Gpg4win für Einsteiger

Eine Veröffentlichung des Gpg4win Projekts

Basierend auf einem Original von

Manfred J. Heinze, Karl Bihlmeier, Isabel Kramer

Dr. Francis Wray und Ute Bahn

Überarbeitet von

Werner Koch

Version 2.0.1 vom 26. April 2006

Impressum gpg4win

Die Angaben auf der **folgenden Seite** sind nicht mehr korrekt; wir können diese Seite allerdings nicht abändern, da die Regeln der GFDL hier falsch angewandt wurden. Neue Copyright Hinweise sollten deswegen hier eingestellt werden.

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

Inhaltsverzeichnis

1. Über dieses Handbuch

Das Gpg4win-Anleitungs- und Übungsmaterial besteht aus drei Teilen:

- **dem Schnelleinstieg, „Gpg4win für Einsteiger“,** in dem Sie gerade lesen,
- **dem Handbuch „Gpg4win für Durchblicker“** im PDF-Format, welches Sie nach der Installation von Gpg4win auf Ihrer Festplatte finden,
- **dem Übungsroboter Adele,** mit dem Sie die E-Mail-Ver- und Entschlüsselung so oft üben können, wie Sie wollen. Um mit Adele zu üben, brauchen Sie eine Internet-Verbindung.

„Gpg4win für Einsteiger“ führt Sie kurz und knapp durch die Installation und die alltägliche Benutzung der Gpg4win-Software. Der Zeitbedarf für das Durcharbeiten des Schnelleinstiegs hängt unter anderem davon ab, wie gut Sie sich mit Ihrem PC und Windows auskennen. Sie sollten sich in etwa eine halbe Stunde Zeit nehmen.

„Gpg4win für Durchblicker“ liefert Hintergrundwissen, das Ihnen die grundlegenden Mechanismen von Gpg4win verdeutlicht und die etwas seltener benutzten Fähigkeiten erläutert.

Beide Handbuchteile liegen als PDF Dateien vor. Falls Sie keine gedruckte Version erhalten haben, so können Sie sie auch selbst ausdrucken.

Die Handbuchteile können unabhängig voneinander benutzt werden. Zu Ihrem besseren Verständnis sollten Sie aber möglichst beide Teile in der angegebenen Reihenfolge lesen.

♠ Dieses Symbol weist auf auf den Wechsel in das andere Buch hin.

Der Übungsroboter Adele steht Ihnen im Internet zur Verfügung. Adele empfängt und sendet verschlüsselte E-Mails und entschlüsselt sie auch. Sie können also mit Adele einen kompletten Verschlüsselungsdialog so lange üben, bis Sie sich völlig mit dem Gebrauch der Software vertraut gemacht haben.

Adele ist im Rahmen des alten GnuPP Projektes entstanden und läuft dort noch immer. „Gpg4win für Einsteiger“ verwendet diesen zuverlässigen Übungsroboter und dankt den Inhabern von gnupp.de für den Betrieb von Adele.

2. Was ist Gpg4win?

Das Projekt Gpg4win (GNU Privacy Guard for Windows) ist eine vom Bundesamt für Sicherheit in der Informationstechnik beauftragte Email-Verschlüsselungssoftware. Gpg4win bezeichnet ein Gesamtpaket, welches die folgenden Programme umfasst:

GnuPG: das Kernstück, die Verschlüsselungs-Software
GPA: der GNU Privacy Assistent, eine Schlüsselverwaltung
WinPT: Schlüsselverwaltung, unterstützt auch Verschlüsselung per Clipboard
GPGol: ein Plugin für Microsoft Outlook, es integriert dort die Bedienung von GnuPG
GPGee: ein Plugin für den Windows Explorer, per rechter Maustaste können Dateien verschlüsselt werden
Sylpheed-Claws: ein komplettes Email-Programm mit integrierter GnuPG-Bedienung

Mit dem Verschlüsselungsprogramm GnuPG (GNU Privacy Guard) kann jedermann Emails sicher, einfach und kostenlos verschlüsseln. GnuPG kann ohne jede Restriktion privat oder kommerziell benutzt werden. Die von GnuPG eingesetzte Verschlüsselungstechnologie ist sehr sicher und kann nach dem heutigen Stand von Forschung und Technik nicht gebrochen werden.

GnuPG ist Freie Software[1]. Das bedeutet, dass jedermann das Recht hat, sie nach Belieben kommerziell oder privat zu nutzen. Jedermann darf den Quellcode, also die eigentliche Programmierung des Programms, genau untersuchen und auch selbst Änderungen durchführen und diese weitergeben.[2]

Für eine Sicherheits-Software ist diese garantierte Transparenz des Quellcodes eine unverzichtbare Grundlage. Nur so läßt sich die Vertrauenswürdigkeit eines Programmes prüfen.

GnuPG basiert auf dem internationalen Standard OpenPGP (RFC 2440), ist vollständig kompatibel zu PGP und benutzt die gleiche Infrastruktur (Schlüsselserver etc.).

PGP („Pretty Good Privacy“) ist keine Freie Software, sie war lediglich vor vielen Jahren kurzzeitig zu ähnlichen Bedingungen wie GnuPG erhältlich. Diese Version entspricht aber schon lange nicht mehr dem Stand der Technik.

Weitere Informationen zu GnuPG und den Projekten der Bundesregierung zum Schutz des Internets finden Sie auf der Website www.bsi-fuer-buerger.de des Bundesamtes für Sicherheit in der Informationstechnik.

[1] oft ungenau auch als Open Source Software bezeichnet
[2] Obwohl dies ausdrücklich erlaubt ist, sollte man ohne ausreichendes Fachwissen nicht leichtfertig Änderungen durchführen da hierdurch die Sicherheit der Software beeinträchtigt werden kann.

3. Sie installieren Gpg4win

Sollte bereits eine GnuPG basierte Anwendung, wie z.B. GnuPP, GnuPT, WinPT oder GnuPG Basics, auf Ihrem System installiert sein, so lesen sie jetzt bitte zuerst den Anhang B, um zu erfahren wie Sie Ihre vorhandenen Schlüssel übernehmen können.

Falls Sie Gpg4win auf einer CD-ROM erhalten haben:

Legen Sie diese CD-ROM in das CD-ROM-Laufwerk Ihres PCs und melden Sie sich als Administrator an. Öffnen Sie Ihren „Arbeitsplatz“ und klicken Sie dort auf das CD-ROM- Icon mit dem Titel „Gpg4win“. Wenn sich das CD-ROM-Icon geöffnet hat, klicken Sie auf das Installations-Icon mit dem Titel „Gpg4win“.

Haben Sie Gpg4win aus dem Internet heruntergeladen, so klicken Sie bitte auf diese neu abgespeicherte Datei, die den Namen `gpg4win-1.0.1.exe` (oder höhere Versionnummer) haben sollte. Achten Sie unbedingt darauf, dass Sie die Datei von einer vertrauenswürdigen Seite erhalten haben.

Die weitere Installation ist dann identisch:

Die Frage, ob Sie das Programm installieren wollen, beantworten Sie mit [Ja].

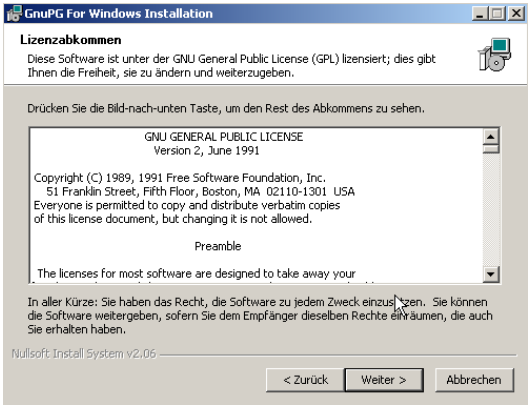
Es begrüßt Sie dieser Screen:

Beenden Sie alle möglicherweise auf Ihrem Rechner laufenden Programme, und klicken Sie dann auf [Weiter].

Auf der Seite mit dem Lizenzabkommen, können Sie Informationen zu den Lizenzen dieser Software lesen.

Wenn Sie die Software lediglich installieren und einsetzen wollen, so haben Sie immer das Recht dazu und sind nicht angehalten diese Texte zu lesen.

Geben Sie allerdings diese Software weiter oder wollen Sie sie verändern, so müssen Sie sich mit den Bedingungen der Lizenzen vertraut machen.

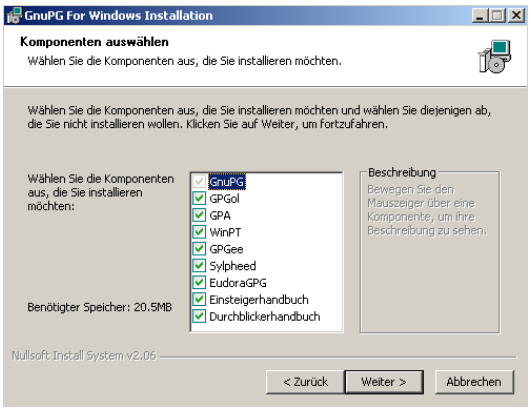


Klicken Sie auf [Weiter].

Auf der Seite mit der Komponentenauswahl können Sie entscheiden welche Programme Sie installieren möchten.

Wenn Sie mit der Maus über die Auswahl laufen, dann erscheint jeweils rechts eine Kurzbeschreibung die Ihnen bei der Entscheidung hilft.

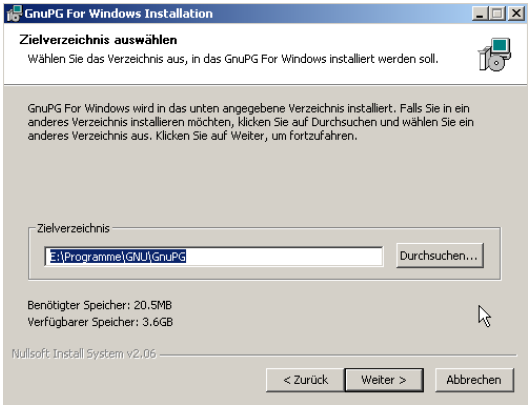
Die Anzeige des benötigen Speichers auf der Festplatte hilft Ihnen vielleicht ebenfalls weiter.



Sinnvoll ist es, mindestens GnuPG, GPA, WinPT und die Handbücher zu installieren. Den Rest können Sie bei Bedarf auch später installieren.

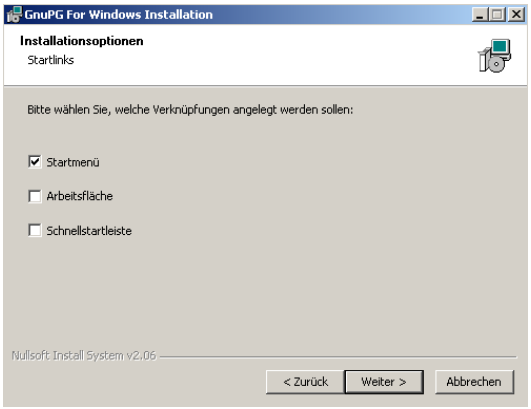
Klicken Sie auf [Weiter].

