

April 2009

## **Sichere E-Mail-Kommunikation zur datenschutz cert GmbH – Merkblatt**

---

### **1. Einleitung**

Da sich E-Mails mit ein wenig Know-how auf dem Weg durch die elektronischen Netze relativ leicht mitlesen lassen, ist das Verschlüsseln von E-Mails – gerade bei vertrauenswürdigen Inhalten – wichtig.

Aus diesem Grund möchten wir Ihnen mit diesem Dokument einen kleinen Überblick verschaffen, wie Sie möglichst einfach vertrauenswürdig mit der datenschutz cert GmbH per E-Mail kommunizieren können.

Dazu schlagen wir vor, das weit verbreitete GPG- oder GnuPG-Verfahren (GNU Privacy Guard) zu nutzen, wobei nach Absprache natürlich auch andere kryptographische Verfahren zur sicheren Kommunikation möglich sind. GPG (GNU Privacy Guard) ist ein asymmetrisches Verfahren und wurde als freie Alternative zum bekannten Quasi-Standard PGP (Pretty Good Privacy) entwickelt. GPG stellt in diesem Kontext die Grundlage zum Ver- und Entschlüsseln von E-Mails mit asymmetrischen Kryptoverfahren bereit.

Um E-Mails mit GPG zu verschlüsseln und verschlüsselte E-Mail entschlüsseln zu können, haben wir zwei praktikable – und kostenlose – Möglichkeiten ausgewählt:

- Erweiterung für den E-Mail-Client Mozilla Thunderbird, so dass Sie durch ein einfaches „Häkchen-Setzen“ E-Mails verschlüsseln, vgl. Abschnitt 2;
- oder: Ver- und Entschlüsselung von Dateien mit dem separaten Tool WinPT, vgl. Abschnitt 3.

Diese beiden Alternativen werden in diesem Dokument ausführlich mit Screenshots zur Installation, Konfiguration und Nutzung erläutert. Im Anhang finden Sie weitere Informationen über den praktischen Einsatz von asymmetrischer Kryptographie.

---

### **2. Erweiterung des E-Mail-Client Mozilla Thunderbird**

Für die Erweiterung von Mozilla Thunderbird ist zunächst die Installation von GPG notwendig.

---

#### **2.1 GPG (GNU Privacy Guard)**

##### **2.1.1 Installation von GPG**

Das Programm GnuPG ist die Basis für das Ver- und Entschlüsseln von E-Mails. Dieses Programm ist kostenlos unter [www.gnupg.org](http://www.gnupg.org) erhältlich.

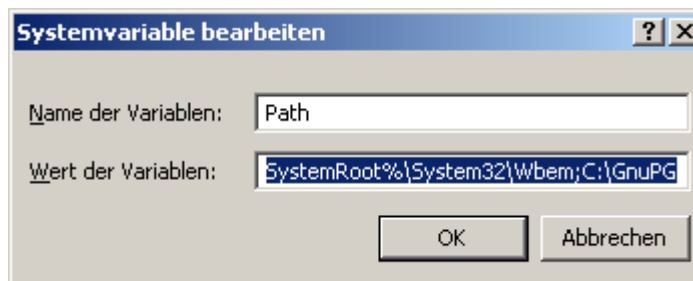
Nach dem Download wird mit einem Doppelklick die Installation gestartet. Da der Installationspfad geändert wird, werden keine Administratorenrechte benötigt; der entsprechende Warnhinweis kann somit ignoriert werden.

Im Installationsprozess bleiben alle Einstellungen bei ihrem Standard, bis auf den Installationspfad. Dieser wird in unserem Beispiel auf C:\GnuPG\ geändert.

Sollten die Installation ohne Administratorrechten durchgeführt worden sein, muss nach der erfolgreichen Installation die Umgebungsvariable „PATH“ auf den Pfad von GnuPG gesetzt werden, damit die nachfolgenden Tools genau wissen, wo GnuPG zu finden ist, damit diese darauf zugreifen können. Hierfür werden einmalig Administratorrechte benötigt. Die Umgebungsvariable wird wie folgt gesetzt:

Unter Systemsteuerung > System > Erweitert > Umgebungsvariable > PATH > Bearbeiten anfügen: C:\GnuPG.

Bitte beachten Sie, dass mehrere Variablen immer mit einem Semikolon ( ; ) getrennt werden. Vor C:\GnuPG muss also ein Semikolon gesetzt sein oder, falls noch nicht vorhanden, gesetzt werden.



### 2.1.2 Konfiguration und Nutzung von GPG

Nachdem Sie GPG installiert haben, können Sie eine der folgenden beiden Alternativen nutzen, um Ihre E-Mail-Kommunikation abzusichern:

- Verschlüsselung des gesamten Emailverkehrs oder der Anhänge mittels der Thunderbird-Erweiterung Enigmail (Abschnitt 2.2) oder
- Ver- und Entschlüsseln von Dateien mit dem separaten Tool WinPT (Abschnitt 3).

