GPG / PGP

Verschlüsseln von Emails und Dateien
–
Ein Basis-Workshop

Ein Workshop von Nico Wehnemann
Mail: Nico@attac.de

attac

? PGP ?

- PGP ist ein Verschlüssellungssystem welches für Emails entwickelt wurde.
- Seit 1997 ist es kommerziell
- Aus dem alten SourceCode wurde GPG (GNUPG) ein PGP Clone auf der GNU Public Licence
- PGP gibt es allerdings für Privat User auch kostenlos, es ist nur fraglich wie sicher die PGP Schlüssel sind, da sie kommerziell Verwendung finden.

attac

? PGP ?

Wie arbeitet PGP?

- **"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-----
```

attac

? PGP ?

Ist PGP wirklich 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.

attac

? PGP ?

- PGP ist doch verboten !
  - NÖ!
    - Die USA hat in ihren Sicherheitsbestimmungen den (digitalen) Export von Verschlüsslungsmethoden über 128 Bit untersagt.
    - In Ländern wie Frankreich und den USA ist die Verschlüsselung von Daten über 64bit untersagt.
    - Der PGP Algorythmus wurde offiziell analog im Rest der Welt verbreitet.

attac

1024 bit

- Warum sind 1024 bit sicher genug?
  - 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.

Warum eigentlich?

Verschlüsseln & Signieren von Mails und Daten

