Datensicherheit & Verschlüsselung

Journalistischer Kompetenzblock

Robert Bienert

Nordhessen Media e.V.

18. Juni 2009

- URI: `http://hnawatchblog.de/vortrag/datensicherheit`
- Es ist gestattet, das Werk vervielfältigen, verbreiten und öffentlich zugänglich machen, zu folgenden Bedingungen: 
  -  Namesnennung
  -  Nicht-Kommerziell
  -  Keine Bearbeitung und abgeleitete Werke
  - ( Creative Commons by-nc-nd)

Abbildung: Diverse Medien zur Datenspeicherung/Backups.

Abbildung: Diverse Medien zur Datenspeicherung/Backups.

- unbefugten Zugriff verhindern
  - vor Sicherheits- und Geheimdienste
  - auf externe Datenträgern
  - ...

- unbefugten Zugriff verhindern
  - vor Sicherheits- und Geheimdienste
  - auf externe Datenträgern
  - ...
- eigene und Privatsphäre anderer schützen

- unbefugten Zugriff verhindern
  - vor Sicherheits- und Geheimdienste
  - auf externe Datenträgern
  - ...
- eigene und Privatsphäre anderer schützen
- Kommunikation in nicht vertrauenswürdigen Umgebungen

Dieses Seminar geht auf folgende Aspekte und Werkzeuge genauer ein:

Dieses Seminar geht auf folgende Aspekte und Werkzeuge genauer ein:

- GnuPG[a] und GPA[b] zur Email- und Datenverschlüsselung sowie -signierung
- TrueCrypt zur Daten- und Datenträgerverschlüsselung
- SSH[c] für den sicheren Datentransport

[a] GNU Privacy Guard
[b] GNU Privacy Assistant
[c] Secure Shell

Funktionsprinzip

- wahlweise
  - symmetrische Verschlüsselung (ein Schlüssel)
  - *asymmetrische Verschlüsselung (einer fürs Ver-, einer fürs Entschlüsseln)*