## 2.2 Erweiterung des E-Mail-Clients Mozilla Thunderbird mit Enigmail

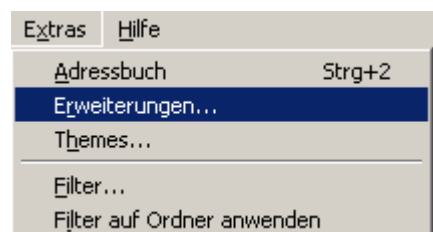
Um mit dem E-Mail-Client Mozilla Thunderbird das Ver- und Entschlüsseln von E-Mails mit GnuPG zu ermöglichen, wird die Erweiterung Enigmail für Thunderbird benötigt.

### 2.2.1 Installation von Enigmail

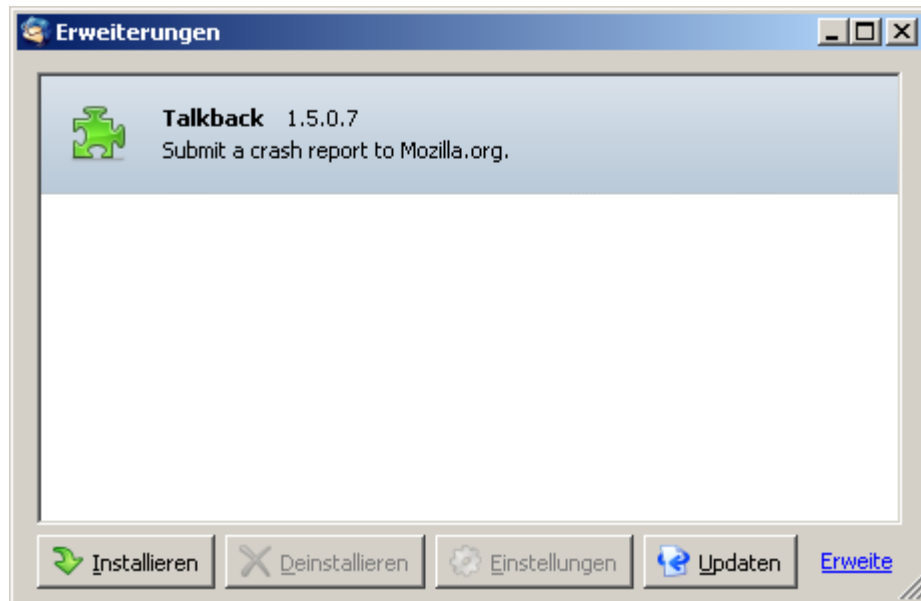
Enigmail ist auf <http://enigmail.mozdev.org> kostenlos verfügbar.

Achtung: Falls Mozilla FireFox benutzt wird, muss die Datei mit „Rechtsklick -> Ziel speichern unter...“ gespeichert werden, da der Browser sonst versucht, diese Erweiterung für FireFox zu installieren.

Nachdem die Datei heruntergeladen wurde, muss diese noch in Thunderbird installiert werden. Dazu wird das Programm – falls nicht bereits erfolgt – gestartet und in der oberen



Registerkarte „Extras“ die Option „Erweiterungen“ ausgewählt. Dort öffnet sich dann folgendes Fenster:



Nachdem Sie auf „Installieren“ geklickt haben, öffnet sich ein Fenster, in dem Sie aufgefordert werden, die .xpi-Datei zu suchen. Nachdem Sie die Datei gewählt und auf „Öffnen“ geklickt haben, öffnet sich ein weiteres Fenster, in dem Sie gefragt werden, ob Sie diese Erweiterung installieren möchten. Zwar findet sich dort der Hinweis, dass die Erweiterung nicht signiert ist; allerdings kann die Erweiterung installiert werden. Sobald auf „Jetzt installieren“ geklickt wurde, wird Enigmail in der Liste der Erweiterungen aufgelistet.

Anschließend muss der E-Mail-Client Thunderbird neu gestartet werden, damit die Änderungen aktiv werden. Nach dem Neustart von Thunderbird erscheint die neue Registerkarte „OpenPGP“.

Die Erweiterung Enigmail ist auf Englisch. Sie können allerdings das deutsche Sprachpaket installieren, welches ebenfalls von den Internetseiten von Enigmail bezogen werden kann (<http://enigmail.mozdev.org/langpack.html>). Hier wird aus der Liste das deutsche Sprachpaket ausgewählt und – da es sich auch hier um eine Erweiterung handelt – mit „Rechtsklick -> Ziel speichern unter...“ lokal abgespeichert. Um das Paket zu installieren, wird wieder das Erweiterungs Fenster im Thunderbird geöffnet und das Sprachpaket installiert – genau so wie die Erweiterung selbst. Auch hier muss Thunderbird nach der erfolgreichen Installation des Sprachpaketes neu gestartet werden, damit die Änderungen aktiv werden.