Ein Workshop von Nico Wehnemann
Mail: Nico@attac.de

attac

Warum?

- Nix zum Mitlesen!
  - 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 FUNKTIONIERT's?

Verschlüsseln & Signieren von Mails und Daten

Ein Workshop von Nico Wehnemann
Mail: Nico@attac.de

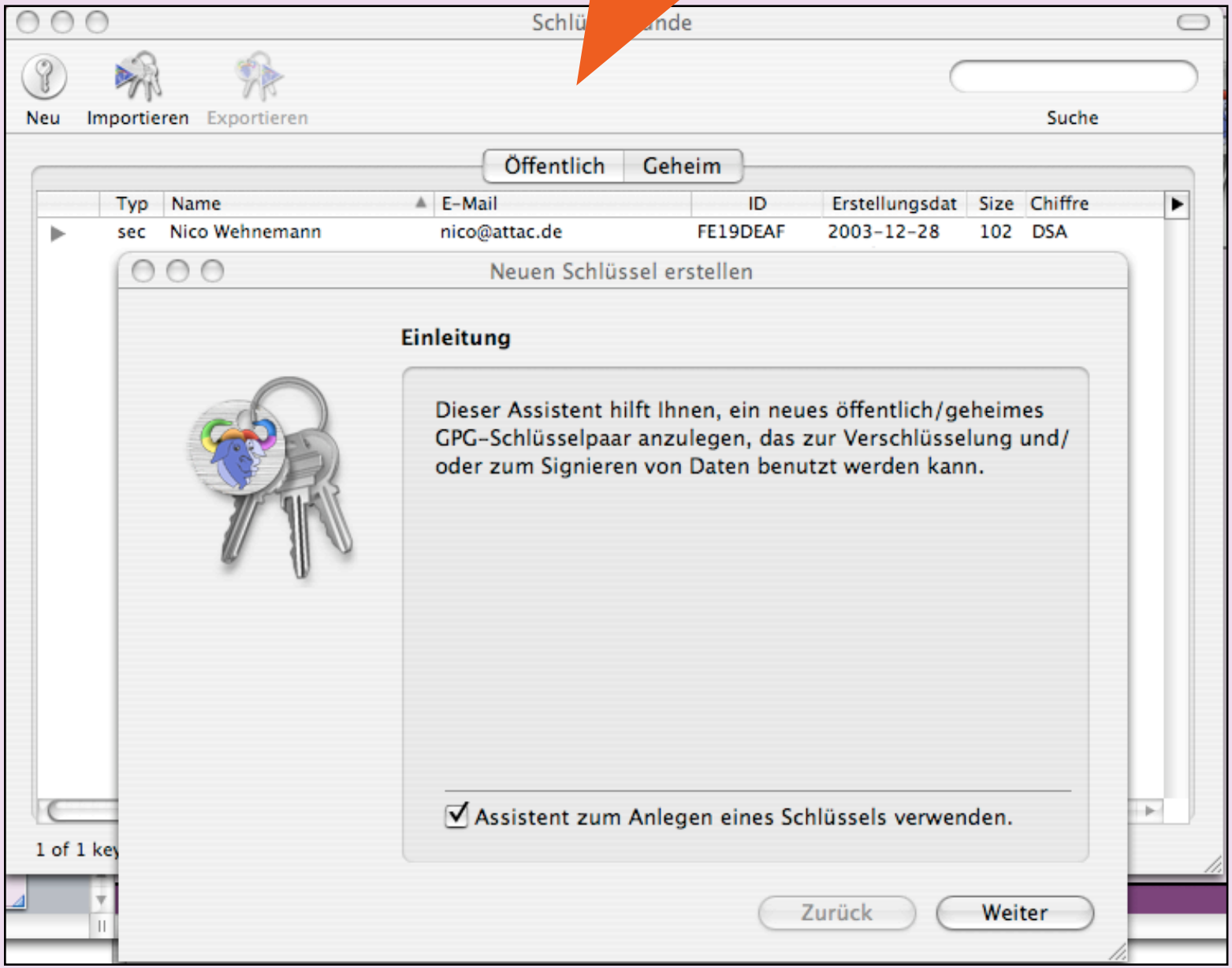
attac

Wie gehts?

- 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

attac

Schlüssel

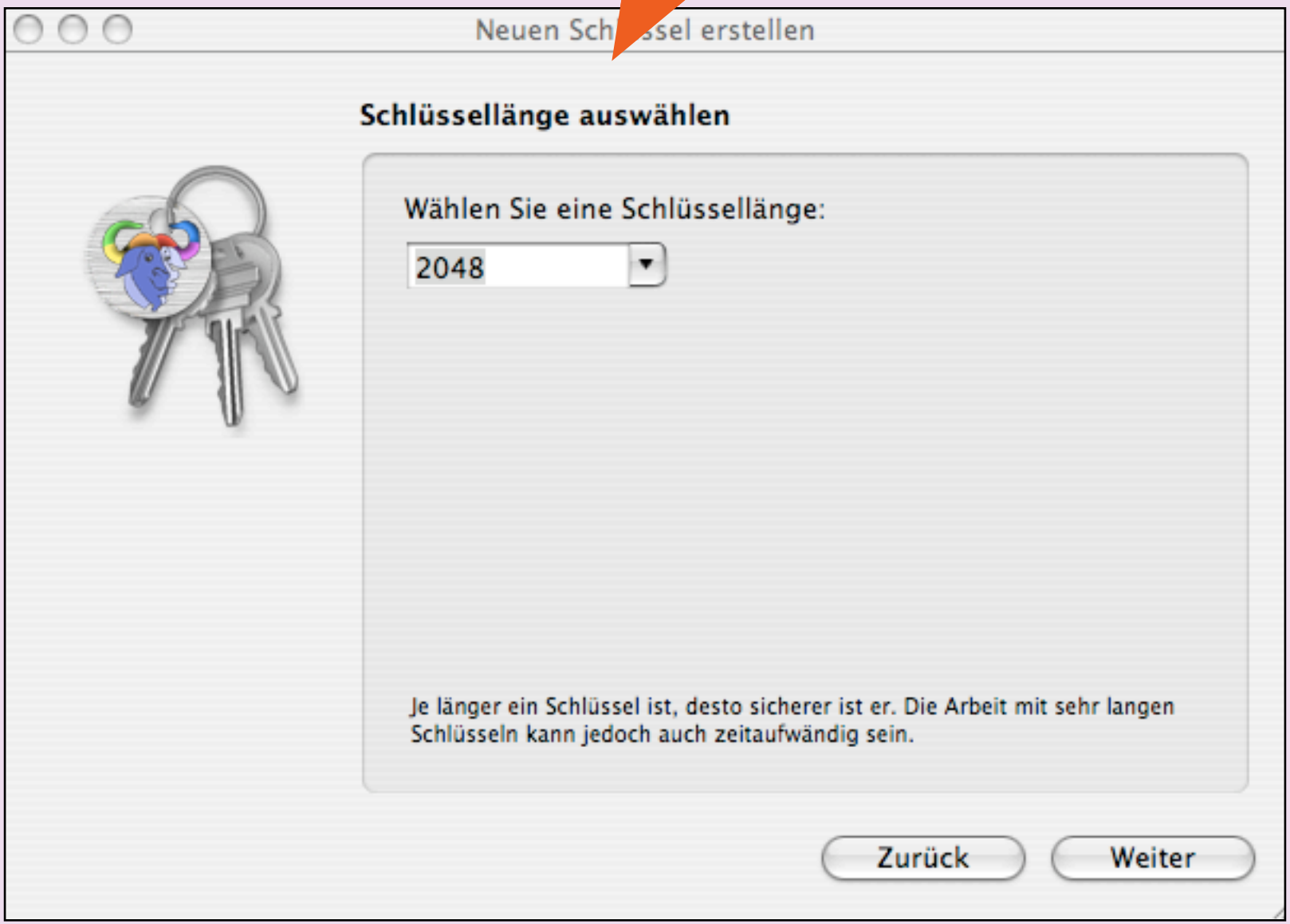


attac

Schlüssel

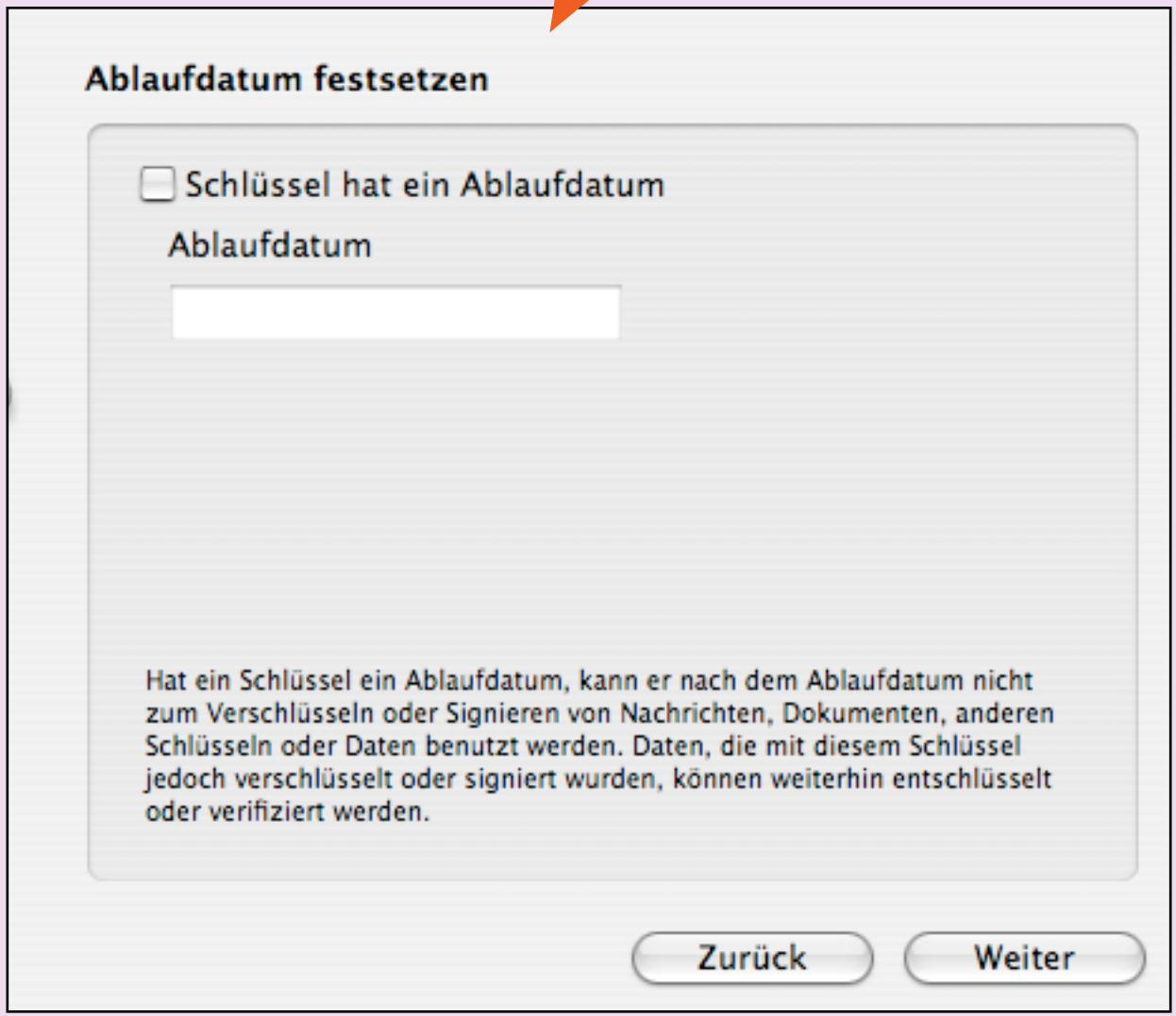
attac

Schlüssel



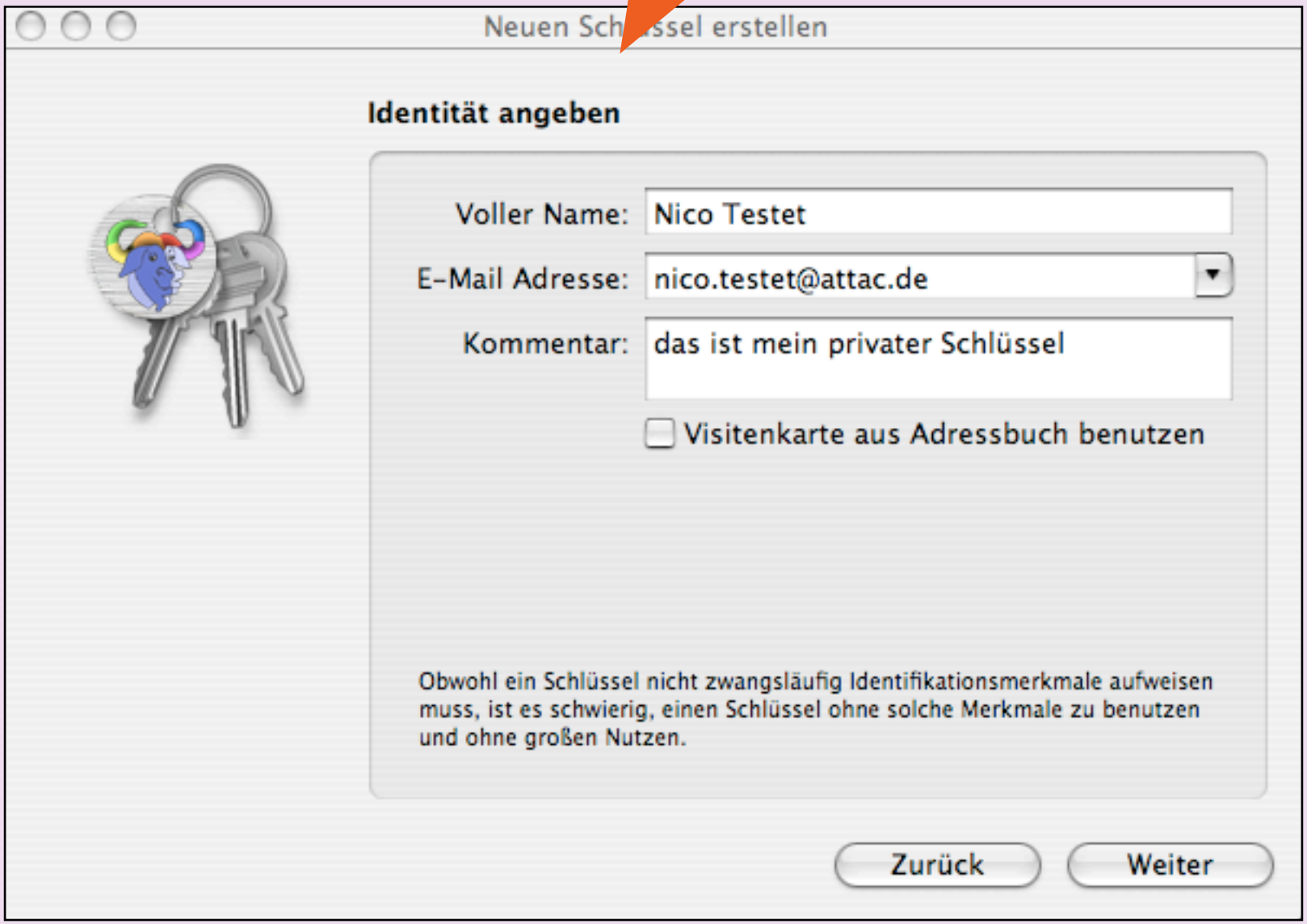
attac

Schlüssel



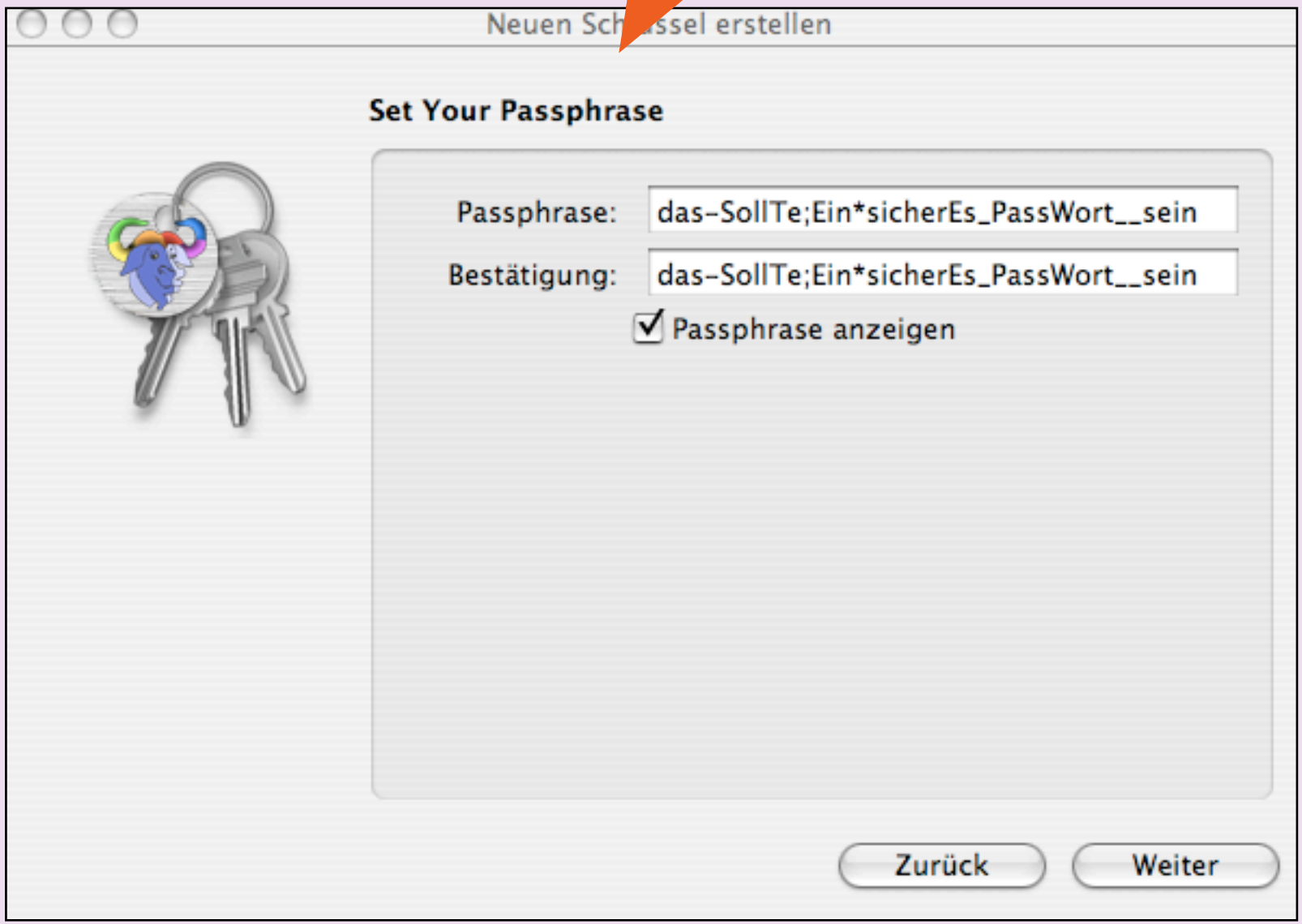
attac

Schlüssel



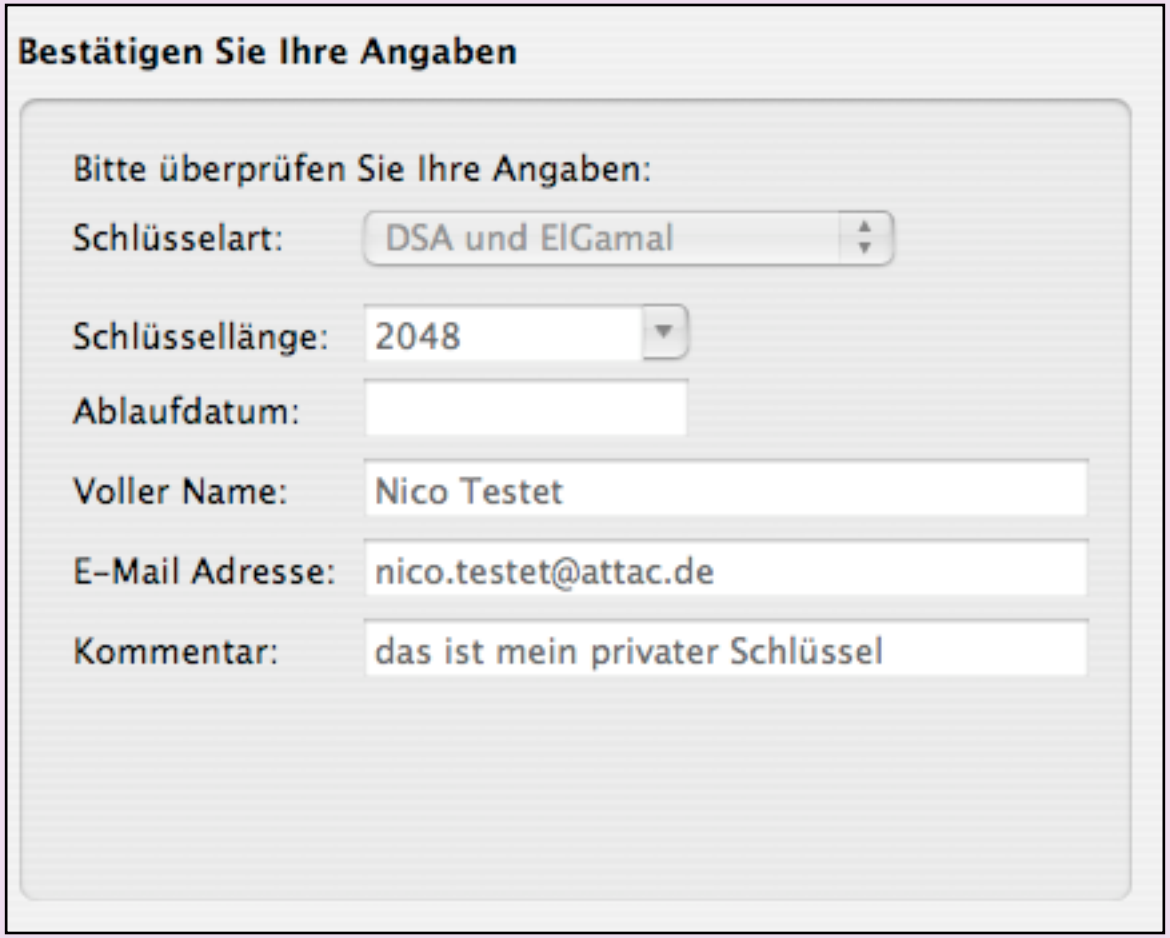
attac

Schlüssel



attac

Schlüssel



attac

!MERKE!

- 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.

attac

Was noch?

- Kann PGP nur Mails verschlüsseln?
  - NÖ!
  - PGP verschlüsselt Dateien
  - PGP verschlüsselt ganze Festplatten
  - PGP signiert Mails

die Software

Verschlüsseln & Signieren von Mails und Daten

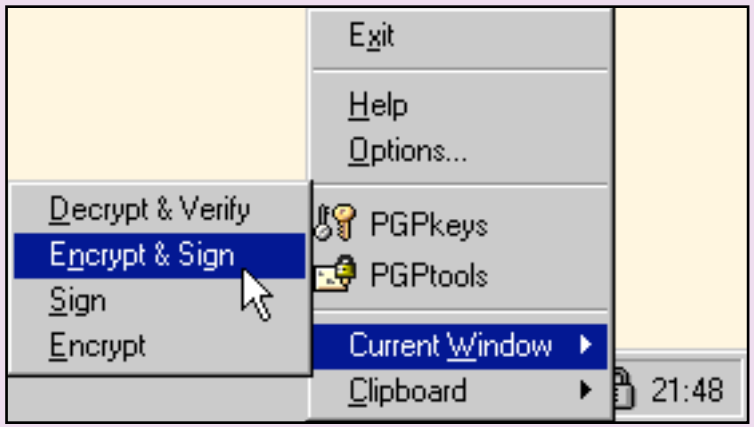
Ein Workshop von Nico Wehnemann
Mail: Nico@attac.de

attac

PGP-Software

PGPtray

