or others.

PLEASE NOTE: ALTHOUGH THERE ARE NO INDICATIONS THAT SPAMMERS ARE CURRENTLY COLLECTING ADDRESSES FROM KEYSERVERS, IT IS TECHNICALLY POSSIBLE TO DO SO. WE DO NOT, THEREFORE, RECOMMEND PUBLISHING YOUR KEY TO A KEY SERVER IF YOU DO NOT HAVE AN EFFECTIVE SPAM FILTER.

Choose your key by clicking on it. Then click on *Server* → *Send key* which is found under *Server* → *Server*. A popup window will alert you that your key is about to be sent to a public key server.



This window also displays a default key server. If you click on [Yes], your key will be automatically sent to the server, from where it is sent to a network of worldwide key servers. Now anyone can download your key, and use it to send you a secure email.

If this is a practice run, do NOT send your practice key to the key server because once sent, it cannot be removed.

Summary: You now know how to distribute your key via a key server on the Internet.

♠ Chapter 6 of the manual "Gpg4win for Advanced Users" explains how to find someone else's key on a keyserver.

7. Decrypting an email

Adele has received your public key, and uses it to encrypt an email which she sends back to you.



The email will look like this:

```
From: Adele (The friendly email-Robot) <adele@gnupp.de>
Subject: Re: my publis key
To: larrys@gpg4win.de
Date: Thu, 12 Jan 2006 09:17:28 +0100
```

```
-----BEGIN PGP MESSAGE-----
```

```
Version: GnuPG v1.4.1 (GNU/Linux)
```

```
hQE0A9FS8I3hSvdPEAP/W6W6f4MBwqTdzd9O/7FOTDhH//bQ+GUWoT0k9Y0i96UZ
QO1VhQSia6a8DZrFQj7SlJWmB1MM7RNhkmhfZsD5Bn9ICmwwOt2xJDBkCQ34gu5N
NxQ92WXZjHcaI0dSlynNziNbK8Ik26YPBYkQjLUDhHN4CRZ7q67eVED/B9DI04wD
```

```
....
```

```
ujbjyj09L/9NvoBniWrgqVUayKr1Ls8OIZkyiex6mKypPGADJFAzvTwjubj5S6zJ
A+QvSXUB9Hj8Ft2Nt3j0B/gWn5no3Er2/15UcBn/UPSxW9or0w9seDxCuSXvpakX
bcneOm/pcJNEHcApXWXpONoxRZ1MksM300w+79M6p2w=
=VCHb
```

```
-----END PGP MESSAGE-----
```

(Please note that the encryption sequence has been considerably shortened to save space in this manual.)

Using WinPT to decrypt this email.

WinPT (Windows Privacy Tray key management tool) serves as PnuPG's "front end". This program is used to encrypt and decrypt emails; it also creates and verifies digital signatures. One of WinPT's advantages is that it works with all email programs.

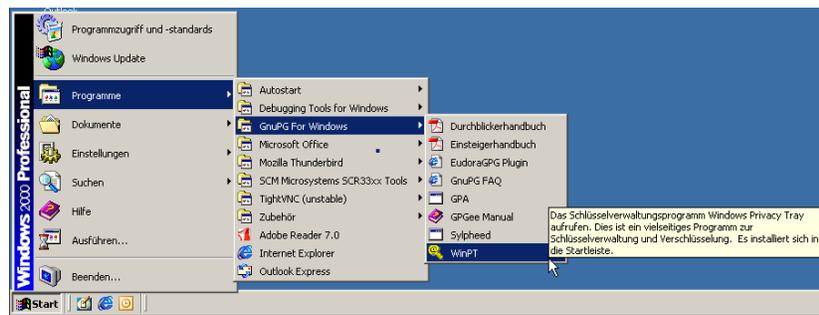
Most email programs (e.g. MS Outlook for Windows) also have special plug-ins which can encrypt and decrypt email directly within the program.

♠ **Chapter 8 of the manual "Gpg4win for Advanced Users" provides more information on this particular function.**

WinPT performs the en/decryption function using your computer's memory. This means that any text to be en/decrypted must be copied onto the computer's clipboard.