Die Installation ist somit abgeschlossen. Das Erweiterungs-Fenster sollte, nachdem Enigmail und das dazugehörige deutsche Sprachpaket installiert wurden, so aussehen:

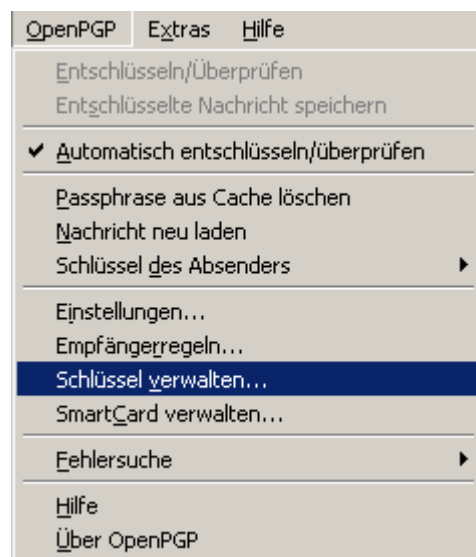


### 2.2.2 Konfiguration von Enigmail

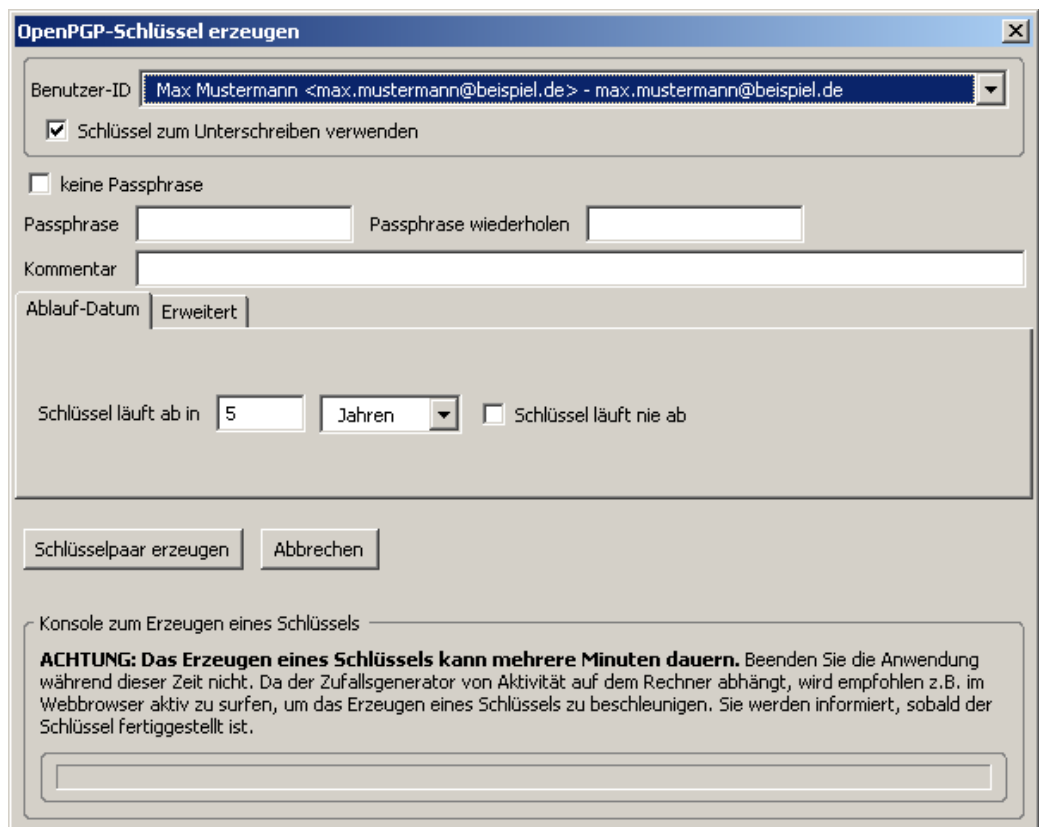
#### Erzeugen eines Schlüsselpaares

Enigmail bietet eine graphische und leicht verständliche Oberfläche zum Erzeugen der Schlüssel. Hierfür wählen Sie unter der Registerkarte „OpenPGP“ den Punkt „Schlüssel verwalten“ aus.

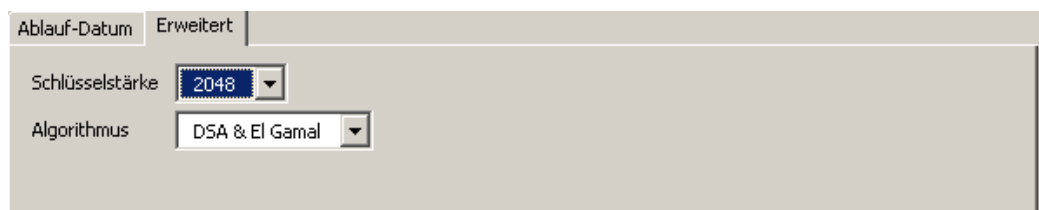
Nun öffnet sich ein neues Fenster, das – sofern noch keine Schlüssel hinzugefügt wurden – leer ist. In diesem Fenster wird die Registerkarte „Erzeugen“ ausgewählt und dort der Punkt „Neues Schlüsselpaar“.