Nach der Installation finden sich PGPtray (ein Menü mit den PGP-Funktionen) als Symbol in der Taskleiste neben der Uhr. Es wird als Schloß dargestellt. Von PGPtray aus können alle anderen Programmteile erreicht werden.
Sollte PGP nicht im Autostartordner sein, ist das Symbol eventuell noch nicht neben der Uhr zusehen.

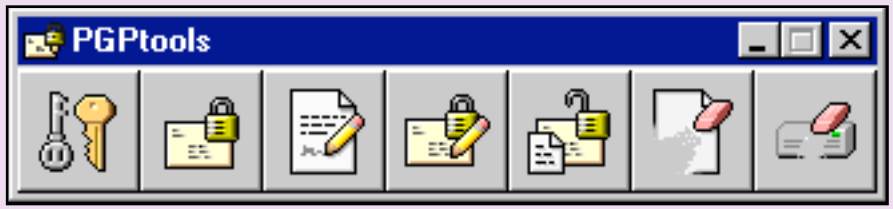


attac

PGP Software

- **PGPtools**
  Wenn Du nicht ausschließlich mit der Zwischenablage (Clipboard) arbeiten willst, gibt PGPtools. Du wählst einfach den Weg über das Startverzeichnis.

- Außerdem kannst Du natürlich mit Deiner Mail-Software arbeiten, wenn es ein PGP-Plugin dafür gibt.

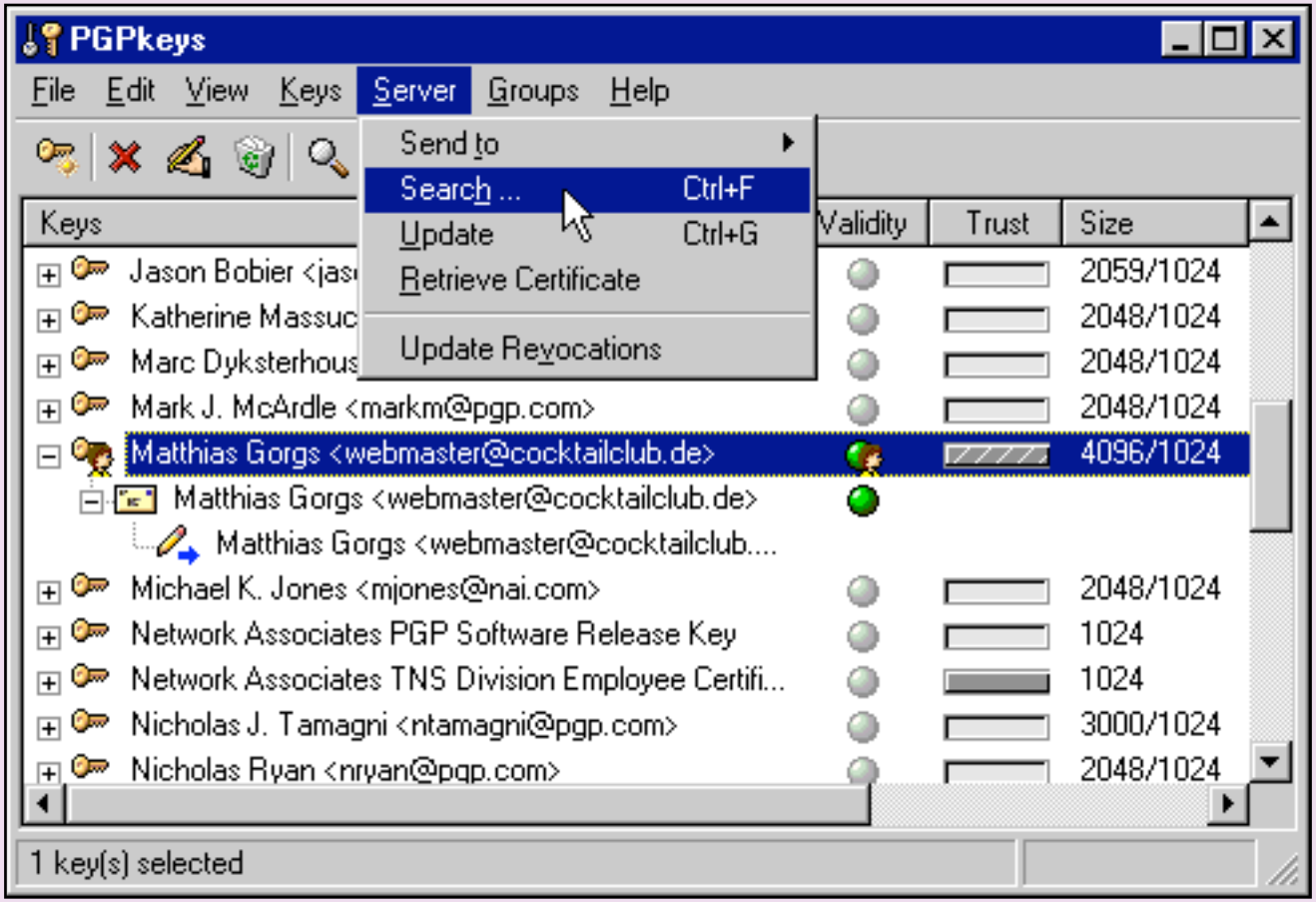


attac

PGP Software

PGPkeys

Hier werden die Schlüssel verwaltet. PGPkeys kannst Du über PGPtray, PGPtools, das Startmenü oder über das PGP-Menü in unterstützter Software öffnen.



attac

Schlüssel verteilen

- 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| und den Namen der Datei an, 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

attac

Schlüssel verteilen

- **Auf Keyserver veröffentlichen**
  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.

attac

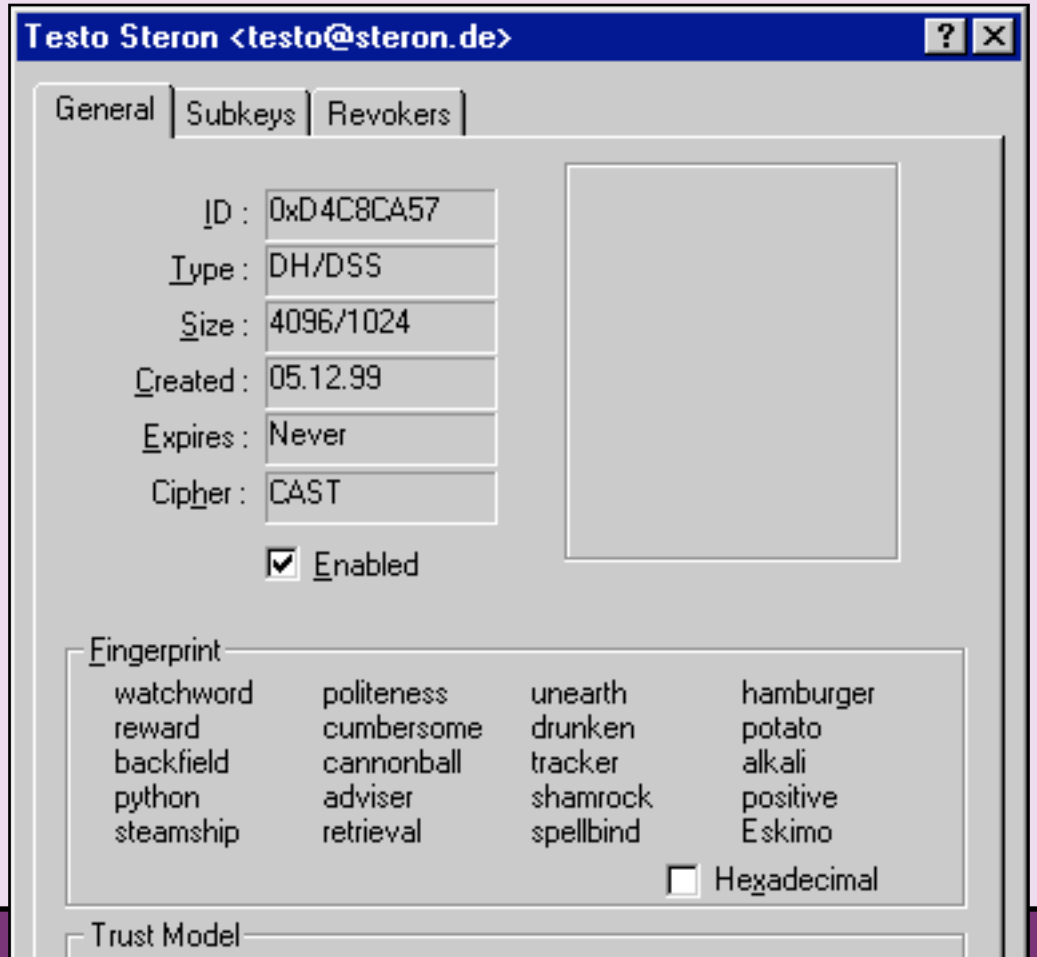
Fingerprint

Fingerprint zum Vertrauen