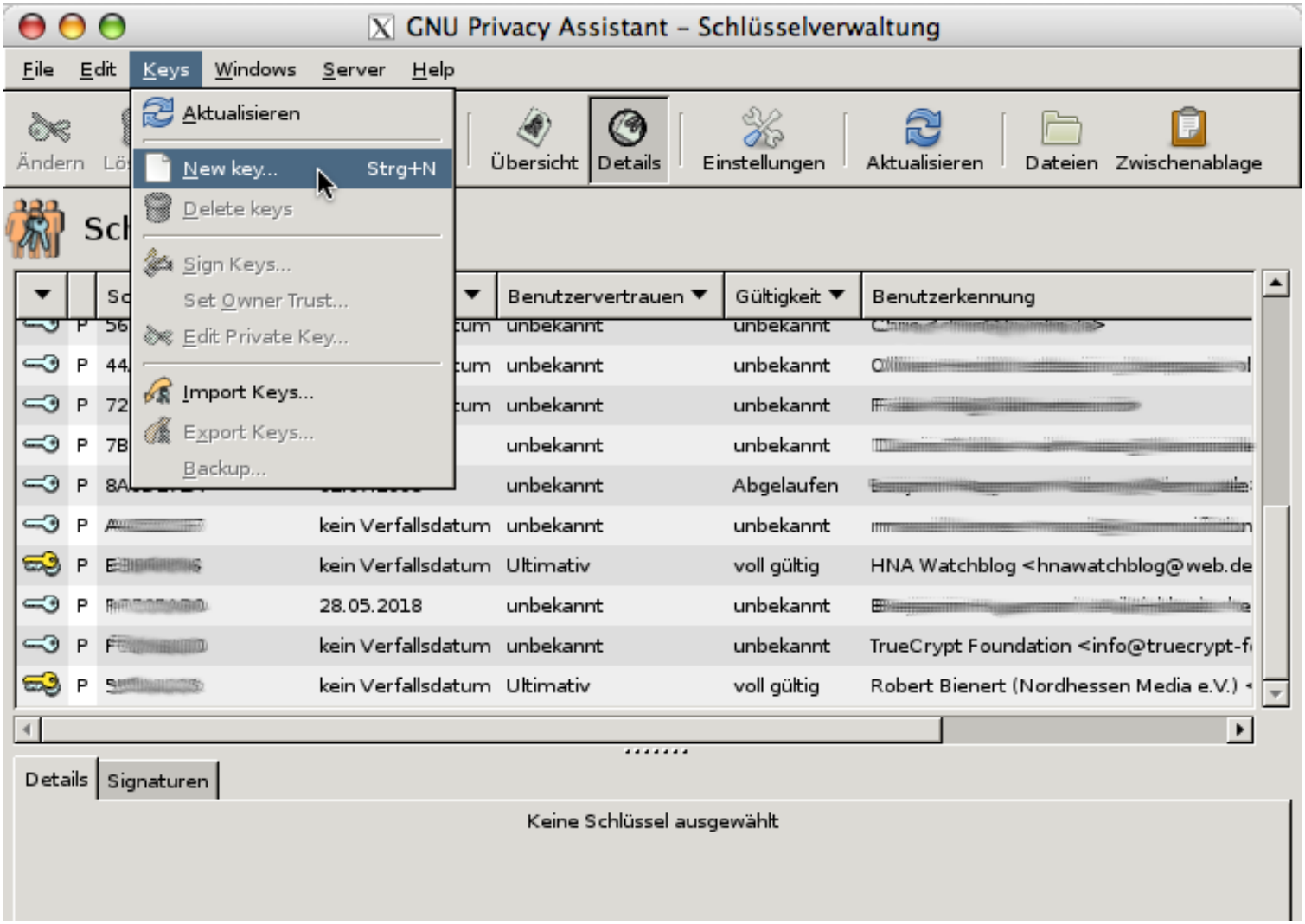
Funktionsprinzip

- wahlweise
  - symmetrische Verschlüsselung (ein Schlüssel)
  - *asymmetrische Verschlüsselung (einer fürs Ver-, einer fürs Entschlüsseln)*
- asymmetrisch:

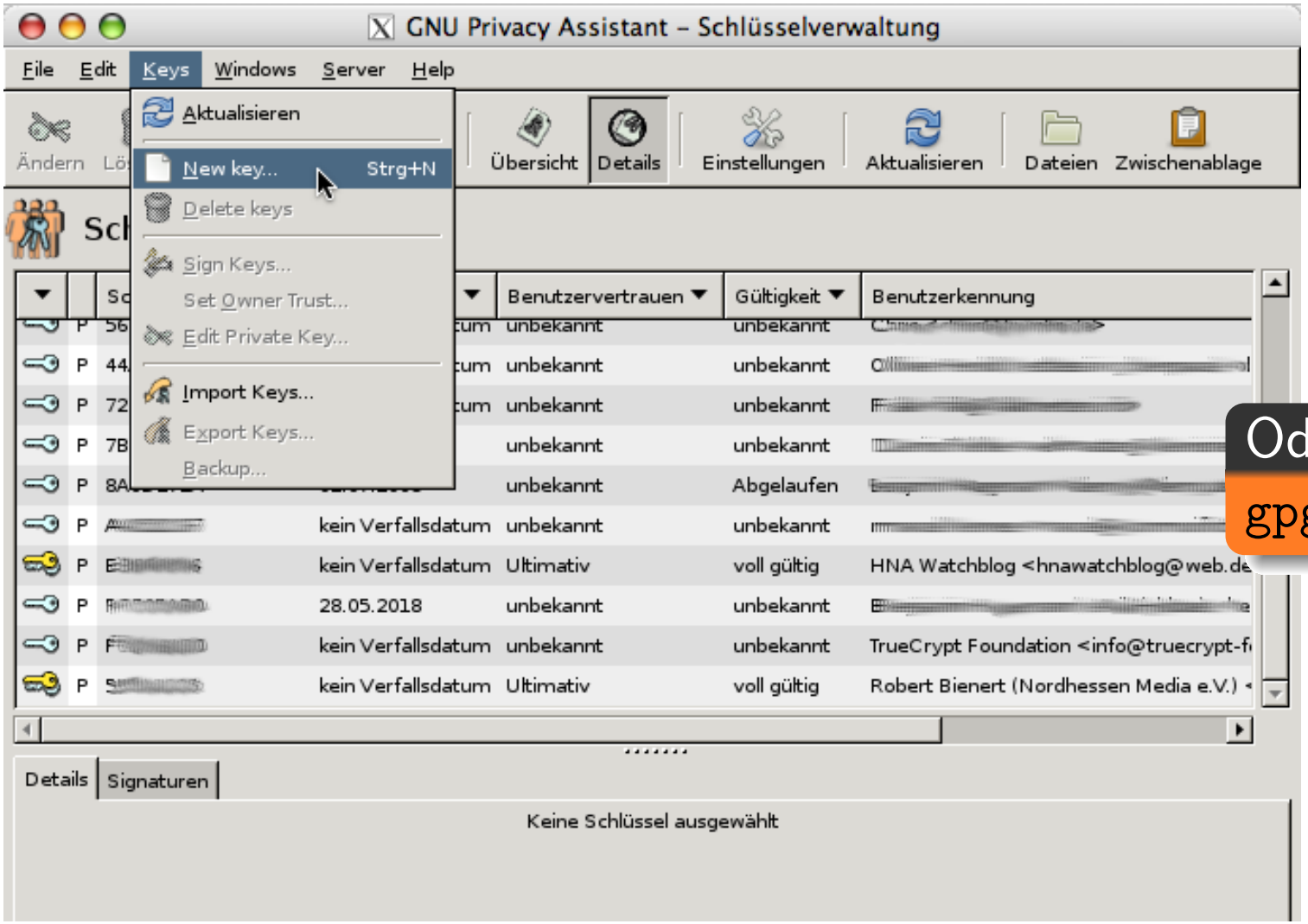
  Public-Key: Verschlüsseln, Signatur Prüfen