In der nun folgenden Dateiauswahl können Sie einen Ordner auf Ihrem PC aussuchen, in dem Gpg4win installiert wird. Sie sollten hier im Normalfall den voreingestellten Ordner
`C:\Programme\GNU\GnuPG`
übernehmen.



Klicken Sie anschließend auf [Weiter].

Auf der folgenden Seite können Sie festlegen, welche Verknüpfungen installiert werden. Voreingestellt ist lediglich eine Verknüpfung mit dem Startmenü. Bitte beachten Sie, daß sie diese Verknüpfungen auch jederzeit später mit den Bordmitteln von Windows verändern können.

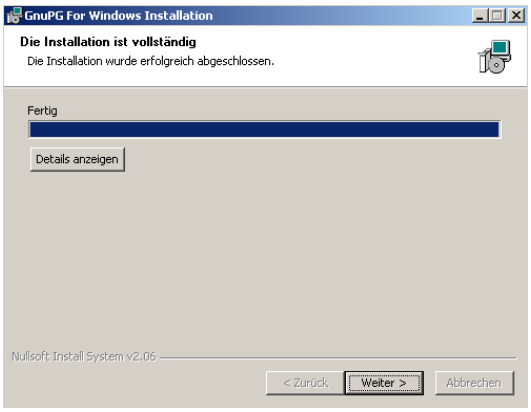


Klicken Sie anschließend auf [Weiter].

Falls Sie auf der vorhergehenden Seite eine Verknüpfung mit dem Startmenü ausgewählt haben (dies ist die Voreinstellung), so wird Ihnen nun eine Seite angezeigt, mit der Sie den Namen dieses Startmenüs auswählen können.

Am einfachsten übernehmen Sie die vorgeschlagene Einstellung und klicken dann auf [Installieren].

Während der nun folgenden Installation sehen Sie einen Fortschrittsbalken und Informationen, welche Datei momentan installiert wird. Sie können jederzeit auf [Details anzeigen] drücken um ein Protokoll der Installation sichtbar zu machen.



Nachdem die Installation abgeschlossen ist, drücken Sie bitte auf [Weiter].

Die letzte Seite des Installationsvorgangs wird nun angezeigt:

Klicken Sie auf [Fertig stellen].

In einigen Fällen kann es vorkommen, dass Windows neu gestartet werden muss. In diesem Fall sehen Sie statt der vorherigen die folgende Seite:

Sie können hier auswählen, ob Windows sofort neu gestartet werden soll oder später manuell.

Klicken Sie hier auch auf [Fertig stellen].

Das war’s schon!

Sie haben Gpg4win installiert und können es gleich zum ersten Mal starten.

Vorher sollten Sie aber im Handbuch „Gpg4win für Durchblicker“ (PDF-Datei) die Kapitel 3 und 4 lesen. Wir erklären dort den genialen Trick, mit dem Gpg4win Ihre E-Mails sicher und bequem verschlüsselt. Gpg4win funktioniert zwar auch, ohne dass Sie verstehen warum, aber im Gegensatz zu anderen Programmen wollen Sie Gpg4win schließlich Ihre geheime Korrespondenz anvertrauen. Da sollten Sie schon wissen, was vor sich geht.

Außerdem ist die ganze Angelegenheit ziemlich spannend. . .

Weiter geben wir Ihnen einige Tipps, mit denen Sie sich einen sicheren und trotzdem leicht zu merkenden Passwortsatz ausdenken können.

♠ Lesen Sie jetzt im Handbuch „Gpg4win für Durchblicker“ die Kapitel 3 und 4, und lesen Sie bitte erst danach hier weiter.

4. Sie erzeugen Ihr Schlüsselpaar

Nachdem Sie gelesen haben, warum GnuPG so sicher ist und wie ein guter Passwortsatz als Schutz für Ihren geheimen Schlüssel entsteht, werden wir Ihr Schlüsselpaar erzeugen.

Eigentlich müsste man so einen wichtigen Schritt ein paar Mal üben können. . .

Und genau das können Sie auch tun: Sie können den gesamten Ablauf der Schlüsselerzeugung, Verschlüsselung und Entschlüsselung durchspielen, so oft Sie wollen, bis Sie ganz sicher sind.

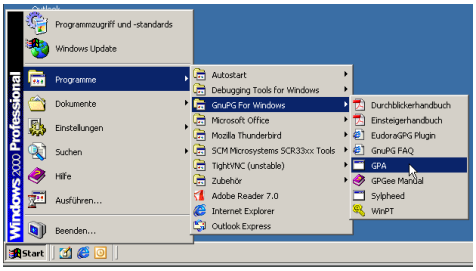
Ihr Vertrauen in Gpg4win wird sich durch diese „Trockenübung“ festigen, und die „heisse Phase“ der Schlüsselerzeugung wird danach kein Problem mehr sein.

Ihr Partner bei diesen Übungen wird Adele sein.

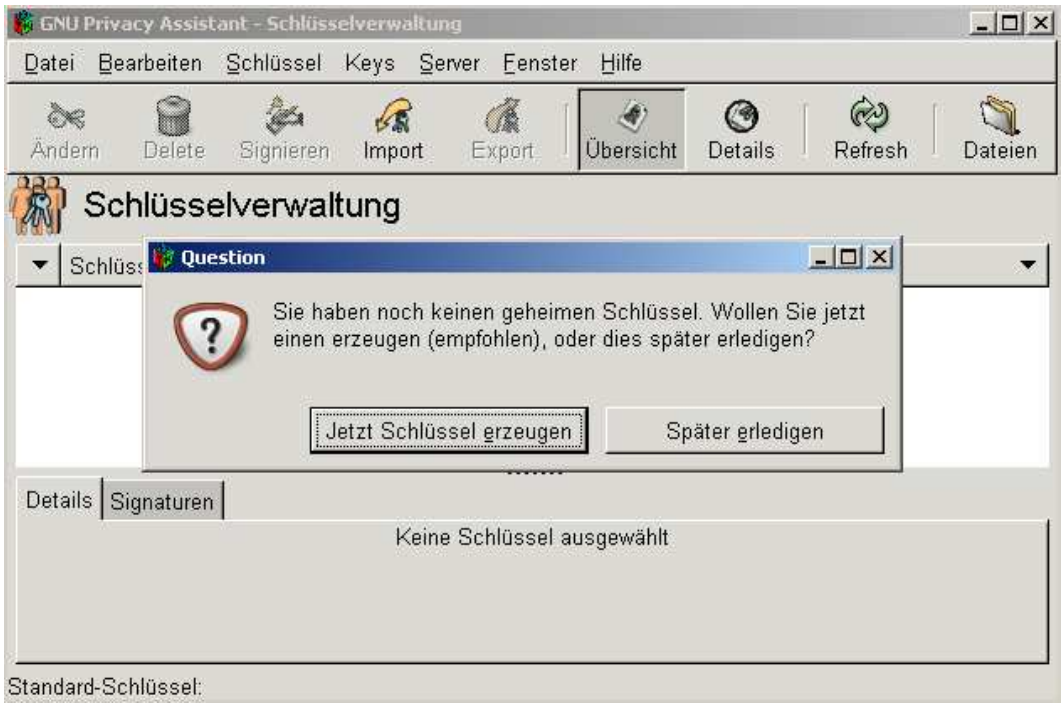
Adele ist ein Testserver, der noch aus dem alten GnuPP Projekt stammt. Mit Hilfe von Adele können Sie Ihre Schlüssel, die wir gleich erzeugen werden, ausprobieren und testen, bevor Sie damit Ernst machen. Doch dazu später mehr.

Los geht's!

Rufen Sie das Programm GPA über das Windows Startmenü auf:

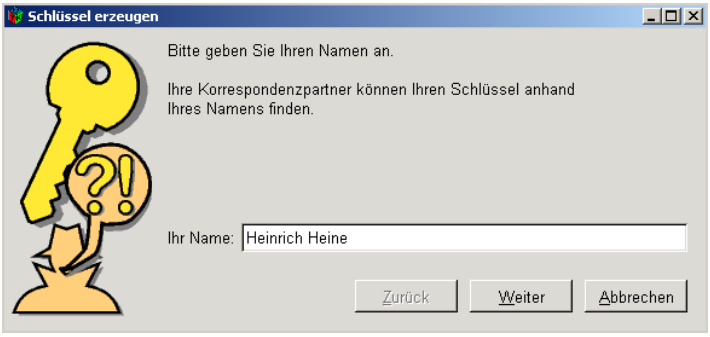


Daraufhin sehen Sie diesen Dialog:



Klicken Sie auf [Jetzt Schlüssel erzeugen].

Wenn Sie die Schlüsselerzeugung zunächst einmal testen wollen, dann können Sie im nun folgenden Fenster einen beliebigen Namen eingeben, z.B. „Heinrich Heine“.

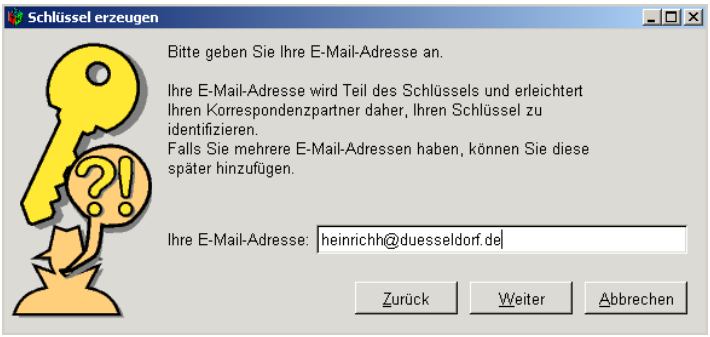


Oder Sie können auch gleich „Ernst machen“ und Ihren richtigen Namen eingeben.

Klicken Sie auf [Weiter], wenn Sie fertig sind.

Als nächstes geben Sie Ihre eigene E-Mail-Adresse an.

Wieder gilt: Sie können die Schlüsselerzeugung zunächst einmal mit irgendeiner ausgedachten E-Mail-Adresse durchtesten, z.B. „`heinrichh@gpg4win.de`“



Oder Sie können auch gleich Ihre echte E-Mail-Adresse eingeben.

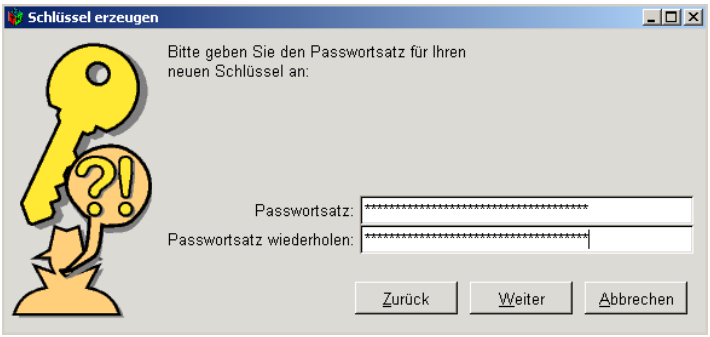
Klicken Sie auf [Weiter], wenn Sie die E-Mail-Adresse eingegeben haben.

