

## **PGP-Verschlüsselung beim email-Versand von Dateien in der Micro-Epsilon-Gruppe**

Verschlüsselungsverfahren können in zwei grundsätzlich verschiedene Klassen eingeteilt werden:

- Symmetrische Verfahren, z.B. Zip
- Asymmetrische Verfahren, z.B. PGP

## Symmetrische Verfahren:



Gleicher Schlüssel zum Ver- und Entschlüsseln der Datei

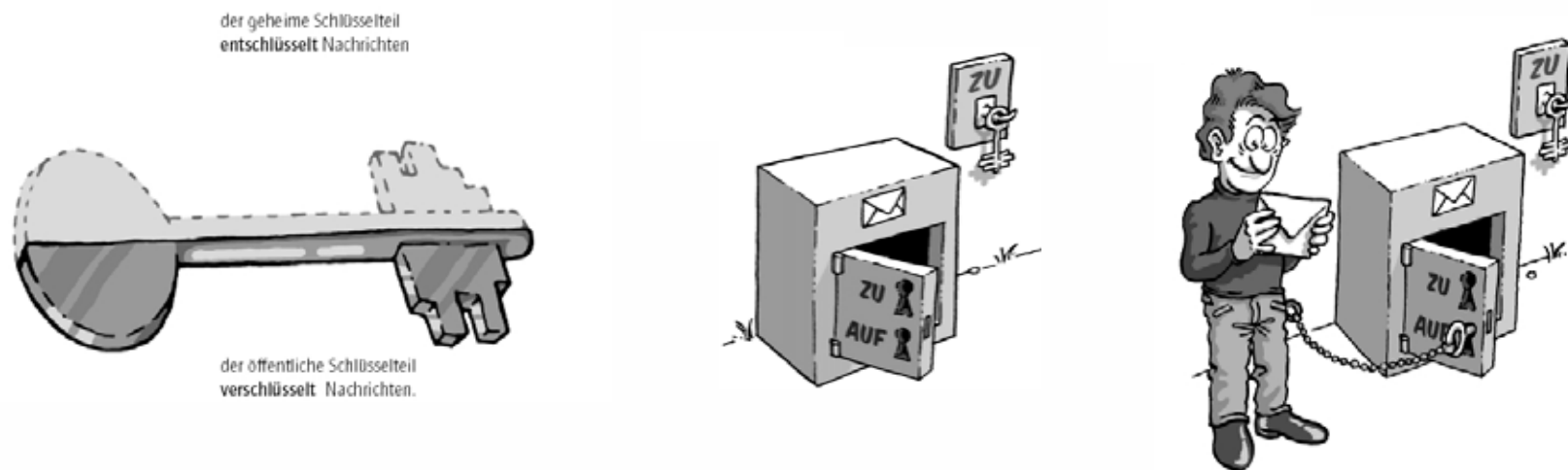
Problem: Schlüsselübergabe

Unsicher (per email oder andere elektronische Medien)

Unpraktisch (per Telefon o.ä)

Wegen Notwendigkeit der Übergabe: Schlüssellänge nicht ausreichend

## Aymmetrische Verfahren (Public Key-Prinzip):



Ein Schlüssel zum Verschlüsseln der Datei, Public Key, nicht geheim, auf Schlüsselservern verfügbar

Ein Schlüssel zum Entschlüsseln, Private Key, durch Passphrase/Mantra geschützt, bleibt beim Adressaten der Datei

➔ **Problem der unsicheren/unkomfortablen Schlüsselübergabe gelöst**

Wichtigster Vertreter der Public Key-Verfahren:

## **PGP – Pretty Good Privacy**

- 1991 von Phil Zimmermann erfunden um die Kommunikation von Atomkraftgegner vor dem Staat (USA) zu verbergen
- Sicherheit: Zeitdauer um eine Datei 1024 Bit-Schlüssel (default) mit normalen PCs zu knacken:  $10^{18}$  Jahre, Verfahren wird von Experten als absolut sicher eingestuft
- Der PGP-Algorithmus wurde im Internet-Standard OpenPGP (RFC 2440) festgeschrieben

