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

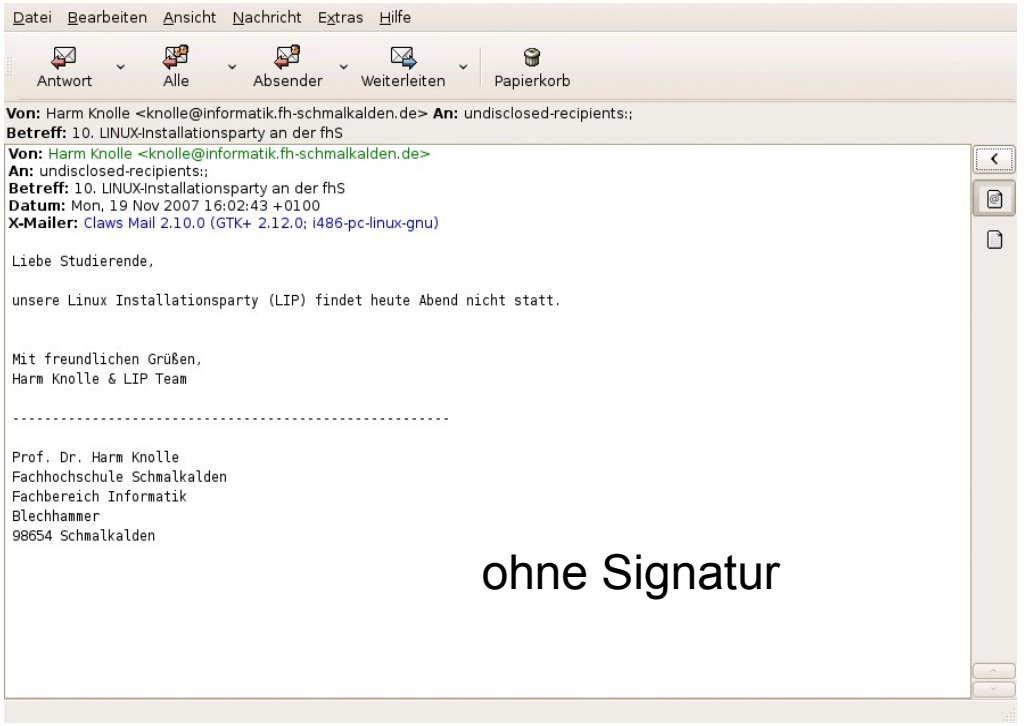
GNU = rekursive Akronym für „**G**NU is **n**ot **U**nix“