Anschliessend können Sie einen Kommentar zum Schlüssel eingeben. Normalerweise bleibt dieses Feld leer; wenn sie aber einen Testschlüssel erzeugen sollten Sie dort als Erinnerung „test“ eingeben. Dieser Kommentar ist Teil Ihrer User-ID und genau wie der Name und die E-Mail-Adresse später öffentlich sichtbar. Klicken Sie auch dort anschließend auf [Weiter].

Jetzt folgt der wichtigste Teil: die Eingabe Ihres Passwortsatzes.

Erinnern Sie sich an das Kapitel 4, „Der Passwort-Satz“ im Handbuch „Gpg4win für Durchblicker“ das Sie eben durchgelesen haben? Wir haben Ihnen dort einige Tipps zur Erzeugung eines sicheren Passwortsatzes gegeben.

Dann sollten Sie nun einen geheimen, einfach zu merkenden und schwer zu knackenden Passwortsatz parat haben und hier eintragen.



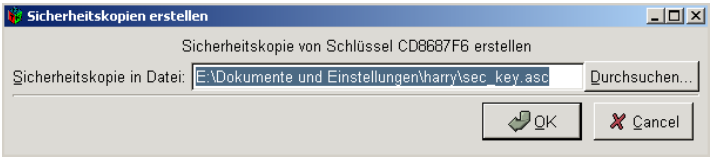
Falls der Passwortsatz nicht sicher genug sein sollte, werden Sie darauf hingewiesen.

Auch an dieser Stelle können Sie – wenn Sie wollen – zunächst einen Test-Passwortsatz eingeben oder auch gleich „Ernst machen“.

Wenn Sie Ihren geheimen Passwortsatz zweimal eingegeben haben, klicken Sie auf [Weiter].

Nun wird Ihr Schlüsselpaar angelegt. Dies kann kann u.U. einige Minuten dauern. Sie können in der Zwischenzeit mit einer anderen Anwendung Ihres Rechner weiterarbeiten und erhöhen hierdurch sogar leicht die Qualität des erzeugten Schlüsselpaars.

Sobald die Schlüsselgenerierung abgeschlossen ist, werden Sie den folgenden Dialog sehen:



Sie werden hier gebeten, eine Sicherheitskopie Ihres Schlüssels anzulegen. Tun Sie das jetzt, auch wenn Sie den Ablauf nur üben:

Wenn Sie mit dem voreingestellten Dateinamen zufrieden sind, so klicken Sie auf [OK]. Falls Sie das Backup woanders speichern möchten, so wählen Sie bitte vorher einen anderen Dateinamen aus.

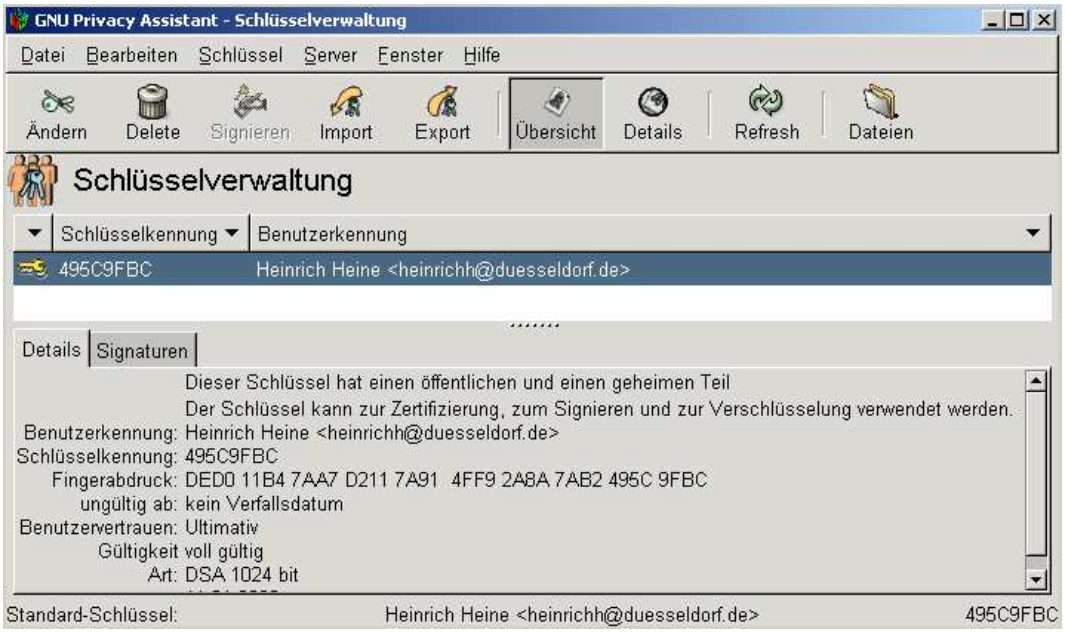
Wichtig: Falls Sie die Datei — wie voreingestellt — auf der Festplatte abgespeichert haben, so sollten Sie baldmöglichst diese Datei auf einen anderen Datenträger (USB Stick, Diskette oder CDROM) kopieren und diese Orginaldatei löschen. Bewahren Sie diesen Datenträger sicher auf.

Sie können eine Sicherungskopie auch jederzeit später anlegen; wählen Sie hierzu aus dem Hauptmenü *Schlüssel→Sicherheitskopie anlegen*.

Damit ist die Installation von Gpg4win und die Erzeugung Ihres Schlüsselpaares abgeschlossen. Sie besitzen nun einen einmaligen und sicheren digitalen Schlüssel.

Sie sehen jetzt wieder das Hauptfenster von GPA. In der Mitte des Fensters – hinter dem Symbol der doppelten Schlüssel – sehen Sie Ihr soeben erzeugtes Schlüsselpaar.

Wenn Sie Ihr Schlüsselpaar anklicken, sehen Sie einige Details, die Sie gleich nachlesen können.



Was bedeuten die Anmerkungen über Ihren Schlüssel? Ihr Schlüssel ist unbegrenzt gültig d.h., er hat kein „eingebautes Verfallsdatum“. Man kann die Gültigkeit nachträglich verändern – dazu später mehr.

Ein Schlüssel mit einer Länge von 1024 Bit ist ein sicherer Schlüssel, der trotzdem nicht zuviel Rechenkraft auf Ihrem Computer beansprucht.

♠ Lesen Sie nun im Handbuch „Gpg4win für Durchblicker“ Kapitel 5 „Schlüssel im Detail“ weiter. Sie können dieses Kapitel jetzt lesen oder später, wenn Sie diese Informationen benötigen

5. Sie veröffentlichen Ihren Schlüssel per E-Mail

Beim täglichen Gebrauch von Gpg4win ist es sehr praktisch, dass Sie es beim Ver- und Entschlüsseln stets nur mit den „ungeheimen“ öffentlichen Schlüsseln zu tun haben. Solange Ihr eigener geheimer Schlüssel und der ihn schützende Passwortsatz sicher sind, haben Sie das Wichtigste zur Geheimhaltung bereits erledigt.

Jedermann darf und soll Ihren öffentlichen Schlüssel haben, und Sie können und sollen öffentliche Schlüssel von Ihren Korrespondenzpartnern haben — je mehr, desto besser.

Denn:

Um sichere E-Mails austauschen zu können, müssen beide Partner jeweils den öffentlichen Schlüssel des anderen besitzen und benutzen.

Wenn Sie also an jemanden verschlüsselte E-Mails schicken wollen, müssen Sie dessen öffentlichen Schlüssel haben und zum Verschlüsseln benutzen.

Wenn – andersherum – jemand Ihnen verschlüsselte E-Mails schicken will, muss er Ihren öffentlichen Schlüssel haben und zum Verschlüsseln benutzen.

Deshalb werden Sie nun Ihren öffentlichen Schlüssel öffentlich zugänglich machen. Je nachdem, wie groß der Kreis Ihrer Korrespondenzpartner ist, gibt es zwei Möglichkeiten:

- **direkt per E-Mail** an bestimmte Korrespondenzpartner
- **oder auf einem Schlüsselserver** — weltweit für jedermann zugänglich

Die erste Möglichkeit, Ihren öffentlichen Schlüssel zu verbreiten, besteht wie gesagt darin, dass Sie ihn per E-Mail an einen oder mehrere Korrespondenzpartner schicken. Bei der zweiten Möglichkeit ist Ihre E-Mail-Adresse weltweit für jedermann zugänglich. Dies birgt leider das Risiko, dass Ihnen auch ungebetene Personen E-Mails schreiben können und die SPAM-Menge für Ihre E-Mail-Adresse dadurch zunehmen kann. Sie sollten daher im zweiten Fall einen ausreichenden SPAM-Schutz nutzen.

Zum Üben dieses Vorgangs kommt nun Adele ins Spiel:

Adele ist ein sehr netter E-Mail-Roboter, mit dem Sie zwanglos korrespondieren können. Weil man gewöhnlich mit einer klugen und netten jungen Dame lieber korrespondiert als mit einem Stück Software (was Adele in Wirklichkeit natürlich ist), haben wir sie uns so vorgestellt:

Adele schicken Sie zunächst Ihren öffentlichen Schlüssel. Wenn Adele Ihren Schlüssel empfangen hat, verschlüsselt sie damit eine E-Mail an Sie und sendet sie zurück.

Diese Antwort von Adele entschlüsseln Sie mit Ihrem eigenen geheimen Schlüssel. Damit Sie wiederum Adele verschlüsselt antworten können, legt Adele ihren eigenen öffentlichen Schlüssel bei.

Adele verhält sich also genau wie ein richtiger Korrespondenzpartner. Allerdings sind Adeles E-Mails leider bei weitem nicht so interessant wie die Ihrer echten Korrespondenzpartner. Andererseits können Sie mit Adele so oft üben, wie Sie wollen – was Ihnen ein menschlicher Adressat wahrscheinlich ziemlich übel nehmen würde.

Wir exportieren also nun Ihren öffentlichen Schlüssel, kopieren ihn in eine E-Mail und senden diese an Adele.