To do this, highlight the complete text in Adele's email and copy it onto the Clipboard using the copy function or the shortcut Ctrl-C.

Starting WinPT from Windows Start Menu:

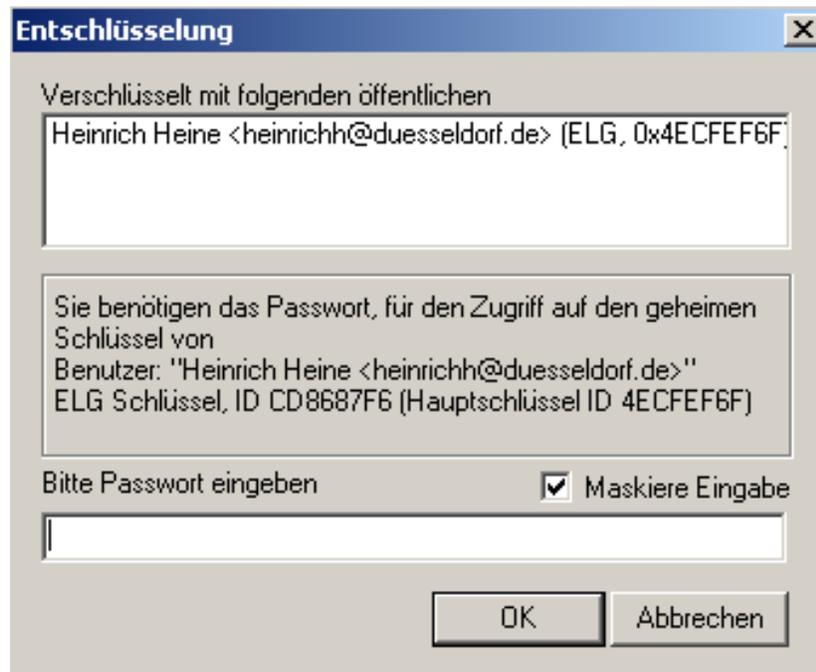


Once you open the program, the WinPT icon (a key) appears in the Windows taskbar, which is located in the lower right hand corner of the screen.



Right-click on the icon to open the menu box, and click on *Clipboard*→*Decrypt/Verify*.

The program will then ask you for your secret passphrase and proceed to decrypt Adele's email.



A popup window window will notify you when the decryption process is complete.

The decrypted text is now located on the clipboard, much in the same way as was done during the encryption process. You can copy the text (using shortcut key Ctrl-V) into your text editor or email program.

Adele's decrypted email will look something like this³:

Hello Larry Smith,

here is an encrypted response to your email.

I received your public key with the ID 57251332CD8687F6 and a description '<larrys@gpg4win.de>'.
'

I have enclosed the public key of adele@gnupp.de.

Sincerely,
adele@gnupp.de

The text sequence following this message is Adele's public key.

The next section shows you how to import someone's public key and attach it to your key ring, which allows you to use this key anytime to encrypt messages to that person (in this case, Adele) or to verify a digital signature.

Summary:

1. You know how to decrypt an encrypted email using your private key.
2. You know how to send an encrypted response using the public key of the sender.

³Depending on Adele's software version, it might look slightly different.

8. Attaching a key to your key ring

You can store your friends' public keys on your "key ring" so they do not have to send you their public key every time they write to you.

First Option:

To import a public key (ie. attach it to your key ring), you can save the key as a text block, much like you did with your own key.

To do this:

Highlight the public key portion of the email you received, from

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

to

```
-----END PGP PUBLIC KEY BLOCK-----
```

and use Copy & Paste to insert it into your text editor. We recommend using a file and folder name that is easily found later; e.g. `adeles-key.asc` in folder `My Documents`.

