Verschlüsselung mit GPG4Win

Was ist GPG4Win?

Gpg4win (GNU Privacy Guard for Windows) ist ein Kryptografie-Werkzeugpaket zum Verschlüsseln und Signieren unter Windows. Mit Gpg4win kann jeder E-Mails, Dateien und Datei-Ordner einfach und kostenlos ver- und entschlüsseln, sowie ihre Integrität (Unveränderheit) und Herkunft (Authentizität) absichern und überprüfen. Gpg4win und die darin enthaltenen Komponenten sind Freie Software (OSS). Gpg4win wurde beauftragt vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

Die wesentlichen Komponenten von GPG4Win sind:

- GnuPG als das eigentliche Verschlüsselungsprogramm und
- Kleopatra als Benutzeroberfläche, die eine einheitliche Benutzerführung für alle Krypto-Dialoge bereitstellt

Woher bekomme ich GPG4Win?

GPG4Win ist unter folgender Adresse erhältlich: www.gpg4win.de.

I. Installation

Nach dem Herunterladen steht die Datei gpg4win-2.2.1.exe im Downloadverzeichnis. Durch Doppelklick startet das Installationsprogramm (Administratorberechtigung erforderlich!).

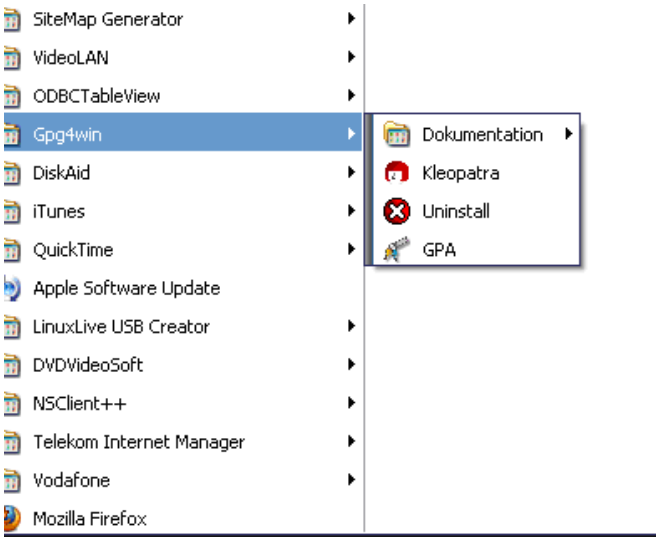
Sofern Sie noch kein Schlüsselpaar haben, müssen Sie später eines erzeugen. Hierfür brauchen Sie das Programm Gnu Privacy Assistant (GPA). Achten Sie darauf, dass Sie dieses dann im Installationsdialog anhaken.

Wählen Sie ein Zielverzeichnis für die Installation des Programms aus. Die angebotene Konfiguration von S/MIME-Wurzelzertifikaten können Sie übergehen.

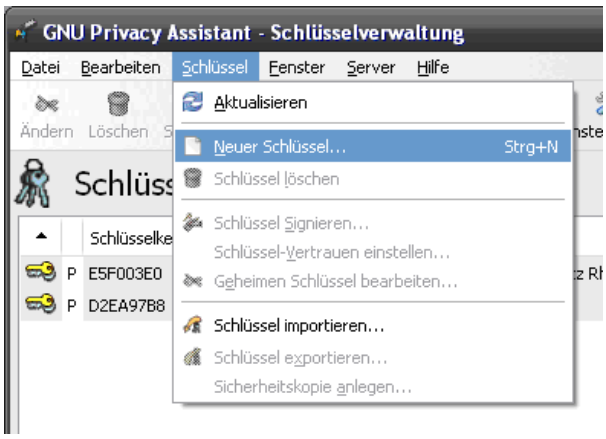
Der Installationsvorgang ist im Einzelnen im GPG4Win-Kompendium beschrieben http://www.gpg4win.de/doc/de/gpg4win-compendium_11.html.

