

**Benchmark-Projekt der NKG  
für psychiatrische und  
psychosomatische Krankenhäuser und  
Fachabteilungen**

**Hinweise zur  
Verschlüsselung der  
Datenlieferung**

# PGP-Verschlüsselung

„Pretty Good Privacy“ (PGP) ist ein Methode für die Ver- und Entschlüsselung von Daten.

Das Verfahren PGP (Pretty Good Privacy) basiert auf einem asymmetrischen Verfahren, dieses bedeutet, dass die Ver- und Entschlüsselung mit zwei Schlüsseln geschieht.

Asymmetrische Verfahren, insbesondere PGP, werden bei erhöhten Authentizitäts-Anforderungen verwendet und bieten den höchstmöglichen Schutz gegen unbefugten Zugriff auf Daten.

PGP ist inzwischen das am weitesten verbreitete Verschlüsselungsverfahren.

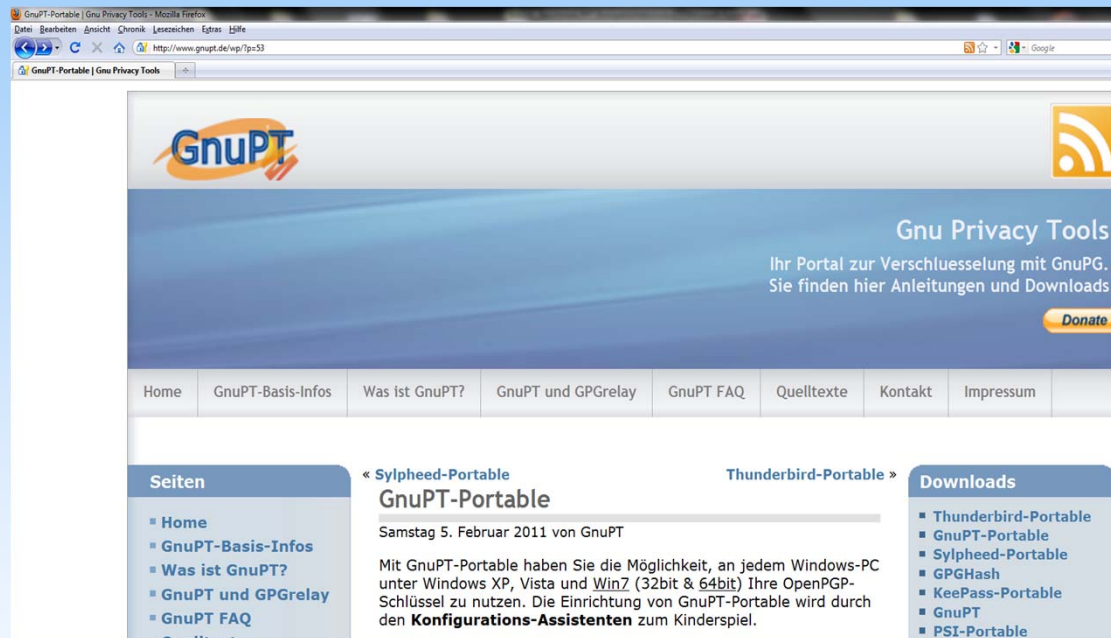
Bei PGP besitzt jeder Kommunikationspartner zwei Schlüssel: Einen privaten und einen öffentlichen.

Mit dem öffentlichen Schlüssel können Dateien nur verschlüsselt, nicht aber gelesen werden. Wenn eine Datei mit dem öffentlichen Schlüssel kodiert wurde, kann nur der Besitzer des passenden privaten Schlüssels den Text wieder entschlüsseln.