Vorteil: volle Kompatibilität zwischen allen PGP-Programmen

- Kommerziell: PGP 9.0 von Network Associates
- Freeware: GnuPG

### Verwendung des Open Source/Freeware- Softwarepakets GnuPT

Besteht aus den zwei Programmen:

- **GnuPG** (Gnu Privacy Guard): Engine, führt die eigentliche Verschlüsselung nach dem PGP-Standard durch  
relativ unkomfortables Kommandozeilenprogramm
- **WinPT** (Windows Privacy Tray): dazugehörige grafische Benutzeroberfläche, fügt sich nahtlos in Windows ein

Beide Programme des GnuPT-Pakets (GnuPG + WinPT) sind  
**Freeware/Opensource-Software**

Vorteile

- Freeware: Kostenlos
- Opensource: Quelltext für jedermann einsehbar →
  - vollständige Transparenz der Programmierung
  - Garantiert Vertrauenswürdigkeit des Programms (keine Hintertüren o.ä.)

Beide Programme (download als Installationspaket möglich) sind Bestandteile des **GnuPP** (GNU Privacy Project)

Initiative des Bundesministeriums für Wirtschaft und Arbeit und des Bundesministeriums des Innern, bei der eine starke Verschlüsselungstechnologie für die allgemeine Öffentlichkeit nutzbar gemacht werden soll ([www.gnupp.de](http://www.gnupp.de))

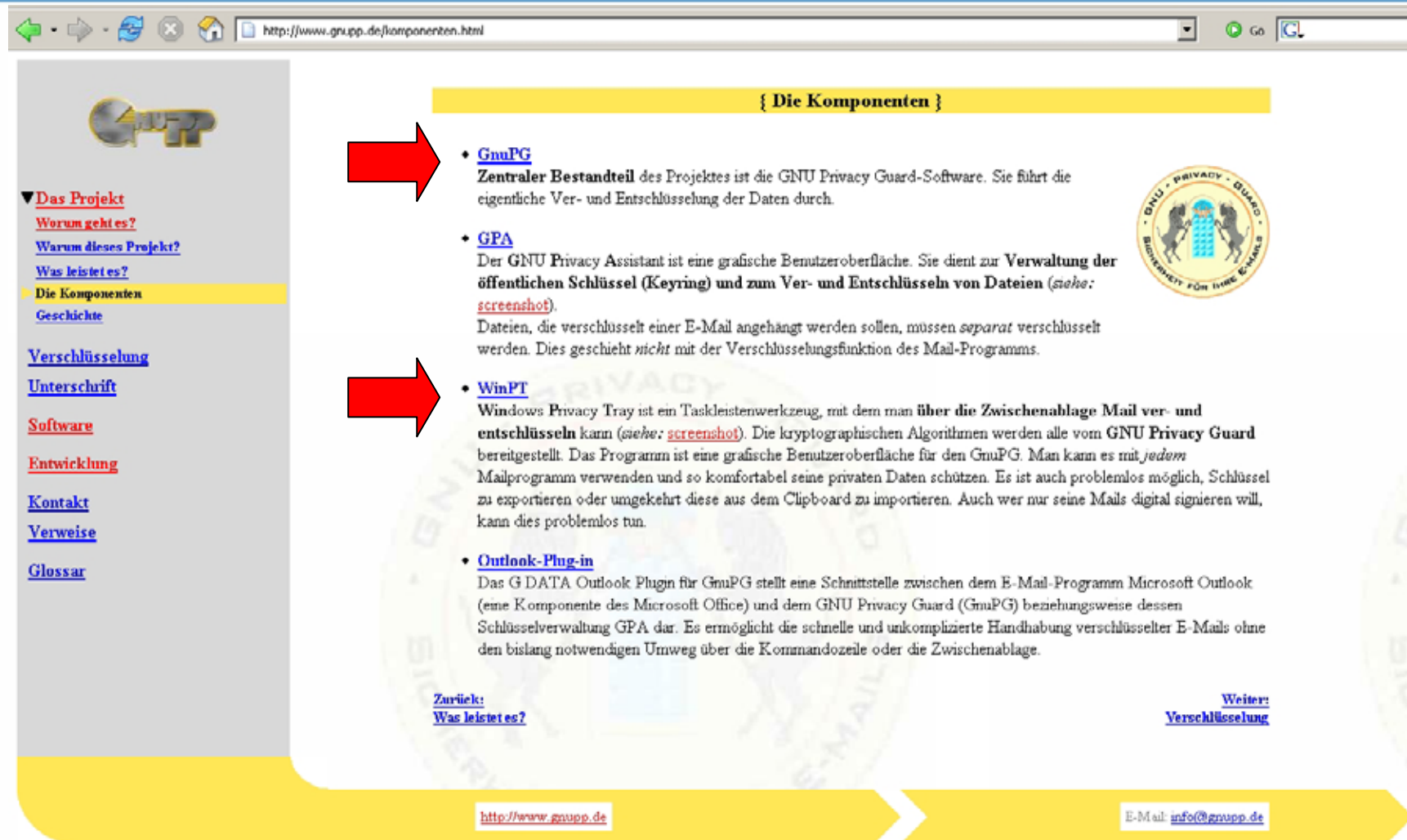
**Sicherheit für E-Mail,  
E-Commerce und E-Government.**

