PGP / GPG

Email Verschlüsselung – Workshop

Von Nico Wehnemann • Attac WebTeam

Donnerstag, 15. Juni 2006

Vorwort

Anlässlich der Repressionen gegen Linke Projekte, ja sogar gegen „normale“ Reformistische Aktivitäten wie der aktuelle Fall der Überwachung von Prof. Peter Grottian in Berlin zeigt (der das Sozialforum in Berlin gegründet hatte und seit dem vom Verfassungsschutz überwacht wurde) rückt das Thema Email-Verschlüsselung und Sicherheit im Internet wieder ins Blickfeld der sozialen Bewegungen.

Wir stehen kurz vor den Protesten gegen das Treffen der G8 (http://www.attac.de/heiligendamm). Bei der Vorbereitungen eines solchen Events, bei Aktionen des zivielen Ungehorsams, ja selbst in der alltäglichen politischen Arbeit ist es wichtig seine Nachrichten und Vorberitungen geheim zu halten.

Wie fatal es ist von der Polizei abgehört zu werden zeigen einige Aktionen aus dem Streik der Berliner Studierenden im Winter 2003/2004. Viele Maillinglisten, viele Emailkonten und Telefonanschlüsse wurden überwacht und so letztlich einige gut vorbereitete Aktionen vereitelt.

Dabei ist die Lösung so einfach, sie ist kostenlos und einfach zu handhaben. Das Stichwort heit PGP oder GPG (GnuPG). Mit dieser Software ist es jedem Leihen möglich im Handumdrehen seine Daten vor den Zugriffen fremder zu schützen, und per Email sicher zu kommunizieren.
Das alles doch so einfach ist, wenn Mensch einige wenige Dinge beachtet, möchte ich in diesem Workshop zeigen.

Der Workshop bietet einen Einstieg in das Verschlüsseln von Mails. Er ist kein Workshop für Krypographie. In die Technik werde ich nur wenig eingehen.

Was ist PGP/GPG?

Phil Zimmermann schrieb die erste Version 1991. Sein Ziel war es, dass alle Bürger und insbesondere Bürgerbewegungen auch vor dem Zugriff durch Geheimdienste sicher verschlüsselte Nachrichten austauschen können (starke Verschlüsselung).

PGP durfte in seinen Anfangsjahren nicht lizenzfrei aus den USA exportiert werden, da es, ähnlich wie Waffen, unter das US-Exportgesetz fiel. Danach unterlagen Kryptosysteme mit Schlüsseln von mehr als 40 Bit Länge für die symmetrische Verschlüsselung besonderen Exportbestimmungen. Die ersten PGP-Versionen verwendeten den IDEA mit 128 Bit Schlüssellänge. Ende der 90er Jahre liberalisierten die USA diese Gesetze.

Um die Exportbeschränkung zu umgehen, wurde der vollständige Quellcode 1995 in dem Buch „PGP Source Code and Internals“ von Phil Zimmermann veröffentlicht. Als Buch konnte die Software legal aus den USA exportiert werden. Es wurde von über 60 Freiwilligen per Hand eingescannt. Aus dem gescannten Programmcode wurde dann eine international verfügbare Version von PGP (PGPi) kompiliert.

Die Firma *PGP Corporation* stellte bis Version 8 mit *PGP Freeware* ein eigenständiges Produkt für nicht-kommerzielle Nutzer bereit. Seit Version 9 gibt es stattdessen nur noch die Testversion von *PGP Desktop Professional 9*. Für 30 Tage kann sie uneingeschränkt genutzt werden. Nach Ablauf der Frist werden Funktionsumfang und Nutzungsrechte auf einen Umfang reduziert, der etwa dem ehemaligen *PGP Freeware* entspricht. Ver- und Entschlüsselung von E-Mails ist auch nach Ablauf der Testphase möglich, aber nur für nicht-kommerzielle Zwecke zulässig.