Der öffentliche Schlüssel kann ohne weiteres nach außen gegeben werden. Den öffentlichen PGP-Schlüssel kann man sich wie ein offenes Vorhängeschloss vorstellen, das dem Kommunikationspartner in die Hand geben wird. Mit diesem Vorhängeschloss kann er Post "verschließen", aber niemand kann dieses Schloss wieder öffnen, weil nur er den Schlüssel dazu besitzt - seinen privaten PGP-Schlüssel. Nur mit dem privaten Schlüssel kann das „Vorhängeschloss“ öffentlicher Schlüssel geöffnet werden.

Wenn Sie die Psychbenchmark-Dateien an die NKG senden wird der öffentliche PGP Schlüssel der NKG benötigt. Dieser ist auf der NKG-Homepage zu finden, oder wird auf anfrage per Mail versandt.

# PGP-Verschlüsselung am Beispiel des Programmes GnuPT-Portabel



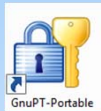
GnuPT – Portabel ist eine vereinfachte Oberfläche für das ebenfalls kostenlose Programm WinPT . Bei der Installation wird WinPT automatisch mit installiert

Das Programm ist kostenlos von der Internetseite <http://www.gnupt.de> herunterladbar.

Dieses Programm hat einen deutschen Konfigurations-Assistenten.  
Ein weiterer Vorteil ist : Portabel – das Programm befindet sich und speichert alles in einem Verzeichnis (auch die dll's und Steuerdateien).  
Das vereinfacht die Datensicherung erheblich!!!

# GnuPT-Portabel

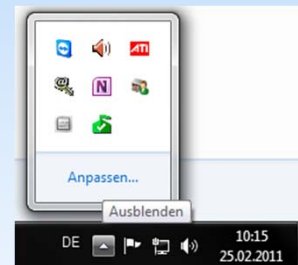
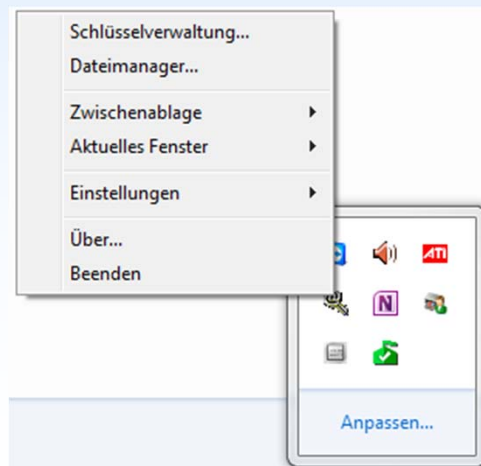
Nach der Installation, bei der Dank des Konfigurations-Assistenten auch die beiden benötigten Schlüssel ganz einfach erzeugt werden, muss das Programm gestartet werden.



Zum Beispiel mit einem Doppelklick auf das Desktopicon des installierten Programmes.

Nun ist das Programm über die Symbolleiste von Windows am rechten unteren Bildrand erreichbar.

Durch Klicken auf das Schlüsselsymbol → werden die Schlüsselverwaltung und der Dateimanager gestartet.



# Schlüsselverwaltung

Benutzerkennung	SchlüsselID	Typ	Größe	Chiffre	Gültigkeit	Vertrauen	Erstellung
BWKKG Stuttgart (PGP-Schlüssel DRG Be...)		pub	1024/1024	DSA/ELG	Keine	Keine	18.03.2008
		pub	2048/2048	RSA/R...	Keine	Keine	26.11.2010
		pub	1024/1024	DSA/ELG	Keine	Keine	08.04.2004
		pub	1024/1024	DSA/ELG	Keine	Keine	08.02.2011
		pub	2048/2048	RSA/R...	Absolut	Absolut	29.11.2010
		pub	1024/2048	DSA/ELG	Keine	Keine	21.05.2008
		pub	2048/2048	RSA/R...	Keine	Keine	25.01.2010
		pub	2048/2048	RSA/R...	Keine	Keine	10.11.2010
		pub	1024/2048	DSA/ELG	Keine	Keine	02.02.2011
		pub	2048/2048	RSA/R...	Keine	Keine	11.07.2005
		pub/sec	1024/2048	DSA/ELG	Absolut	Absolut	10.11.2010
		pub	1024/1024	DSA/ELG	Keine	Keine	15.11.2004
		pub	2048/2048	RSA/R...	Keine	Keine	18.02.2011
		pub	1024/1024	DSA/ELG	Keine	Keine	28.01.2011
	Wagener NKG <wagener@nkgev.de>		pub/sec	1024/2048	DSA/ELG	Absolut	Absolut

