

Leitfaden zur eBrief-Verschlüsselung mit GnuPG

Von der

**HEIMATTREUEN BEWEGUNG VORDERPFALZ /
AKTIONSGRUPPE DATENSCHUTZ RHEIN-NECKAR**

Inhaltsverzeichnis

1. Tragweite der sicheren Kommunikation?	3
2. Was ist PGP/GnuPG/OpenPGP?.....	4
3. Was kann GnuPG?.....	4
4. Allgemeines	6
5. Installation und Vorbereitung.....	7
6. Schlüsselverwaltung	10
6.1. Eigenen öffentlichen Schlüssel versenden	10
6.2. Fremden öffentlichen Schlüssel importieren	11
7. Datenversand	13
7.1. Dateien verschlüsseln und versenden.....	13
7.2. Dateien entschlüsseln	15
8. Nachwort & Kontakt	17
9. Empfehlung.....	19

1. Tragweite der sicheren Kommunikation?

Wie wichtig eine abhörsichere Kommunikation ist, kann am Beispiel der ENIGMA demonstriert werden: (http://de.wikipedia.org/wiki/Enigma_%28Maschine%29). Welche geschichtlichen Konsequenzen es haben kann, wenn der Feind die Nachrichten entschlüsseln und in Klartext lesen kann, verdeutlicht der Absatz "Geschichtliche Konsequenzen" desselben Artikels. Die übliche Übermittlung eines eBrief geschieht unverschlüsselt und kann von jedermann gelesen oder verändert werden. Die Übermittlung der Nachricht geschieht ähnlich einer Postkarte im wirklichen Leben. Das Geschriebene wird auf einem Stück Papier ohne Umschlag weitergereicht und kann folglich von jedem, der die Postkarte in die Hand nimmt, gelesen oder auch verändert werden. Die Übermittlung der Nachricht per Rechner geschieht auf eine ähnliche Weise, die Nachricht wird einfach in Klartext von Server (Rechner im Weltnetz) zu Server weitergegeben, bis sie den Empfänger erreicht hat.

Um einen eBrief sicher - ohne daß jemand mitlesen kann - zu übermitteln, muß somit die Nachricht verschlüsselt werden. Die Verschlüsselung ist also der Umschlag für die Postkarte. Auch die Anhänge an der eBrief können auf die Weise verschlüsselt übertragen werden.

Es gibt seit längerem für die sichere Kommunikation über die eBrief ausgereifte Verfahren und benutzerfreundliche Programme. Als abhörsicherer Standard hat sich GnuPG durchgesetzt (<http://de.wikipedia.org/wiki/GnuPG>). Das Programm ist für alle Betriebssysteme verfügbar und der Programmtext liegt offen vor, was heißt, daß keine Hintertürchen oder allgemeingültige Schlüssel eingebaut sind. Somit entspricht das Programm dem Grundsatz jeder Verschlüsselung, wonach "die Sicherheit eines Kryptosystems nicht von der Geheimhaltung des Algorithmus abhängen darf. Die Sicherheit darf sich nur auf die Geheimhaltung des Schlüssels gründen."

2. Was ist PGP/GnuPG/OpenPGP?

PGP (Pretty Good Privacy) wurde von Phil Zimmermann entwickelt um allen Personen die Möglichkeit zu geben, ihre Privatsphäre zu schützen. Die im Folgenden verwendete Open-Source Version des Programms wurde unter dem Namen GnuPG von Werner Koch entwickelt. Um die Interoperabilität zu gewährleisten wurde das von PGP verwendete Dateiformat festgehalten und Erweiterungen definiert. Dieses Format nennt sich OpenPGP und wird von PGP und GnuPG größtenteils eingehalten. PGP und GnuPG ist für viele Plattformen verfügbar, wie z.B. DOS, Windows, Macintosh oder Unix.

Das Verfahren von PGP und GnuPG beruht auf einem Public Krypto Keysystem. Die Ver-/Entschlüsselung wird mit Hilfe der zwei Schlüssel realisiert: öffentlichem und geheimen. Diese beiden Schlüssel zusammen bilden ein Schlüsselpaar. Mit dem öffentlichen Schlüssel kann die Nachricht an den Besitzer des geheimen Schlüssels nur verschlüsselt werden. Entschlüsselt werden kann diese Nachricht nur mit dem geheimen Schlüssel. Der öffentliche Schlüssel kann nach Belieben und frei verteilt werden. Der geheime Schlüssel muß dagegen auf das Sorgfältigste aufbewahrt werden.

3. Was kann GnuPG?

GnuPG ist ein Programm, das primär der Verschlüsselung des Klartexts von eBriefen, Instant Messaging Chats und Kurznachrichten in Ciphertexte dient, so dass nur Sender und Empfänger einer Nachricht, die im Besitz der passenden Schlüssel sind, den Ciphertext wieder in lesbaren Klartext entschlüsseln können. Neben der Nachrichtenverschlüsselung wird GnuPG auch zur Verschlüsselung von Dateien verwendet, die zum Beispiel lokal auf der eigenen Festplatte gespeichert sind.

Darüber hinaus kann man mit GnuPG Klartexte, Dateien oder Programme mit einer digitalen Signatur versehen, um auch im elektronischen Bereich, in dem eine handschriftliche Unterschrift nicht möglich ist, die Überprüfung der Authentizität elektronisch vorliegender Texte und Daten zu ermöglichen.