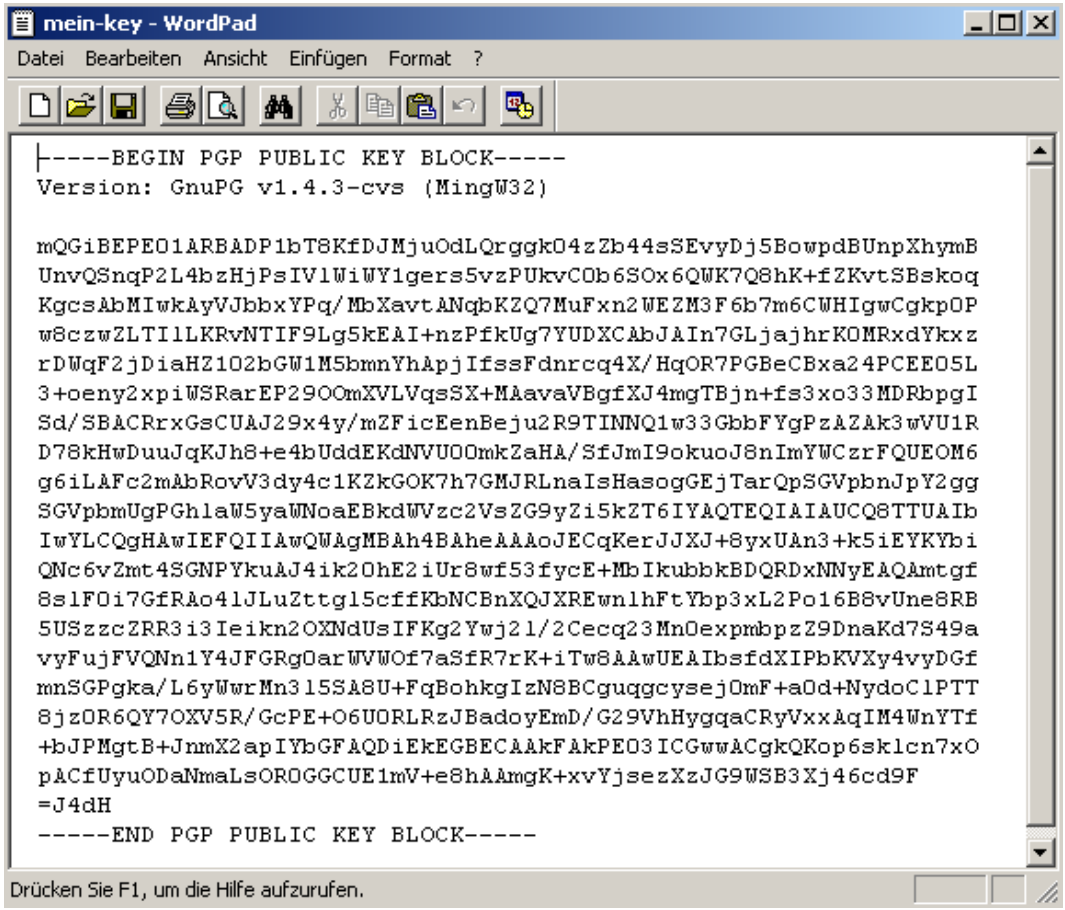
Die hier zuerst gezeigte Möglichkeit funktioniert immer, selbst wenn Sie – z.B. bei manchen E-Mail-Services im Web – keine Dateien anhängen können. Zudem bekommen Sie so Ihren Schlüssel zum ersten Mal zu Gesicht und wissen, was sich dahinter verbirgt und woraus der Schlüssel eigentlich besteht.

Und so geht's:
Selektieren Sie den zu exportierenden Schlüssel (durch klicken auf die entsprechende Zeile in der Liste der Schlüssel) und klicken Sie dann auf [Export] in der Iconleiste von GPA. Wählen Sie dann einen geeigneten Ordner auf Ihrem PC aus und speichern Sie den Schlüssel dort z.B. als `mein-key.asc`.

Über den Erfolg dieser Operation werden Sie durch eine Hinweisbox informiert. Klicken Sie dort dann auf [OK].

Sehen Sie sich dann diese Datei mit dem Explorer an. Sie müssen hierzu denselben Ordern auswählen, den Sie beim Exportieren angegeben haben.

Öffnen Sie diese Datei mit einem Texteditor, z.B. mit WordPad. Sie sehen Ihren öffentlichen Schlüssel im Texteditor so, wie er wirklich aussieht – ein ziemlich wirrer Text- und Zahlenblock:



Markieren Sie nun den gesamten Schlüssel von

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

bis

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

und kopieren Sie ihn mit dem Menübefehl oder mit dem Tastaturkürzel Strg+C. Damit haben Sie den Schlüssel in den Speicher Ihres Rechners – bei Windows Zwischenablage genannt – kopiert.

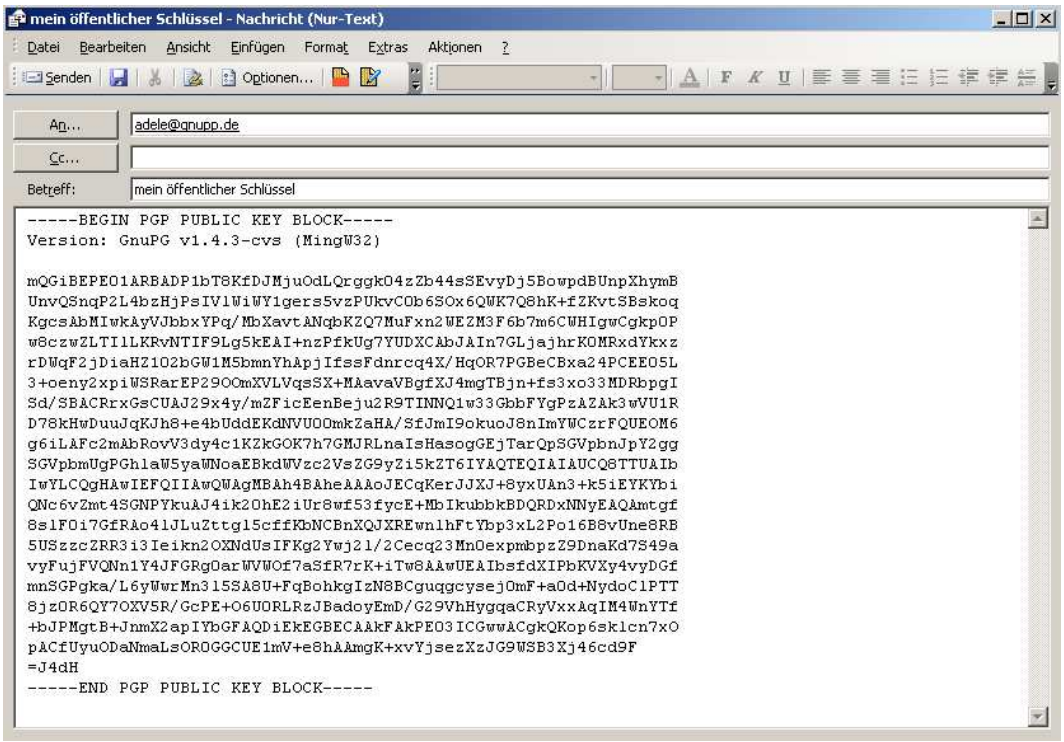
Nun starten Sie Ihr Mailprogramm – es spielt keine Rolle, welches Sie benutzen – und fügen Ihren öffentlichen Schlüssel in eine leere E-Mail ein. Der Tastaturbefehl zum Einfügen („Paste“) lautet bei Windows Strg+V. Es ist sinnvoll vorher das Mailprogramm so zu konfigurieren, dass reine Textnachrichten gesendet werden und keine HTML formatierte Nachrichten.

Diesen Vorgang – Kopieren und Einfügen – kennen Sie sicher als „Copy & Paste“.

Adressieren Sie nun diese E-Mail an `adele@gnupp.de` und schreiben in die Betreffzeile:

mein öffentlicher Schlüssel

So etwa sollte Ihre E-Mail nun aussehen:



Schicken Sie die E-Mail an Adele nun ab. Nur zur Vorsicht: natürlich sollten Ihre E-Mails **nicht** `heinrichh@gpg4win.de` oder ein andere Beispieladresse als Absender haben, sondern *Ihre eigene E-Mail-Adresse*. Denn sonst werden Sie nie Antwort von Adele bekommen. . .

Genauso gehen Sie vor, wenn Sie Ihren Schlüssel an eine echte E-Mail-Adresse senden. Natürlich können Sie dann auch noch ein paar erklärende Sätze dazuschreiben. Adele braucht diese Erklärung nicht, denn sie ist zu nichts anderem als zu diesem Zweck programmiert worden.

Fassen wir kurz zusammen: Sie haben Ihren öffentlichen Schlüssel per E-Mail an einen Korrespondenzpartner geschickt.

♠ Im Handbuch „Gpg4win für Durchblicker“ Kapitel 7 beschreiben wir, wie Sie Ihren Schlüssel auch als Dateianhang versenden.

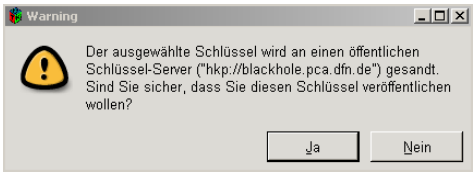
Das ist oftmals das einfachere und gebräuchlichere Verfahren. Wir haben Ihnen hier die „Copy & Paste“-Methode zuerst vorgestellt, weil sie transparenter und leichter nachzuvollziehen ist. Sie können dieses Kapitel jetzt lesen oder später, wenn Sie diese Funktion benötigen.

6. Sie veröffentlichen Ihren Schlüssel per Keyserver

Diese Möglichkeit bietet sich eigentlich immer an, selbst wenn Sie nur mit wenigen Partnern verschlüsselte E-Mails austauschen. Ihr Schlüssel ist dann sozusagen „stets griffbereit“ auf einem Server im Internet vorhanden.

VORSICHT: OBWOHL ES NOCH KEINE HINWEISE GIBT, DASS SPAMMER ADRESSEN WIRKLICH VON DEN KEYSERVERN SAMMELN, SO IST DIES JEDOCH TECHNISCH MÖGLICH. FALLS SIE KEINEN WIRKSAMEN SPAMFILTER BENUTZEN, SOLLTEN SIE U.U. VON DER VERÖFFENTLICHUNG IHRES SCHLÜSSELS AUF EINEM KEYSERVER ABSEHEN.

Klicken Sie Ihren Schlüssel an und wählen Sie dann den Menüpunkt *Server→Schlüssel verschicken*.



Wie Sie sehen, ist ein Keyserver bereits voreingestellt. Wenn Sie auf [Ja] klicken, wird der Schlüssel an den Server geschickt und von dort aus an die anderen, weltweit verbundenen Keyserver weitergereicht. Jedermann kann ihn von dort herunterladen und dazu benutzen, Ihnen eine sichere E-Mail zu schreiben.

Wenn Sie den Ablauf im Moment nur testen, dann schicken Sie den Übungsschlüssel nicht ab. Er ist wertlos und kann nicht mehr vom Schlüsselserver entfernt werden. Sie glauben nicht, wieviele Testkeys mit Namen wie „Julius Caesar“, „Helmut Kohl“ oder „Bill Clinton“ dort herumliegen schon seit Jahren. . .

Fassen wir kurz zusammen: Sie wissen nun, wie Sie Ihren Schlüssel auf einen Schlüsselserver im Internet schicken können.

♠ Wie Sie den Schlüssel eines Partners auf den Schlüsselservern suchen und finden, beschreiben wir im Handbuch „Gpg4win für Durchblicker“ Kapitel 6. Sie können dieses Kapitel jetzt lesen oder später, wenn Sie diese Funktion benötigen.