II. Schlüsselpaar erzeugen

Gpg4Win nutzt eine Verfahren, das für die Ver- bzw. Entschlüsselung einem Schlüsselpaar aus einem öffentlichen und einem geheimen Schlüssel arbeitet. Sie brauchen also ein solches Schlüsselpaar. Dies erzeugen Sie mit dem Programm "GPA.exe" aus Ihrem GnuPG-Verzeichnis:

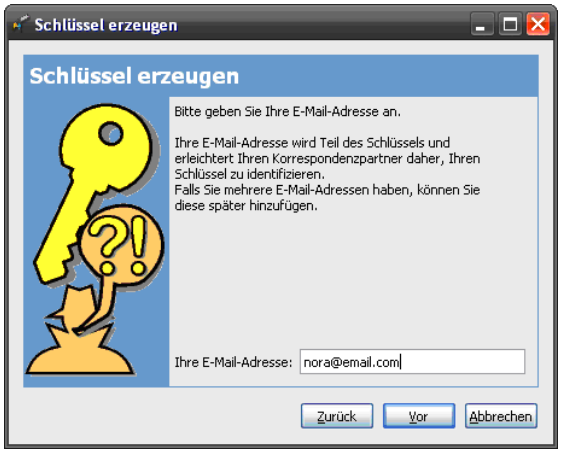


Gnu Privacy Assistant (gpa.exe) starten und im Menü "SCHLÜSSEL - NEUER SCHLÜSSEL" auswählen.



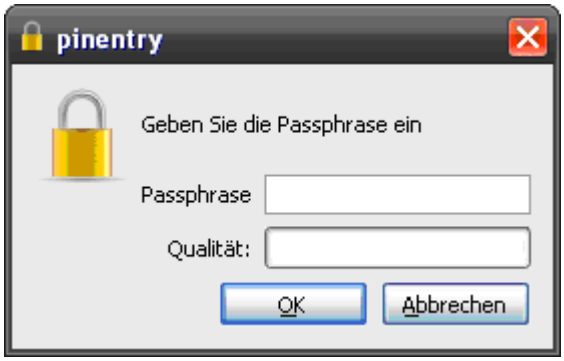
Geben Sie Ihrem Schlüssel einen Namen ...

... und weisen Sie ihm eine E-Mail-Adresse zu. Sie werden anschließend gefragt, ob Sie eine Sicherheitskopie anlegen möchten. Tun Sie dies und speichern Sie dies später an einer sichern Stelle.

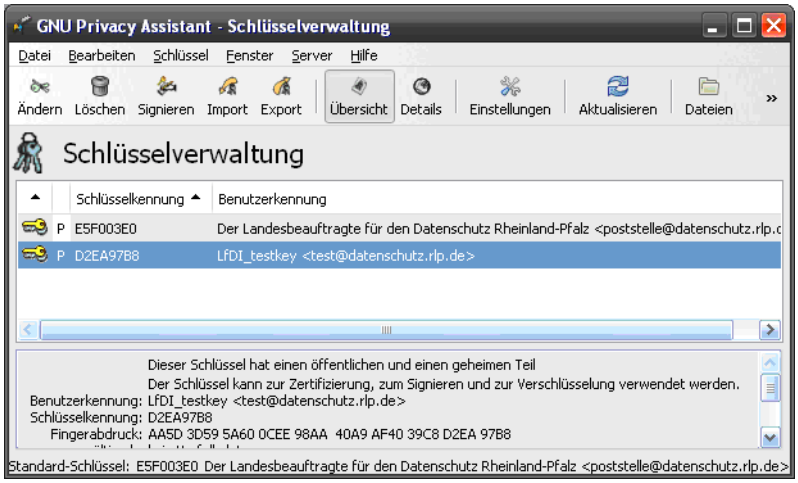


Dann müssen Sie noch eine "Passphrase" eingeben. Wählen Sie hierbei eine längere Zeichenfolge, die auch Ziffern oder Sonderzeichen enthält. Die Passphrase müssen Sie zur

Sicherheit zwei Mail eingeben. Sie wird künftig immer abgefragt, wenn Sie den Schlüssel verwenden wollen.