Sowohl zur Verschlüsselung als auch zur Signierung setzt GnuPG mathematische Verschlüsselungsfunktionen ein - kryptografische Algorithmen, die in der Welt der Kryptografie als anerkannt sicher vor Entschlüsselung, bzw. Errechnen der originalen Daten (z. B. des Klartexts einer EMail) aus der verschlüsselten Form durch nicht autorisierte, dritte Parteien eingestuft werden.

Ein kurzer Blick auf die Struktur und Funktionsweise des Weltnetzes reicht aus, um sich die Notwendigkeit der Verschlüsselung und Signierung vor Augen zu führen.

Beispiel eMail Überwachung

Wenn ein eMail versendet wird, werden die Datenpakete des eMail zum Mailserver des Providers übertragen, von dort versendet der Mailserver den eMail an den Ziel-Mailserver des Empfängers. Dabei wird der eMail meistens mehrere Rechner im Internet passieren, bis dieser am Zielsystem ankommt. Der Mailserver des Empfängers überträgt schließlich den eMail auf den Rechner des Empfängers. Während des ganzen Transportweges werden die Datenpakete stets in lesbarem Klartext übertragen.

D. h. an verschiedenen Stationen des Weges kann der eMail abgefangen und auch verändert werden: Auf dem Weg vom eigenen Rechner zum Mailserver, zwischen den einzelnen Rechnern während des Transportes und vom Ziel-Mailserver zum Empfänger. Verschafft sich eine Person einen illegalen Zugang zu einem der beteiligten Rechner, kann auch dort direkt der eMail abgefangen werden. Zu diesem Zweck gibt es spezielle Programme wie die Paket-Sniffer, mit denen Datenpakete abgefangen werden können. Die abgefangenen Pakete können auch in ihrem Inhalt verändert und wieder in den Datenstrom eingespeist werden.

Zusätzlich können Geheimdienste und Polizeibehörden aufgrund gesetzlicher Befugnisse und mit richterlicher Erlaubnis eMails von dem Provider, der den Mailaccount zur Verfügung stellt, zu Überwachungszwecken anfordern.

4. Allgemeines

Im Folgenden möchten wir euch nur die wesentlichen Funktionen von GnuPG erläutern, ohne dabei aus unserer Sicht unwichtige Funktionen und Anwendungen näher zu beleuchten. Wir nutzen in unserem Leitfaden nie die Funktion der Zwischenablage, sondern vielmehr den Dateimanager. Wir werden auch nicht auf die technischen Hintergründe verschiedener Anwendungen eingehen, sondern nur kurz und knapp euch den Umgang bzw. die Nutzung mit GnuPG zum sicheren Datenverkehr unter Kommunikationspartnern aufzeigen.

Für uns als nationale Sozialisten, die unter permanenter staatlicher Beobachtung stehen, ist es von enormer Bedeutung, einen verhältnismäßig sicheren E-Post-Verkehr gewährleisten zu können. Auch linke Kreise bedienen sich dieser Verschlüsselung und der BRD-Apparat hat große Schwierigkeiten diese Verschlüsselung zu knacken und somit Informationen über die politische Opposition zu sammeln. Die 100%ige Sicherheit im Weltnetz bzw. dem elektronischen Datenverkehr kann und wird es nie geben. Man muß leider immer von der Möglichkeit ausgehen, dass der Feind mit liest. Machen wir es ihm aber möglichst schwer... und nutzen daher GnuPG!

5. Installation und Vorbereitung

Eine Bemerkung vorweg: Das hier behandelte Verschlüsselungstool heißt GnuPG (Gnu Privacy Guard). Die dazugehörige graphische Benutzeroberfläche nennt sich WinPT (Windows Privacy Tools). Im Folgenden wird der Einfachheit halber immer von GnuPG gesprochen.

Die von uns verwendete Version 1.3.1 (GnuPG 1.4.9 + WinPT 1.3.0) könnt ihr unter <http://www.infoportal24.org/sicherheit.php> runterladen.