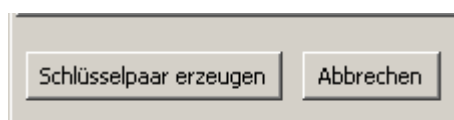
Nun öffnet sich das Fenster zum Erzeugen des Schlüsselpaares:



Oben wird das in Thunderbird eingetragene Profil automatisch erkannt. Falls mehrere Profile eingerichtet wurden, besteht natürlich die Möglichkeit, sich das gewünschte auszuwählen. Nun wählen Sie eine sichere Passphrase sowie optional einen Kommentar. Als nächstes wird ein Ablauf-Datum ausgewählt. Es empfiehlt sich, nicht die Option „Schlüssel läuft nie ab“ zu wählen, sondern nach einer gewissen Zeit den Schlüssel zu ändern, da Schlüssel „altern“. Nach dem diese Einstellungen vorgenommen wurden, wird die Registerkarte „Erweitert“ ausgewählt.



Als Standard-Wert ist bei der Schlüsselstärke „2048“ und beim Algorithmus „DSA & El Gamal“ vorgegeben. Beide Werte werden so beibehalten. Nun kann der Schlüssel erzeugt werden.



Nun wird nochmals nachgefragt, ob der Schlüssel erzeugt werden soll. Die Option „Ja“ wird ausgewählt. Der Schlüssel wird nun erzeugt. Danach wird gefragt, ob ein Widerrufs-zertifikat erstellt werden soll, mit dem es im Fall eines Missbrauches durch Dritte möglich ist, den Schlüssel für ungültig zu erklären. Da dies zu empfehlen ist, wird auch hier die Option „Ja“ gewählt. Anschließend wird darum gebeten, einen Speicherort für das Widerrufs-zertifikat anzugeben. Wenn der Schlüssel erzeugt wurde und der Speicherort bestimmt, erscheint die Aufforderung, die zuvor eingegebene Passphrase einzutippen. Wenn diese korrekt eingegeben wurde, erscheint die Bestätigung, dass das Widerrufs-zertifikat erfolgreich erstellt wurde. Nun ist der Schlüssel im Fenster „Schlüssel verwalten“ zu finden.

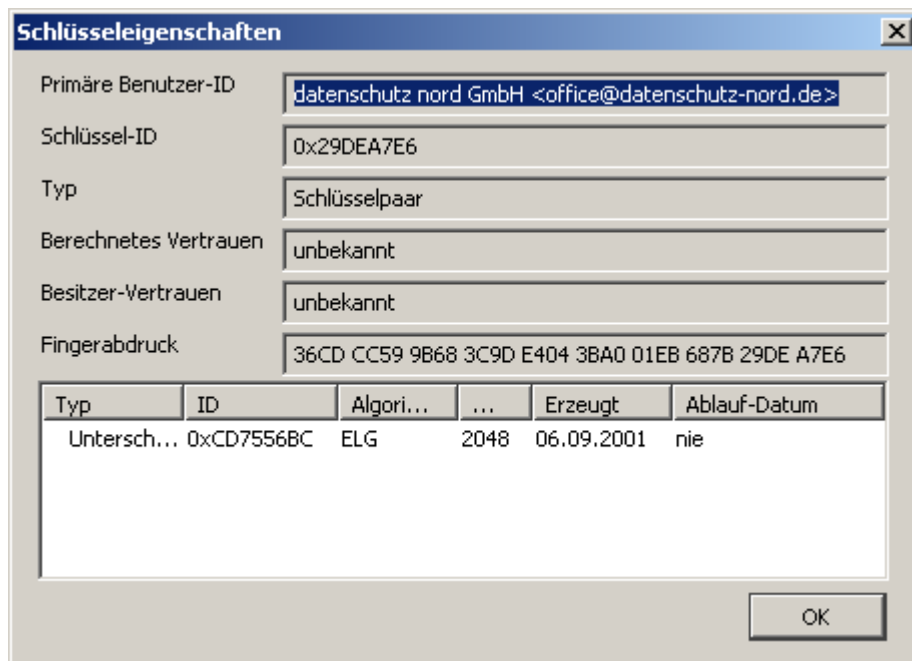
Die Schlüssel sind nun fertig erstellt.

### Import eines öffentlichen Schlüssels

Wenn der Schlüssel bereits lokal als Datei vorliegt, kann dieser mit wenigen Schritten importiert werden.

Hierzu wird in Thunderbird die Registerkarte „OpenPGP“ geöffnet und der Menüpunkt „Schlüssel verwalten...“ ausgewählt. Nun kann über „Datei -> Importieren ...“ eine lokale Datei gewählt werden, die den Schlüssel enthält. Bei Dateien, die Schlüssel enthalten, können mehrere Dateitypen auftreten. Damit der Schlüssel trotzdem gefunden werden kann, empfiehlt es sich, bei Dateityp die Option „Alle Dateien“ auszuwählen.