7. Sie entschlüsseln eine E-Mail

Adele erhält nun Ihren öffentlichen Schlüssel, verschüsselt damit eine E-Mail und sendet sie an Sie zurück. Nach kurzer Zeit erhalten Sie Adeles Antwort.

So sieht sie aus:

```
From: Adele (Der freundliche E-Mail-Roboter) <adele@gnupp.de>
Subject: Re: mein öffentlicher Schlüssel
To: heinrichh@duesseldorf.de
Date: Thu, 12 Jan 2006 09:17:28 +0100

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.1 (GNU/Linux)

hQEOA9FS8I3hSvdPEAP/W6W6f4MBwqTdzd9O/7FOTDHh//bQ+GUWoT0k9Y0i96UZ
QO1VhQSia6a8DZrFQj7SlJWmB1MM7RNhkmhfZsD5Bn9ICmwwOt2xJDBkCQ34gu5N
NxQ92WXZjHCaI0dSlynNziNbK8Ik26YPBYkQjLUDhHN4CRZ7q67eVEd/B9DI04wD
....
ujbjyj09L/9NvoBniWrgqVUayKr1Ls8OIZkyiex6mKypPGADJFAzvTwjubj5S6zJ
A+QvSXUB9Hj8Ft2Nt3j0B/gWn5no3Er2/15UcBn/UPSxW9or0w9seDxCuSXvpakX
bcneOm/pcJNEHcApXWXpoNOxRZ1MksM300w+79M6p2w=
=VCHb
-----END PGP MESSAGE-----
```

(Aus Gründen der Übersichtlichkeit haben wir den Verschlüsselungsblock stark gekürzt.)

Diese E-Mail werden Sie nun mit dem Programm WinPT entschlüsseln.

WinPT ist ein sogenanntes „Frontend“ für GnuPG. Es dient zur eigentlichen Ver- und Entschlüsselung der E-Mails und zur Erzeugung und Überprüfung von digitalen Unterschriften. Und zwar – und das ist einer seiner Vorteile – mit jedem beliebigen Mailprogramm.

Für die meisten Mailprogramme – z.B. MS Outlook für Windows, gibt es außerdem spezielle PlugIns, mit denen die Ver- und Entschlüsselung direkt im jeweiligen Mailprogramm erledigt werden kann.

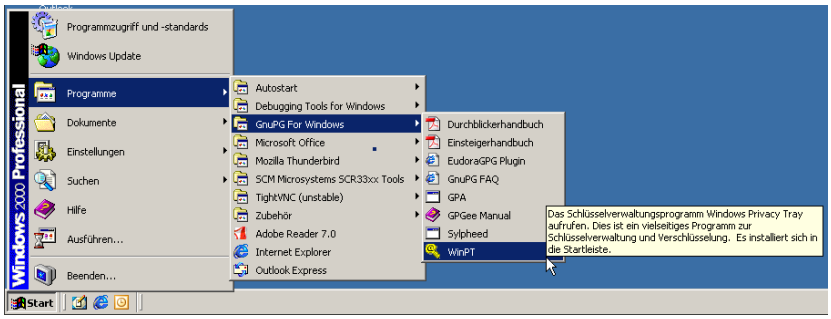
♠ Hinweise zu diesen Lösungen finden Sie im Handbuch „Gpg4win für Durchblicker“ Kapitel 8. Sie können dieses Kapitel jetzt lesen oder später, wenn Sie diese Funktion benötigen.

WinPT hat dagegen den Vorteil, dass es nicht mit einem bestimmten, sondern mit jedem Mailprogramm funktioniert. Es erledigt nämlich die Ver- und Entschlüsselung einfach im Speicher des Rechners. Das bedeutet, dass man den Text, der ver- oder entschlüsselt werden soll, zunächst in die Zwischenablage des Rechners zu kopieren ist.

Markieren Sie also den gesamten Text aus Adeles E-Mail und kopieren Sie ihn mit dem entsprechenden Menübefehl oder Tastaturkürzel (Strg+C).

Damit haben Sie den Schlüssel in den Speicher Ihres Rechners – bei Windows Zwischenablage oder Clipboard genannt – kopiert.

Starten Sie nun WinPT aus dem Windows-Startmenü:

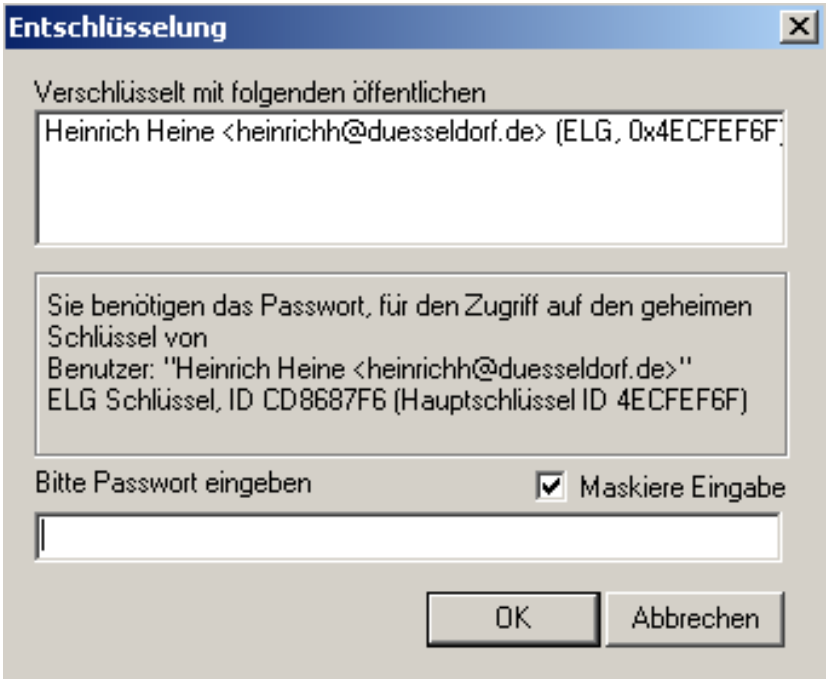


Während WinPT startet, erscheint kurz ein Hinweis darauf, dass das Programm die bereits vorhandenen Schlüssel einlädt.

Nachdem das Programm gestartet wurde, sehen Sie unten rechts in der Windows-Taskleiste das Schlüsselsymbol von WinPT:

Klicken Sie mit der rechten Maustaste auf dieses Icon. Daraufhin öffnet sich das WinPT-Menü. Hier klicken Sie auf *Zwischenablage→Entschlüsseln/Überprüfen*.

Es erscheint dieser Dialog: Geben Sie nun Ihren geheimen Passwortsatz ein. Adeles E-Mail wird nun entschlüsselt.



Kurz darauf erscheint ein kurzer Hinweis, dass die Entschlüsselung beendet ist.

Der entschlüsselte Text befindet sich jetzt, genau wie beim Verschlüsseln, wieder in der Zwischenablage von Windows. Kopieren Sie ihn mit Einfügen (Strg+V) in den Texteditor oder auch in Ihr Mailprogramm.

Die entschlüsselte Antwort von Adele sieht so aus[3]:

```
Hallo Heinrich Heine,

hier ist die verschlüsselte Antwort auf Ihre E-Mail.

Ihr öffentlicher Schlüssel mit der Schlüssel-ID
57251332CD8687F6 und der Bezeichnung
‘Heinrich Heine <heinrichh@duesseldorf.de>’
wurde von mir empfangen.

Anbei der öffentliche Schlüssel von adele@gnupp.de,
dem freundlichen E-Mail-Roboter.

Viele Grüße,
adele@gnupp.de
```

Der Textblock, der darauf folgt, ist der öffentliche Schlüssel von Adele.

Wir werden anschließend diesen öffentlichen Schlüssel importieren und an Ihrem Schlüsselbund befestigen. So können Sie ihn jederzeit zum Entschlüsseln der Nachrichten Ihres Korrespondenzpartners benutzen.

Fassen wir kurz zusammen:

1. Sie haben eine verschlüsselte E-Mail mit Ihrem geheimen Schlüssel entschlüsselt.
2. Der Korrespondenzpartner hat seinen eigenen öffentlichen Schlüssel beigelegt, damit Sie ihm verschlüsselt antworten können.

[3] Abhängig von der Softwareversion von Adele kann dies auch etwas unterschiedlich aussehen

8. Sie befestigen einen Schlüssel am Schlüsselbund

Ihr Korrespondenzpartner muss nicht etwa jedes Mal seinen Schlüssel mitschicken, wenn er Ihnen signiert schreibt. Sie bewahren seinen öffentlichen Schlüssel einfach an Ihrem GnuPG-„Schlüsselbund“ auf.

1. Möglichkeit:

Um einen öffentlichen Schlüssel zu importieren (an Ihrem Schlüsselbund zu befestigen), speichern Sie ihn am einfachsten als Textblock ab, so wie Sie es vorhin schon bei Ihrem eigenen Schlüssel getan haben.

Also:

markieren Sie den öffentlichen Schlüssel, den Sie von Ihrem Korrespondenzpartner erhalten haben, von

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

bis

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

und setzen ihn mit Copy & Paste in einen Texteditor ein. Speichern Sie den Schlüssel unter einem Namen in einem Ordner, den Sie leicht wiederfinden, z.B. als `adeles-key.asc` im Ordner `Eigene Dateien`.