- Ein Beispiel: Carolin will Dir eine vertrauliche Nachricht zukommen lassen. Wenn sie den Schlüssel von Dir persönlich (d.h. Du hast ihr den Schlüssel auf Diskette selbst überreicht) erhalten hat, ist das Risiko, daß ein gefälschter Schlüssel verwendet wird, sehr gering. Aber wenn Carolin Ihren öffentlichen Schlüssel von einem Server aus dem Internet holt oder per Email erhält, ist es möglich, daß ein unbefugter Dritter einen öffentlichen Schlüssel erzeugt hat, der Deinen Namen trägt. Carolin, die Dir eine geheime Nachricht schicken will, wird diesen Schlüssel verwenden, weil sie denkt, es sei Deiner. Besagter unbefugter Dritter muß nur noch die an Dich adressierte Nachricht abfangen (was technisch nicht weiter schwer ist). Er kann sie dann entschlüsseln, weil er der wahre Eigentümer des Schlüssels ist. Danach könnte er die Nachricht mit Deinem richtigen öffentlichen Schlüssel wieder verschlüsseln. Du merkst also nicht, daß die Nachricht zwischendurch gelesen wurde (man-in-the-middle-attack).

Fingerprint

- Jeder Schlüssel hat einen Fingerprint.. (siehe unten)
- Überhaupt keinen Sinn macht die Verbreitung des Fingerprints per Email, denn der Fingerprint kann ohne weiteres im Email verändert werden.



attac

Import

- Schlüssel importieren