Standardschlüssel: 0x722C269C      2 geheime(r) Schlüssel      15 Schlüssel

Es gibt nur 2 Schlüsselsorten :



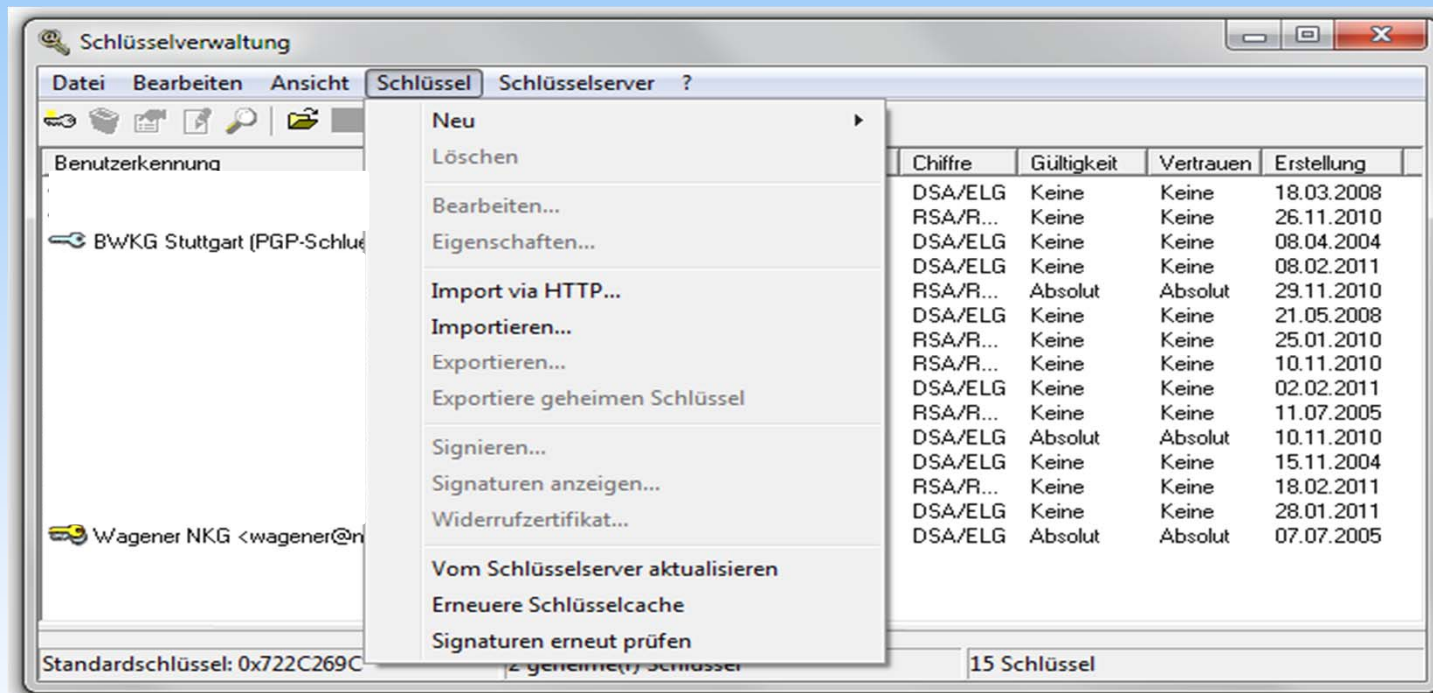
- Öffentlicher Schlüssel (pub)