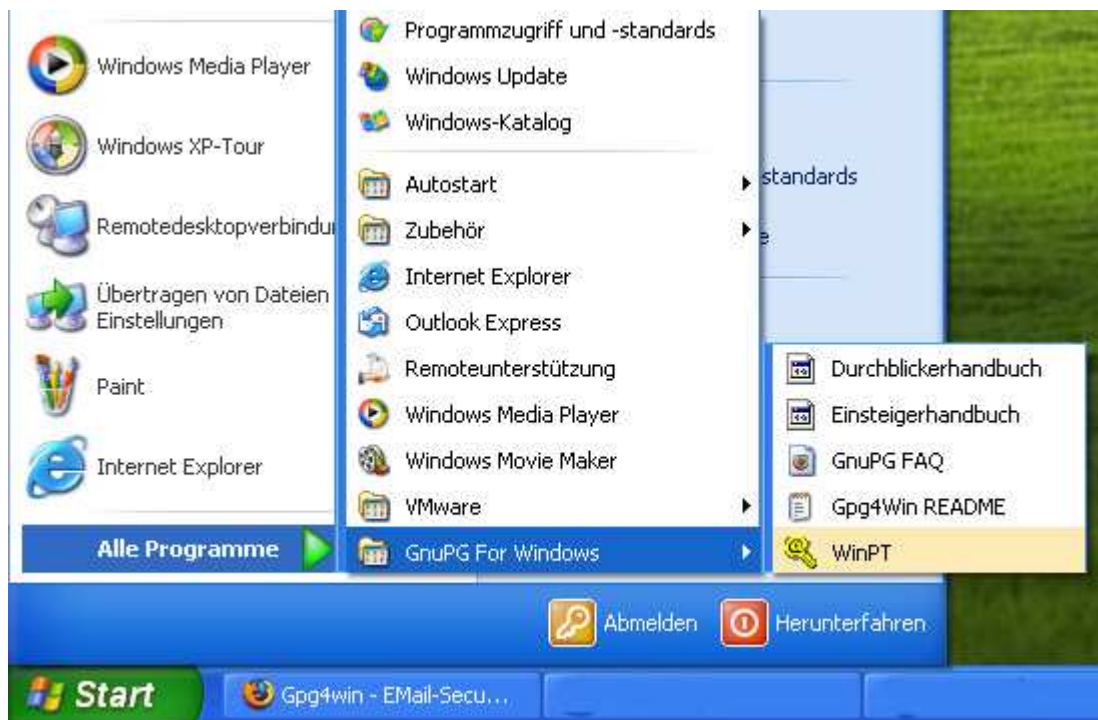
Starte zur Installation die Datei gnupt_3.6.2. Wähle zwischen den Sprachen Deutsch oder Englisch. Akzeptiere die Nutzungsbedingungen und wähle dein Zielverzeichnis, in das du GnuPG installieren möchtest, aus.

Als nächstes müßt ihr das Zielverzeichnis für deine Schlüsselringe wählen. Dieses sollte aus Sicherheitsgründen nicht in das Verzeichnis gelegt werden, in dem auch GnuPG installiert wurde. In diesem Ordner werden dann zukünftig dein noch zu erstellendes Schlüsselpaar und die öffentlichen Schlüssel deiner Kommunikationspartner abgelegt sein.

Wähle die vollständige Installation aus. Setze Hacken bei allen zusätzlichen „Aufgaben auswählen“. GnuPG wird dann zukünftig automatisch beim Start deines Rechners in der Task-Leiste angezeigt.

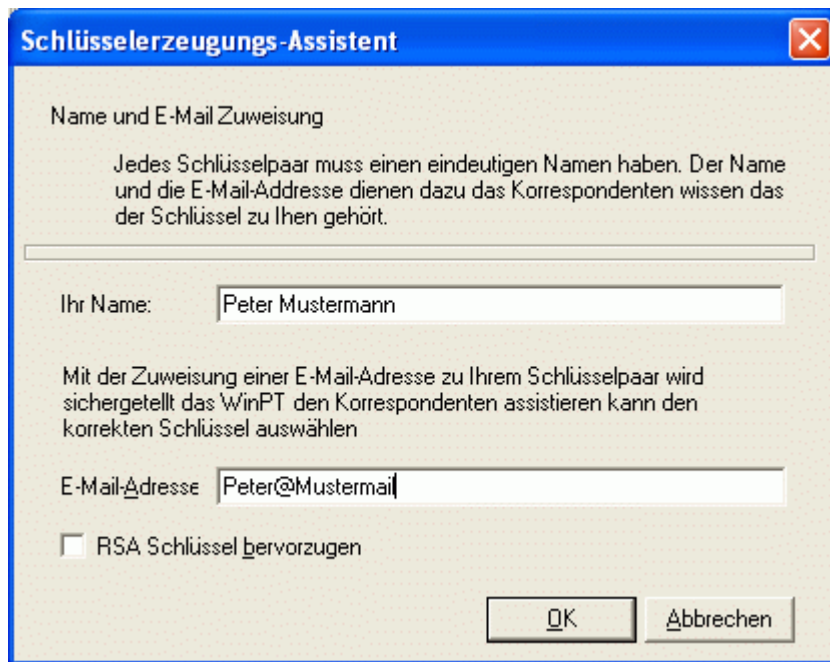
Starte nun die Installation.

Nach Ende der Installation müßt ihr das Tray-Programm manuell starten. Rufe dazu im Startmenü die Datei Windows Privacy Tray auf.



Bevor man mit GnuPG eBriefe ver- und entschlüsseln kann, muss man sich ein Schlüsselpaar generieren. Dieses besteht aus einem sog. öffentlichen und einem privaten Schlüssel. Verschlüsselt wird immer mit dem öffentlichen Schlüssel des Empfängers, den der Empfänger zum Beispiel per eBrief zugesandt hat und der sich nach dem Import jetzt im eigenen Schlüsselring befindet. Der Empfänger benutzt zum entschlüsseln des eBriefes seinen privaten Schlüssel.

Da ihr noch kein Schlüsselpaar besitzt, fragt GnuPG, ob der Schlüsselerzeugungs-Dialog gestartet werden soll. Füllt nach einem Klick auf „Ja“ die Felder der Eingabemaske entsprechend aus:



Bei „Ihr Name“ solltet ihr den Namen wählen, unter den ihr zukünftig kommunizieren wollt. Gleiches gilt für die E-Brief-Adresse. Nach Abschluss der Schlüsselgenerierung bietet das Programm an, Sicherungen der gerade erzeugten Schlüssel zu erstellen. Folgt den Anweisungen und speichert sowohl den öffentlichen als auch den privaten Schlüssel auf einem Datenstift ab. Danach schließt ihr das Fenster mit Klick auf "Ende".