Das ist das Ziel des **GNU Privacy Projekts (GnuPP)**!



Als Partner der Aktion "Sicherheit im Internet" des Bundesministeriums für Wirtschaft und Arbeit (BMWA) und des Bundesministeriums des Innern (BMI) entwickeln Spezialisten eine frei verfügbare Verschlüsselungssoftware für **jedermann**.

Auch **Sie** können mithelfen, die Voraussetzungen für eine sichere Kommunikationsinfrastruktur zu schaffen.



<http://www.gnupp.de/komponenten.html>

## { Die Komponenten }

- **GnuPG**  
Zentraler Bestandteil des Projektes ist die GNU Privacy Guard-Software. Sie führt die eigentliche Ver- und Entschlüsselung der Daten durch.
- **GPA**  
Der GNU Privacy Assistant ist eine grafische Benutzeroberfläche. Sie dient zur **Verwaltung der öffentlichen Schlüssel (Keyring) und zum Ver- und Entschlüsseln von Dateien** (siehe: [screenshot](#)).  
Dateien, die verschlüsselt einer E-Mail angehängt werden sollen, müssen *separat* verschlüsselt werden. Dies geschieht *nicht* mit der Verschlüsselungsfunktion des Mail-Programms.
- **WinPT**  
Windows Privacy Tray ist ein Taskleistenwerkzeug, mit dem man **über die Zwischenablage Mail ver- und entschlüsseln** kann (siehe: [screenshot](#)). Die kryptographischen Algorithmen werden alle vom GNU Privacy Guard bereitgestellt. Das Programm ist eine grafische Benutzeroberfläche für den GnuPG. Man kann es mit *jedem* Mailprogramm verwenden und so komfortabel seine privaten Daten schützen. Es ist auch problemlos möglich, Schlüssel zu exportieren oder umgekehrt diese aus dem Clipboard zu importieren. Auch wer nur seine Mails digital signieren will, kann dies problemlos tun.
- **Outlook-Plug-in**  
Das G DATA Outlook Plugin für GnuPG stellt eine Schnittstelle zwischen dem E-Mail-Programm Microsoft Outlook (eine Komponente des Microsoft Office) und dem GNU Privacy Guard (GnuPG) beziehungsweise dessen Schlüsselverwaltung GPA dar. Es ermöglicht die schnelle und unkomplizierte Handhabung verschlüsselter E-Mails ohne den bislang notwendigen Umweg über die Kommandozeile oder die Zwischenablage.