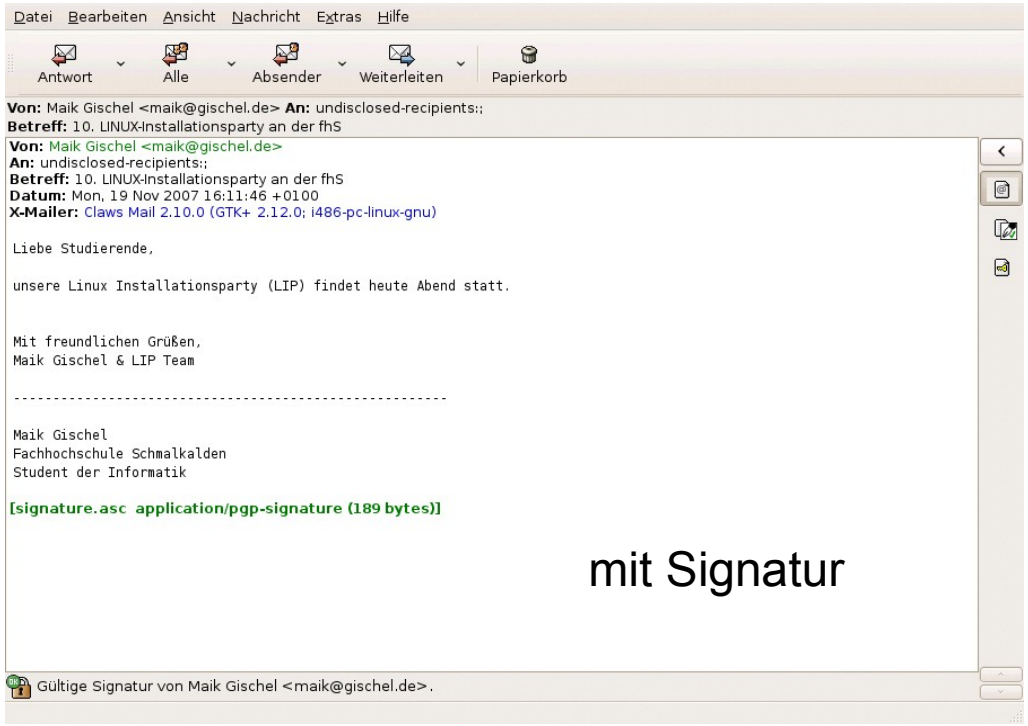
PG = **P**rivacy **G**uard

- 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?

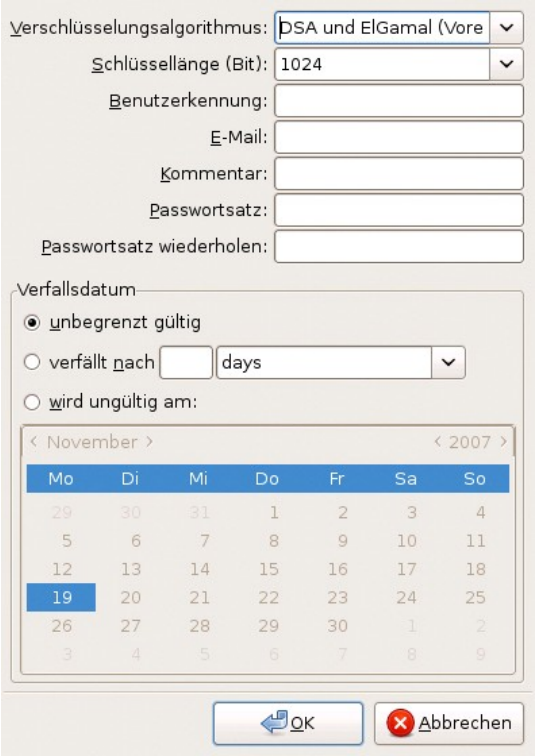
- e.mails sind wie Postkarten -> von jeden lesbar und veränderbar
- Passwörter / private Daten sind nicht sicher
- Identität des Absenders ist nicht sichergestellt





Wie erstelle ich ein Schlüsselpaar?

GUI: (z.B. „Gnu Privacy Assistant“)



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>

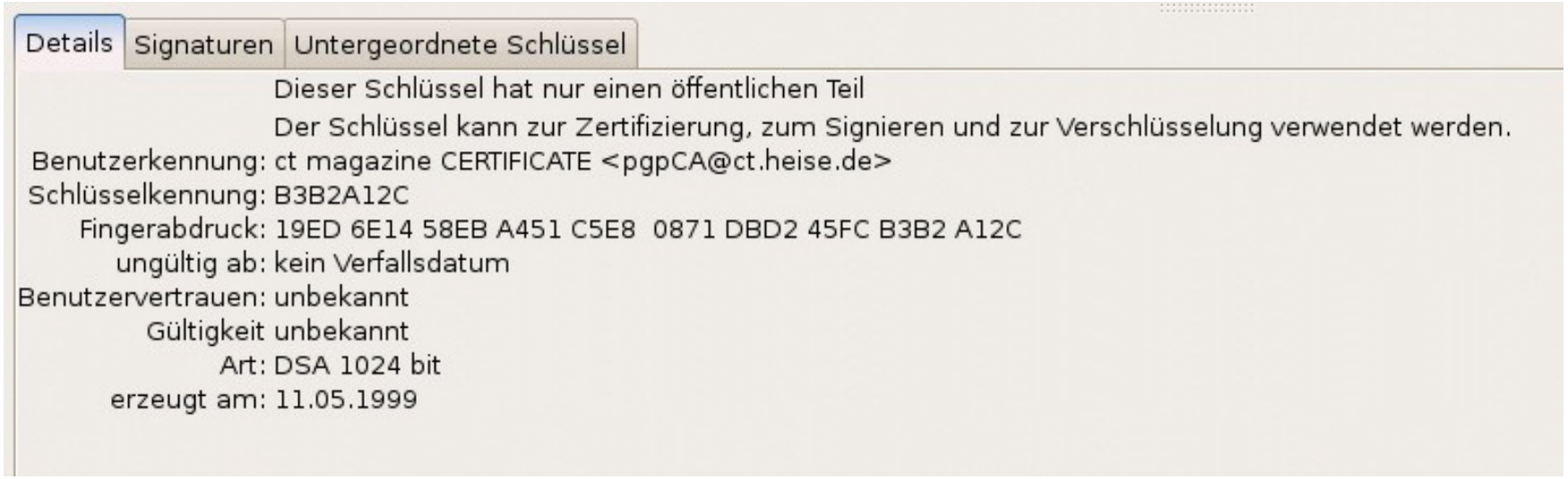
name.asc --> *öffentliche Schlüssel zum weitergeben*