- Geheimer Schlüssel (sec)

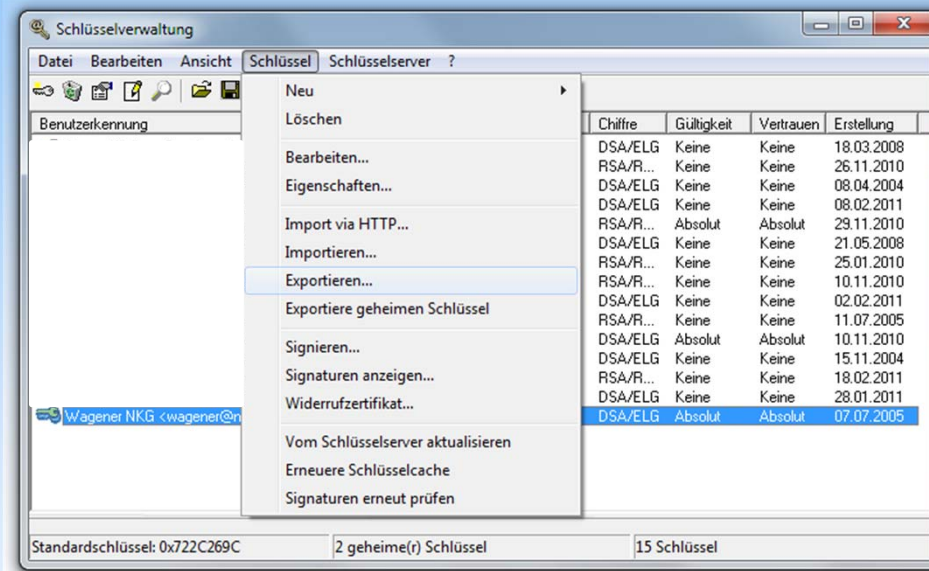
Die Schlüsselverwaltung wird zum Importieren von öffentlichen Schlüsseln der Kommunikationspartner und zum Exportieren des eigenen öffentlichen Schlüssel benötigt.

# Schlüsselverwaltung – Import

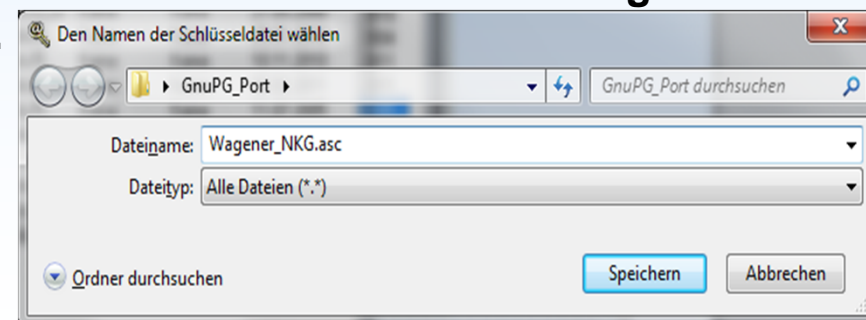


**Einen Schlüssel zu importieren ist einfach:  
Über das Menü der Schlüsselverwaltung: -Schlüssel -Importieren wird eine entsprechende Datei eines öffentlichen Schlüssels ausgewählt und importiert.  
Anschließend ist der Schlüssel in der Schlüsselverwaltung aufgeführt.**