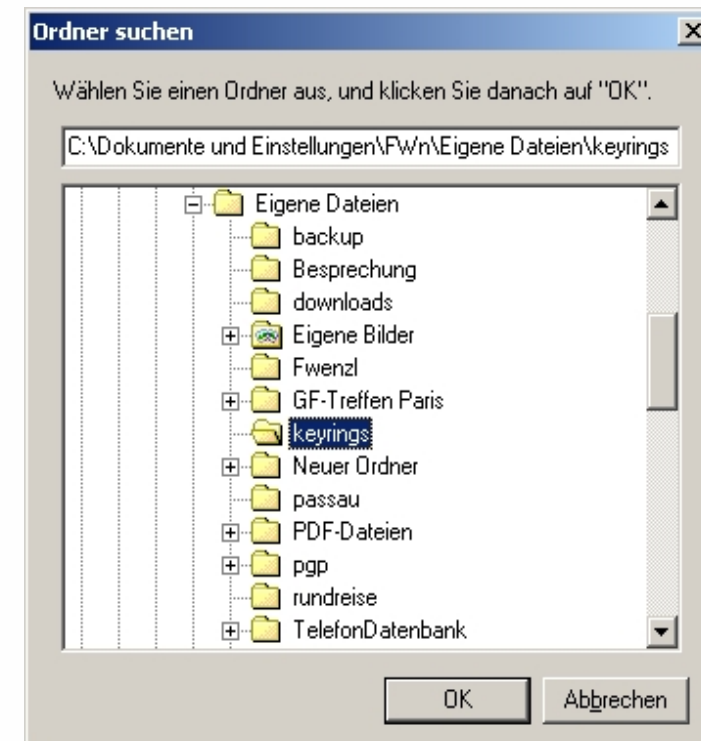
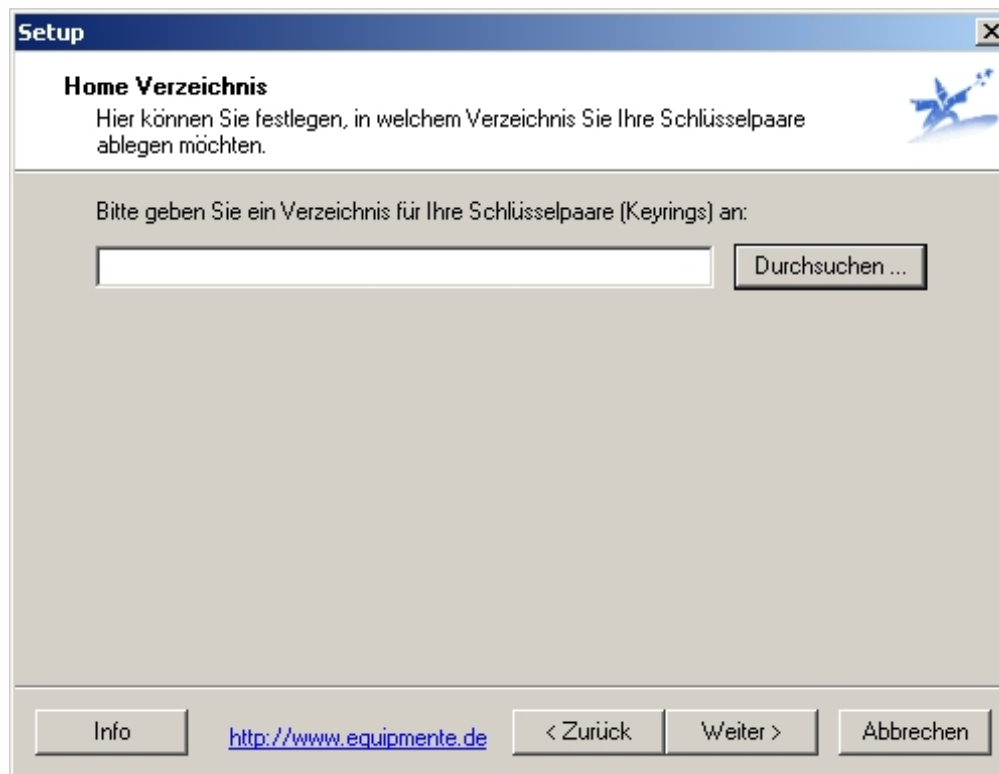
Zurück: [Was leistet es?](#) Weiter: [Verschlüsselung](#)