2nd Option:

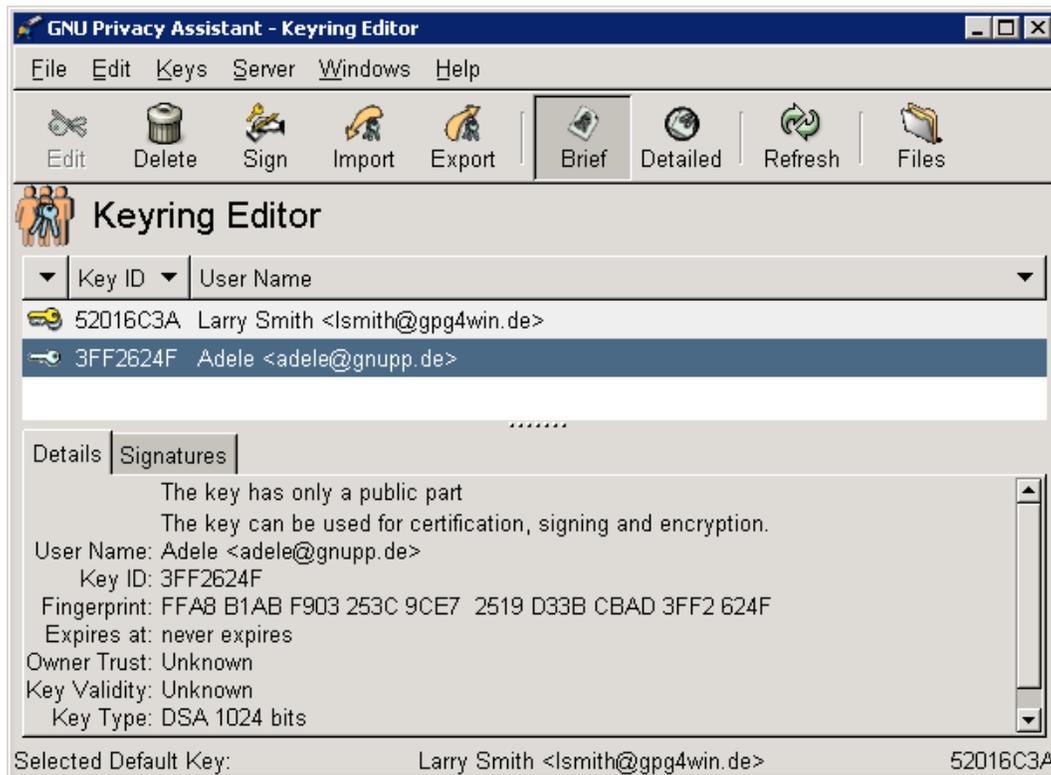
The key is sent to you as a file attachment to the email. No matter which mail program you use, you can always save attachments onto your hard drive. Do this now (again using names you will easily recognize and find later on, e.g. My Documents).

It does not matter whether you save the key as text or directly as an email attachment, as both methods import the key into your GnuPG-"Key Ring".

This is how it works:

Start the GNU Privacy Assistant (GPA) from Windows (this is necessary only if you shut it down after the previous practice session).

Click on Import, then select and load the key file.



You have now imported someone else's (in this case Adele's) public key and attached it to your key ring. Now you can use this key to send encrypted messages to the owner of that public key, as well as to verify his or her signature.

Before continuing, it is important to address the following concern:

It is possible that the email was sent by someone else using Adele's name, therefore how do you know that the public key sent to you is really Adele's key?

♠ **Chapter 9 ("Key Verification") in the "Gpg4win for Advanced Users" manual deals with this important question. You may want to read that section now before continuing with this manual.**

Chapter 9 of the manual "Gpg4win for Advanced Users" shows you how to validate a key as well as how to sign a message (i.e. attach a signature) using your private key.

Chapter 10 of the advanced manual also discusses ways to attach a signature to email messages. This is the equivalent of attaching an electronic seal to your message, allowing the recipient to verify whether the email has been altered during transmission (and that it came from you).

The signature verification process is simple. For this, you need the sender's public key on your Gpg4win-"key ring" (see Chapter 8 of "Gpg4win for Advanced Users" for more information).