Zur Verschlüsselung wird ein Verfahren namens RSA (<http://de.wikipedia.org/wiki/RSA-Kryptosystem>) verwendet, mit einer Schlüssellänge von bis zu 4096 Bit. Schlüssel in dieser Länge sind aufgrund der hieraus entstehenden Kombinationsmöglichkeiten und dem daraus resultierenden technischen Aufwand für die Entschlüsselung nicht in annehmbarer Zeit zu knacken. Ein Versuch, einen 640 Bit- (etwa 72 Bit symmetrisch) langen Schlüssel zu knacken, dauerte mit 80 Rechnern à 2,2 GHz rund 10 Monate. Der 4096 Bit- (etwa 200 Bit symmetrisch) Schlüssel hat $3,4^{38}$ (also 34 mit 37 Nullen dahinter) mehr Variationen. Die Entschlüsselungszeit wird um denselben Faktor länger. Somit ist die Verschlüsselung an sich sehr sicher und wird in den nächsten Jahrzehnten auch sicher bleiben. Vorausgesetzt natürlich, daß der geheime Schlüssel zum Entschlüsseln nicht entwendet wird. Der ist allerdings mit einem Paßwort geschützt, welches verständlicherweise gut gewählt sein sollte. Setzt euer Passwort aus Buchstaben, Sonderzeichen und Zahlen zusammen und verwendet mindestens Acht Stellen.

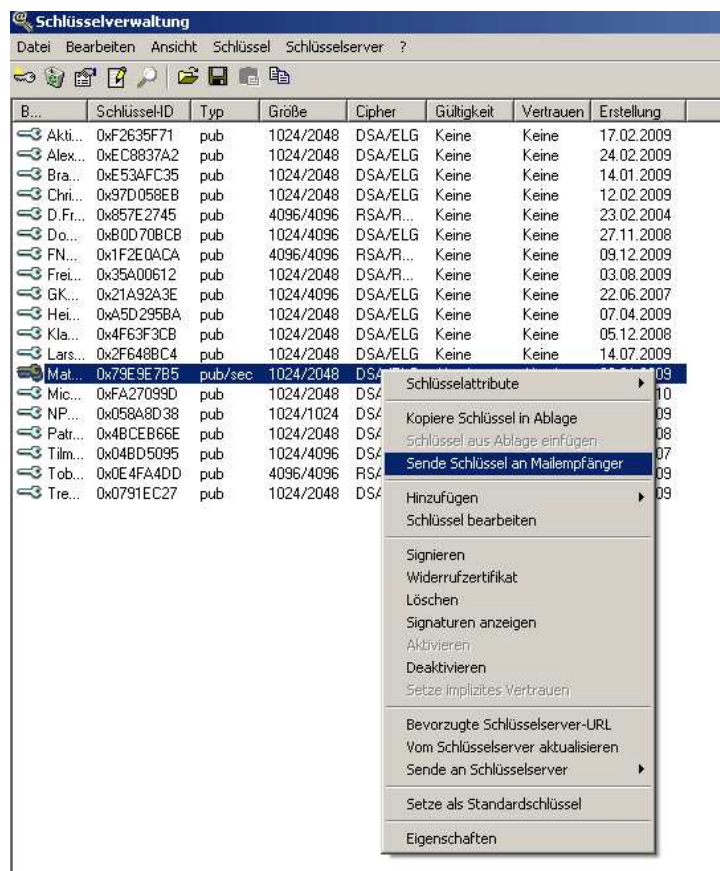
6. Schlüsselverwaltung

6.1. Eigenen öffentlichen Schlüssel versenden

Die Schlüsselverwaltung von GnuPG erreicht ihr fortan über ein kleines Symbol im Systray:



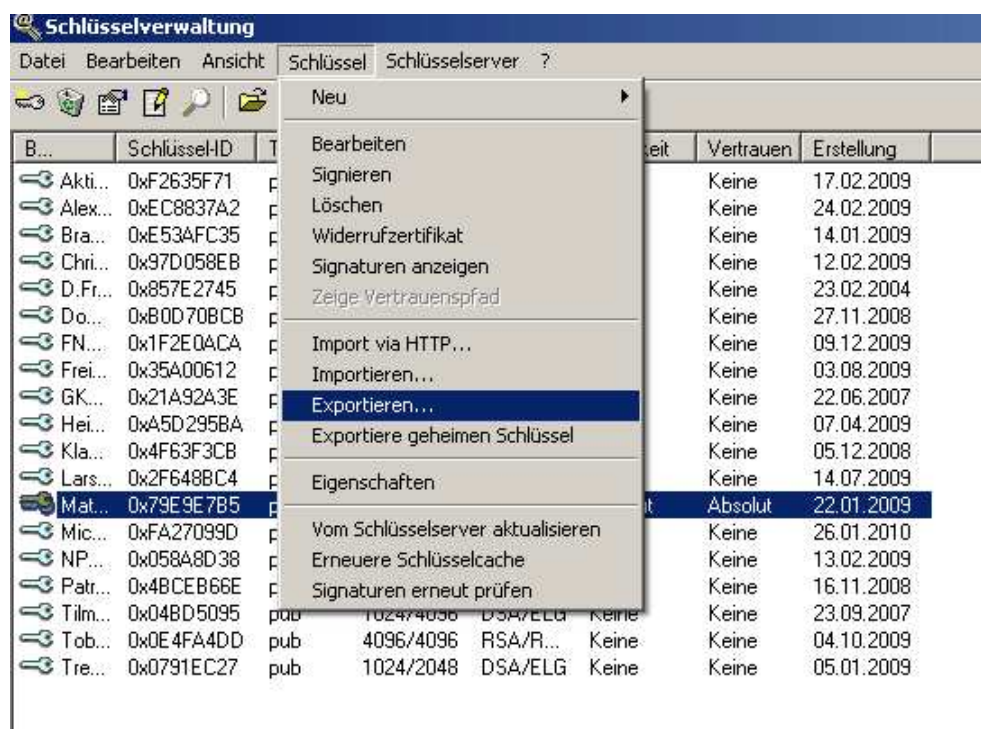
Startet die die Schlüsselverwaltung entweder durch Doppelklick auf das Schlüssel-Icon oder wählt nach einem Rechtsklick den entsprechenden Menüpunkt aus.