  - wie exportieren
  - Schlüssel per Mail bekommen oder vom Keyserver holen
  - Schlüssel werden im Programm “PGP-Keys” importiert
    - zum Vertrauen sollte man den Fingerprint anfordern sofern man den Schlüssel nicht pers. überreicht bekommen hat. (Diskette, CD) oder der Email genug vertraut.

Ver- & Entschlüsseln

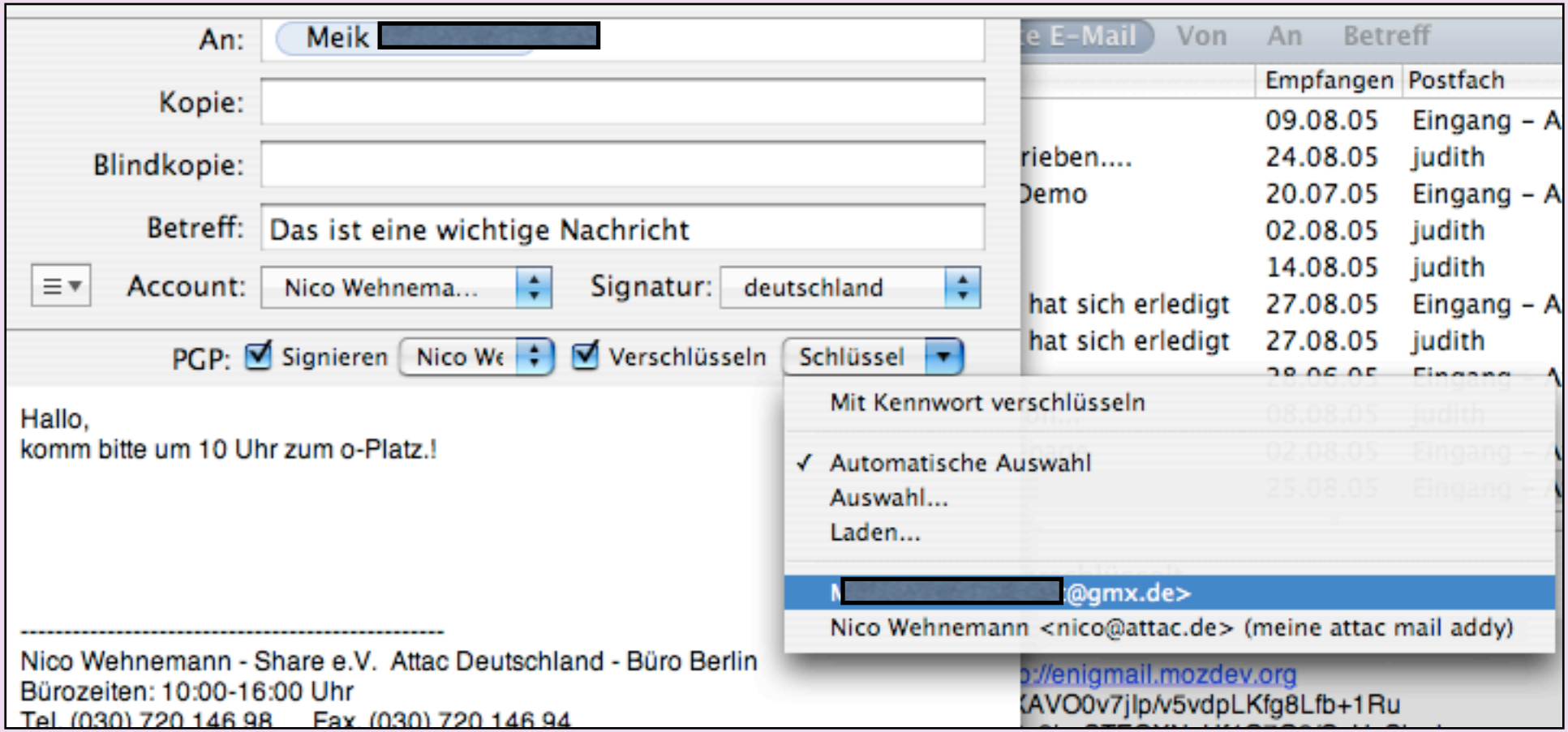
Verschlüsseln & Signieren von Mails und Daten

Ein Workshop von Nico Wehnemann
Mail: Nico@attac.de

attac

Ver-schlüsseln

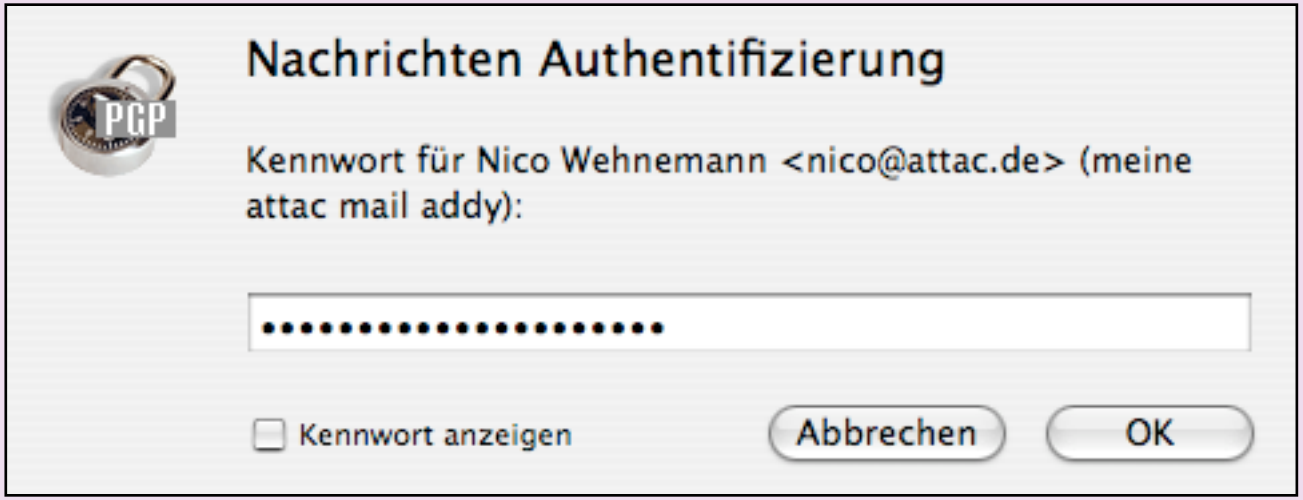
Wie verschlüssel ich eine Nachricht?



attac

Ver-schlüsseln

Verschlüsseln



attac

Das ist eine wichtige Nachricht — Gesendet

E-Mail(s) löschen | Ist Werbung | Antworten | An alle | Weiterleiten | Drucken

Diese Nachricht wurde mit PGP verschlüsselt. Entschlüsseln

Von: Nico Wehnemann____Attac <nico@attac.de>
Betreff: **Das ist eine wichtige Nachricht**
Datum: 13. September 2005 11:45:30 MESZ
An: Meik [redacted]

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

hQEOA56fE4hX2tE/EAQAIjCPHZtqxKkkJezdkIPoc2pmvaoUizWuWi5wjXGlUmV+
r17qmRFa7C4cYqOFYG4IAyx17KvrhtQLExUk3lxVL+G3bzblgRz3wbGmVP6/6Fg1
l69voQ1Svt9m9FQT4QeYAPC/aX4+Mqo8ImFUYfBCagoBmiCCDt/Db5ZlOL69veED