# Schlüsselverwaltung- Export



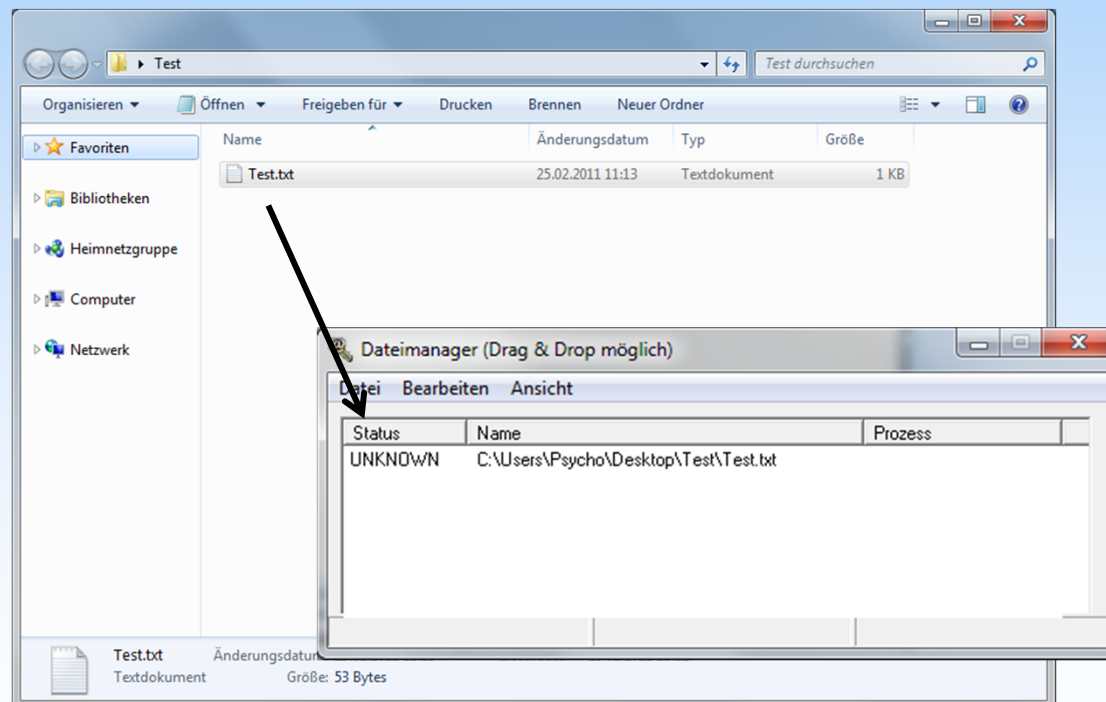
Zum Exportieren des eigenen öffentlichen Schlüssels muss dieser in der Schlüsselverwaltung ausgewählt sein:  
 Über das Menü der Schlüsselverwaltung : Schlüssel – Exportieren wird eine entsprechende Datei des öffentlichen Schlüssels als Textdatei erzeugt. Diese Datei kann nun veröffentlicht werden.