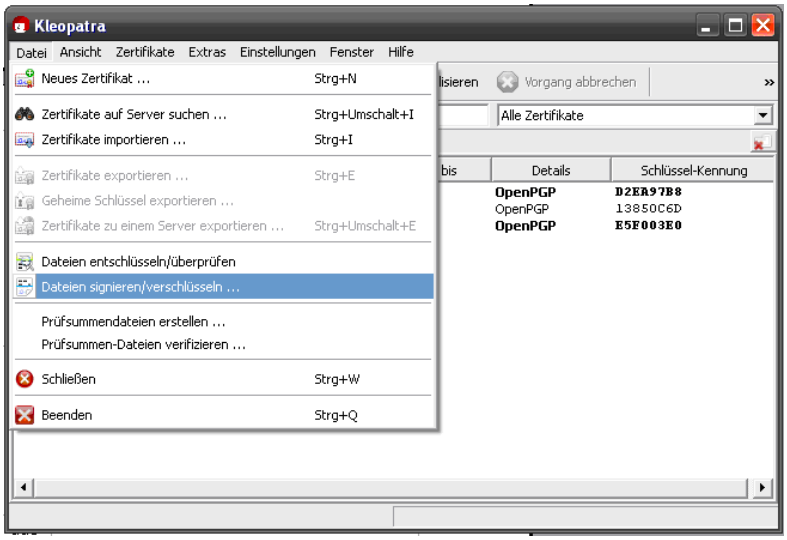


Wenn alles geklappt hat, erscheint Ihr Schlüssel in der Übersicht des Gnu Privacy Assistenten.

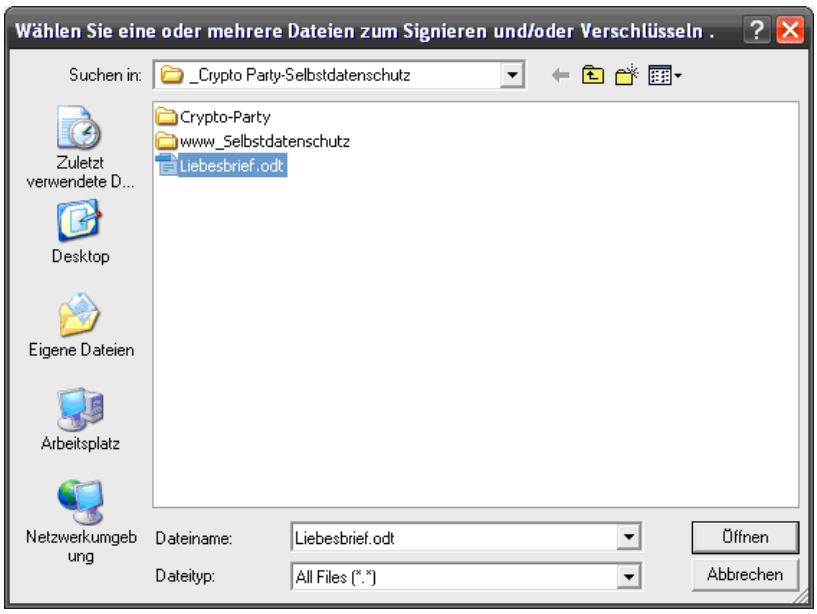


III. Dateien verschlüsseln

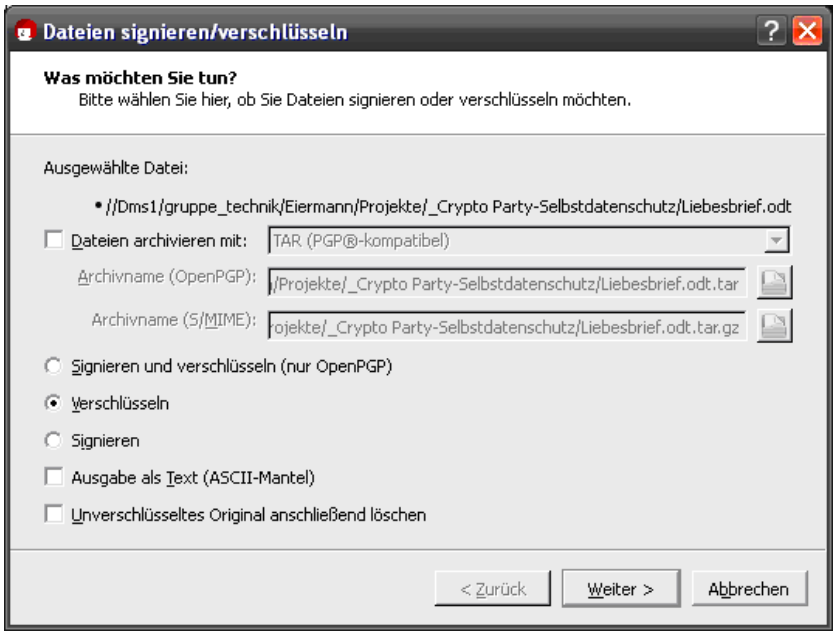
Um einzelne Dateien zu verschlüsseln und sie als Anlage einer Mail beizufügen, gehen Sie wie folgt vor: Starten Sie das Programm "Kleopatra" aus dem GnuPG4Win-Paket und wählen Sie den Menüpunkt DATEIEN SIGNIEREN/VERSCHLÜSSELN