Aufgrund der Tatsache, dass der Quelltext von PGP zeitweilig nicht offengelegt wurde und Features implementiert wurden, welche die automatische Verschlüsselung an einen weiteren Empfänger ermöglichten, wurde bis 1998 der OpenPGP-Standard entwickelt. Das unter der GNU-GPL stehende Programm GnuPG war ursprünglich die erste Implementation von OpenPGP und wurde als freie Alternative zu PGP entwickelt. Zu PGP gibt es mittlerweile viele Erweiterungen des OpenPGP-Standard, so dass der reibungslose Austausch von Daten nicht garantiert ist.

GnuPG oder **GPG** (**Gnu P**rivacy **G**uard, englisch für *GNU-Wächter der Privatsphäre*) ist ein freies Kryptographie-System, d.h. es dient zum Ver- und Entschlüsseln von Daten sowie zum Erzeugen und Prüfen elektronischer Signaturen.

Das Programm implementiert den OpenPGP-Standard nach RFC 2440 und wurde als Ersatz für PGP entwickelt.

Versionen ab 1.9 implementieren auch den S/MIME-Standard. GnuPG benutzt nur patentfreie Algorithmen und wird unter der GNU-GPL vertrieben. Es kann unter Linux, Mac OS X und diversen anderen Unix-Varianten sowie unter Microsoft Windows betrieben werden.

Entstanden ist OpenPGP im Jahr 1998 als Reaktion auf diverse Entwicklungen:

- die in PGP verwendeten Algorithmen (IDEA und RSA) waren patentiert und konnten nicht beliebig verwendet werden. Insbesondere gab es in den USA Gesetze, die den Export von starker Veschlüsselung (ab 40 Bit) verboten.
- das Programm PGP wurde kommerziell durch die Firma PGP Inc. vertrieben und es gab (*falsche*) Gerüchte, dass eine Hintertür in dem Programm eingebaut wäre, da es über eine sogenannte ADK-Funktion (Additional Decryption Key) verfügte.
- Ende 1997 wurde PGP Inc. von Network Associates Inc. (NAI) übernommen, die Mitglied der *Key Recovery Alliance* waren.

Das OpenPGP-Protokoll wird mittlerweile von vielen Produkten unterstützt. Prominente Vertreter sind das kommerzielle PGP und das unter der GNU-GPL stehende GnuPG.

Soweit zur Technischen Seite von PGP.

Wie sieht so ein KEY eigentlich aus / Wie sieht eine verschlüsselte Nachricht aus?

"öffentliches Schlüsselsystem" (public key cryptography)