# PGP - Verschlüsseln

## 1. Schritt:

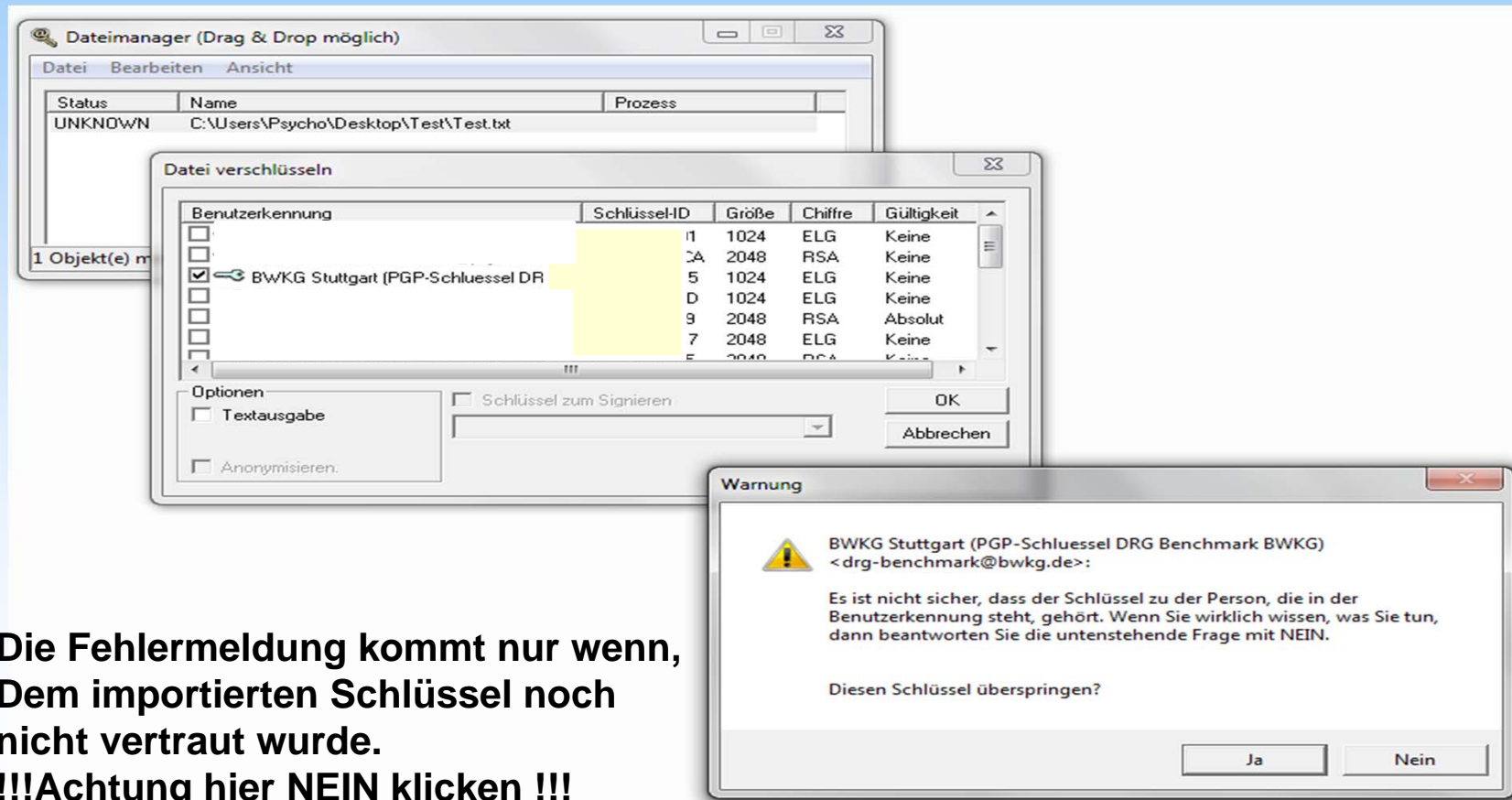
Das Verschlüsseln erfolgt per „Drag and Drop“ mit dem Dateimanager:  
Die Schlüsselverwaltung wird nur zum Importieren von öffentlichen Schlüsseln der Partner und zum Exportieren des eigenen öffentlichen Schlüssel benötigt.



# PGP - Verschlüsseln

## 2. Schritt:

Menü des Dateimanagers: Datei - Verschlüsseln und Auswahl des entsprechenden Schlüssels im nächsten Fenster.



Die Fehlermeldung kommt nur wenn,  
Dem importierten Schlüssel noch  
nicht vertraut wurde.

!!!Achtung hier NEIN klicken !!!

Bei vertrauten importierten Schlüsseln kommt diese Meldung nicht.

# PGP - Verschlüsseln

Fertig:

Die ausgewählte Datei wurde verschlüsselt und kann nun nur noch von dem Besitzer des Geheimen Schlüssels (im Beispiel die BWKG) geöffnet werden. Noch nicht einmal wir selbst können diese Datei entschlüsseln.

Die Datei ist fertig zum Versand und befindet sich im Ursprungsverzeichnis.