Weiterhin besteht auch die Möglichkeit, einen Schlüssel folgendermaßen zu importieren: Registerkarte „OpenPGP“ öffnen und dort in dem Untermenü von „Schlüssel des Absenders“ die Option „Schlüssel importieren“ wählen.

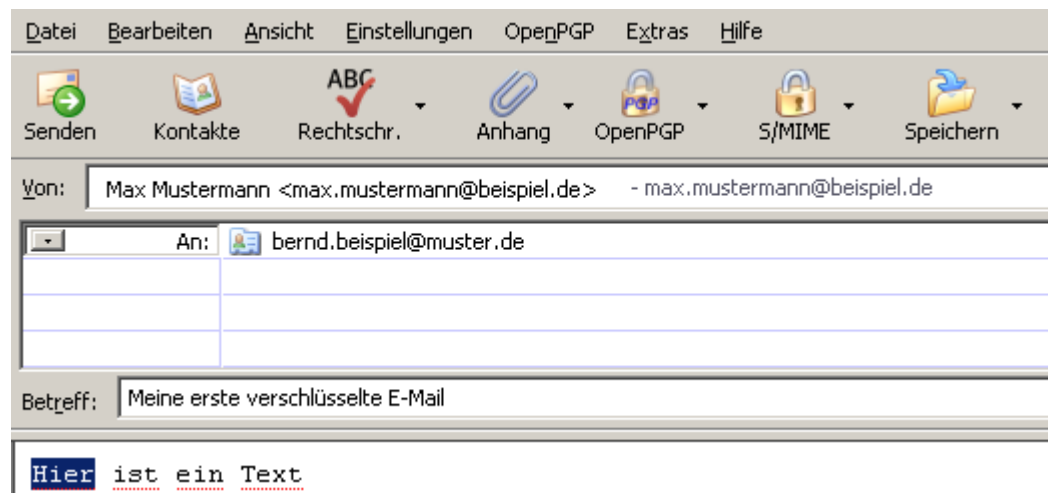


Über „OpenPGP -> Schlüssel verwalten...“ können Sie sich für jeden Schlüssel über die Schlüsseleigenschaften den Fingerprint des Schlüssels anzeigen lassen.

### 2.2.3 Nutzung von Enigmail

#### Eine E-Mail verschlüsseln

Zum Ausprobieren wird nun eine neue E-Mail verfasst.

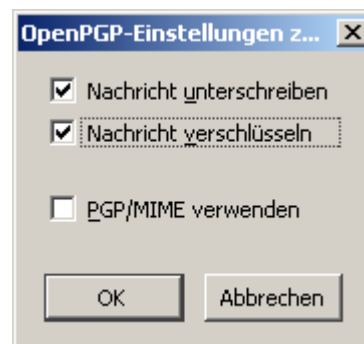


Zum Verschlüsseln dieser E-Mail bitte auf den Button „OpenPGP“ klicken.

Dann öffnet sich ein kleines Fenster, in drei Optionen zur Auswahl stehen.

Da die Nachricht verschlüsselt abgeschickt werden soll, wird die Option „Nachricht verschlüsseln“ ausgewählt.

Optional: Damit Ihr Kommunikationspartner sicher sein kann, dass die E-Mail auch wirklich von Ihnen stammt, können Sie zusätzlich die Option „Nachricht unterschreiben“ auswählen. „PGP/MIME verwenden“ bleibt deaktiviert. Danach auf OK klicken.



Nun leuchten in der unteren rechten Ecke des Fensters ein grüner Stift und ein grüner Schlüssel. Fährt man mit der Maus über die Symbole, wird beim Stift „Nachricht wird unterschrieben“ und beim Schlüssel „Nachricht wird verschlüsselt“ angezeigt. Anschließend kann die Nachricht versendet werden.

#### Eine verschlüsselte E-Mail entschlüsseln

Wenn Sie eine verschlüsselte E-Mail erhalten haben und dieses Kryptogramm nun entschlüsseln möchten, werden Sie beim Anklicken der Nachricht von Thunderbird aufgefordert, Ihre Passphrase einzugeben. Hierbei handelt es sich um die private Passphrase, die beim Erzeugen des eigenen Schlüssels eingegeben wurde. Bei Eingabe einer falschen Passphrase wird die E-Mail nicht entschlüsselt; in diesem Fall wird von Enigmail angezeigt:

**OpenPGP:** Fehler - geheimer Schlüssel wird zur Entschlüsselung benötigt; klicken Sie bitte auf das Zeichen mit dem Schlüssel für Details

### 3. WinPT

Mit (WinPT Windows Privacy Tray) können Sie einzelne Dateien ver- und entschlüsseln. WinPT hat den Vorteil, dass es auf die bereits installierte GnuPG-Software samt der kryptographischen Schlüssel aufsetzt, Sie also dadurch die bereits importierten Schlüssel einfach nutzen können. Zusätzlich bietet WinPT die Möglichkeit der Schlüsselverwaltung.