/39b32zVIR+gU9DTmWqqKtYht9ezPQhPOB49DHwNTyhgRbGsdwlv+zNg1qkhBL/v
SdhBl9K2AWXl/9fTq6dmqhvpUNh1loG8VAsdZ2O0+fFZsbSY0zsetMfjqNgtVJBr
QiwuOml3pme8trZ+DEatidhFkCJwYxoUFtz6QJhJLzoNhQlOA87xgebUfCXVEAf/
Utd19wl33gHG4esiJGMmarBSlDpaWXaSmHU7rZnnYxF4B/aViPMWehaUtkAmiv12
HmFlRvkFZ9wHA+epY0MOVlasRJoTsq+ltntZlRwPjao2pfpeWkWGnJFi4uBhG3El
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
1lw6WF+1UW+mrmLUEe911W8guVKEu5vwCTyU88lk5Ub77pOgjCwzVc3atdk3SYC0
HHiGb0kowlb8hFtUcEXxl/jhiOUUDCLs2gkcXXl7X2qqovh4DNOX9FWnHM+rmVGY
kYHCLtjPVw5rHidS1B7j12LDcAkT4XGslYffr6AaFYl129LBEAEcDBtzp43avd0a
g2JJOcvuOyCua5QUgrXfcFNA0K677FGOOBGjW26c2ls/4sd8Walj2aheEbnso0ep
DVVYGgCh2oi4QwcnmtpsNXJBWnKq+5s2wtNNjjby4HQ0NmH2eoHVYbgYflMxE2ga
G2Nbsb0c+OyUBuALV4CxMsHOaBvaEBmb6FNN8kVpep7tTsM+7B03E+uQowDJ7xH8
Lj6AMwC3m9p6EQD2K5hgKL2tb8dg8h8atA5/6LS7rFkb5/MSehcy7AEnGWqOVBOm
Ok3fjAjCUydG10Zl/9bwHStP4zn6T5MlTu2ysiVuePbzjjF2lcW0f6UEqB++ezLJ
BTEl3aNPXxDKWJu4s0iLFru53eOqm+uTbM1yRaHnsjOC0Qld+AZXDpMb6nM9Y7re
F/UYfAzR1WrkPHMqRgQGZmxOQSxm5d0us+Ds0RU5wY5aQf5F2qP35eERYbr9QzXk
JyNJ8MzqTMdpnJUzLr0W189eWwxwT4QRWbX8G+50d+UkL9i554Li93YuBGejiQLM
XX5eB9D0HDgcOo163ye1j/KEXNQVnTcpCxMUeQn2BzPmfGXj1P63WACodSy28SPv
GSyD/N9yufrsgQi1ZGd4AE6sVRbD
=Kavz
-----END PGP MESSAGE-----
```