Button: „Export“ - öffentlicher Schlüssel wird exportiert

Web of Trust - Echtheit der Schlüssel

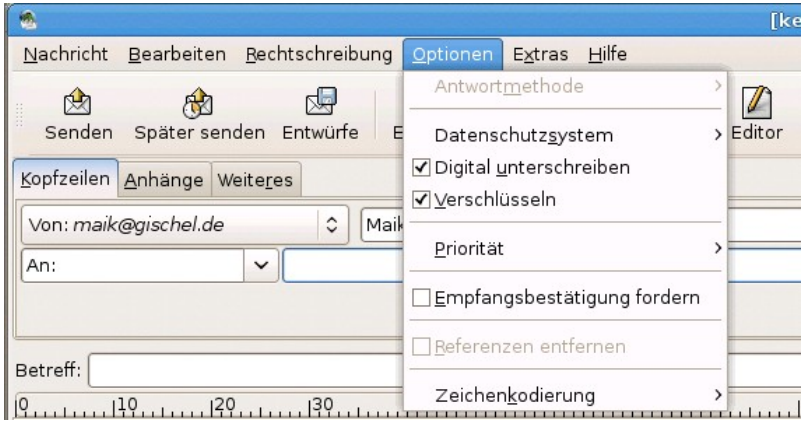
- gegenseitiges signieren der Schlüssel
- je mehr Signaturen --> Echtheit der Person wahrscheinlicher
- Zertifizierungsstellen (z.B. „c't Zeitschrift“) --> Kontrolle des Personalausweises

- Vergleich des digitalen Fingerabdrucks



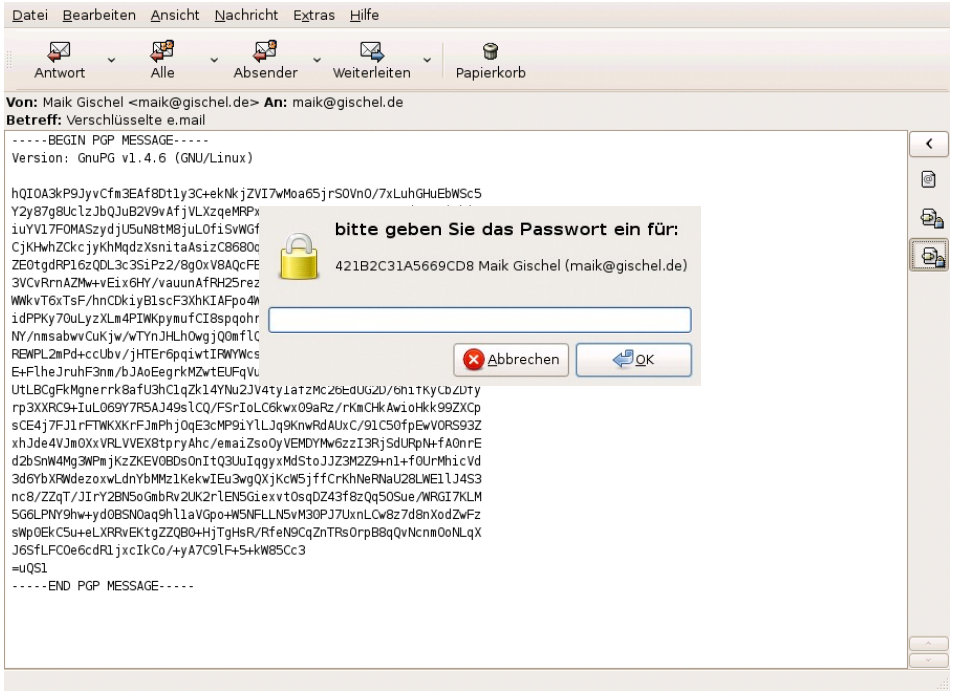
Wie signiere / verschlüssele ich eine e.mail?