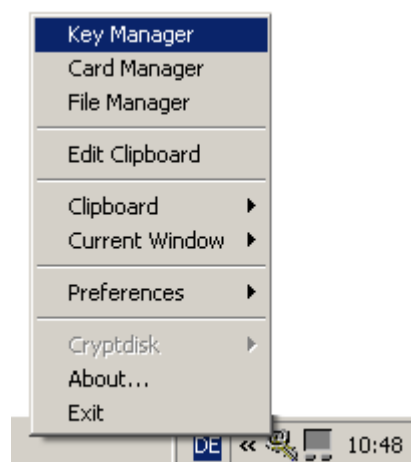
#### 3.1 Installation und Konfiguration von WinPT

WinPT kann kostenlos bezogen werden über: <http://winpt.gnupt.de/wp/>. Sollten Sie das notwendige GnuPG nicht installiert haben, so können Sie auch ein Komplettpaket aus GnuPG und WinPT unter <http://www.gnupt.de/wp/> beziehen.

Nach dem Download wird die Installation mit einem Doppelklick gestartet, woraufhin sich WinPT installiert.

Zum Starten der Anwendung führen Sie bitte WinPT.exe aus.

In der Taskleiste rechts erscheint sodann ein kleines „WinPT-Schlüssel“-Symbol und das rechts dargestellte Auswahlfenster, sobald Sie mit der rechten Maustaste auf das „WinPT-Schlüssel“-Symbol klicken.

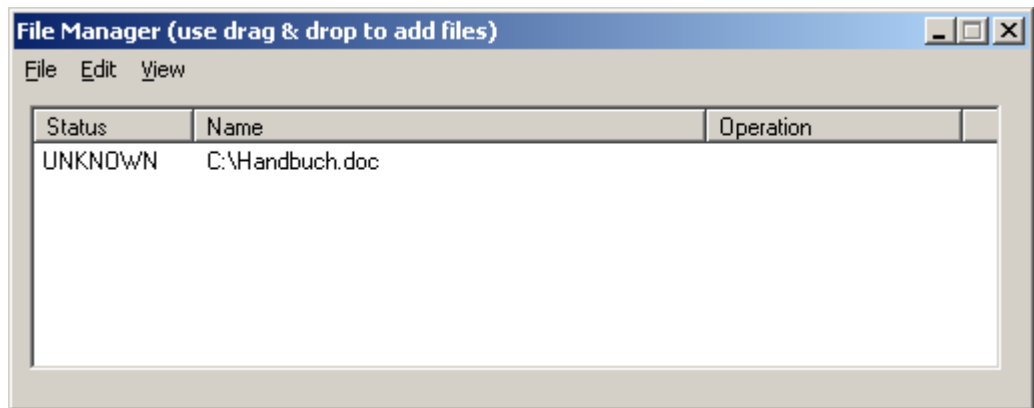


Über den Key Manager können Sie die kryptographischen Schlüssel verwalten, wobei Sie dabei dieselben Schlüssel verwalten, auf die auch Enigmail zugreift.

#### 3.2 Nutzung von WinPT

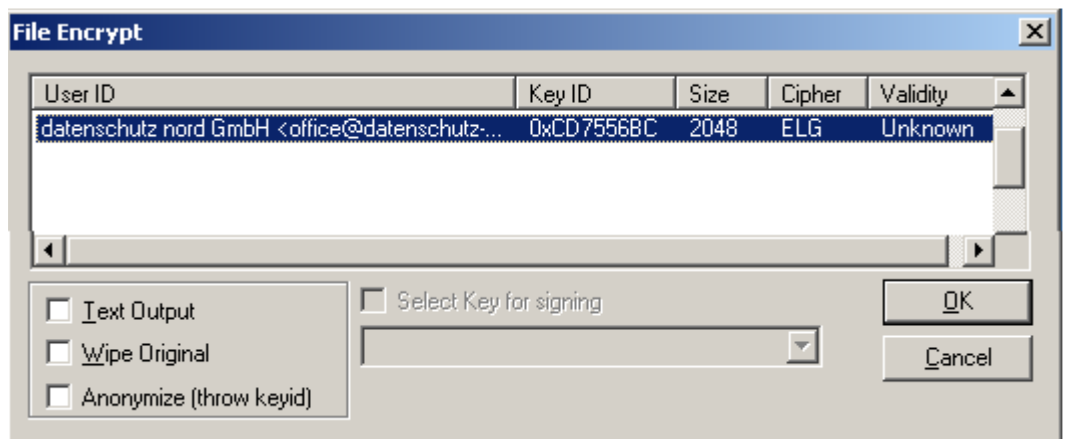
##### 3.2.1 Verschlüsseln einer Datei

Zum Verschlüsseln einer Datei starten Sie bitte die Anwendung WinPT.exe und öffnen durch Betätigung des kleinen „WinPT-Schlüssel“-Symbol mit der rechten Maustaste den Auswahlpunkt „File Manager“, woraufhin sich ein Fenster öffnet, in welches Sie die zu verschlüsselnde Datei (in diesem Beispiel „Handbuch.doc“) durch „Drag & Drop“ aus dem Explorer „ziehen“ oder über „File -> Open...“ öffnen.