<http://www.gnupp.de> E-Mail: [info@gnupp.de](mailto:info@gnupp.de)

# PGP-Verschlüsselung – Installation von GnuPT (GnuPG+WinPt)



## Verzeichnis für Keyrings (Schlüsselbünde) festlegen

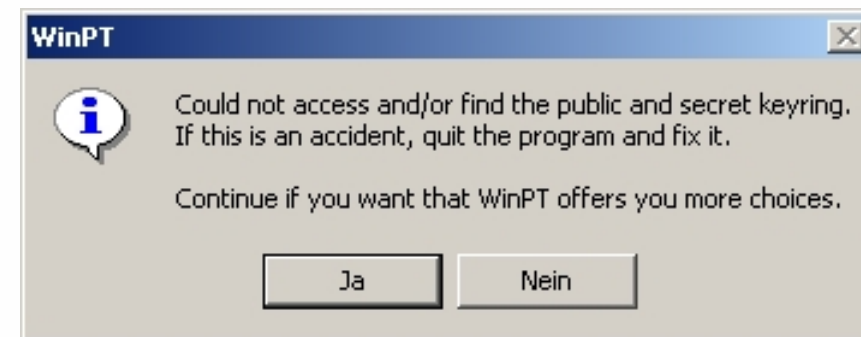
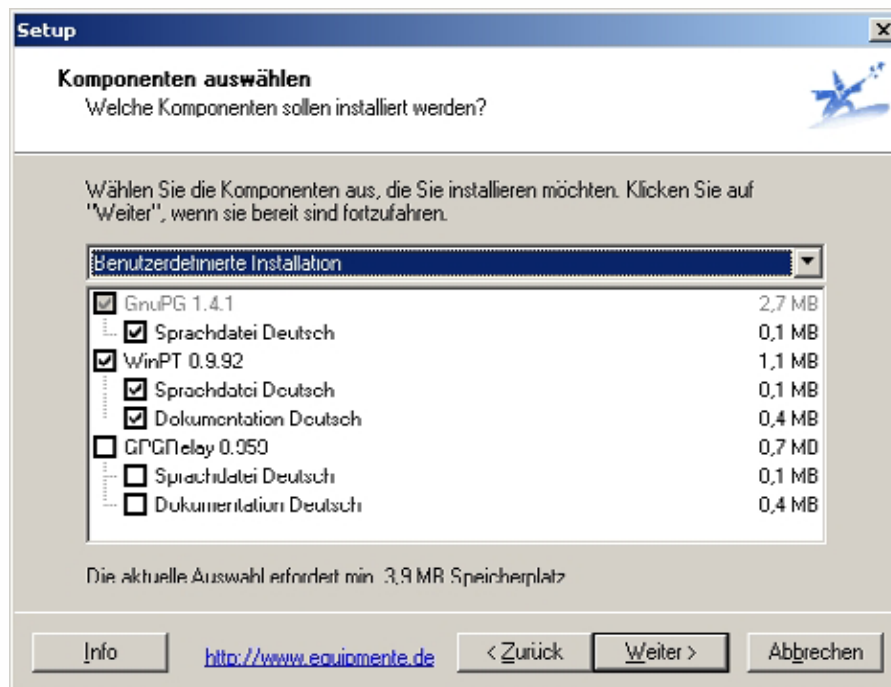


# PGP-Verschlüsselung – Installation von GnuPT (GnuPG+WinPt)



Nur WinPT und GnuPG installieren

Eigenes Schlüsselpaar erzeugen



Beim Installieren nicht „mit Windows starten“ wählen

## Dateiverschlüsselung

- Voraussetzung: Öffentlicher Schlüssel des Adressaten
- Zwei Möglichkeiten einen neuen öffentlichen Schlüssel in den eigenen Schlüsselbund aufzunehmen
  - **Import aus Datei** (per email, download von Website etc.)  
Durchführung: Schlüsselverwaltung starten, Menüpunkt „Key“, Unterpunkt „Import“ wählen
  - **(Download vom Schlüsselserver)**  
Wird vorerst nicht verwendet  
Durchführung: Schlüsselverwaltung starten, Menüpunkt „Schlüsselserver“ wählen, Server wählen, nach Namen suchen  
Anschließend „Erneuere Schlüsselcache“ zum Aktualisieren