  Secret-Key: Entschlüsseln, Signieren

Schlüssel erzeugen



Schlüssel erzeugen



Oder:

```
gpg --gen-key
```

Schlüssel erzeugen

Wichtig:

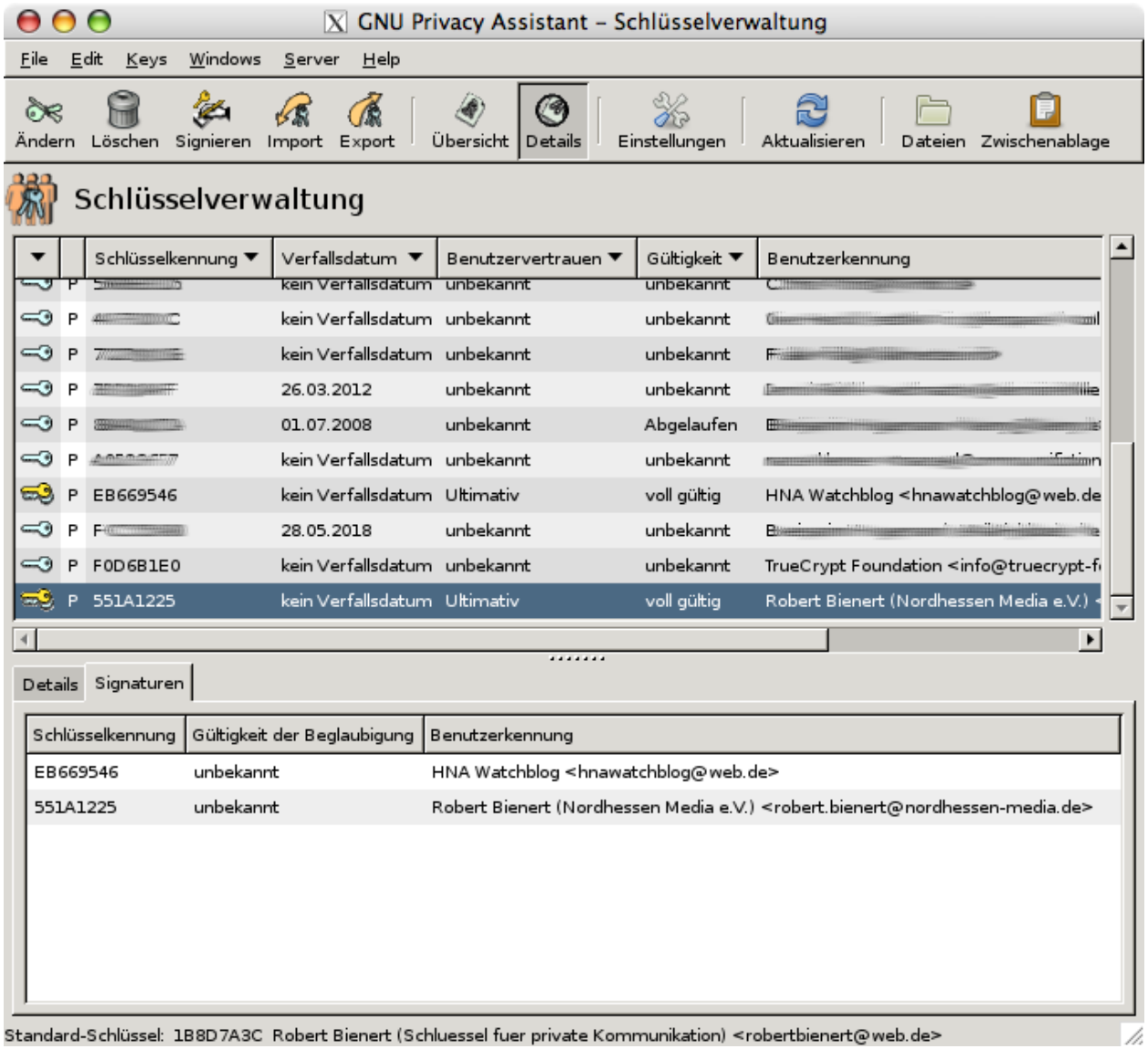
- sichere Passphrase
- langer Schlüssel
- guter Algorithmus
- Secret-Key gut und *sicher* aufbewahren