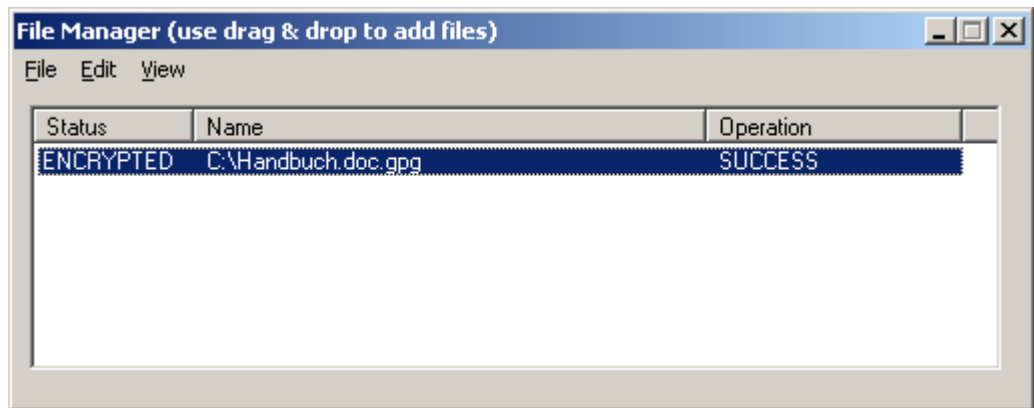


Anschließend betätigen Sie unter „File“ die Auswahl „Encrypt“ für Verschlüsseln, woraufhin Sie den Schlüssel des Empfängers auswählen können, mit dem die Datei verschlüsselt wird.

Analog können Sie über dieses Auswahlmenü auch Dokumente signieren.

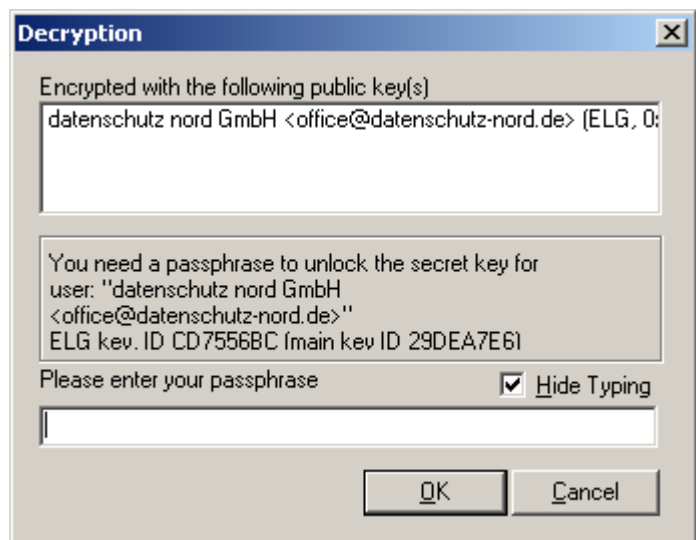


Anschließend finden Sie folgende Meldung sowie das verschlüsselte Dokument mit der Endung „.gpg“ an dem Speicherort, wo auch das „Klartext“-Dokument liegt.



### 3.2.2 Entschlüsseln einer verschlüsselten Datei

Zum Entschlüsseln verfahren Sie wie oben in Abschnitt 3.2.1 beschrieben, wobei Sie allerdings im File Manager unter „File“ statt der Auswahl „Encrypt“ nun „Decrypt“ für Entschlüsseln auswählen, woraufhin Sie nach Ihrer Passphrase gefragt werden.



## 4. Schlüssel der datenschutz cert GmbH

Auf den Internetseiten der datenschutz cert GmbH finden Sie unter „Über uns“ Ihre Ansprechpartner mit ihren Kontaktdaten und ihrem öffentlichen Schlüssel.

Bei Fragen: Kontaktieren Sie uns. Unsere Kontaktdaten:

datenschutz cert GmbH

Barkhausenstr. 2  
27568 Bremerhaven

Tel.: 0471/300-11-0  
Fax.: 0471/300-11-11

E-Mail: [office@datenschutz-cert.de](mailto:office@datenschutz-cert.de)

Internet: [www.datenschutz-cert.de](http://www.datenschutz-cert.de)

Key: [http://www.datenschutz-cert.de/kontakt/datenschutz\\_cert\\_GmbH.asc](http://www.datenschutz-cert.de/kontakt/datenschutz_cert_GmbH.asc)