## Dateiverschlüsselung

- Windows Explorer und Dateimanager von WinPT starten
- Zu verschlüsselnde Datei per Drag and Drop in den Dateimanager ziehen und dort markieren
- Menüpunkt „Verschlüsseln“ wählen
- Schlüssel des Adressaten auswählen
- („Sind Sie sicher...“ bestätigen)

Ergebnis: verschlüsselte Datei mit gleichem Dateinamen + .pgp im gleiche Ordner, kann jetzt per email verschickt werden

## Dateientschlüsselung

- Windows Explorer und Dateimanager von WinPT starten
- Zu entschlüsselnde Datei per Drag and Drop in den Dateimanager ziehen und dort markieren
- Menüpunkt „Entschlüsseln“ wählen
- Mantra (=Schutz des eigenen Private Key) eingeben und bestätigen

Ergebnis: entschlüsselte Datei mit gleichem Dateinamen ohne .pgp im gleiche Ordner, kann jetzt bearbeitet werden

### **Public Key(s) „verbreiten“ (eigener oder andere)**

Schlüsselverwaltung starten, Schlüssel wählen

- Menüpunkt „Key“, Unterpunkt „Export“ wählen  
→ Schlüssel wird als ascii-Datei gespeichert
- Diese .asc-Datei kann dann als email-Anlage versendet werden
- Tip: Wählen Sie als Verzeichnis den „Keyrings“-Ordner, dann können Sie von dort aus ihren eigenen öffentlichen Schlüssel immer wieder verschicken

## Backup

Grund: ohne den eigenen Privat Key sind verschlüsselte Nachrichten wertlos

### Sichern des „keyrings“-Ordners

- Enthält in jeweils einem Schlüsselbund alle Public Keys (pubring.pgp) sowie alle Private Keys (secring.pgp)
- Darüberhinaus: Konfiguration, Einstufung der Vertrauenswürdigkeit der Schlüssel usw.

D.h. das „eigene“ PGP ist auch nach z.B. Windowsneuinstallation oder Rechnerwechsel 100% wiederherstellbar

### **Zusätzliche Funktionen von GnuPG/WinPT**

- Ver-/Entschlüsseln der Zwischenablage
- Symmetrische Verschlüsselung
- Signieren von Dateien/Schlüsseln

## 1. Was ist GnuPP?

Das Projekt GnuPP (GNU Privacy Project) ist eine vom Bundeswirtschaftsministerium geförderte E-mail Verschlüsselungssoftware. GnuPP bezeichnet das Gesamtpaket, das die Programme GnuPG, GPA, WinPT und andere Komponenten enthält.

Mit dem Verschlüsselungsprogramm GnuPG (GNU Privacy Guard) kann jedermann E-Mails sicher, einfach und kostenlos verschlüsseln. GnuPG kann privat oder kommerziell eingesetzt werden. Die Verschlüsselung von GnuPG kann nach dem heutigen Stand von Forschung und Technik nicht gebrochen werden.

GnuPG ist Freie Software oder Open-Source-Software. Das bedeutet, dass jedermann das Recht hat, sie nach Belieben kommerziell oder privat zu nutzen.

Und es bedeutet, daß jedermann den Quellcode, also die eigentliche Programmierung des Programms, genau untersuchen soll und darf.

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

### **GnuPG ist vollständig kompatibel mit PGP**

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

PGP ("Pretty Good Privacy") ist keine freie Software, sie wird seit mehreren Jahren nicht mehr unter der freien Softwarelizenz GNU General Public License (GNU GPL) vertrieben.