Schlüssel erzeugen

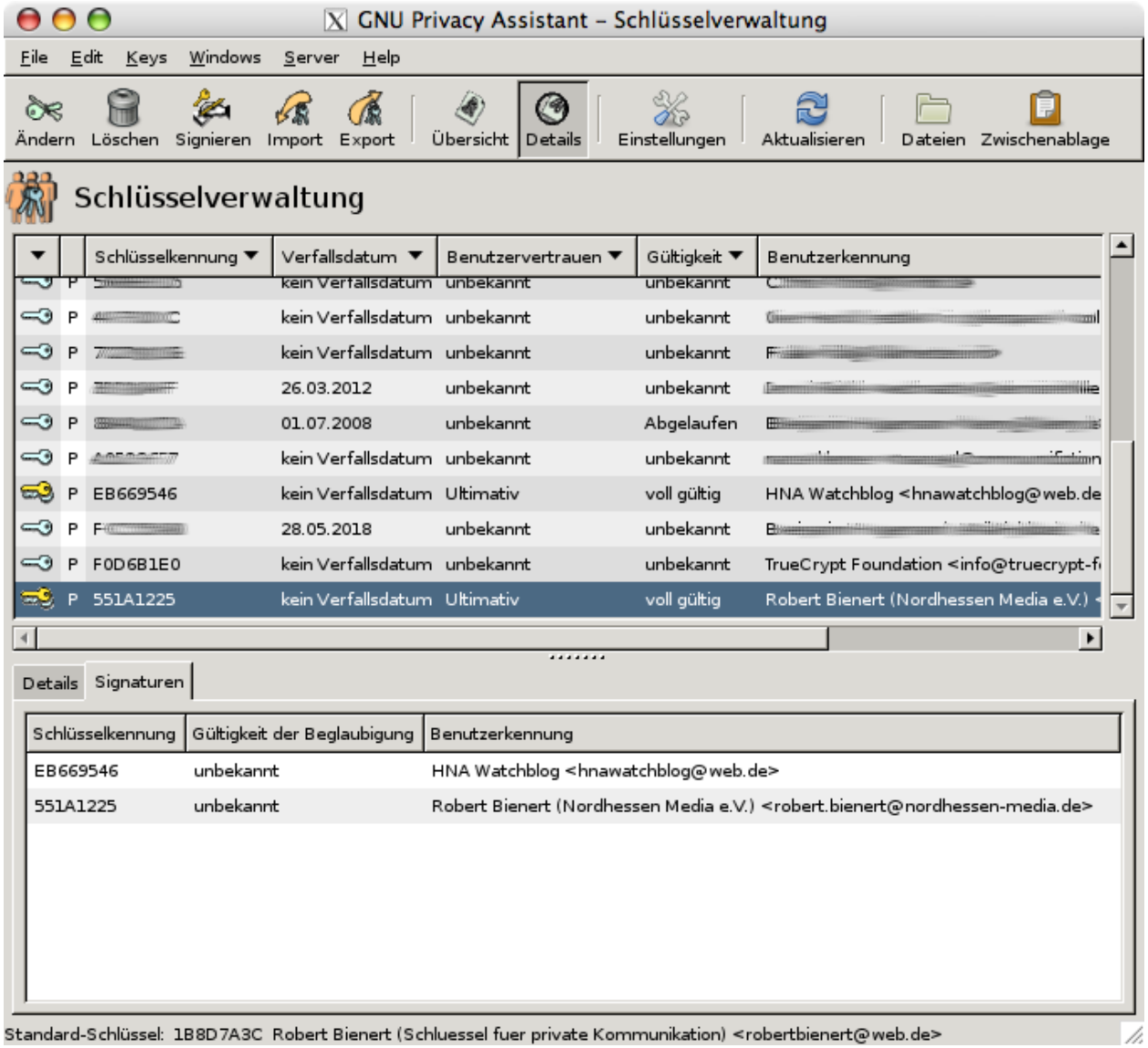
Wichtig:

- sichere Passphrase
- langer Schlüssel
- guter Algorithmus
- Secret-Key gut und *sicher* aufbewahren
- Public-Key veröffentlichen