2. Möglichkeit:

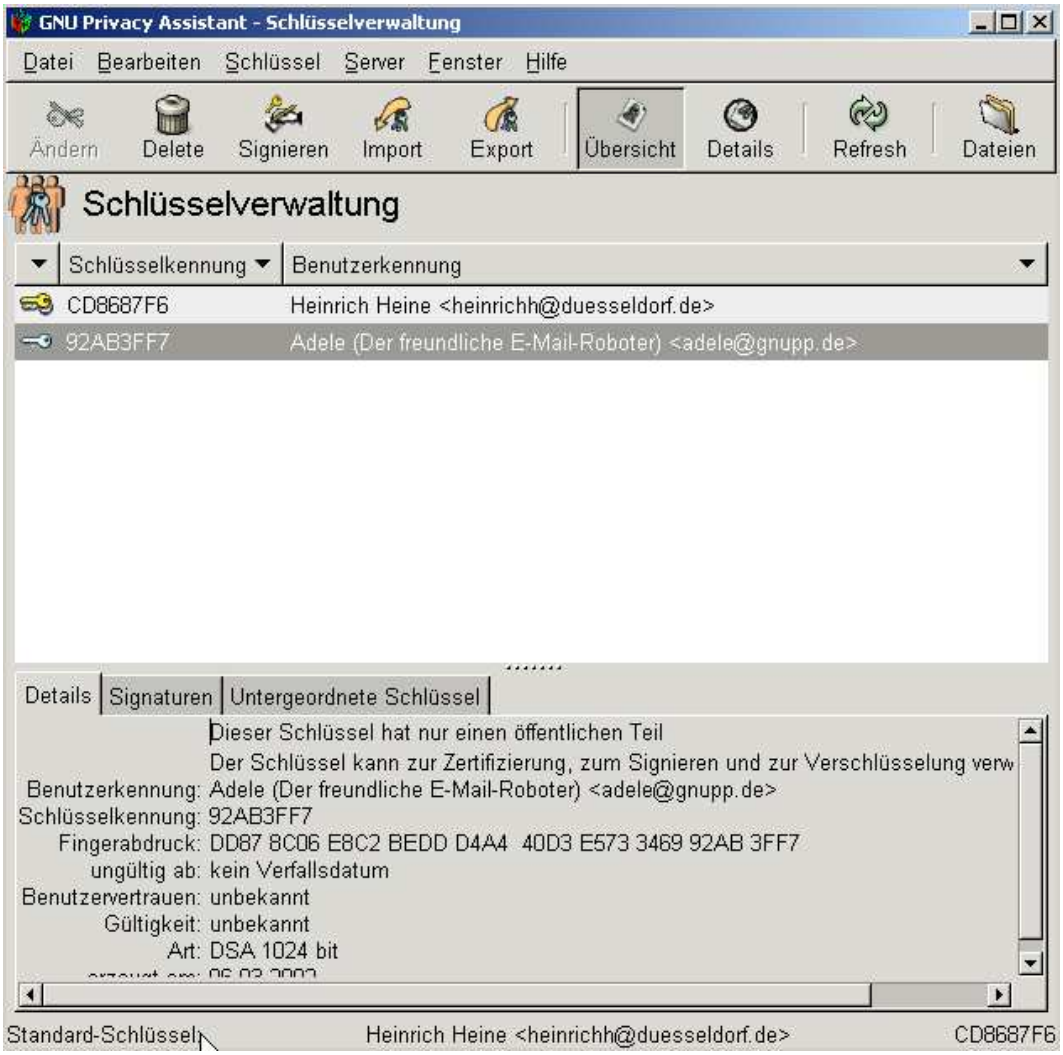
Der Schlüssel liegt der E-Mail als Dateianhang bei. Welches Mailprogramm Sie auch immer benutzen, Sie können stets Dateianhänge („Attachments“) auf Ihrer Festplatte abspeichern. Tun Sie das jetzt (am besten wieder in einem Ordner, den Sie leicht wiederfinden, z.B. `Eigene Dateien`).

Ob Sie nun den Schlüssel als Text oder als E-Mail-Anhang abgespeichert haben, ist egal: in beiden Fällen importieren Sie diesen abgespeicherten Schlüssel in den GnuPG-„Schlüsselbund“.

Und zwar so:

Starten Sie den GNU Privacy Assistant (GPA) im Windows-Menü, falls Sie ihn in der letzten Übung ausgeschaltet haben.

Wenn der GNU Privacy Assistant läuft, klicken Sie auf die Schaltfläche Import, suchen die eben abgespeicherte Schlüsseldatei und laden sie. Der importierte Schlüssel wird nun im GNU Privacy Assistant angezeigt:



Damit haben Sie einen fremden öffentlichen Schlüssel – in diesem Beispiel den von Adele – importiert und an Ihrem Schlüsselbund befestigt. Sie können diesen Schlüssel jederzeit benutzen, um verschlüsselte Nachrichten an den Besitzer dieses Schlüssels zu senden und Signaturen zu prüfen.

Bevor wir weitermachen, eine wichtige Frage:
woher wissen Sie eigentlich, dass der fremde öffentliche Schlüssel wirklich von Adele stammt? Man kann E-Mails auch unter falschem Namen versenden – die Absenderangabe besagt eigentlich gar nichts.

Wie können Sie also sichergehen, dass ein Schlüssel auch wirklich seinem Absender gehört?

♠ Diese Kernfrage besprechen wir im Handbuch „Gpg4win für Durchblicker“ Kapitel 9: „Die Schlüsselprüfung“. Lesen Sie jetzt bitte dort weiter, bevor Sie danach an dieser Stelle fortfahren.

Sie haben in Kapitel 9 des Handbuchs „Gpg4win für Durchblicker“ gelesen, wie man sich von der Echtheit eines Schlüssels überzeugt und ihn dann mit seinem eigenen geheimen Schlüssel signiert.

In Kapitel 10 des Handbuchs „Gpg4win für Durchblicker“ besprechen wir, wie man nicht nur einen Schlüssel, sondern auch eine komplette E-Mail-Nachricht signieren kann. Das bedeutet, dass man die E-Mail mit einer Art elektronischem Siegel versieht.

Der Text ist dann zwar noch für jeden lesbar, aber der Empfänger kann feststellen, ob die E-Mail unterwegs manipuliert oder verändert wurde.

Die Überprüfung einer solchen Signatur ist sehr einfach. Sie müssen dazu natürlich den öffentlichen Schlüssel des Absenders bereits an Ihrem Gpg4win-„Schlüsselbund“ befestigt haben, wie in Kapitel 8 von „Gpg4win für Einsteiger“ besprochen.

Wenn Sie eine signierte E-Mail erhalten, sehen Sie, dass der Text am Anfang und Ende von einer Signatur eingerahmt ist. Sie beginnt mit

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

und endet unter der E-Mail-Nachricht mit

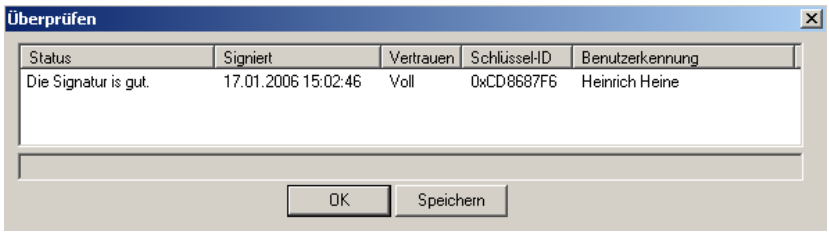
```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.2 (MingW32)

iEYEARECAAYFAjxeqy0ACgkQcwePex+3Ivs79wCfW8u
ytRsEXgzCrfPnjGrDDtb7QZIAn17B8l8gFQ3WIUUDCMfA5cQajHcm
=O6lY
-----END PGP SIGNATURE-----
```

Markieren Sie den gesamten Text von *BEGIN PGP SIGNED MESSAGE* bis *END PGP SIGNATURE* und kopieren Sie ihn mit Strg+C in die Zwischenablage.

Nun fahren Sie genauso fort wie bei der Entschlüsselung einer E-Mail, wie wir es in Kapitel 7 dieses Handbuchs besprochen haben:

Sie öffnen WinPT aus der Windows-Taskleiste und wählen
Zwischenablage→ Entschlüsseln/Überprüfen.

Sie sollte daraufhin folgendes Fenster sehen:



Falls Sie dort aber in der Statusspalte *Die Signatur ist nicht gültig!* erhalten, wurde die Nachricht bei der Übertragung verändert. Aufgrund der technischen Gegebenheiten im Internet ist es nicht auszuschließen, dass die E-Mail durch eine fehlerhafte Übertragung verändert wurde. Das ist zunächst der wahrscheinlichste Fall. Es kann jedoch auch bedeuten, dass der Text nachträglich verändert wurde.

♠ **Wie Sie in einem solchen Fall vorgehen sollten, erfahren Sie im Handbuch „Gpg4win für Durchblicker“ Kapitel 10. „E-Mails signieren“. Lesen Sie jetzt bitte dort weiter, bevor Sie danach an dieser Stelle fortfahren.**

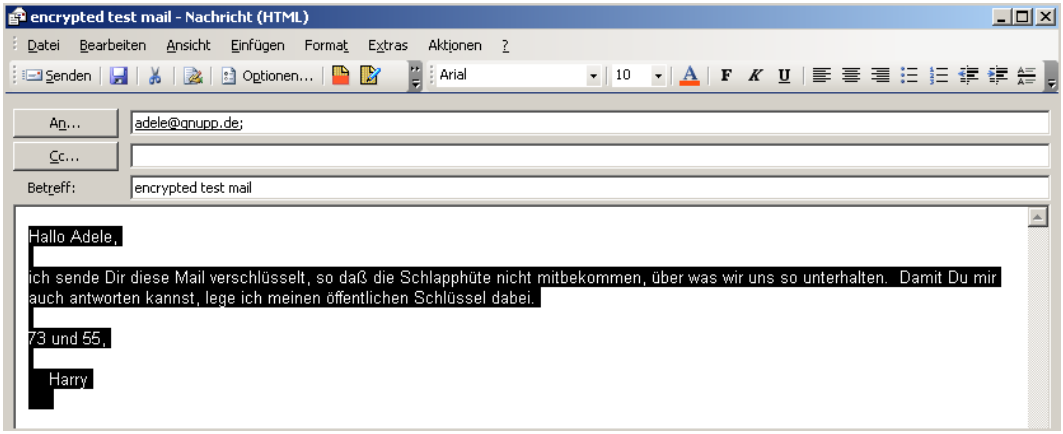
9. Sie verschlüsseln eine E-Mail

Jetzt wird es nochmal spannend:

Sie verschlüsseln eine E-Mail und senden sie an Adele. Wenn Sie einen ebenso geduldigen menschlichen Korrespondenzpartner haben, dann senden Sie Ihre E-Mail eben an diesen.

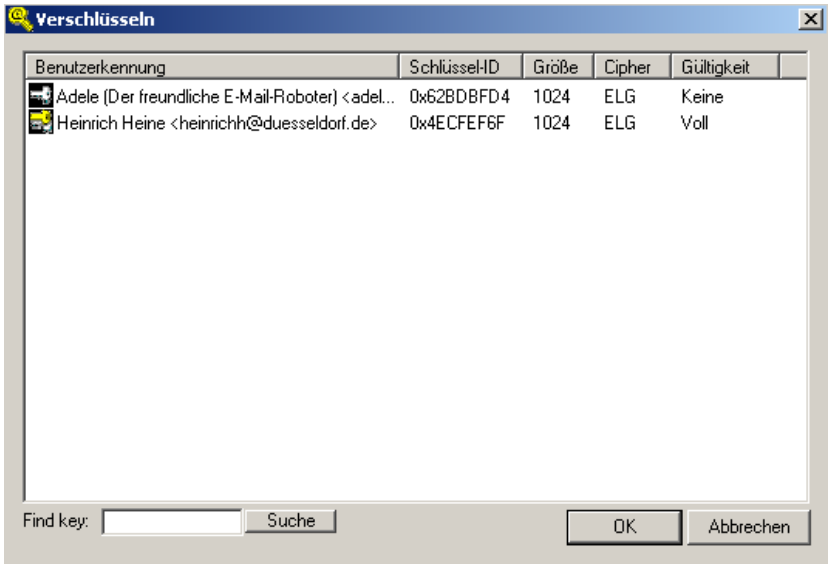
Starten Sie nun Ihr E-Mailprogramm. Schreiben Sie eine Nachricht – es ist egal, was: Adele kann nicht wirklich lesen. . .

