

Inhalt:

1. Was ist GnuPG?
2. Warum sollte man GnuPG verwenden?
3. Wie erstelle ich ein Schlüsselpaar?
4. Web of Trust - Echtheit der Schlüssel
5. Wie signiere / verschlüssele ich eine e.mail?
6. Resümee

Anhang:

- nützliche Webseiten
- gpg Konsolenbefehle

Was ist GnuPG?

GnuPG = GNU + PG

GNU = rekursive Akronym für „**G**NU is **n**ot **U**nix“

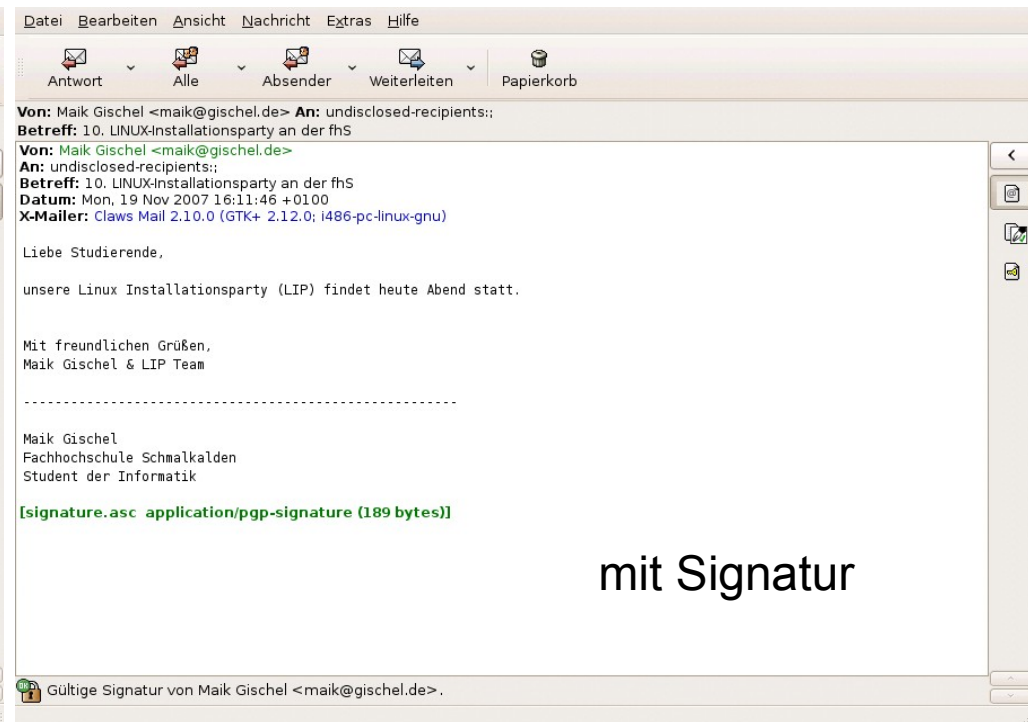
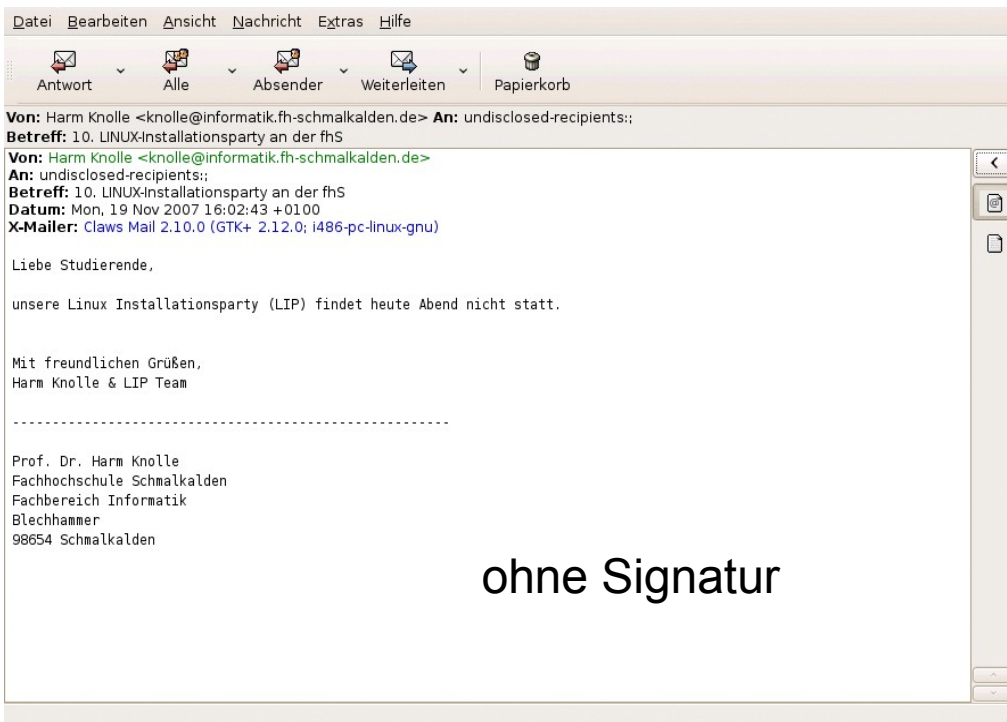
PG = **P**rivacy **G**uard