Wähle dein eigenes Schlüsselpaar aus (gekennzeichnet durch Typ pub/sec) und drücke rechte Maustaste und wähle anschließend „Sende Schlüssel an Mail-Empfänger“.

Dein öffentlicher Schlüssel wurde nun automatisch an einen eBrief (z.B. im Microsoft Outlook) angehängt.

Wenn das nicht gehen sollte: Eigenen Schlüssel anklicken, im Menu „ Schlüssel“ auswählen und „Exportieren...“ wählen. Anschließend den eigenen öffentlichen Schlüssel abspeichern und als Dateianhang an den Kommunikationspartner versenden.



Dein Kommunikationspartner wird dann zukünftig Nachrichten an dich mit deinen eigenen öffentlichen Schlüssel verschlüsseln.

6.2. Fremden öffentlichen Schlüssel importieren

Startet die die Schlüsselverwaltung entweder durch Doppelklick auf das Schlüssel-Icon oder wählt nach einem Rechtsklick den entsprechenden Menüpunkt auf.

Hier könnt ihr sehen, mit wem ihr Schlüssel ausgetauscht habt, ob diese noch gültig sind und bekommt einen Überblick über Stärke und Typ der Schlüssel. Im Moment sieht das Ganze noch etwas trostlos aus. Ihr habt nur einen einzigen Schlüssel: Euren eigenen.

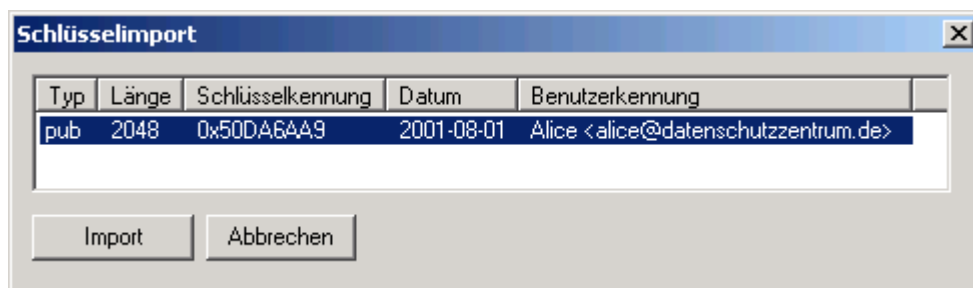
Um mit einem Partner verschlüsselte eBriefe auszutauschen, benötigt ihr dessen öffentlichen Schlüssel. Den bekommt ihr normalerweise direkt von ihm per eBrief oder auf einen Datenstift oder von einem Schlüsselserver. Dabei handelt es sich um Rechner im Weltnetz, an die jeder seinen öffentlichen Schlüssel schicken kann. Von dort kann sich dann ein Kommunikationspartner den Schlüssel herunterladen, auch wenn der Besitzer gerade im Urlaub ist.

Normalerweise erhält man einen öffentlichen Schlüssel per eBrief mit einem Dateianhang (Format asc). Dieser Dateianhang ist der öffentliche Schlüssel des Kommunikationspartners und dieser öffentliche Schlüssel muß in die eigene Schlüsselverwaltung importiert werden. Zukünftig werden wir nun alle Nachrichten an diesen Kommunikationspartner mit seinem öffentlichen Schlüssel verschlüsseln. Dieser kann dann nach Erhalt der verschlüsselten Nachrichten mit seinem dazugehörigen privaten Schlüssel die an ihn mit seinem öffentlichen Schlüssel verschlüsselten Nachrichten entschlüsseln. Man verwendet also immer das eigene Schlüsselpaar, bestehend aus öffentlichen und privaten Schlüssel, zur sicheren Verschlüsselung.

Zuerst speichert man den erhaltenen öffentlichen Schlüssel in dem bei der Installation gewählten Ordner für die Schlüsselpaare (siehe Kapitel 4) ab.

Nun öffnet man die Schlüsselverwaltung. Man Startet entweder die Schlüsselverwaltung durch Doppelklick auf das Schlüssel-Icon oder wählt nach einem Rechtsklick den entsprechenden Menüpunkt aus.

Nun öffnet man den Menüpunkt „Schlüssel“, „Importieren...“ und fügt den erhaltenen Schlüssel hinzu.