Wählen Sie die die zu verschlüsselnde Datei (im Beispiel: Liebesbrief.odt") über den Datei-Explorer aus und klicken den Button "Öffnen"



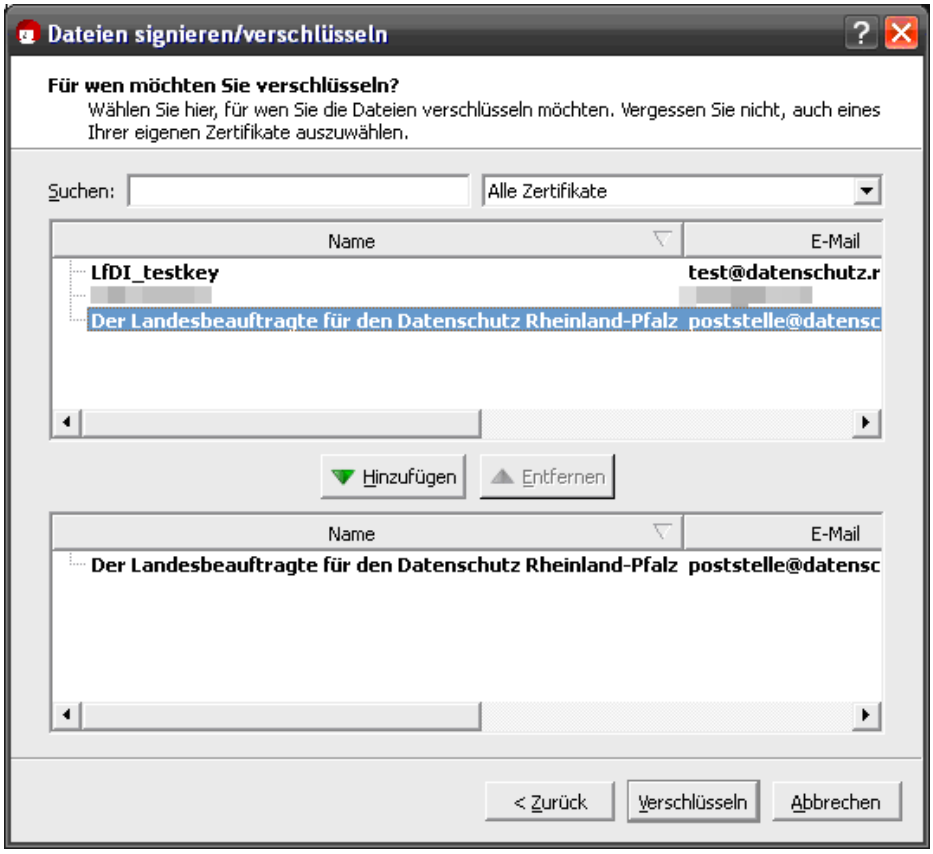
Wählen Sie den Punkt "Verschlüsseln" und klicken Sie "Weiter"