Fingerprint: 1966 A2FC 2FoE o8F3 2979 188A 8A8D Ao5D 66Eo Doo3

---

## Anhang: Kleiner Exkurs zum Thema „Verschlüsselung“

Verschlüsselungssysteme unterscheidet man generell in symmetrische und asymmetrische Verfahren. Der namensgebene Unterschied besteht darin, dass bei symmetrischen Verfahren derselbe Schlüssel für die Verschlüsselung und die Entschlüsselung verwendet wird. Beide Vorgänge sind daher in gewissem Sinne symmetrisch zueinander. Asymmetrische Verfahren besitzen dagegen ein Schlüsselpaar. Verschlüsselt man eine Nachricht mit dem einen Schlüssel dieses Paares, so lässt sie sich nicht mit demselben Schlüssel wieder dechiffrieren. Dies ist ausschließlich mit dem zweiten Schlüssel dieses Paares möglich. Hierbei sind die Rollen der beiden Schlüssel theoretisch beliebig vertauschbar. In der Praxis aber bestimmt man einen Schlüssel als privaten Schlüssel (*private key*). Dieser wird geheim gehalten. Den anderen bezeichnet man als öffentlichen Schlüssel (*public key*) und gibt diesen an seine Kommunikationspartner weiter.

---

### Die Kommunikation in der Praxis

Wenn Sie Ihrem Kommunikationspartner eine verschlüsselte E-Mail senden möchten, verschlüsseln Sie diese E-Mail mit seinem öffentlichen Schlüssel. Dieses Chiffre ist nun ausschließlich mit dem zweiten Schlüssel aus dem entsprechenden Schlüsselpaar zu entschlüsseln. Dieser zweite Schlüssel ist sein *private key*, den nur er kennt.

Die aktuell verwendeten Kryptoverfahren – die asymmetrischen Verfahren RSA, DSA und ElGamal sowie die Hashfunktionen SHA-1 und RIPEMD-160 – sind für mindestens 1024 Bit – besser noch 2048 Bit – lange Schlüssel gegenwärtig als sicher zu erachten, so dass es praktisch nicht möglich ist, aus dem öffentlichen Schlüssel Ihren privaten zu berechnen oder eine verschlüsselte E-Mail zu entschlüsseln.

Darüber hinaus kann man die GPG-Schlüssel verwenden, um eine E-Mail digital zu signieren. Auf diese Weise kann man die Authentizität und die Integrität einer E-Mail überprüfen. Hierfür wird mit einer sogenannten Hashfunktion eine Prüfsumme über den Inhalt der E-Mail gebildet und diese mit dem *private key* verschlüsselt. Der Empfänger, der im Besitz des öffentlichen Schlüssels ist, kann die verschlüsselte Prüfsumme entschlüsseln. Hierdurch wird Ihre Identität verifiziert, da nur Sie – im Besitz des privaten Schlüssels – in der Lage waren, die Prüfsumme mit diesem Schlüssel zu verschlüsseln. Außerdem kann der Empfänger nun ebenfalls die Prüfsumme über den Inhalt der E-Mail generieren und mit der von Ihnen verschlüsselten Prüfsumme vergleichen. Auf diese Weise wird überprüft, dass der Inhalt der E-Mail nicht manipuliert worden ist.

Um die Herkunft eines öffentlichen Schlüssels überprüfen zu können, bedient man sich eines sogenannten *fingerprint* (Fingerabdruck). Dies ist ein Hashwert über den öffentlichen Schlüssel. Dieser *fingerprint* ist deutlich kürzer als der Schlüssel selbst und lässt sich daher leicht z. B. telefonisch mitteilen und abgleichen. Eine Alternative sind die sogenannten *Zertifikate*, in denen eine vertrauenswürdige Instanz die Verbindung von öffentlichem Schlüssel zum Schlüsselinhaber bestätigt.

Für die sichere Kommunikation ist damit der öffentliche Schlüssel des jeweiligen Empfängers notwendig. Der Austausch der öffentlichen Schlüssel lässt sich auf ver-

schiedene Weise realisieren. So kann dies z.B. über E-Mails erfolgen oder über persönlichen Austausch auf einem Datenträger – beispielsweise einem USB-Stick. Außerdem gibt es sogenannte Schlüsselservers, die die Möglichkeit bieten, seinen eigenen öffentlichen Schlüssel abzulegen, so dass jeder auf diesen Zugriff hat.

---

### **Kurze Übersicht**

Zum Verschlüsseln einer E-Mail verwenden Sie den öffentlichen Schlüssel Ihres Kommunikationspartners. Ausschließlich dieser ist in der Lage, die Nachricht zu entschlüsseln. Auf diese Weise ist eine vertrauliche Kommunikation möglich.

Zum Signieren von E-Mails verwenden Sie Ihren eigenen privaten Schlüssel. Ihr Kommunikationspartner, der im Besitz Ihres öffentlichen Schlüssels ist, kann die Integrität und die Authentizität der E-Mail überprüfen.

Grundsätzlich ist dabei wichtig, dass Sie sicherstellen, dass der Schlüssel tatsächlich zum behaupteten Kommunikationspartner gehört: Die Authentizität stellen Sie beispielsweise dadurch fest, dass der Schlüssel durch einen anderen Schlüssel, dem Sie vertrauen, signiert wurde, oder dass Sie mit Ihrem Kommunikationspartner den *fingerprint* telefonisch abgleichen.