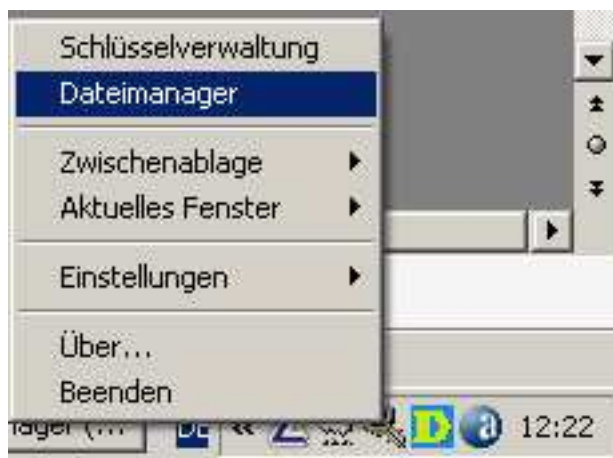
Mit einem Klick auf „Importieren“ wird der Vorgang abgeschlossen. Ihr habt somit den öffentlichen Schlüssel des Kommunikationspartners in eurem Schlüsselbund aufgenommen.

7. Datenversand

7.1. Dateien verschlüsseln und versenden

Man schreibt die Nachricht, welche man an den Kommunikationspartner versenden möchte, entweder in einem Word-Dokument oder in einem reinen Textdokument. Man speichert diese ab und schließt die Datei.

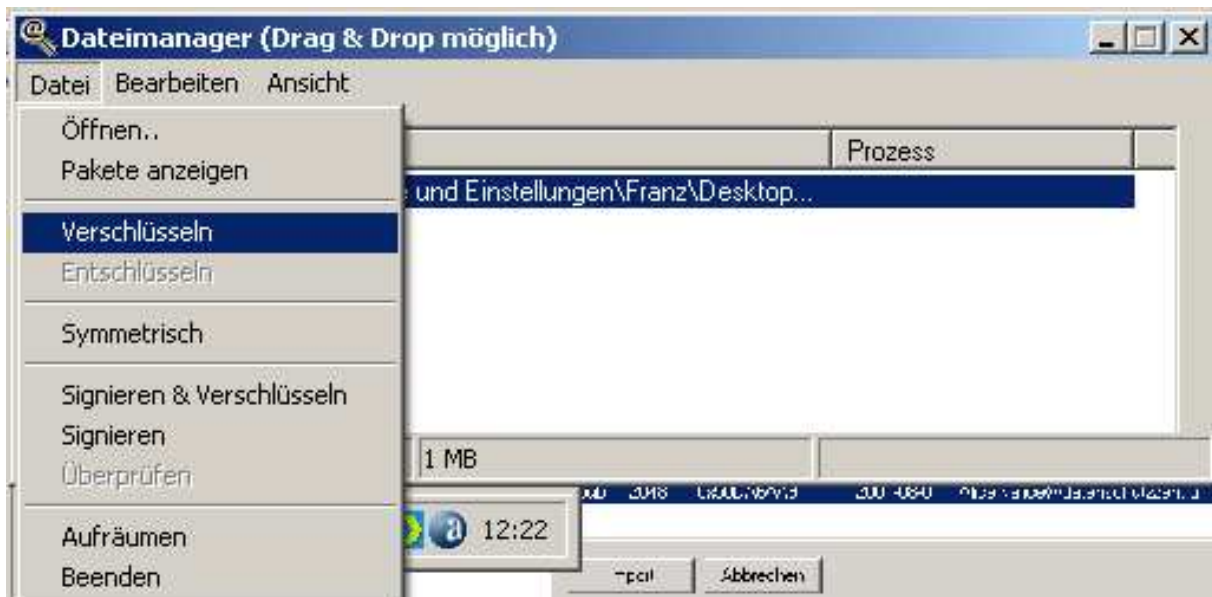
Nun öffnet man den Dateimanager



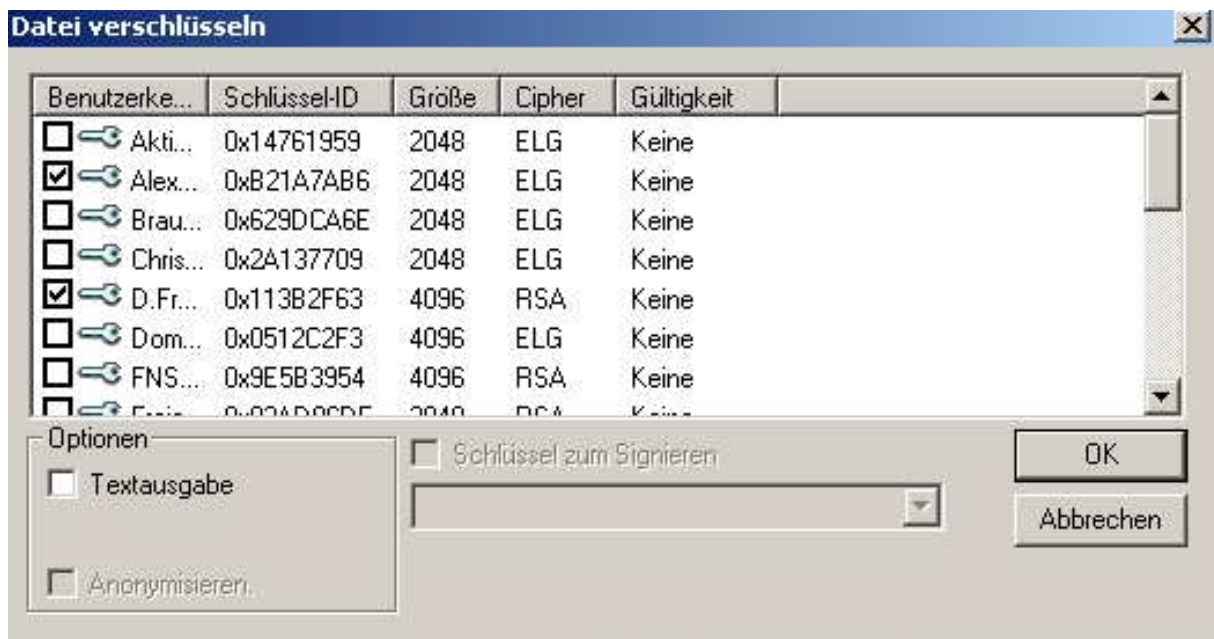
und schiebt (per Drag and Drop) die eben abgespeicherte Datei in den Dateimanager hinein.