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.7

mQA9Ai2wD2YAAAEBgJ18cV7rMAFv7P3eBd/cZayI8EEO6XGYkhEO9SLJOw+DFyHg
Px5o+IiR2A6Fh+HguQAFEbQZZGVtbyA8ZGVtb0B3ZWxsLnNmLmNhLnVzPokARQIF
EC2wD4yR2A6Fh+HguQEB3xcBfRTi3D/2qdU3TosScYMAHfgfUwCelbb6wikSxoF5
ees9DL9QMzPZXCioh42dEUXP0g==
=sw5W
-----END PGP PUBLIC KEY BLOCK-----
```

Was kommt dann?

GPG verschlüsselt Nachrichten, indem es asymetrische Schlüsselpaare verwendet, die von den GPG Nutzern individuell erstellt wurden. Die so entstehenden Öffentlichen Schlüssel können mit anderen Nutzern über eine Vielzahl von Kanälen ausgetauscht werden, z.B. Internet Keyserver.

Ist PGP überhaupt sicher?

- Hervorragende Kryptoanalytiker und Computerexperten haben vergeblich versucht PGP zu knacken.
- Wer auch immer nachweist, dass er PGP entschlüsselt hat, würde schnell zu Ruhm unter den Kryptographen kommen. Er würde viel Beifall ernten und eine Menge Geld angeboten bekommen.
- Die PGP Programmierer würden es sofort bekanntgeben.

Warum sind 1024 Bit sicher genug?

Natürlich kann sich jeder auch einen 2000er oder 4000er bit Schlüssel erstellen. Ich selbst habe einen mit der Länge von 1024 Bit.
Warum ist das schon ausreichend?
Rein rechnerisch ergibt sich die Wahrscheinlichkeit von xx das 1024 bit geknackt werden.
11 <- 2 bit = 00 01 10 11 (4 Möglichkeiten)
1010101010 (10 bit) = 10.000.000.000 Möglichkeiten
u.s.w.

Wenn alle mitmachen / und nicht so faul wären...

Wenn man alle Emails die man versendet verschlüsselt_ist es für Niemanden mehr möglich herauszufiltern was relevant ist und was nicht.

Der Aufwand so viele verschlüsselte Mails zu entschlüsseln ist um so größer je mehr Mails überhaupt verschlüsselt werden

Mails an Mutti mit Inhalten “wie gehts Pappa und der Katze?” verursachen eine enorme Datenflut die das BKA, oder sonst wer, NIE auswerten kann.

Wie geht’s denn nun?

1. eigenen geheimen Schlüssel erstellen
Der eigene “geheime Schlüssel” ist nur für einen selbst bestimmt

Gib ihn NIE aus der Hand!