- ein freies Kryptographiesystem
- verwendet keine patentierten Algorithmen
- verwendet OpenPGP-Standard nach RFC 4880
- Ver- / Entschlüsseln von Daten
- Erzeugen / Prüfen elektronischer Signaturen



Warum sollte man GnuPG verwenden?

- e.mails sind wie Postkarten -> von jeden lesbar und veränderbar
- Passwörter / private Daten sind nicht sicher
- Identität des Absenders ist nicht sichergestellt



Wie erstelle ich ein Schlüsselpaar?

GUI: (z.B. „Gnu Privacy Assistant“)

Verschlüsselungsalgorithmus: DSA und ElGamal (Vore)
 Schlüssellänge (Bit): 1024
 Benutzerkennung:
 E-Mail:
 Kommentar:
 Passwortsatz:
 Passwortsatz wiederholen:
 Verfallsdatum:
 unbegrenzt gültig
 verfällt nach days
 wird ungültig am:
 < November > < 2007 >

Mo	Di	Mi	Do	Fr	Sa	So
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

 OK Abbrechen

Konsole:

`user@host: gpg --gen-key`

* Beantworten der Abfragen zu:

- des Algorithmus
- der Schlüssellänge
- der Gültigkeit
- der persönlichen Daten
- des Passwortes

`gpg -a --output name.asc --export <ID oder Name>`

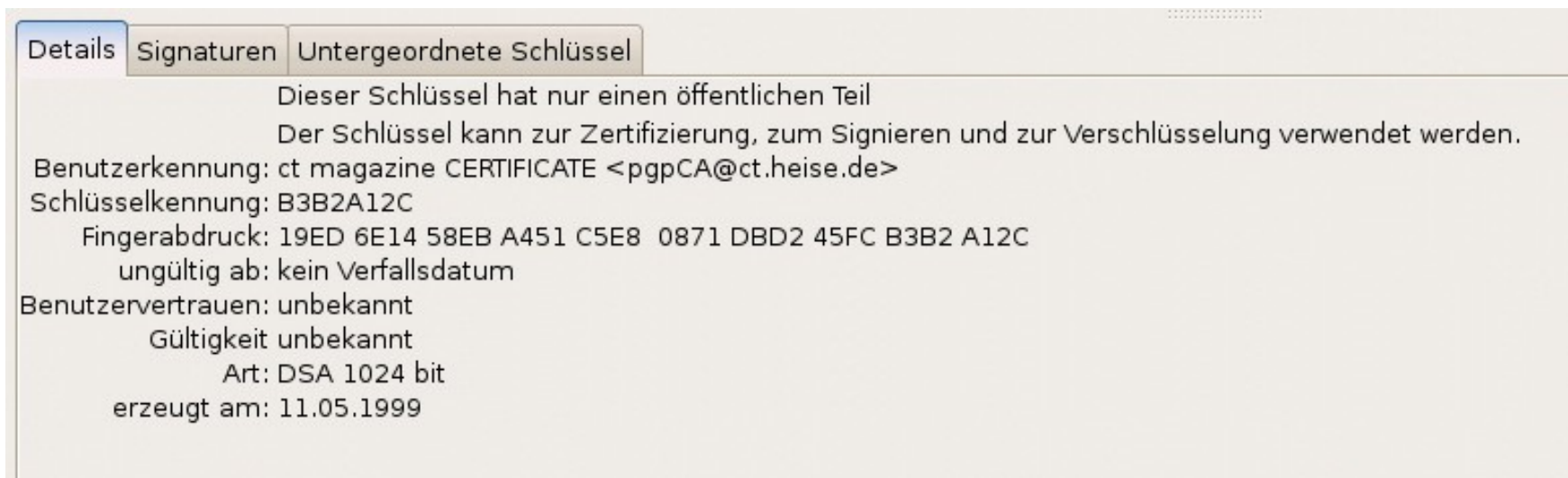
name.asc --> öffentliche Schlüssel zum weitergeben