You can tell whether an email has been electronically signed if the text of the email is framed with the sender's signature (like a border). It will look something like this:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
```

and ends email-message with

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.2 (MingW32)

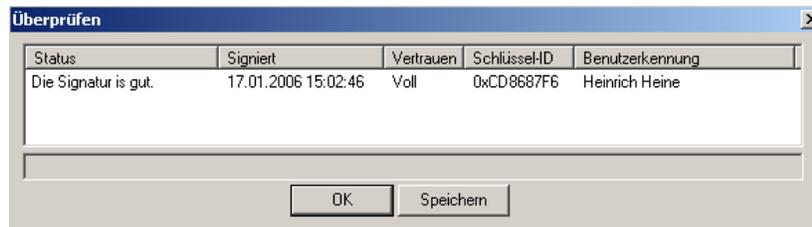
iEYEARECAAYFAjxeqy0ACgkQcwePex+3Ivs79wCfW8u
ytRsEXgzCrFpnjGrDDtb7QZIAN17B8l8gFQ3WIUUDCMfA5cQajHcm
=O6lY
-----END PGP SIGNATURE-----
```

Highlight the text starting from *BEGIN PGP SIGNED MESSAGE* to *END PGP SIGNATURE* and copy it (using Ctrl-C) to your clipboard.

Now continue to decrypt the email as shown in Chapter 7 of this manual.

Right-click on the WinPT icon on your Windows taskbar and select *Clipboard* → *Decrypt/Verify*.

You should see the following window:

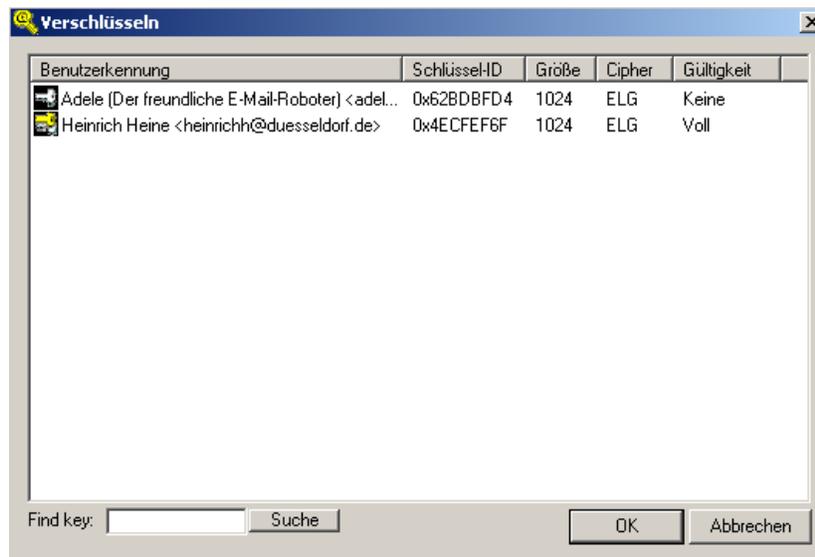


If the status line on the window displays the following message *Invalid Signature*

it means that the message has been altered after being sent. This does not always mean that a third party has altered the message, as it could also have been altered by a technical error during transmission through the Internet.

♠ **Before continuing, you may want to read Chapter 10 of the manual "Gpg4win for Advanced Users" which contains additional information on how to deal with invalid signatures.**

You should now see a window containing the keys on your key ring. Using the examples featured in this guide, you would see Adele's key (the one she sent to you), as well as your own key, which you created in Chapter 2 (FIXME: Use dynamic reference).



Click on Adele's key to encrypt the message you just composed, keeping in mind the following principle:

In order to send someone encrypted emails, you need to have that person's public key in order to encrypt the message properly.

Clicking on [OK] starts the encryption process, which will be confirmed by the program if successful.

10. How to archive/store encrypted emails

It is probably not wise to store the readable (clear)text of your encrypted emails on your computer (after all, they were encrypted for a reason). Therefore it is sensible to store encrypted copies of the emails.