- 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.)

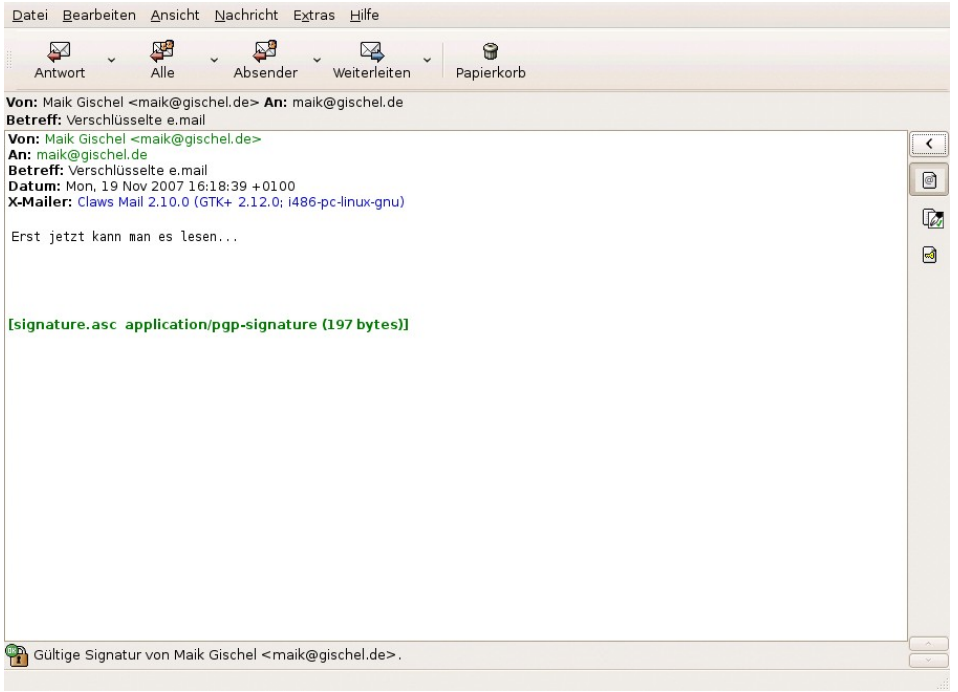


Wie signiere / verschlüssele ich eine e.mail?

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)/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	- geheime Schlüssel anzeigen
gpg –list-keys	- öffentliche Schlüssel anzeigen
gpg --fingerprint <ID oder Name>	- Fingerprint anzeigen
gpg –gen-key	- Schlüssel erzeugen
gpg --import name.asc	- Schlüssel importieren
gpg -a --output name.asc --export <ID oder Name>	- Schlüssel exportieren
gpg --edit-key <ID oder Name>	- Schlüssel bearbeiten
gpg –gen-revoke	- Schlüssel widerrufen
gpg --delete-key <ID oder Name>	- Schlüssel aus Schlüsselbund löschen
gpg –send-keys <ID>	- Schlüssel zum Server senden
gpg –recv-keys <ID>	- Schlüssel vom Server holen
gpg –refresh-keys	- Schlüssel aktualisieren
gpg --search-keys "Vorname Nachname"	- Schlüssel finden
gpg --keyserver wwwkeys.eu.pgp.net	- Keyserver festlegen