Bewahre ihn nur auf deiner Festplatte und vielleicht noch auf einer Diskette auf. (Die allerdings an einem sicheren Ort)

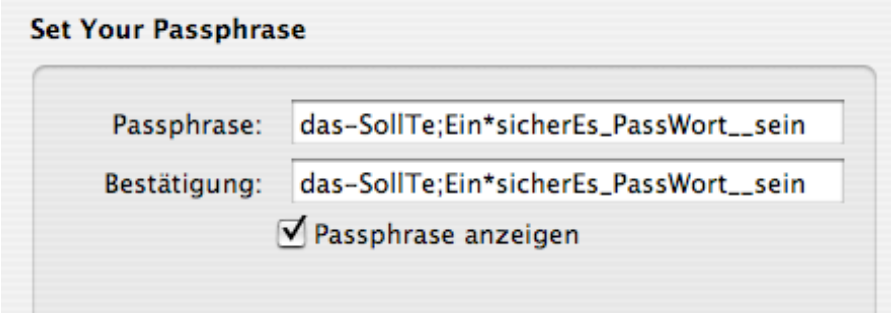
Mit diesem Schlüssel kannst DU DEINE Daten ver- und entschlüsseln.

GPG und auch PGP bieten Grafische Einrichtungsassistenten an. Mit deren Benutzung ist die Einrichtung so einfach wie eine Email zu lesen.

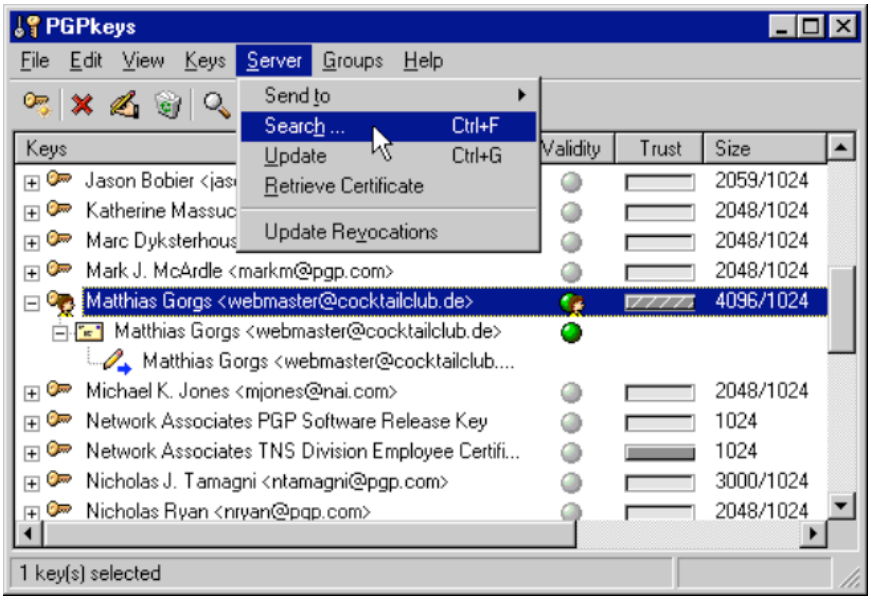
Eine Schrittweise erklärung des Assistenten habe ich unter www.attac.de/service/gruppensupport/ veröffentlicht. Aus Gründen der Papierkosten habe ich in diesem Reader darauf verzichtet.

Das ist beim geheimen Schlüssel wichtig:

- mind. 1024 Bit Verschlüsselung
- sicheres Passwort
- mind. 10 Zeichen
- auch Großbuchstaben verwenden
- KEINE UMLAUTE (gibts nur Deutschland)
- auch Sonderzeichen verwenden (nur Internationale)
- !$%/()=;*_ u.s.w.



Genauso wie es eine Einrichtungssoftware gibt, stellt PGP und auch GPG eine Tools bereit die einem das Leben leichter machen.
Sinnvoll ist die Grafische KeyVerwaltung. Dort können einfach bei Drag and Drop Öffentliche Keys von Freunden verwaltet werden. Dort kann auch ein neuer geheimer Schlüssel erstellt werden.



Ich habe einen Schlüssel – und nun?

Um mit anderen Menschen verschlüsselte Nachrichten auszutauschen, musst Du Ihren Kommunikationspartnern Ihren öffentlichen Schlüssel (public key) geben. Das besagte Leute PGP installiert haben müssen, versteht sich von selbst. Es gibt mehrere Methoden, um den öffentlichen Schlüssel zu verteilen.

In Datei exportieren_In PGPkeys auf |Keys|Export| klicken und den Namen der Datei angeben, in die der öffentliche Schlüssel exportiert werden soll. Am Besten ist es den Schlüssel in eine Ascii Datei zu exportieren, da diese auch von GNU PG gelesen werden kann und Systemunabhängig ist.

In Email einfügen_Den Schlüssel dann einfach als Anhang zum Empfänger senden.

Per Diskette_Noch sicherer ist es wenn der Key Per Diskette verteilt wird.

Auf Keyserver_Kontextmenü 'Send Key to Server', danach einen Server auswählen.