Nun markieren Sie den gesamten Text und kopieren Sie ihn mit dem entsprechenden Menübefehl oder Tastaturkürzel (Strg+C). Damit haben Sie den Text in den Speicher Ihres Rechners – bei Windows Zwischenablage oder Clipboard genannt – kopiert.



Sie öffnen nun WinPT aus der Windows-Taskleiste und wählen *Zwischenablage→Verschlüsseln.*

Daraufhin öffnet sich ein Fenster mit den Schlüsseln, die Sie an Ihrem Schlüsselbund haben. In unserem Beispiel sind das Adeles Schlüssel, den sie Ihnen vorhin geschickt hat, und Ihr eigener Schlüssel, den Sie in Kapitel 2 erzeugt haben.



Klicken Sie auf Adeles Schlüssel, denn damit muss die Nachricht ja verschlüsselt werden.

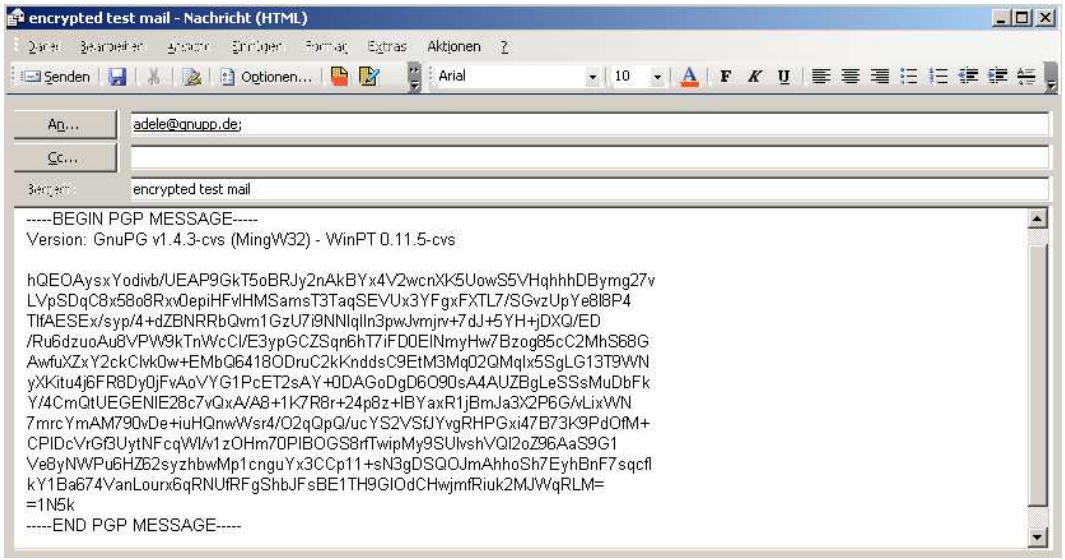
Sie erinnern sich an den Grundsatz:

Wenn Sie an jemanden verschlüsselte E-Mails schicken wollen, müssen Sie dessen öffentlichen Schlüssel haben und zum Verschlüsseln benutzen.

Nachdem Sie auf [OK] geklickt haben, wird Ihre Nachricht verschlüsselt. Nach kurzer Zeit erscheint eine Meldung die dies bestätigt.

Die verschlüsselte Nachricht befindet sich noch in der Zwischenablage (Clipboard) und kann nun mühelos in das E-Mail-Fenster hineinkopiert werden. Löschen Sie den unverschlüsselten Text oder kopieren die den Inhalt der Zwischenablage einfach darüber.

So ähnlich sollte das Ergebnis aussehen:



Senden Sie nun Ihre E-Mail wieder an Adele. Nur zur Vorsicht: natürlich sollten Ihre E-Mails **nicht** `heinrichh@gpg4win.de` als Absender haben, sondern Ihre eigene E-Mail-Adresse. Denn sonst werden Sie nie Antwort von Adele bekommen. . .

Herzlichen Glückwunsch! Sie haben Ihre erste E-Mail verschlüsselt!

10. Wie Sie Ihre E-Mails verschlüsselt archivieren

Eine Einstellung müssen Sie noch vornehmen, damit Sie Ihre E-Mails verschlüsselt aufbewahren können. Natürlich können Sie einfach eine Klartextversion Ihrer Texte aufbewahren, aber das wäre eigentlich nicht angebracht. Wenn Ihre Mitteilung geheimhaltungsbedürftig war, sollte sie auch nicht im Klartext auf Ihrem Rechner gespeichert sein. Also sollte immer ein verschlüsselte Kopie der E-Mail aufbewahrt werden.

Sie ahnen das Problem: zum Entschlüsseln der archivierten E-Mails braucht man den geheimen Schlüssel des Empfängers – und den haben Sie nicht und werden Sie nie haben. . .

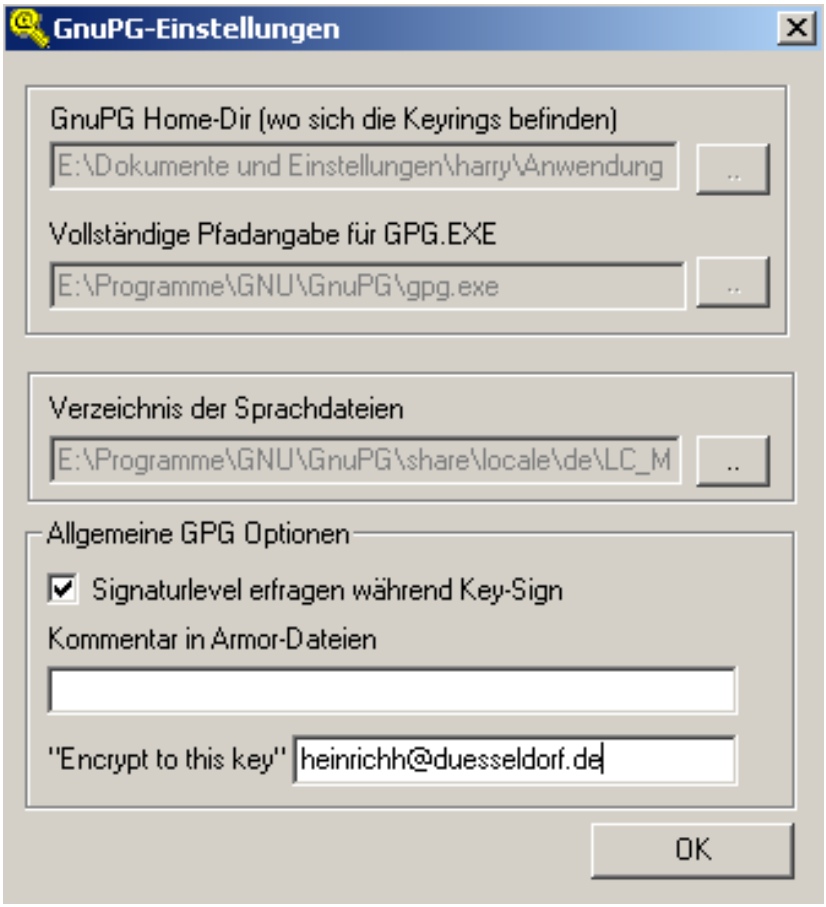
Also was tun?

Ganz einfach: Sie verschlüsseln zusätzlich auch an sich selbst.

Die Nachricht wird für den eigentlichen Empfänger (z.B. Adele), als auch mit Ihren eigenen öffentlichen Schlüssel verschlüsselt. So können Sie den Text auch später noch einfach mit Ihrem eigenen Geheimschlüssel wieder lesbar machen.

Da Gpg4win nicht wissen kann, welchen Schlüssel Sie benutzen – Sie können ja auch mehrere haben – müssen Sie dem Programm dies mitteilen.

Um diese Option zu nutzen, genügt ein Mausklick: Öffnen Sie WinPT und dort das Menü *Einstellungen → GPG*.



In dem Einstellungsfenster, das sich nun öffnet, tragen Sie unter „Encrypt to this key“ Ihren Schlüssel ein, und zwar einfach mit der dazugehörigen E-Mail-Adresse.

Eine entsprechende Option finden Sie auch bei allen E-Mailprogrammen, die GnuPG direkt unterstützen.

Fassen wir kurz zusammen:

1. Sie haben mit dem öffentlichen Schlüssel Ihres Partners eine E-Mail verschlüsselt und ihm damit geantwortet.
2. Sie haben WinPT mitgeteilt, dass Archivkopien Ihrer E-Mails auch zusätzlich mit Ihrem eigenen Schlüssel verschlüsselt werden sollen.

Das war's! Willkommen in der Welt der freien und sicheren E-Mail-Verschlüsselung!

♠ Lesen Sie nun die Kapitel 10 bis 12 im Handbuch „Gpg4win für Durchblicker". Sie erfahren dort unter anderem, wie man E-Mails signiert und einen bereits vorhandenen Geheimschlüssel in GnuPG importiert und verwendet.

♠ Ab Kapitel 13 des Handbuchs „Gpg4win für Durchblicker" können Sie weiterhin in zwei spannenden Kapiteln lesen, auf welchen Verfahren die Sicherheit von GnuPG beruht.

Und Sie können lesen, wie die geheimnisvolle Mathematik hinter GnuPG im Detail funktioniert.

Genau wie das Kryptographiesystem Gpg4win wurden diese Texte nicht nur für Mathematiker, Geheimdienstler und Kryptographen geschrieben, sondern

für jedermann.

A. Hinweise zum Outlook Plugin *GPGol*

GPGol ist ein Plugin für Microsoft Outlook, es integriert dort die Bedienung von GnuPG. Wir geben hier einige Hinweise zur Benutzung.

Aufgrund technischer Schwierigkeiten der Integration von OpenPGP in Outlook ist dieses Plugin nicht so komfortabel zu bedienen wie die OpenPGP Unterstützung in anderen E-Mail-Programmen. GPGol funktioniert in der aktuellen Version nur mit Outlook 2003 SP2 und gibt einen Warnhinweis aus, falls eine ältere Outlook Version benutzt wird.