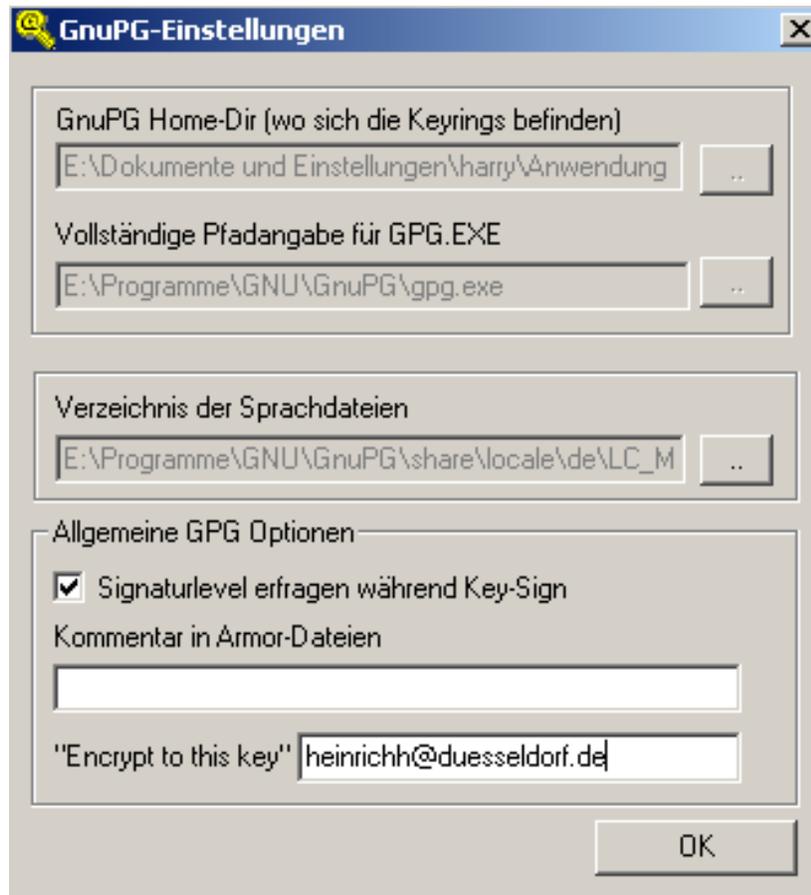
You may already have guessed resulting problem: To decrypt the archived emails you need the private key of the recipient, which will (should) never be available to you. . . .

The solution: You encrypt the messages to yourself as well.

You can encrypt a message designated for a recipient (e.g. Adele) using their own as well as your own public key, which allows you to decrypt the text later using your own private key.

Since Gpg4win cannot tell the difference between the different keys used to encrypt a message (ie. you could have more than one key), you need to set up the program accordingly.

To use this option, right click on the WinPT icon select *Preferences* → *GPG*.



This opens the GnuPG Preferences Window. You can add your key in the "Encrypt to this key" field using your email address.

email programs which directly support GnuPG will also feature this option.

Summary:

1. You responded to the recipient by encrypting an email with his/her public key.
2. You also set up WinPT to encrypt archived copies of your emails with your own public key.

And that's it - welcome to the world of free and secure email encryption!

♠ **We recommend you read Chapter 10 to 12 of the manual " Gpg4win for Advanced Users" for additional information on adding signatures to emails, as well as importing and using an existing private key in GnuPG.**

♠ **Furthermore, Chapters 13 and 14 of the manual "Gpg4win for Advanced Users" give you additional information about the ideas behind GnuPG's security features, as well as detailed insights into the mathematical concepts used. These chapters are easy to read, they were written for the every day user, not mathematicians and cryptographers.**

A. Suggestions regarding the Outlook plugin *GPGol*

GPGol, a Microsoft Outlook plugin, integrates the operation of GnuPG. Here are some tips about the operation of this plugin.

While it is fairly easy to operate the plugin in other email programs, technical difficulties associated with its integration of OpenPGP into Outlook make it harder to operate in this context.

The current version of GPGol works only with Outlook 2003 SP2 and will notify you if you are using an older version.

