Einführung in PGP

Auch: Einführung in OpenPGP und GnuPG

Alexander Dahl

http://www.lespocky.de/

2017-09-25

PGP

- Phil Zimmermann (1991)
- Public-Key-Verfahren: asymmetrische Verschlüsselung
- Öffentlicher Schlüssel zum Verschlüsseln und Signaturen prüfen
- Privater, geheimer Schlüssel, mit Passwort geschützt
  - Entschlüsseln
  - Signieren
- Symmetrische Verschlüsselung der Daten
- Asymmetrische Verschlüsselung der symmetrischen Schlüssel

OpenPGP und GnuPG

- Standard OpenPGP von 1998 (RFC 4880)
- GnuPG von Werner Koch (1997)
- Portierung auf Microsoft Windows vom BMWA und BMI gefördert (2001/2002)
- Standard bei Linux-Distributionen
- Verschiedene Front-Ends verfügbar

E-Mail

- Enigmail für Mozilla Thunderbird
- Plugins für viele MUAs
  - Claws Mail
  - Evolution
  - Microsoft Outlook
  - KMail
  - Mutt
  - Webmailer
- `https://emailselfdefense.fsf.org/de/`

Web of Trust

- Alice signiert den Schlüssel von Bob und vertraut Bobs Schlüsselsignaturen
- Bob signiert den Schlüssel von Carl
- Somit betrachtet Alice den Schlüssel von Carl als gültig

Web of Trust

- Alice signiert den Schlüssel von Bob und vertraut Bobs Schlüsselsignaturen
- Bob signiert den Schlüssel von Carl
- Somit betrachtet Alice den Schlüssel von Carl als gültig

- Welche Schlüssel sind vertrauenswürdig?
- Keysigning
- `https://pgp.cs.uu.nl/paths/79be3e4300411886/to/34adcd0072215cc6.html`

Debian

- Pakete
- Metadaten

Git

- Commits
- Tags
- `https://mikegerwitz.com/papers/git-horror-story`

Weitere Anwendungen

- Dateien verschlüsseln
  - pass (Passwortmanager)
- Chat
  - XEP-0027, XEP-0373, XEP-0374 für XMPP (Jabber)

Kontakt

- `http://www.lespocky.de/`
- `http://blog.antiblau.de/`
- *alex@antiblau.de*