attac

Ent-schlüsseln

wie entschlüssel ich eine Nachricht?

Diese Nachricht wurde mit PGP verschlüsselt. Entschlüsseln

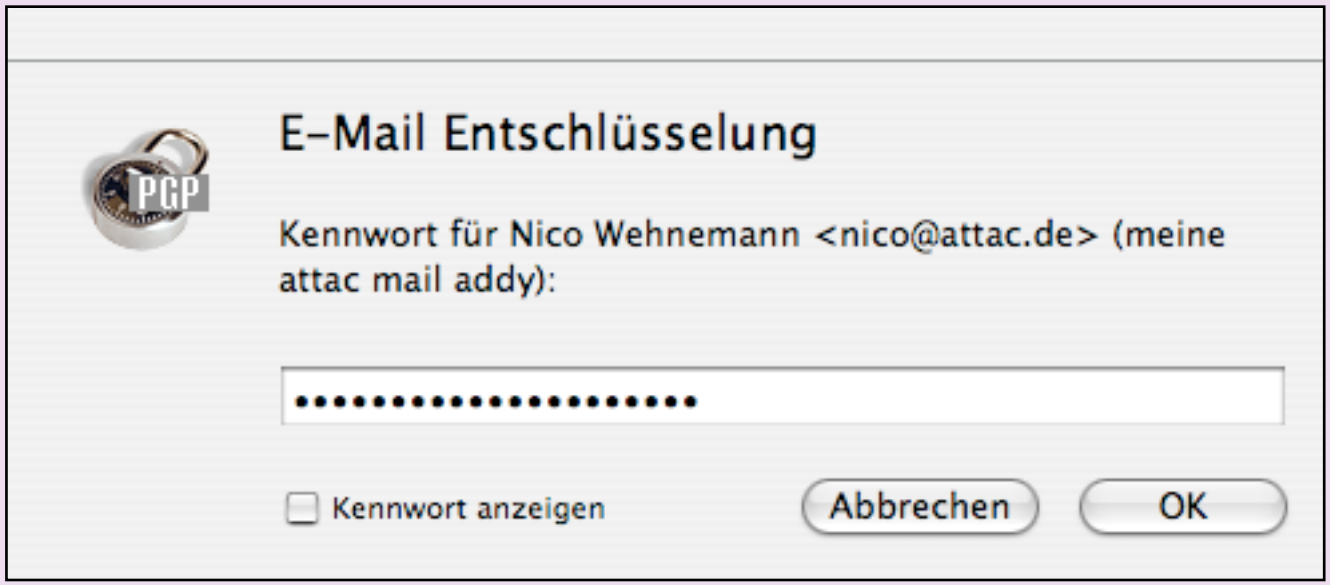
Von: Mike [redacted]
Betreff: **geht doch!!!**
Datum: 25. August 2005 11:55:18 MESZ
An: Nico Wehnemann____Attac <nico@attac.de>
Sicherheit: Verschlüsselt