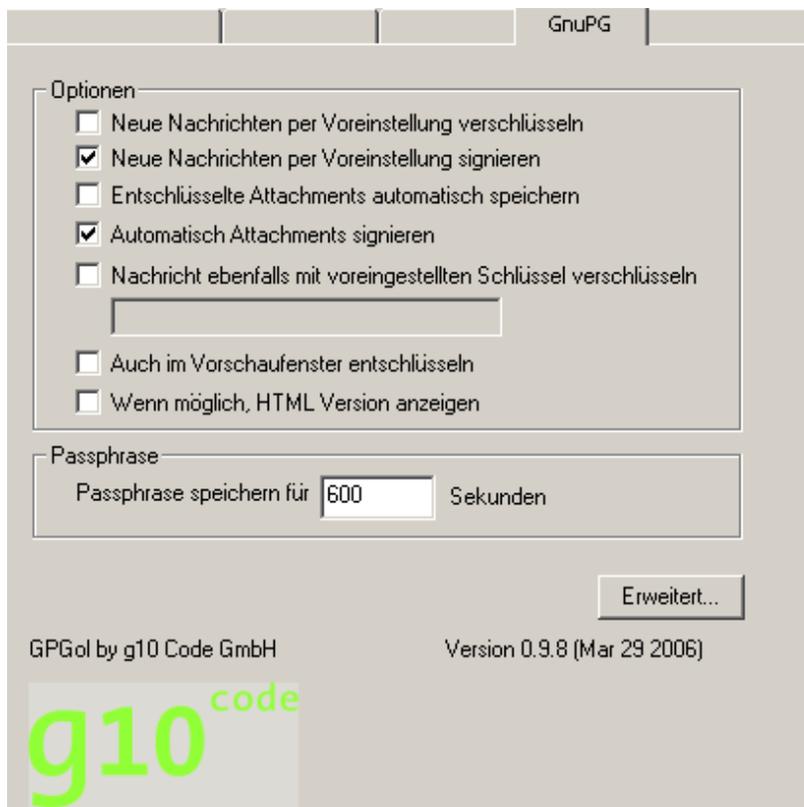
Please be aware of the following limitations:

- Do not use Word as your text editor.
- Inline-PGP or the conventional PGP is fully supported, however, PGP/MIME emails cannot be created.

On the other hand, decryption and signature verification of simple, as opposed to more complex, PGP/MIME emails, is not supported.

A.1. Installation

The plugin can be installed using the the Gpg4win Installer. The next time you start Outlook, a *GnuPG* tab will be added in the *Tools*→*Options* menu :



The first two options of this tab allow you to set default settings to do with encrypting and signing new messages. Note that you can always change these settings when creating new messages.

The option "Save decrypted message automatically" will save attachments as unencrypted text (after decryption). As a result, the attachment can be read anytime without having to decrypt it again.

The option "Automatically sign attachments" ensures that attachments are automatically signed along with your main text. For this purpose, an attachment with a signature is created for every attachment included in the message.

The option "Also encrypt message with the default key" allows you to enter the Key ID of your own key so that your messages are automatically (and additionally) encrypted using your own key. This allows you to later retrieve, decrypt and read messages in the Sent folder.

The option "Also decrypt in preview window" is only feasible with very fast computers; at the present time it has only limited operational capacity.

The option "Show HTML view if possible" enables you to view a message in HTML format. In most cases, or when an HTML format is not available, it will be shown in text format.

There are a number of preset default settings which take effect after initial installation. However, you should also ensure that you are not using **Microsoft Word** to compose messages. We also do not recommend using HTML messages.

You can set these options using the *Mail Format* tab in the *Tools*→*Options* menu. Your settings should look like this:



A.2. Common Questions

Encryption icons are not visible in the notification area/system tray. If the system tray contains a large number of icons, it may not display all of them. Clicking on the arrow at the right end of the system tray (located on the bottom right hand side of most computers) will open up the tray to show all icons, including the Key Manager icon.

Again, make sure that you are not using Microsoft Word to compose messages (see installation instructions).

What is the meaning of the letters included in the GnuPG tab? GPGol lists the components and their associated file names as part of the decryption or message signature verification. File names containing encrypted attachments are prefaced with "E", and signed attachments are marked with an "S".

Where can I locate information regarding the latest version GPGol? Click on the logo on the lower left side of your GnuPG options menu.