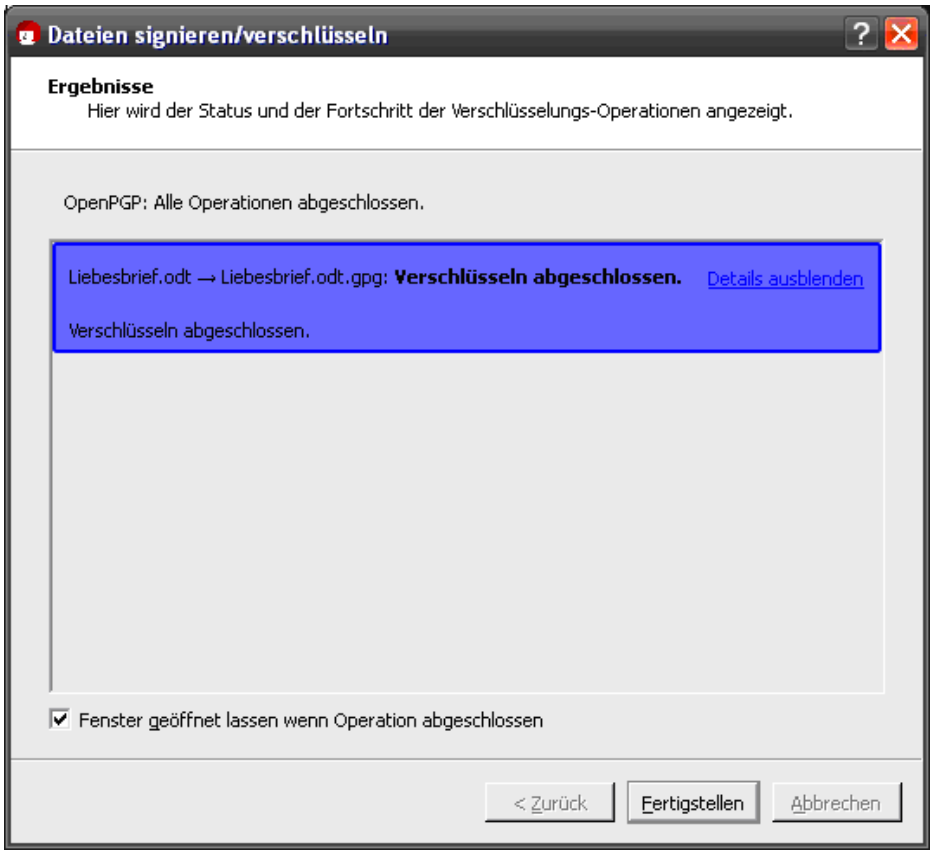
Wählen Sie im folgenden Dialog den Empfänger aus für den Sie die Datei verschlüsseln möchten und klicken Sie "Hinzufügen". Bei mehren Empfängern wiederholen Sie dies.

Klicken Sie auf "Verschlüsseln"

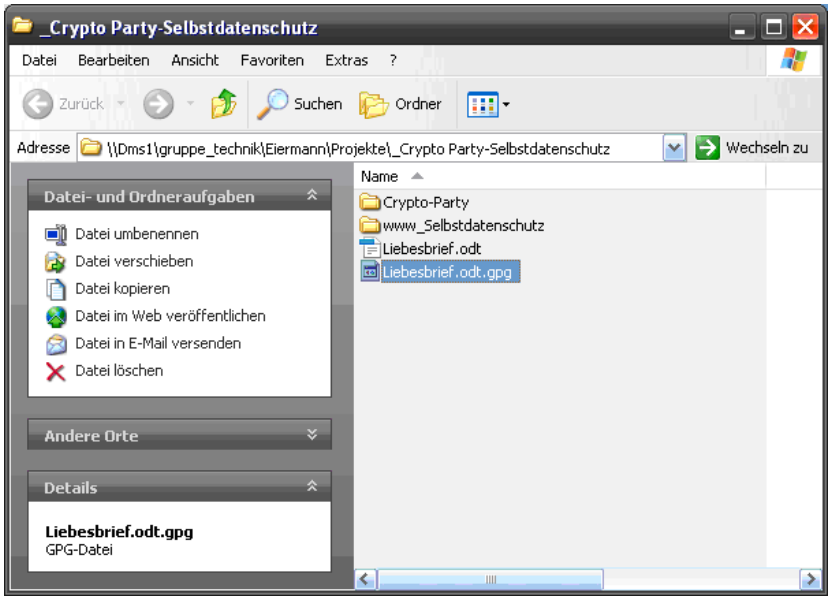
Anmerkung: Sie benötigen von jedem Empfänger, dem Sie die verschlüsselte Datei zukommen lassen wollen, den "öffentlichen GnuPG-Schlüssel". Um sicherzustellen, dass Sie das Chiffrat auch selbst wieder öffnen können, muss der öffentliche Schlüssel des Absenders ebenfalls eingebunden werden.