-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-15
Version: GnuPG v1.4.1 (MingW32)
Comment: Using GnuPG with Thunderbird - http://enigmail.mozdev.org
hQEOA56fE4hX2tE/EAP/RJ8L0KeGX8TTxXjoXAVO0v7jlp/v5vdpLKfg8Lfb+1Ru
KBedblOUMt/ilWYVcae7DrhpmOw65H68lXFrBc2LpSTECXNxHf4O7Q6/CxUvShwh
ONv09j7qfi4ridG930UU9hmkXbtlDTTSLDnG1pFr7B2SJWCKZ6amY2uWQe8OxmkD
Y2nWOsWta7qw7CA8lhCqe7OAjmAgcd9eLdYrx1loeT/YzZNNY70Qe0bvLuGJDlyu
24Tpw+44KuCdnGPltoTaNGQg/Y696gZq9XwLvp8ojR8bVpptdhQShuokDKeT5+7h
OQT4e+hF0S3W2X6qrXGV2etMgTVLUrY0KOjJ+cCuuydNhQlOA87xgebUfCXVEAf/
Y7YtOecKc2mgnyRY0gLoxWPhO/VRphlb8m4GE8BLgMDOdfFe/UFxpJNFuj00lfua
cSHebzCasDYRhmo6cUl97JBzGUc/zxG+ZvtOd6kZOhBP/iCFUwu3lmGOzF5QltBX
lviYkV7pMPJBcShFjlGuHzG9Kr5byQNVLsSgaFBCeVPD7DzTMYMFzAGy6OlrrQ9J
ZNGa1XSD+r3eOeeIm1pb9x87IRO6AAbfK9fYLoENB09L0NQf4vpcdCqFm8yw5fTv
ZMwu8WWFYcWnAjCCDJfeiEmvXiBsUZ9MCnSeXwQlma3izt8QFSo/p12BwTiSvJ1E
8j8/l/v9uueWJMPj8kk7BQf+PgHGys6P6N9nXDODBOh8xEegWhBDbeGmfxHZ4uLR
LQUVciaehjH71nXNXHcDOsR3uJ+7gCgKbdhymhlyAR3+PspXKsLeDGq8beIJVvRx
mNwlMQUOlrvJOnJxtOgxDRw0TZVSbY7wRt9gFgCUC/xDG9S33HYTlmlJV4cHihwL
QXLkJEi9DA8vUA2XF9AEbLNUNKxk5XJ7KLVKZetpdpsg+mhPkHklyi9loGbBSgTX
pM4zmAUQlyHYuzYrosl1mbQqvbm1LpTE4NczWlTaOQbntGiNUefviCWepq7Cg+ZX
SJGBP5kdrOclyxw3x3sEXgPUmdoXUlf7cKRrQwJMyp/zQdJQAXdvev46dYCu4pKV
AQARozB21LjZvmKU7frVhW+vaFkmUXEskVf8RIntS7ZCkm36/LbfFCJ/xlXaZii9
4phTTXZ29PUNumSfLF9pZ9UFkWY=
=LWQS
-----END PGP MESSAGE-----

attac

decrypt

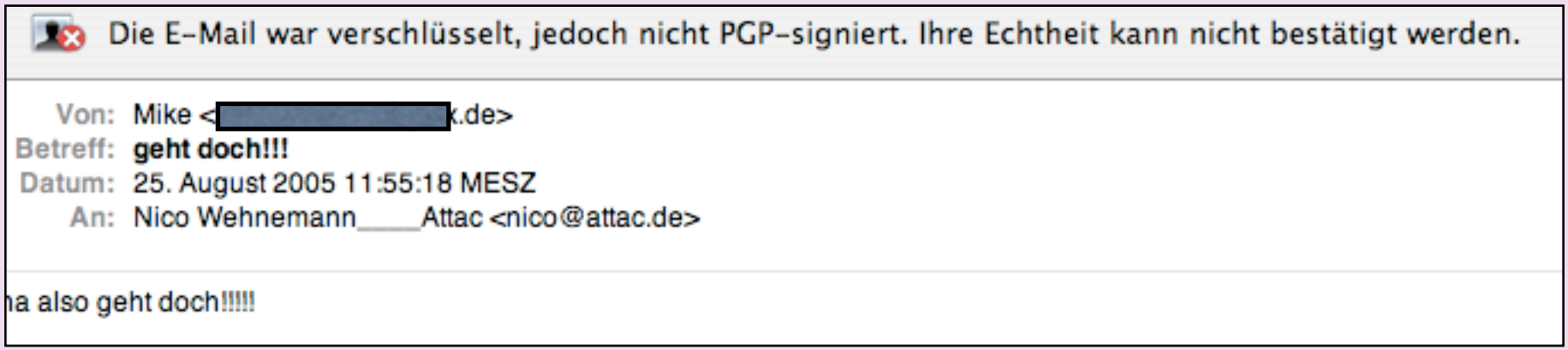
Entschlüsseln mit PlugIn



attac

decrypt

- Es ist entschlüsselt!


Die E-Mail war verschlüsselt, jedoch nicht PGP-signiert. Ihre Echtheit kann nicht bestätigt werden.

Von: Mike <[redacted].de>
Betreff: **geht doch!!!**
Datum: 25. August 2005 11:55:18 MESZ
An: Nico Wehnemann____Attac <nico@attac.de>

ha also geht doch!!!!!

attac

Decrypt

- Entschlüsseln ohne Email Plugin
  - die gesamte Nachricht kopieren
  - PGP Tools öffnen und auf Entschlüsseln (Decrypt) klicken
    - Daten aus der Zwischenablage einfügen (paste) und mit Passworteingabe entschlüsseln

attac

Dateien

- Dateien?
  - ja, Dateien!
  - PGP verschlüsselt die gewünschte Datei und speichert diese als Kopie verschlüsselt ab.
  - Mit dem PGP Datei Clienten kann die Datei wieder entschlüsselt werden.
  - Für jeden Schritt benötigt man das Passwort, sein eigenes oder das des gewünschten Empfängers

attac

GNU PG

- 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 PGP 2.
  - 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

Bezugsquellen

Verschlüsseln & Signieren von Mails und Daten

Ein Workshop von Nico Wehnemann
Mail: Nico@attac.de

attac

GNU PG

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

attac

GNU PG

- 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

attac

GNU PG

- Für Windows
  - Kommandozeilen Tool
  - http://www.winpt.org/ als Grafische Oberfläche
  - Grafische PGP Tools
  - PlugIn für MailProgramme in Arbeit

attac

GNU PG

- Für Linux
  - PlugIns für
    - Kmail
    - Thunderbird
    - und mehr

attac

Windows

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

Wissenswertes

Verschlüsseln & Signieren von Mails und Daten

Ein Workshop von Nico Wehnemann
Mail: Nico@attac.de

attac

Mailing-listen

Benutzung mit 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.

attac

Staff

- www.attac.de/wissensallmende
  - AG Wissensallmende und freier Informationsfluss
- www.ccc.de
  - Chaos Computer Club
- www.no-epatents.org
- www.offenzu.tk
  - Offener Zivieler Ungehorsam
- www.offeneuni.tk
  - Offene Uni BerlinS

attac

Nächsten Mittwoch

PRAXIS WORKSHOP
in der Offenen Uni BerlinS
um 19:00 Uhr

Ein Workshop von Nico Wehnemann
Mail: Nico@attac.de

lasst uns reden!

wir reden und stellen Fragen die wir ggf. auch sogar beantworten :)

Ein Workshop von Nico Wehnemann
Mail: Nico@attac.de