Dann die Datei anwählen und über den Menüpunkt „Datei“, „Verschlüsseln“ verschlüsseln.



Nun wird man gefragt, an wen man alles diese Nachricht versenden möchte. Setze entsprechend deinen gewünschten Kommunikationspartnern den Hacken. Drücke anschließend „OK“ und beantworte die folgenden Fragen mit „Nein“.



Hierbei können mehrere Kommunikationspartner ausgewählt werden. All diese können dann in Verbindung mit ihrem eigenen privaten Schlüssel deine mit ihren öffentlichen Schlüssel verschlüsselte Nachricht öffnen.

Die verschlüsselte Datei wird unter dem gleichen Verzeichnis abgespeichert aus der man auch die zu verschlüsselte Datei gewählt hatte.

Mit dieser Vorgehensweise lassen sich sämtliche Datei-Formate verschlüsseln.

Anschließend noch die verschlüsselte Datei an den eBrief anhängen und an die ausgewählten Kommunikationspartner versenden.

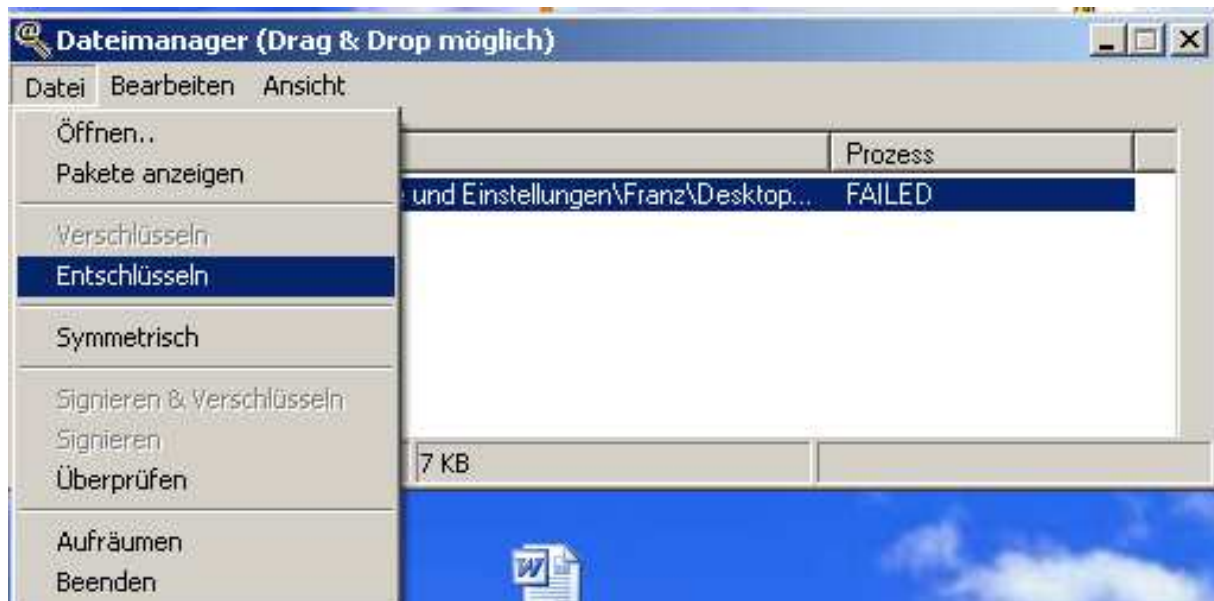
7.2. Dateien entschlüsseln

Den Anhang (verschlüsselte Datei) des erhaltenen eBriefes des Kommunikationspartners in einem Verzeichnis ablegen. Mit einem Doppelklick auf die verschlüsselte Datei öffnet sich ein Fenster.



Sein eigenes Passwort eingeben und Datei wird entschlüsselt im gleichen Verzeichnis wie die verschlüsselte Datei abgelegt.

Sollte dies nicht funktionieren: Einfach die verschlüsselte Datei (per Drag & Drop) in den Dateimanager schieben und dort entschlüsseln.



Eigenes Passwort eingeben und die Datei wird entschlüsselt im gleichen Verzeichnis wie die verschlüsselte Datei abgelegt.