Wenn es geklappt hat, wird es Ihnen angezeigt.



Die verschlüsselte Datei - das so genannte Chiffrat - befindet sich im gleichen Ordner wie die Ausgangsdatei. Sie trägt den gleichen Namen und hat die Namenserweiterung ".gpg". Diese Datei können Sie jetzt z.B. per Mail verschicken.



IV. Verschlüsseln von Texten über die Zwischenablage

Statt einzelne Dateien zu verschlüsseln und diese als Anlage einer E-Mail bezufügen, können Sie Texte auch über die Zwischenablage verschlüsseln.

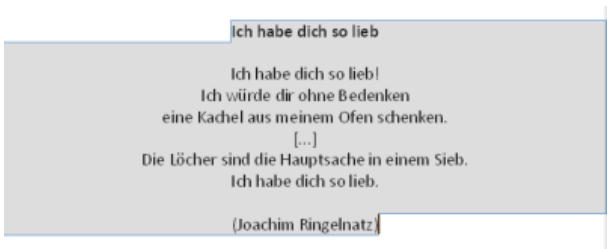
Angenommen, dies ist der Text, den Sie verschlüsseln möchten. Gehen Sie folgendermaßen vor:

Ich habe dich so lieb

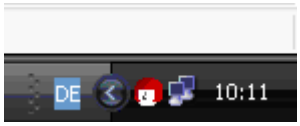
Ich habe dich so lieb!
Ich würde dir ohne Bedenken
eine Kachel aus meinem Ofen schenken.
[...]
Die Löcher sind die Hauptsache in einem Sieb.
Ich habe dich so lieb.

(Joachim Ringelnatz)

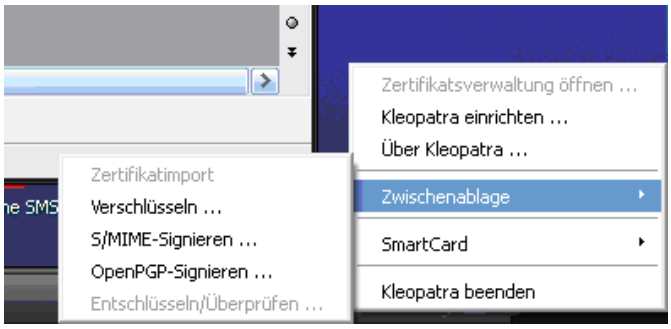
Markieren Sie den zu verschlüsselnden Text und übernehmen Sie ihn über die Menüpunkte BEARBEITEN - KOPIEREN oder die Tastenkombination STRG+C in die Zwischenablage.



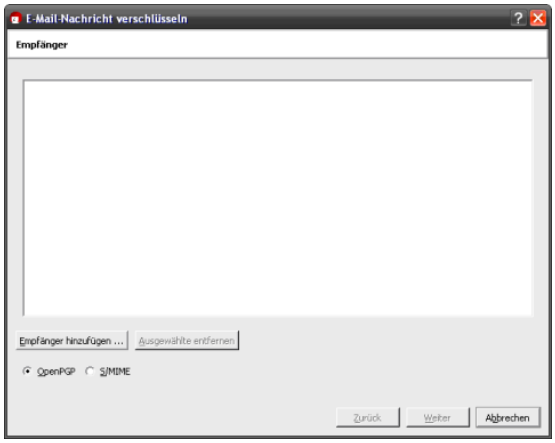
Öffen Sie das Programm Kleopatra aus dem GPG4Win-Paket. In der Windows-Taskleiste sehen Sie das danach Kleopatra-Symbol



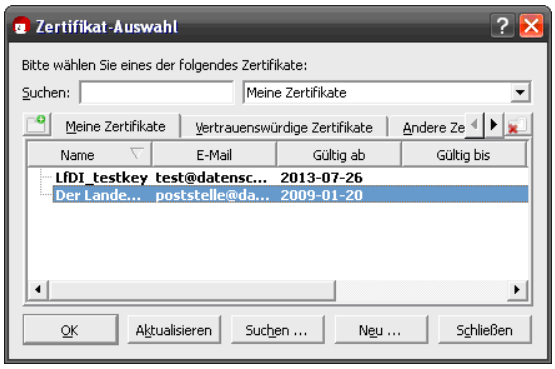
Klicken Sie mit der rechten Maustaste auf das Kleopatra-Symbol und wählen Sie den Punkt ZWISCHENABALAGE und hier den Punkt VERSCHLÜSSELN