Schlüssel verwalten

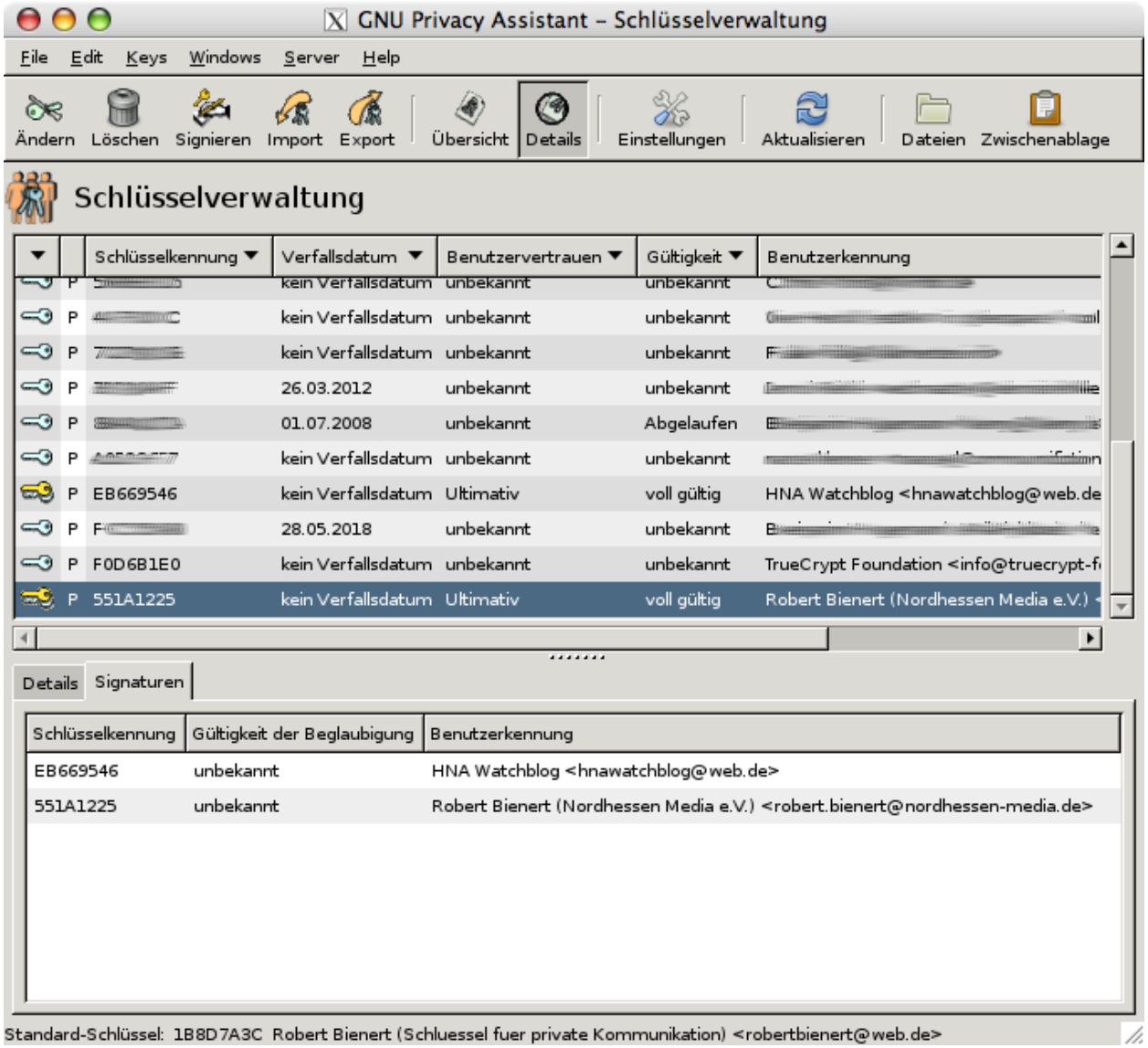


Schlüssel verwalten



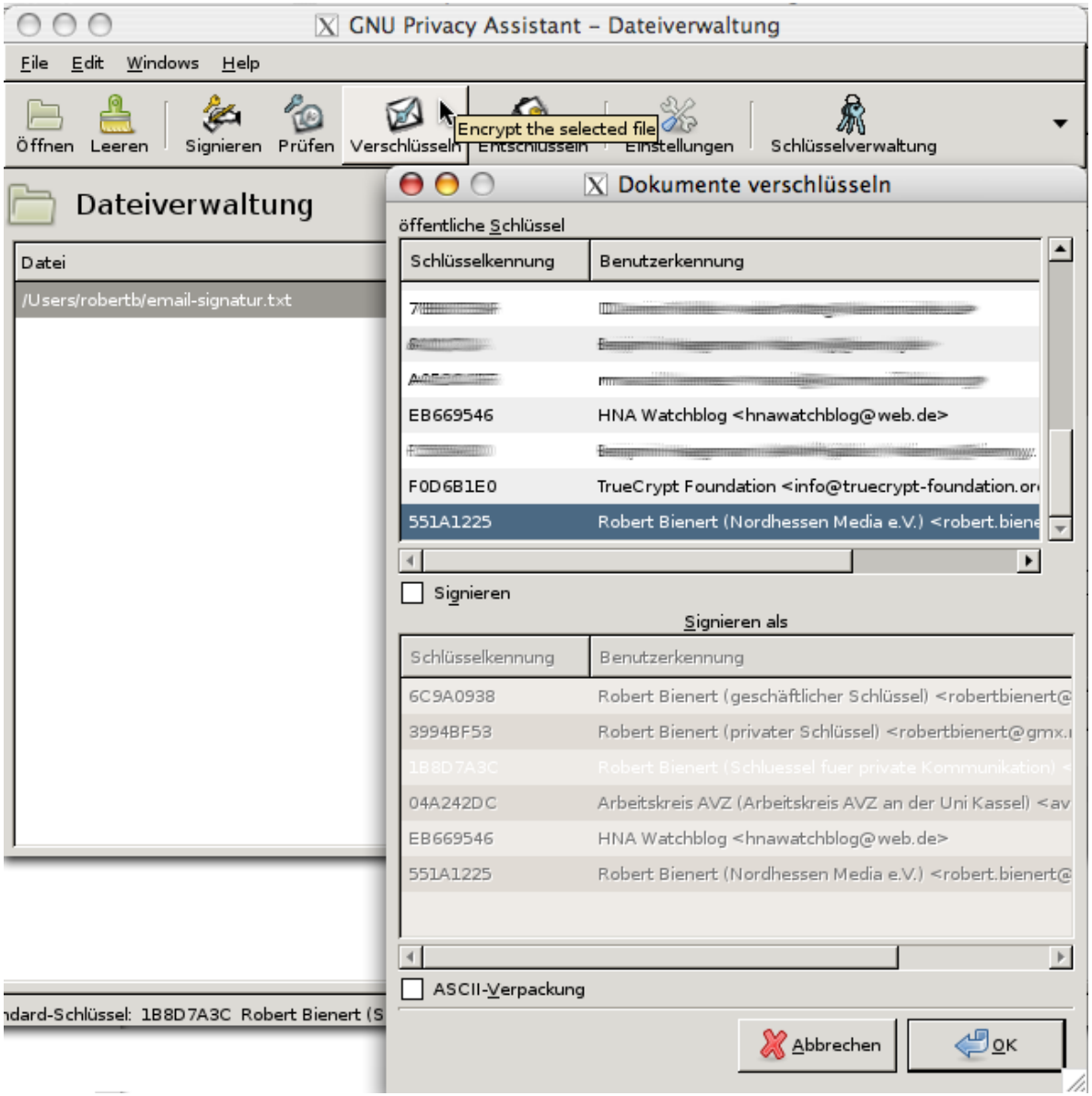
- Schlüsselring
- `gpg --list-keys`
- `gpg --edit-key`
- `gpg --sign-key`
- ...