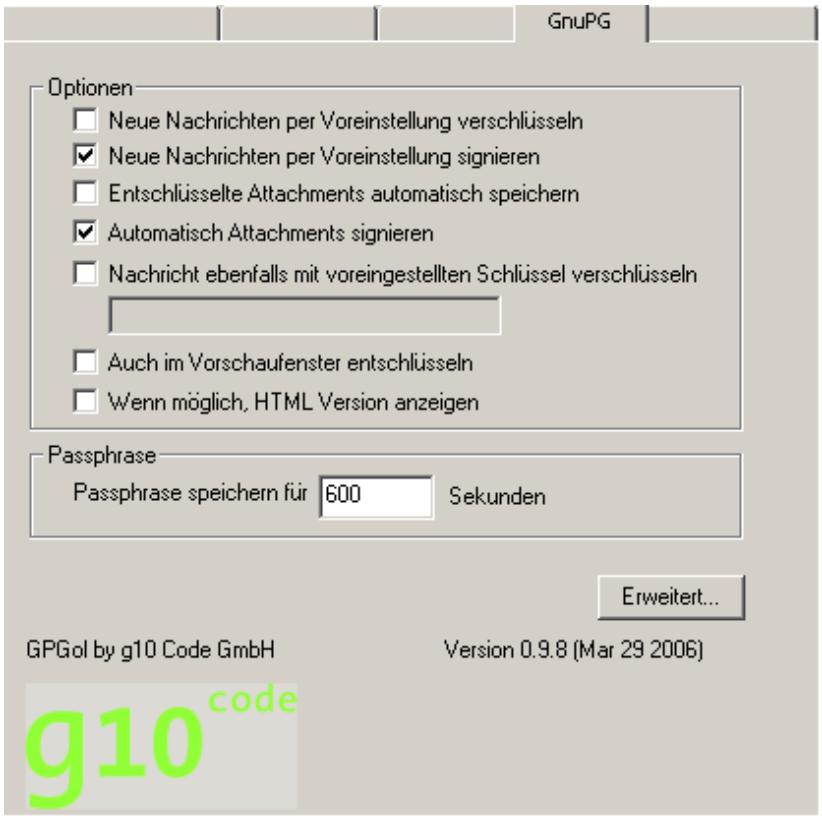
Bitte beachten Sie die beiden folgenden Einschränkungen:

- Als Texteditor darf nicht das Programm Word eingestellt sein.
- Sogenanntes Inline-PGP oder traditionelles PGP wird voll unterstützt. Es können jedoch keine PGP/MIME E-Mails erstellt werden.

  Die Entschlüsselung und Signaturprüfung einfacher (nicht verschachtelter) PGP/MIME E-Mails stellt hingegen kein Problem dar.

A.1. Installation

Die Installation wird durch den gpg4win Installer vorgenommen. Beim nächsten Start von Outlook findet sich im Menü *Extras→Optionen* eine Karteikarte *GnuPG*:



Die beiden ersten Optionen steuern ob per Voreinstellung Nachrichten verschlüsselt oder signiert werden sollen. Sie können dies aber immer noch bei der Erstellung der Nachricht individuell verändern.

Die Option „Entschlüsselte Attachments automatisch speichern“ speichert Anhänge nach der Entschlüsselung im Klartext ab, so dass sie dann jederzeit ohne erneute Entschlüsselung gelesen werden können.

Die Option „Automatisch Attachments signieren“ sorgt dafür, dass mit dem Signieren des Haupttexts auch die Anhänge signiert werden. Dazu wird für jeden Anhang ein weiterer Anhang mit der Signatur angelegt.

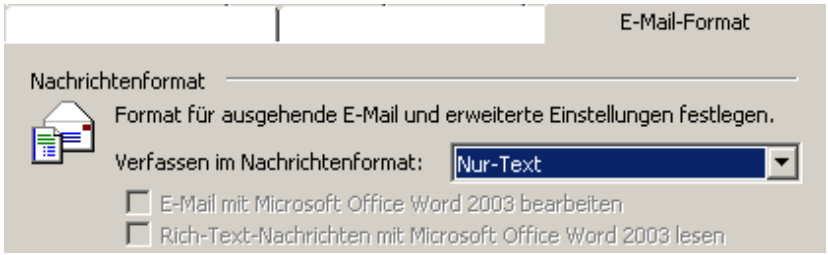
Wenn Sie „Nachricht ebenfalls mit voreingestelltem Schlüssel verschlüsseln“ ankreuzen und in das Eingabefeld die Key-ID Ihres eigenen Schlüssels eintragen, so werden Ihre Nachrichten automatisch auch an sie selbst verschlüsselt. Dies ermöglicht die Nachricht dann selber noch im Order für gesendete Nachrichten entschlüsseln und lesen zu können.

Die Option „Im Vorschaufenster entschlüsseln“ kann nur sinnvoll auf schnellen Rechnern eingesetzt werden und funktioniert z.Z. nur eingeschränkt.

Die Option „Wenn möglich, HTML Version anzeigen“ kann benutzt werden, um die HTML Version einer Nachricht anzuzeigen. Im Normalfall oder falls keine HTML Version vorhanden ist, wird die Text Version angezeigt.

Alle Optionen sind nach einer Neuinstallation bereits sinnvoll vorbelegt. Um aber verschlüsselte Nachrichten versenden zu können, sollten Sie sicherstellen, daß Sie **nicht Microsoft Word zum Verfassen** der Nachrichten benutzen. Desweiteren ist dringend anzuraten auf HTML Nachrichten zu verzichten.

Bitte kontrollieren Sie dies im Menüpunkt *Extras→Optionen* auf der Karteikarte *E-Mail-Format*. Ihre Einstellungen sollten dem folgenden Bildschirmausdruck entsprechen:



A.2. Häufig gestellte Fragen

Die Icons zur Verschlüsselung fehlen in der Symbolleiste Wenn bereits viele Icons vorhanden sind, so zeigt Outlook diese Icons nicht unbedingt direkt an. Sie können diese anzeigen lassen, indem Sie in der Symbolleiste auf das kleine Icon mit dem Pfeil nach unten klicken („Optionen für Symbolleiste“). Dort finden Sie dann alle nicht angezeigten Icons. Ein Klick auf eines dieses Icons verschiebt es in die Symbolleiste. Dasselbe gilt für das Icon zum Aufruf der Schlüsselverwaltung.

Achten Sie auch darauf, daß Sie nicht Microsoft Word zum Verfassen von Nachrichten benuzten. Siehe Installationsanleitung.

Was bedeuten die Buchstaben im Übersichtsdialog? Bei der Entschlüsselung oder Signaturprüfung von Nachrichten mit Anhängen zeigt GPGol eine Liste mit den einzelnen Bestandteilen und deren Dateinamen dar. Vor dem Dateinamen steht eine „E“ falls es sich um einen verschlüsselten Anhang handelt oder eine „S“ für einen signierten Anhang.

Wie finde ich Informationen zur aktuellen Version von GPGol? Klicken Sie in den Optionen für GnuPG auf das Logo links unten.

Warum kann eine Verschlüsselung nicht abgebrochen werden? Wenn Sie auf Senden geklickt haben, beginnt GPGol mit der Verschlüsselung. Outlook hat jedoch seit langem einen Fehler, der verhindert, dass diese Operation abgebrochen werden kann. Als Gegenmaßnahme können Sie Outlook so konfigurieren, dass erstellte Nachrichten nicht sofort versendet werden — das gibt Ihnen die Möglichkeit die Nachricht noch nachträglich zu löschen. Aus Sicherheitsgründen versucht GPGol den Inhalt der Nachricht zu löschen wenn die Verschlüsselung abgebrochen wurde. Dies ist aber nicht immer erfolgreich.

Warum erscheint der Bestätigungsdialog beim Zugriff auf bestimmte E-Mails? Ist GPGol nicht als vertrauenswürdiges Plugin installiert worden, nimmt Outlook an, das Plugin versucht unberechtigt auf interne Informationen zuzugreifen. GPGol versucht derartige Zugriffe zu vermeiden, in einige Fällen sind sie aber notwendig um verschlüsselte oder signierte E-Mails anzeigen zu können.

GPGol ist noch in Entwicklung. Einer der offenen Punkte ist die Registrierung als vertrauenswürdiges Plugin. Zukünftige Versionen sollten die Unanehmlichkeit der expliziten Bestätigung lösen.

Warum kann GPGol keine PGP/MIME Nachrichten erzeugen? Es ist keine Möglichkeit bekannt, Outlook mitzuteilen, dass eine PGP/MIME Nachricht erzeugt werden soll. Outlook legt immer selbst den sogenannten „Content-Type“ fest und ein Plugin ist nicht in der Lage, einen bestimmten Typ vorzugeben. Bitte wenden Sie sich direkt an Microsoft um sich über dieses Verhalten bzw. die fehlende Dokumentation zu beschweren.

Warum werden Signatur-Prüfungen nicht automatisch durchgeführt? In der Tat ist eine wahlweise einschaltbare automatische Signaturprüfung beim öffnen einer E-Mail in Vorbereitung. Eine gute benutzbare Lösung ist jedoch aufgrund technischer Schwierigkeiten bei Outlook nicht einfach zu realisieren.

B. Umstieg von anderen GnuPG Programmen

Wir werden hier erläutern, wie Sie von anderen GnuPG basierten Programmen auf Gpg4win umsteigen können. Das Installationsprogramm erkennt einige dieser Programme und warnt Sie in diesem Fall.

Generell ist es ratsam, eine vorhandene Installation eines anderen GnuPG basierten Programms zu entfernen bevor Gpg4win installiert wird. Es ist hier wichtig, die vorhandenen Schlüssel zu sichern.

Der einzige sinnvolle Weg dies zu tun, ist unter Verwendung der im alten System vorhandenen Möglichkeiten. Suchen Sie nach einem Menüpunkt um die eigenen privaten (geheimen) Schlüssel zu sichern als auch nach einem Menüpunkt um alle vorhandenen öffentlichen Schlüssel zu sichern. Sichern Sie diese dann in eine oder zwei Dateien.

Sobald Sie dann Gpg4win installiert haben, prüfen Sie, ob Ihre alten Schlüssel bereits vorhanden sind. Sie können dies mit GPA oder WinPT machen. Sind die Schlüssel schon vorhanden, so entsprach das alte System bereits den neuen Konventionen zum Speicherort für die Schlüssel und Sie müssen nichts weiter unternehmen.

Wenn die alten Schlüssel nicht erscheinen, so importieren Sie diese einfach aus den erstellten Backupdateien. Lesen Sie hierzu das Kapitel 12 im Handbuch „Gpg4win für Durchblicker“.

Falls das alte System auch GPA verwendet, so können Sie die dort vorhandene Backupmöglichkeit benutzen. Diese sollte sehr ähnlich zu der Funktion in der GPA Version aus Gpg4win sein.

Falls Sie keinen anderen Weg finden, Ihre alten Schlüssel wiederzufinden, so suchen Sie bitte mit den Bordmittel von Windows nach Dateien mit den Namen `secring.gpg` und `pubring.gpg` und importieren diese beiden Dateien mittels GPA.[4]

[4] Dies ist nicht der offizielle Weg, funktioniert aber noch mit allen aktuellen GnuPG Versionen.

C. History

- „GnuPP für Einsteiger“, 1. Auflage März 2002,
  Autoren: 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
  Herausgegeben vom Bundesministerium für Wirtschaft und Technologie.
  Verfügbar unter `http://www.gnupp.de/pdf/einsteiger.pdf`.
- Revidierte nicht-veröffentlichte Version von TextLab text+media.
- „Gpg4win für Einsteiger“, Dezember 2005
  Autoren: Werner Koch, g10 Code GmbH
  Herausgegeben durch das Gpg4win Projekt.

D. GNU Free Documentation License

Version 1.2, November 2002

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

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. Secondarily, 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.