Button: „Export“ - öffentlicher Schlüssel wird exportiert

Web of Trust - Echtheit der Schlüssel

- gegenseitiges signieren der Schlüssel
- je mehr Signaturen --> Echtheit der Person wahrscheinlicher
- Zertifizierungsstellen (z.B. „c't Zeitschrift“) --> Kontrolle des Personalausweises

- Vergleich des digitalen Fingerabdrucks

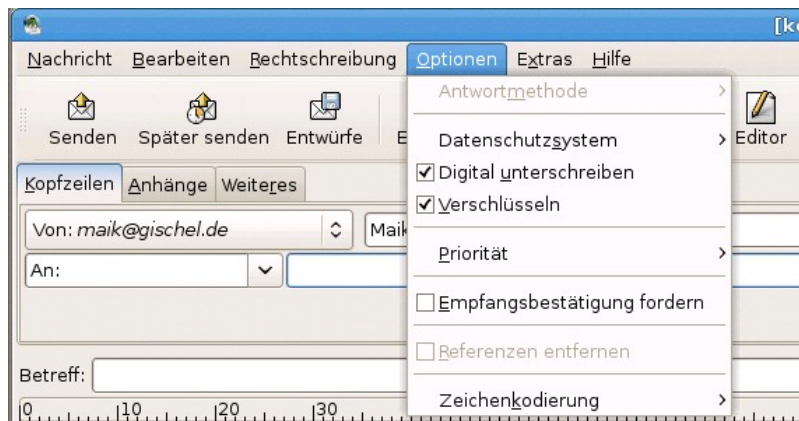


The screenshot shows a window titled 'Details' with three tabs: 'Details', 'Signaturen', and 'Untergeordnete Schlüssel'. The 'Details' tab is active. The text in the window reads:

Dieser Schlüssel hat nur einen öffentlichen Teil
Der Schlüssel kann zur Zertifizierung, zum Signieren und zur Verschlüsselung verwendet werden.
Benutzerkennung: ct magazine CERTIFICATE <pgpCA@ct.heise.de>
Schlüsselkennung: B3B2A12C
Fingerabdruck: 19ED 6E14 58EB A451 C5E8 0871 DBD2 45FC B3B2 A12C
ungültig ab: kein Verfallsdatum
Benutzervertrauen: unbekannt
Gültigkeit unbekannt
Art: DSA 1024 bit
erzeugt am: 11.05.1999

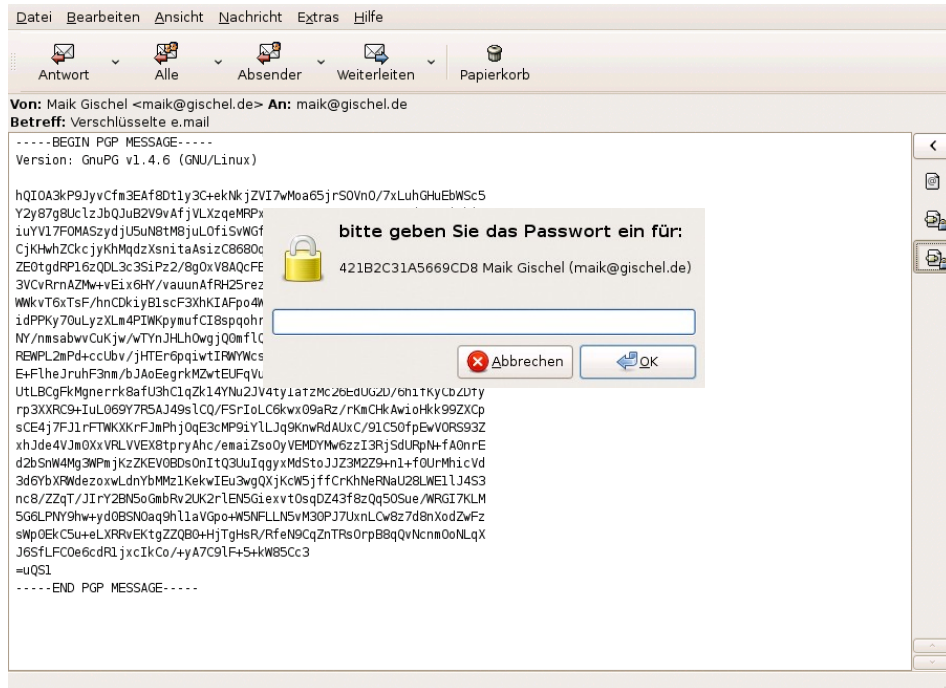
Wie signiere / verschlüssele ich eine e.mail?