Schlüssel verwalten

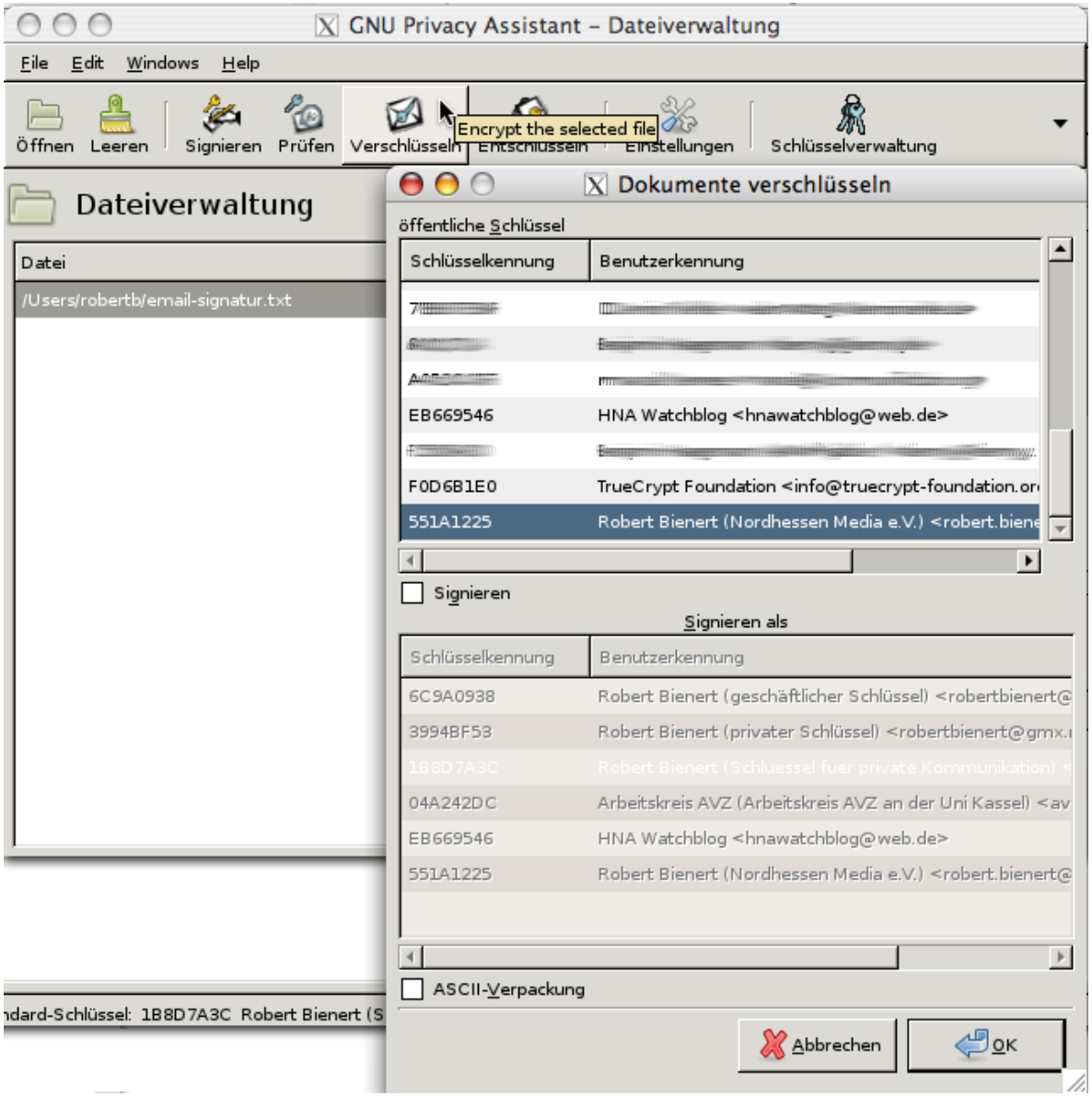


- Schlüsselring
- `gpg --list-keys`
- `gpg --edit-key`
- `gpg --sign-key`
- `...`
- *Web of Trust*