WARNUNG: Ein Schlüssel kann nur dann eindeutig einem Empfänger zugeordnet werden, wenn der Schlüssel von einer vertrauenswürdigen Instanz zertifiziert wurde. Eine andere, allerdings weniger sichere, Möglichkeit ist das Veröffentlichen des sogenannten Fingerprints.

Aber auch Email ist sicher genug, denn es gibt den Fingerprint:

Eine einfache Methode, die Echtheit eines Schlüssels zu prüfen, ist der Vergleich des **Fingerabdrucks**. Dabei handelt es sich um eine Prüfsumme der Schlüsseldaten in Form einer Zahlen-/Buchstabenkolonne (zum Beispiel "72F0 5CA5 0D2B BA4D 8F86 E14C 38AA E0EB"), die sich leicht im direkten Gespräch, per Telefon oder per Brief vergleichen lässt. Diese Prüfsumme steht in der Info zu Deinem Privaten Schlüssel. (Unter PGPKeys einfach auf deinen Schlüssel doppelklicken.)

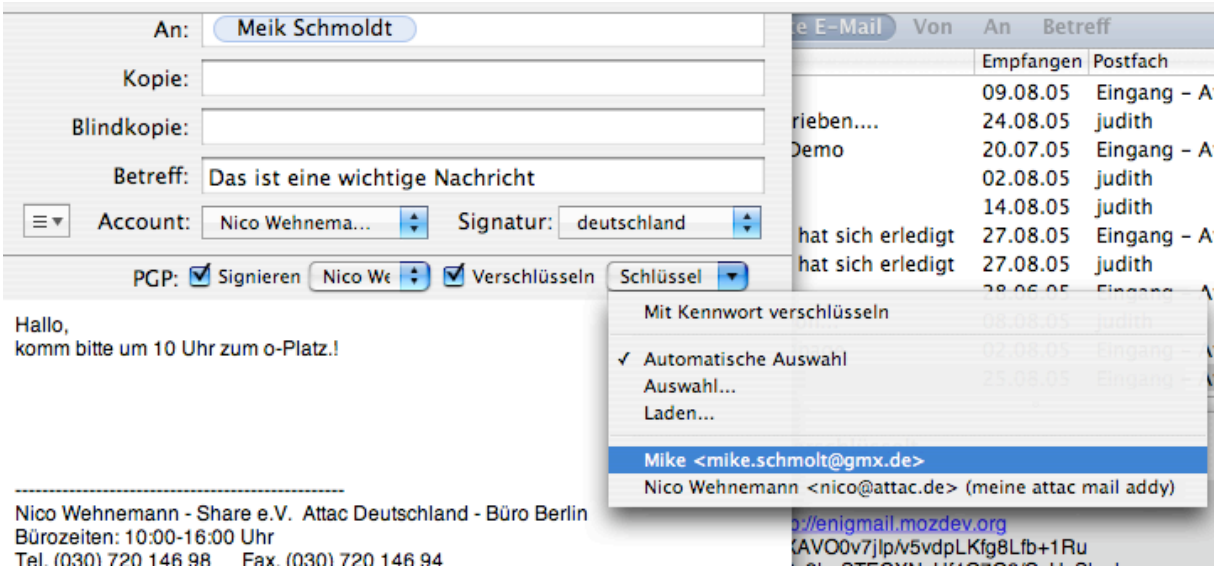
Der Key ist ausgetauscht und was kommt jetzt?

Nun installieren wir uns, wir sind ja doch noch etwas faul, ein passendes Plugin für unser Email Programm. Damit ist dann möglich einfach auf Knopfdruck die Email zu Ver- und Entschlüsseln.

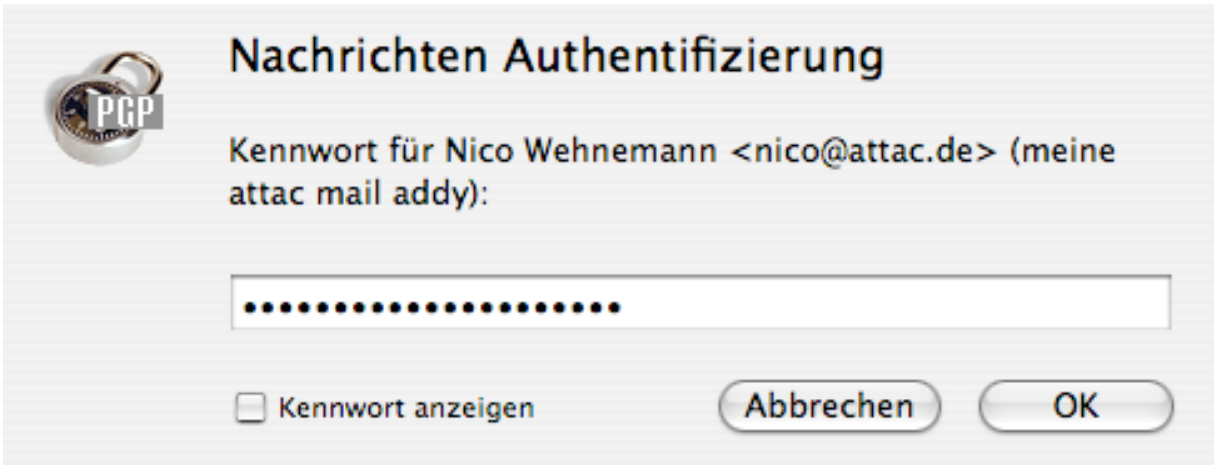
PlugIns gibt es für Bsp. Thunderbird, AppleMail, Endora, TheBAT, Outlook, Outlook Express und viele andere Email Clienten. (Links folgen unten)

Haben wir das hinter uns, haben wir nie mehr Stress. Nun sollte alles von der Hand gehen. Schon nach 2 maliger Benutzung haben wir uns an den Ablauf des Ver- und Entschlüsselns gewöhnt.

Wie verschlüssle ich eine Nachricht?



Erstens – Nachricht schreiben, dann wählen wir Verschlüsseln aus (Häckchen setzen, und noch das Signieren, falls noch nicht ausgewählt.) Neben den Wahlfeldern kann dann der Schlüssel ausgewählt werden mit dem wir verschlüsseln wollen. Normalerweise wird der richtige Schlüssel schon automatisch gewählt.



Dann geben wir einfach unser Passwort ein, dann wird die Nachrichtfür den Empfänger mit seinem Schlüssel und für uns mit unserem verschlüsselt.

Die Nachricht sieht dann so aus und kann versandt werden:


```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.1 (Darwin)

hQEOA56fE4hX2tE/EAQAIjCPHZtqxKkkJezdkIPoc2pmvaoUizWuWi5wjXGlUmV+
r17qmRFa7C4cYqOFYG4IAyx17KvrhtQLExUk3lxVL+G3bzblgRz3wbGmVP6/6Fg1
l69voQ1Svt9m9FQT4QeYAPC/aX4+Mqo8ImFUYfBCagoBmiCCDt/Db5ZlOL69veED
/39b32zVIR+gU9DTmWqqKtYht9ezPQhPOB49DHwNTyhgRbGsdwIv+zNg1qkhBL/v
SdhBl9K2AWXl/9fTq6dmqhvpUNh1loG8VAsdZ2O0+fFZsbSY0zsetMfjqNgtVJBr
QiwuOml3pme8trZ+DEatidhFkCJwYxoUFtz6QJhJLzoNhQlOA87xgebUfCXVEAf/
Utd19wl33gHG4esiJGMmarBSlDpaWXaSmHU7rZnnYxF4B/aViPMWehaUtkAmiv12
HmFlRvkFZ9wHA+epY0MOVlasRJoTsq+ItntZlRwPjao2pfpeWkWGnJFi4uBhG3El
5inh/vMnMBjgB+ZniwM/k+5QUa1hPQB2NWg02Fwg/ePodQ3+WvJ2MuDM6/81UV60
kH6OCVHqvgao4z+eR3DcXV12mk0UgUOSJJKXp+TnDcDlaGMVTo1JpWrz/1/khyZn
oQVGj4jrGPU7gpA4UHYKx4x2/KoPsp5eV6bAR0M9KA2UDwPIDLJkcc8qWZ4ySIlv
oB9aNLdVQ4EEl3Hsgk58XAf/ZFNQfLg9T685otFHRGrZGtVMiGocDCVvC2hVVDSc
CA/hbUa1BCsQ6G7p6+u0i2y+roVRs9aXMBQpsxw+9HcbRN1BuVu6Kup9ifirhdhs
WN3LhG+Nji42WDYy/mdr/M2yGOf7+NIPY9JWEYmKW2Llu571mJaVo82V+SG3D1Ur
1Iw6WF+1UW+mrmLUEe911W8guVKEu5vwCTyU88lk5Ub77pOgjCwzVc3atdk3SYC0
HHiGb0kowlb8hFtUcEXxl/jhiOUUDCLs2gkcXXl7X2qqovh4DNOX9FWnHM+rmVGY
kYHCLtjPVw5rHidS1B7j12LDcAkT4XGslYffr6AaFYl129LBEAEcDBtzp43avd0a
g2JJOcvuOyCua5QUgrXfcFNA0K677FGOOBGjW26c2ls/4sd8Walj2aheEbnso0ep
DVVYGgCh2oi4QwcnmtpsNXJBWnKq+5s2wtNNjjby4HQ0NmH2eoHVYbgYflMxE2ga
G2Nbsb0c+OyUBuALV4CxMsHOaBvaEBmb6FNN8kVpep7tTsM+7B03E+uQowDJ7xH8
Lj6AMwC3m9p6EQD2K5hgKL2tb8dg8h8atA5/6LS7rFkb5/MSehcy7AEnGWqOVBOm
Ok3fjAjCUydG10Zl/9bwHStP4zn6T5MITu2ysiVuePbzjjF2IcW0f6UEqB++ezLJ
BTEl3aNPXxDKWJu4s0iLFru53eOqm+uTbM1yRaHnsjOC0Qld+AZXDpMb6nM9Y7re
F/UYfAzR1WrkPHMqRgQGZmxOQSxm5d0us+Ds0RU5wY5aQf5F2qP35eERYbr9QzXk
JyNJ8MzqTMdpnJUzLr0W189eWwxwT4QRWbX8G+50d+UkL9i554Li93YuBGejiQLM
XX5eB9D0HDgcOo163ye1j/KEXNQVnTcpCxMUeQn2BzPmfGXj1P63WACodSy28SPv
GSyD/N9yufrsgQi1ZGd4AE6sVRbD
=Kavz
-----END PGP MESSAGE-----
```


Das Entschlüsseln funktioniert genauso, nur halt umgekehrt ☺

Es ist natürlich auch möglich einen Text / Email u.s.w. ohne ein PlugIn für das Emailprogramm zu verschlüsseln und zu entschlüsseln.

Wir kopieren einfach den Text den wir verschlüsseln wollen und benutzen das Programm GPG / PGP Tools. Dort wählen wir veschlüsseln. Es öffnet sich ein feld. Dort kopieren wir den Text hinein, wählen den Schlüssel aus, geben unser Passwort ein – FERTIG!

PGP vs. GPG ...

GnuPG selbst ist ein _Kommandozeilenwerkzeug ohne grafische Funktionalitäten. Es stellt die reine Kryptografie-Software dar, die direkt von der Kommandozeile aus genutzt werden kann, so auch in Shell-Scripten oder von anderen Programmen. Es ist also das Back-End für