- öffentliche Schlüssel des Empfängers muss bekannt sein (Keyserver, per mail erhalten, ...)
- eigene öffentliche Schlüssel muss dem Empfänger bekannt sein
- mail Programm mit GnuPG Unterstützung (Claws, Thunderbird, usw.)

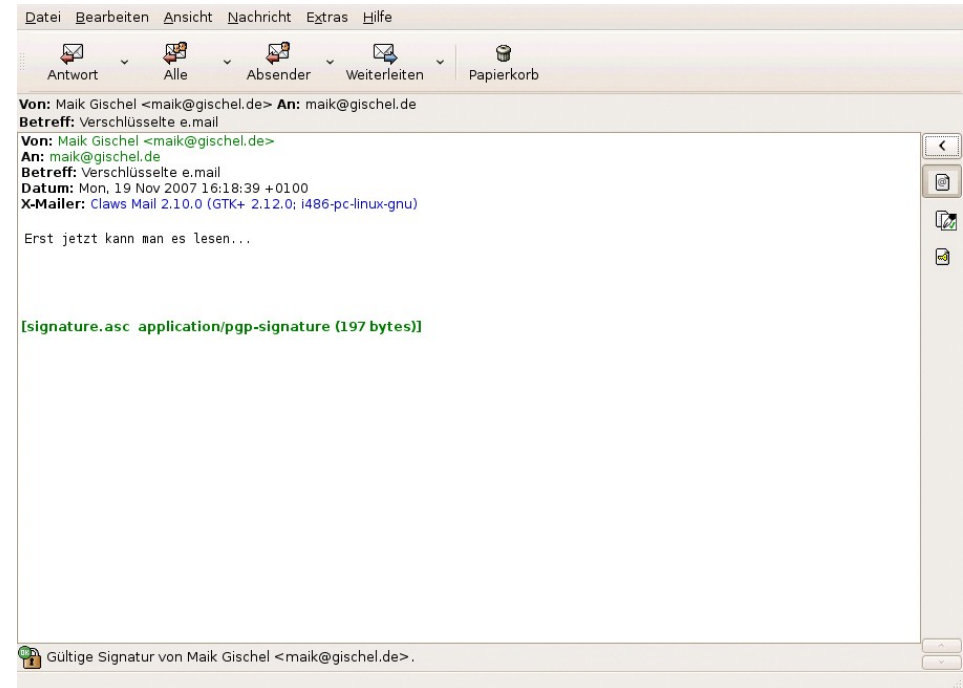


Wie signiere / verschlüssele ich eine e.mail?

falsches/kein Passwort



richtiges Passwort



Resümee:

Wer e.mails ohne Signatur und Verschlüsselung versendet, der muss sich im klaren darüber sein, dass sie jeder lesen und verändern könnte.

Jede unverschlüsselte e.mail sollte man immer erst einmal anzweifeln und für sich hinterfragen, ob der Inhalt stimmen könnte.

Sicheren e.mail Verkehr gibt es nur durch Signatur und Verschlüsselung!

- Danke für eure Aufmerksamkeit! -

Anhang:

Webseiten:

<http://de.wikipedia.org/wiki/Gnupg>

<http://wiki.ubuntuusers.de/GnuPG>

[http://www.gnupg.org/\(de\)/index.html](http://www.gnupg.org/(de)/index.html)

[http://www.gnupg.org/\(de\)/howtos/de/index.html](http://www.gnupg.org/(de)/howtos/de/index.html)

<http://www.pl-berichte.de/berichte/gnupg.html>

<http://www.stefanrusche.de/e-mail-verschlusselung-mit-gpg>

Befehle:

gpg --list-secret-keys

gpg --list-keys

gpg --fingerprint <ID oder Name>

gpg --gen-key

gpg --import name.asc

gpg -a --output name.asc --export <ID oder Name>

gpg --edit-key <ID oder Name>

gpg --gen-revoke

gpg --delete-key <ID oder Name>

gpg --send-keys <ID>

gpg --recv-keys <ID>

gpg --refresh-keys

gpg --search-keys "Vorname Nachname"

gpg --keyserver wwwkeys.eu.pgp.net

- geheime Schlüssel anzeigen
- öffentliche Schlüssel anzeigen
- Fingerprint anzeigen
- Schlüssel erzeugen
- Schlüssel importieren
- Schlüssel exportieren
- Schlüssel bearbeiten
- Schlüssel widerrufen
- Schlüssel aus Schlüsselbund löschen
- Schlüssel zum Server senden
- Schlüssel vom Server holen
- Schlüssel aktualisieren
- Schlüssel finden
- Keyserver festlegen