Dateien verschlüsseln



Dateien verschlüsseln



analog:

- Entschlüsseln
- Signieren

Funktionsprinzip

Verschlüsselung von

- Partitionen
- externen Datenträgern
- Teilen von Partitionen, Dateicontainer

Funktionsprinzip

Verschlüsselung von

- Partitionen
- externen Datenträgern
- Teilen von Partitionen, Dateicontainer

- mehrere Verschlüsselungsverfahren hintereinander
- Keyfiles
- transparent (beim Arbeiten)
- *Konzept der glaubhaften Abstreitbarkeit*:

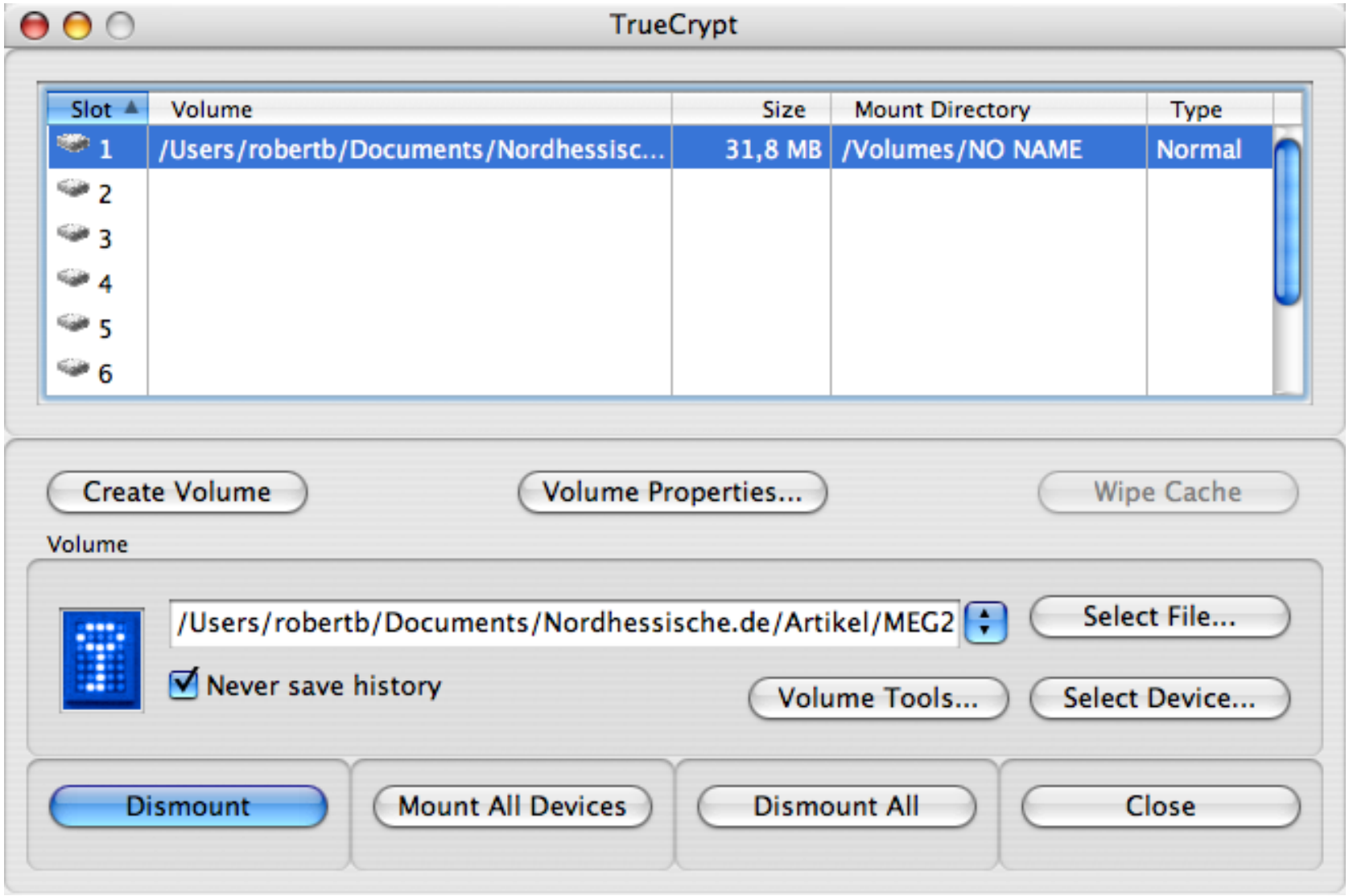
Funktionsprinzip

Verschlüsselung von

- Partitionen
- externen Datenträgern
- Teilen von Partitionen, Dateicontainer

- mehrere Verschlüsselungsverfahren hintereinander
- Keyfiles
- transparent (beim Arbeiten)
- *Konzept der glaubhaften Abstreitbarkeit*:
  - Dateien oder Partitionen nicht identifizierbar
  - versteckte Container

Datenträger-Verwaltung



SSH nur kurz

- **S**ecure **Sh**ell
- sichere und authentifizierte Remote-Verbindung
- Public-Key-Authentifizierung möglich
- Absichern beliebiger Anwendungen
- SSHFS für „entfernte Ordner“
- sicheres Kopieren von Dateien (`scp`, WinSCP, . . .)