Why is it not possible to cancel an encryption process? GPGol begins the encryption process as soon as you press the Send button. An error contained in Outlook prevents you from interrupting or cancelling this process. To avoid this, we recommend configuring Outlook so that messages are not sent immediately. This gives you the opportunity to cancel the message before it is sent. As a security measure, GPGol will try to erase the contents of the message if the encryption process is interrupted, but this is not always successful.

Why does the confirmation window appear when accessing certain emails? If

GPGol is not installed as a trusted plugin, Outlook assumes that it is trying to access internal information without authorization. GPGol attempts to prevent this from happening, but sometimes it is necessary in order to properly display encrypted or signed emails.

GPGol is still "in development". One outstanding issue is its registration as a trusted plugin. Future versions of GPGol should be able to solve the issue of needing to confirm some or all emails.

How come GPGol cannot create PGP/MIME messages? At the present, there is no way of telling Outlook that a PGP/MIME message is to be created. Outlook decides on its own which "Content-Type" is to be used, as the plugin is not able to preset a certain type. You may want to contact Microsoft directly to talk about this setting and/or missing documentation regarding this setup.

Why are signature verifications not performed automatically? We are currently working on an automatic signature verification option to be used when opening an email. However, given Outlook's complex technical environment, this is not an easy issue to solve.

B. Transferring from other GnuPG programs

This section explains how to migrate from out GnuPG-based programs to Gpg4win. The installation program recognizes some of these programs and notifies you if that is the case.

As a general rule it is recommended that existing GnuPG-based programs be removed before installing Gpg4win.

Always save a backup of the existing keys. The best way to do this is to use the options in the existing system before installation Gpg4win. Select the option to save any private (secret) keys, as well as all existing public keys. Save these in one or two files.

As soon as Gpg4win is installed, check if your existing keys are listed in the new program (using either GPA or WinPT). If yes, Gpg4win was able to detect the previous key storage and you need take no further action.

If the program does not list the existing keys, you must import them from your backup file(s). For more information on this topic, refer to Chapter 12 in the manual "Gpg4win for Advanced Users".

If your older system also includes GPA, you can use its back-up option, which should be very similar to the operation of GPA in Gpg4win.

If you are not able to locate your existing keys, use the 'Search' function in Windows to find the files named `secring.gpg` and `pubring.gpg` and import them per GPA.⁴

⁴This is not the official procedure, but it works with all current versions of GnuPG.

C. History

- "GnuPP for Beginners", First Edition March 2002,
Authors: Manfred J. Heinze, TextLab text+media
Consulting: Lutz Zolondz, G-N-U GmbH
Illustrations: Karl Bihlmeier, Bihlmeier & Kramer GbR
Layout: Isabel Kramer, Bihlmeier & Kramer GbR
Documentation: Dr. Francis Wray, e-mediate Ltd.
Editor: Ute Bahn, TextLab text+media
Published by the German Federal Ministry for Industry & Technology.
Available at <http://www.gnupp.de/pdf/einsteiger.pdf>.
- Revised unpublished version by TextLab text+media.
- "Gpg4win für Einsteiger", December 2005
Authors: Werner Koch, g10 Code GmbH
Published as part of the Gpg4win project.
- "Gpg4win for Novices", November 2006
Translated by: Brigitte Hamilton
Published as part of the Gpg4win project.

D. GNU Free Documentation License

Version 1.2, November 2002

Copyright ©2000,2001,2002 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document “free” in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The “**Document**”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “**you**”. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A “**Modified Version**” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “**Secondary Section**” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “**Invariant Sections**” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “**Cover Texts**” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “**Transparent**” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “**Opaque**”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “**Title Page**” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

A section “**Entitled XYZ**” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “**Acknowledgements**”, “**Dedications**”, “**Endorsements**”, or “**History**”.) To “**Preserve the Title**” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further

copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some

or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section Entitled “Endorsements”, provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled “History” in the various original documents, forming one section Entitled “History”; likewise combine any sections Entitled “Acknowledgements”, and any sections Entitled “Dedications”. You must delete all sections Entitled “Endorsements”.

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version” applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright ©YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled “GNU Free Documentation License”.

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.