darauf aufsetzende Applikationen.

Auch wenn es "nur" von der Kommandozeile genutzt wird, bietet dieses Werkzeug die gesamte Funktionalität - ein interaktives Menü eingeschlossen. Der Befehlssatz dieses Werkzeugs wird also immer eine Obermenge dessen sein, was diverse Frontends anbieten.

Vollständiger Ersatz für PGP.
Unterliegt der GPL und wurde von Grund auf neu programmiert.
Kann als Filterprogramm genutzt werden.
Vollständige OpenPGP-Unterstützung (siehe RFC2440 auf **RFC Editor**).
Bessere Funktionalität als PGP und erhöhte Sicherheit gemessen an PGP2.

Entschlüsselt auch Nachrichten, die mit PGP 5, 6 oder 7 erstellt wurden.
Einfache Implementierung neuer Algorithmen durch Erweiterungsmodule.
Die Benutzer-ID muss in einem Standard-Format vorliegen.
Unterstützt Verfallsdaten für Schlüssel und Signaturen.
Verfügbar in vielen Sprachen

PGP ist kommerziell und daher nicht wirklich sicher. Ich rate zu GPG!

BEZUGSQUELLEN:

GPG:

www.gnupg.org
für Windows, für Apple Mac OS 8x und OS-X 10.x, für Linux: Debian, Suse, RedHat, Mandrake und viele andere.

Frontends (Grafische Tools)

Für Apple Mac
http://macgpg.sourceforge.net/de/index.html

PlugIns für
Eudora, Entourage,
Apple Mail PlugIN:
http://www.sente.ch/software/GPGMail/English.lproj/GPGMail.html

Für Windows
Kommandozeilen Tool
http://www.winpt.org/ als Grafische Oberfläche
Grafische PGP Tools

PGP

PGPfree - http://www.pgpi.org/
Plugins für
Eudora, Entourage, Outlook & Outlook Express, PegasusMail
und mehr

Zu Maillinglisten:

Die Schlüssel werden beim Plenum am Besten mit Disketten Mensch-zu-Mensch getauscht.

Beim Emailversand dann mehrere Empfängerschlüssel auswählen bzw. beim Verschlüsseln eines Textes mit allen gewünschten Schlüsseln gleichzeitig verschlüsseln.

Jeder für den die Nachricht bestimmt ist kann sie mit seinem pers. Schlüssel decodieren.

Anhang:

Alle Dokumente zu diesem Workshop gibt es unter:
http://www.attac.de/service/gruppensupport/email-adresse/gpg.php

Diesen Workshop kann ich gern auch in Eurer Attac Gruppe halten. Anfragen an mich direkt unter nico@attac.de
(Ich bitte aber um Fahrtkostenerstattung)

Elementar für eine sicher Übertragung von Daten isst und bleibt aber euer Passwort. BITTE: Wählt euch ein langes Passwort mit Sonderzeichen aus. Jeder Schlüssel ist nur so sicher wie sein Passwort. Keine Geburtstage, Jahrestage, Nahmen von Freunden u.s.w.
Auch wenn ein langes Passwort nervig ist, Ihr könnt es schnell erlernen. Nach einigen Tagen geht es schnell von der Hand.

Eine andere Welt ist möglich! – Wenn wir uns nicht ausspionieren lassen. ☺