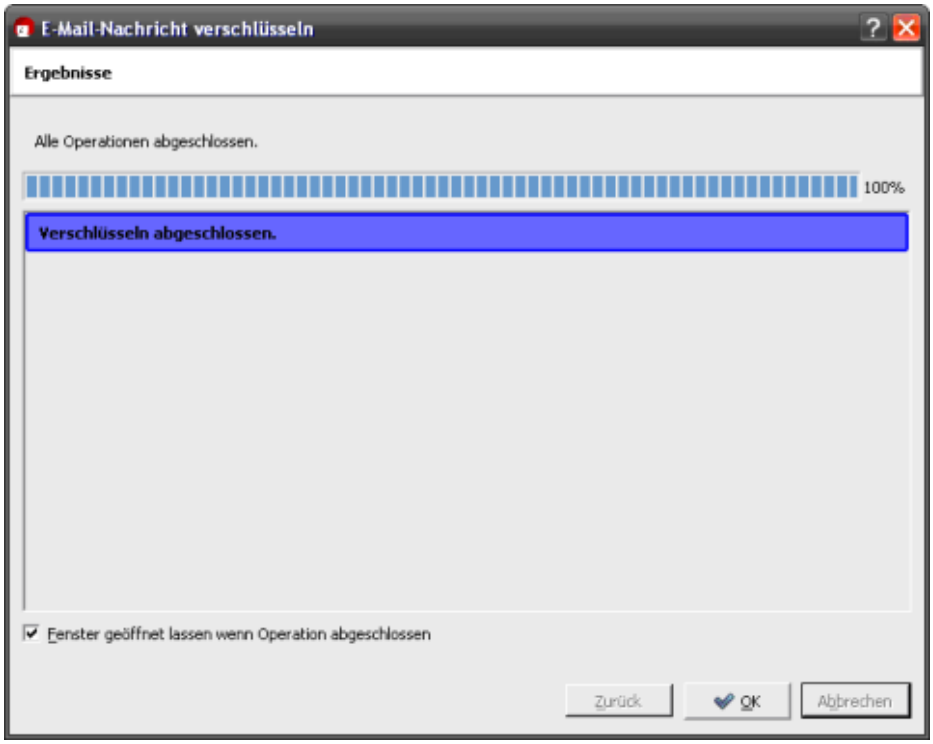
Wählen Sie im folgenden Dialog einen Empfänger aus. Auch hier benötigen Sie den öffentlichen GnuPG-Schlüssel desjenigen, dem Sie die verschlüsselte Nachricht zukommen lassen wollen.



Klicken Sie danach auf OK und anschließend auf WEITER.



Die Verschlüsselung wird Ihnen bestätigt.



Der verschlüsselte Text befindet sich jetzt in der Zwischenablage und kann von dort in eine E-Mail übernommen werden.

Er ist eingschlossen in die Begriffe "---- Beginn PGP Message---- und "----End PGP Message----"

-----BEGIN PGP MESSAGE-----
Version: GnuPG v2.0.20 (MingW32)