8. Nachwort & Kontakt

Unser Projekt lebt von der steten Weiterentwicklung. Die Anwendungsentwicklung ist schnelllebigere denn je, deshalb ist es kaum verwunderlich, wenn eine jetzt noch gültige und funktionierende Anleitung morgen schon unbrauchbar ist, weil eine neue Version des Programms erschienen ist. Wir selbst werden in Zukunft zwar stets daran arbeiten, euch einen aktuellen Leitfaden anzubieten, jedoch dürft ihr uns ebenso gerne kontaktieren, wenn ihr merkt, daß etwas nicht mehr stimmt.

Genauso nehmen wir natürlich gerne auch Anregungen von Kameraden an, welche sich selbst mit der Materie Datenschutz bzw. Kryptografie usw. auskennen. Ziel ist es, für den Laien brauchbare Ratschläge und Anleitungen zu veröffentlichen, welche jeder Besitzer eines Rechners in die Tat umsetzen kann.

Habt ihr Fragen, Anregungen, Vorschläge oder Kritik? Dann meldet euch bei uns über Jabber oder per eBrief:

datenschutz@jabber.ru

datenschutz@pochta.ru

Unser PGP-Schlüssel für eBriefe lautet:

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

Version: GnuPG v1.4.9 (MingW32)

Comment: GnuPT v3.6.2

```
mQGIBekHTF4RBACsmIofzkFfPquOZoPLklYecT2arnB74xthrm6yF0lf4DpUYo1P
rSxkvWeNDmMaC2ea5vv2pH8jl+UkXsZ/JPJzoe+vus8B7DDIUT3np3RYIYK42mqj
CjsnELVwk/V2+2bT7CL9Q62pRXP5RbVfTvIEAMBI7YmMw75afPzSIwU1wwCg+v+D
98jw/TQEz5QNGkN4leasY5kD/RuBPP4BuwRBVBbC5NfinvCy9uvQ3Qqvo/75fpm
CQ6Qm2Eum3dekjnU2sDMYQktqIkYoBmkZj5iq9LOXLMEUDHwXJsIKPdnhV+kH2d+
uJfNHZvUsBVEGmwyOOfmoBthKJKIK7ILSaLyiBikfR84pMUs3zM6CsdoP+f21Ej
9114A/0UHMJ96CqUFgx92nf4+kfe9pGrcHsE5uvQbswtQTUCDrBCpTPKbVKbpWtf
hs9jAwiP+sEsBQLW/JxV5O2T/TcjXmH3vZXHRpomFU6bjxZn7QWwzTVrFYcjegVd
crTzhygsIIgYrhjCrwXAGm50sq+ZfTAxwZ3BhrYHsTE+DfOSnLQxQWt0aW9uc2dy
dXBwZSBEYXRlbnNjaHV0eiA8ZGF0ZW5zY2h1dHpAcG9jaHRhLnJlPohgBBMRAgAg
BQJJB0xeAhsDBgsJCAcDAGQVAaggDBBYCAwECHgECF4AACgkQ8Z5HGGvUcc6pHQCg
4g2qfF9Ixfoh/gfyJAu02Mzwh1sAoJoYQe6lbenY2nSpqtZb3C9qbfCduQINBEkH
TF4QCACAzBssBZIGNuZpdnJP4Wg0Hn20v9HB4ShB84bES7bkhSwoVR1kGD6uzzLS
ehZNA4o9kG9eiDNbJ64roAiz8zgH0gbSvfT22naawaUEDw1BFmIEqa1N2ph8080A
PgAeAOjHdoo3dkJdv6snFbS3cDbutB8LwP+wgxdgu3V1ftqMnkGoR7A7IvH8H25Y
7wi304I3ETDjDx++LjoP67D8btxEUgFzSZoPxGWD1I5wbDS2Bmh7pE2uJIDbZN5p
W3Z5Sa+2RRwwQi4Yb5mbwAkdhYy0QRfqQlm+yglmMlnMNAVPIsoFEmsp2gd0GsGX
38EWJU2mcPpFTOXczAm6ZlcnJjpvAAMFB/4/2SF5HDU9hGEK+xTQO3T7vG5BZNI0
/CGUqXxlCTKC8HBkKyjTO2P/nShwAWyZd2I888POidfwe3CCOixgH/eN+e047w2
L4NwwMuNNxSsSndk6K9YNJ2IgbLU51JbnWSpHTmS3zl0dY6yIbyIgzfPukcnisvv
WBBu05ajhZB9r3j+LGD3c7hTpkTo3EVzaW2sqAVMevd1a0r6K71npHTZPcpw1ivs
oX1sIXvBvWa0f1Nk6SW8B3CE4qHvH4k7sxSFQqxpWZ5xAvxcexKlfNhb3kiZAQo
0I4RP9OjQoHia+CnC4QwfrTKrov6/tKe2sQEehfHwNjqlRj+b3JIET7wiEkEGBEC
AAkFAkkHTF4CGwwACgkQ8Z5HGGvUcc4XsgCff+dVVB83O0NTxiQ8XKR/4ieHBuUA
oMHpb7JI8X8+mAurgdevL1U9YsAJ
=S4Hq
```

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

9. Empfehlung

Leitfaden für Sicherheit & Schutz der digitalen Identität



Zum Runterladen unter: <http://www.infoportal24.org/sicherheit.php>