GPG als Plug-In

Eigenschaften

- Ver- und Entschlüsseln sowie Signieren per Mausklick (Mail und Anhänge)
- Zugriff auf eigenen Schlüsselring
- automatisches Prüfen von Signaturen

GPG als Plug-In

Eigenschaften

- Ver- und Entschlüsseln sowie Signieren per Mausklick (Mail und Anhänge)
- Zugriff auf eigenen Schlüsselring
- automatisches Prüfen von Signaturen

Plug-Ins

Enigmail: Thunderbird

GPGMail: Apple Mail.app

GPG als Plug-In: GPGMail (Apple Mail.app)

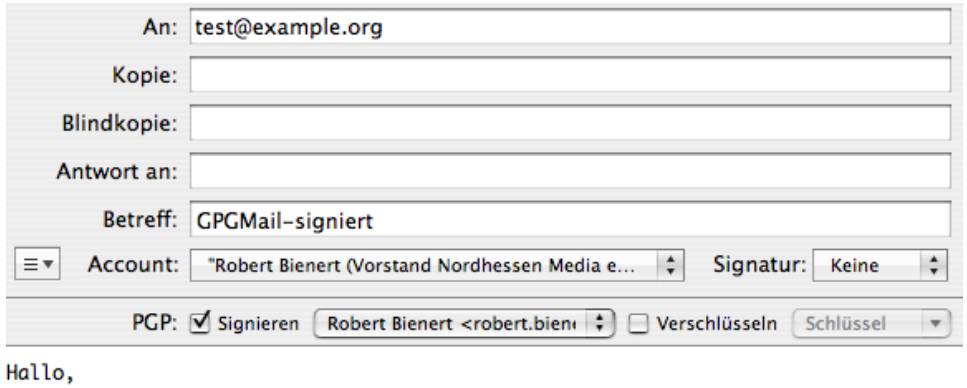


Abbildung: Signieren von Emails

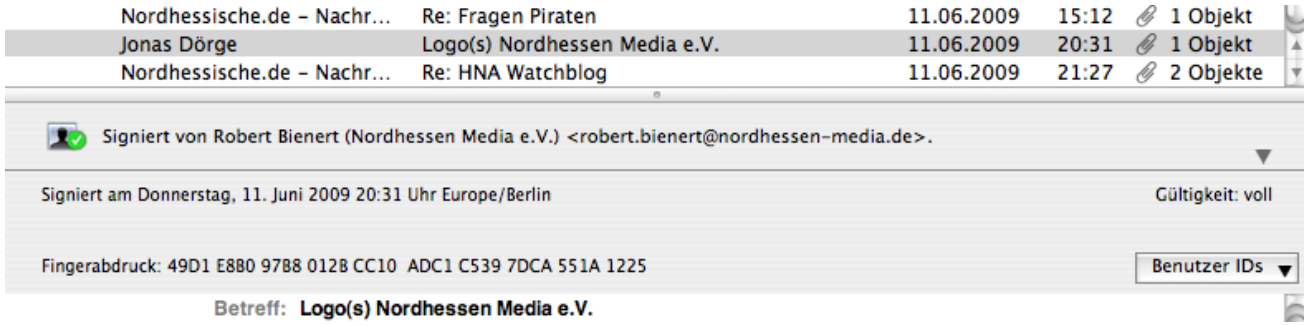


Abbildung: Überprüfen und Anzeigen einer signierten Email

- anonyme Kommunikation (z. B. TOR, Proxies, . . .)
- „tote Briefkästen“
- gemeinsames Schlüssel-Generieren und -Unterschreiben
- . . .

- anonyme Kommunikation (z. B. TOR, Proxies, . . .)
- „tote Briefkästen“
- gemeinsames Schlüssel-Generieren und -Unterschreiben
- . . .

- *dein Wunsch hier*

Referenzen


Kai Raven: *Deutsche GnuPG-Anleitung*.
Online: `http://hp.kairaven.de/pgp/gpg/index.html`, 2001.


TrueCrypt Foundation: *TrueCrypt Documentation*.
Online: `http://www.truecrypt.org/docs/`

Links

GNU Privacy Guard: `http://gnupg.org/`

Enigmail: `http://enigmail.mozdev.org/`

GPGMail: `http://www.sente.ch/software/GPGMail/`