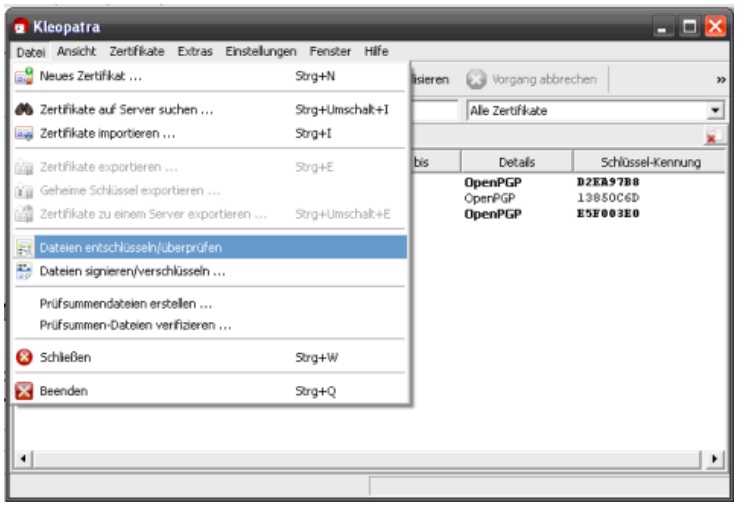
hQEMA0Q1OLgv9TlJAQf7BZjPBs5R5E7aYS+15JjDOiYgktobhSXOsSS98rsZDZyt
KF+5TagfrwUHy6RqzT7Ui+PpeCZ68BfyM43wyiCtiKmsKTGj2AjPnJkHmliswFd1
KZKevOxBpqi0BVeZFfAoPzm74cX0oqHAovDQ61D1HNgER1X8Mb50v2jFQfxu5tbs
Uu4p+59tYUNeo5+cnFHoi7IM1rcWwqpSbex9fRH+wLG6aDGO++3C+kriMgzQC0vA
bsNovPJ+I7Wz4fyinad8sEjZ/elmB+vTe2EeMbcALUCR8Rfsx4Ky30Wy0O4Jt4fC
1XvdTrcDBsqMUbLHgyeyeoDiLly0IP3Urtm/f65LcNLADgGCirIbJo6Q7YGP58Kc
w6/fR6vlf1oCm1NTFXgGO6/QtjYfhEUfcL0qB1EU7ghr3ULICkpu6byKuA5GzaDX
0hLJZmDh+GDsCbVEPh+8Fo3XSY/pnPvQCKj3gGzVxyPz/+HBCeylmwudTcnQo6PL
h0T8eC9tGW2OgsFOXLauNM1cmE82bFKNAMHbk6KEresaFzuTPZMUPys5CctmL7az
797vAIHn82o6khb3rCNCvRC1uoLrEs0X1a8t70l/IpwjlDUPYJX67yfmWHyVae8Z
=haY4
-----END PGP MESSAGE-----

V. Entschlüsseln

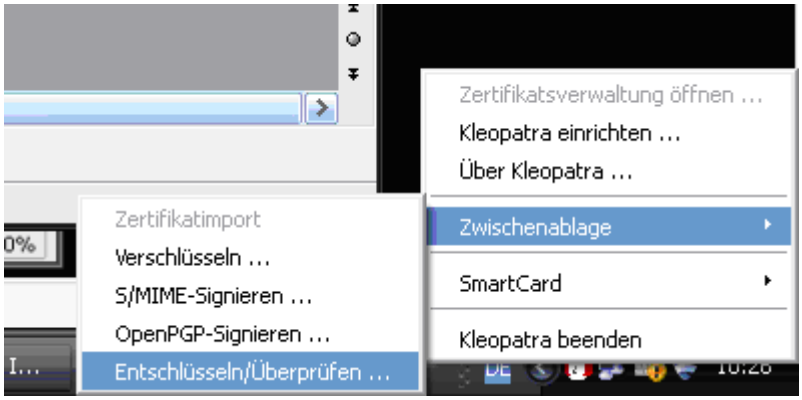
Das Entschlüsseln von Dateien oder von Texten in der Zwischenablage erfolgt in gleicher Weise, nur wählen Sie hier andere Menüpunkte:

Im Programm Kleopatra die Menüpunkte

DATEI - DATEIEN ENTSCHLÜSSELN



Für Texte in der Zwischenablage per rechtem Mausklick ZWISCHENABLAGE und ENTSCHLÜSSELN



VI. Hinweis

Das GNUPG-Verfahren funktioniert plattformübergreifend. Das heißt mit entsprechenden Programmen für Apple Macintosh (OSX), iPad/iPhone (iOS) oder Android-Geräte können Sie auch dort Dateien oder Texte bearbeiten. Dies sind z.B.:

- für Macinstosh Computer (OSX)
  - das kostenlose Programmpaket GPG-Tools (https://gpgtools.org/)
- für iPad und iPhone (iOS)
  - das kostenlose Programm "OpenGP Lite" aus dem App-Store.
- für Android Tabelts und Smartphones
  - das kostenlose Programm APG aus dem Google Play Store