Weitere Informationen zu GnuPG und den Projekten der Bundesregierung zum Schutz des Internets finden Sie auf der Website [sicherheit-im-internet.de](http://sicherheit-im-internet.de) des Bundeswirtschaftsministeriums.



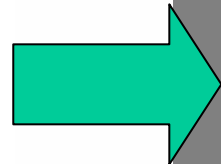
## GnuPP für Durchblicker

Das Hintergrund-KnowHow zum E-Mail-Verschlüsselungssystem GnuPP

Herausgegeben und gefördert vom  
Bundesministerium für Wirtschaft und Technologie  
Scharnhorststr. 34-37  
10115 Berlin

Ansprechpartner:  
Bundesministerium für Wirtschaft und Technologie  
Referat Öffentlichkeitsarbeit

Copyright © Bundesministerium für Wirtschaft und Technologie



### 3.3 Einschätzung der Sicherheit von PGP

In Kapitel 3.1 wurde bereits auf die Kryptoanalyse hingewiesen. Um die Sicherheit von PGP beurteilen zu können, wird kurz auf die Anwendung kryptoanalytischer Attacken auf PGP eingegangen.

#### 3.3.1 Analytische Attacken

Der Quellcode von PGP ist frei erhältlich und folglich sind auch die in PGP benutzten Algorithmen von Kryptoanalytikern gut erforscht. In der Literatur<sup>67</sup> finden sich daher auch unterschiedliche Ansätze, die verwendeten Algorithmen analytisch zu „knacken“. Bei diesen Ansätzen jedoch blieb es, keiner führte zu einem Erfolg. Da man nur vermuten kann, ob jemals eine analytische Attacke auf PGP gelingen wird, nutzt man die Angaben über

<sup>66</sup> Vgl. William Stallings, Datensicherheit mit PGP, 1995, S. 38ff.

<sup>67</sup> Insbesondere bei Reinhard Wotol, Abenteuer Kryptologie.

die Zeitdauer des Durchprobierens aller Schlüssel, um eine Vorstellung von der Sicherheit PGP's zu erhalten.

#### 3.3.2 Brute-Force-Attacke

Die Dauer einer Brute-Force-Attacke wird in erster Linie von zwei Faktoren bestimmt:

- Länge des Schlüssels,
- Rechengeschwindigkeit des Computers, der die Schlüssel prüft.

Beispielrechnungen und Tabellen zu dieser Thematik finden sich in nahezu allen Büchern zur Kryptologie. Beispielhaft steht hier eine Zahl von Richard E. Smith,<sup>68</sup> der für einen 128 Bit IDEA-Schlüssel eine mittlere Suchzeit von  $2 \cdot 10^{18}$  Jahren veranschlagt. Diese Zeit würde ein Rechner brauchen, dessen Leistungsfähigkeit die eines gewöhnlichen PC um ein Vielfaches übertrifft und  $3 \cdot 10^9$  Schlüssel in der Sekunde testet. Für die Faktorisierung eines Public-Key-Schlüssels der Länge von 1024 Bit wird bei gleicher Rechenleistung ungefähr dieselbe Zeitdauer veranschlagt,<sup>69</sup> wobei diese Zeit nicht unbedingt zur Faktorisierung eines PGP-Schlüssels ausreichen würde, denn PGP generiert Public-Keys bis zu 4096 Bit Länge.

Fazit: Für den Anwender sind dies nur Gedankenspielerien, deren weitere Erläuterung sich im Rahmen dieses Buches erübrigt. An gegebenen Stellen in den folgenden Kapiteln wird wiederholt darauf hingewiesen, dass sich Gefahren für verschlüsselte Daten weniger durch kryptoanalytische Attacken als durch Fehler in der Handhabung von PGP ergeben können.

Darüber hinaus sind Gefahren aufgrund gefälschter öffentlicher Schlüssel denkbar. Eine Absicherung gegen gefälschte Schlüssel stellt das *Web of Trust* (Netz der Vertrauens) dar, das im Folgenden kurz vorgestellt wird.