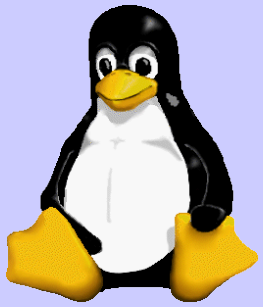
eMail-Verschlüsselung

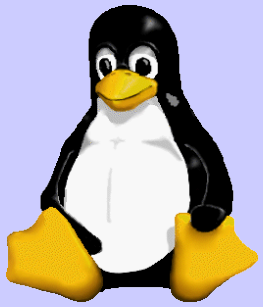
OpenPGP:

PGP & GnuPG



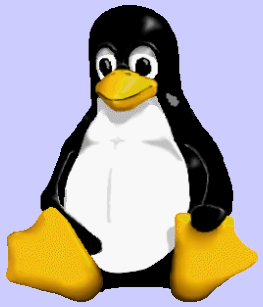
Mail-Crypto-Standards

- OpenPGP (RFC 2440)
  - offener crypto-Standard (mail/file encryption)
  - Bsp: PGP, GnuPG
- S/MIME (X.509)
  - X.509 ist ein ITU Standard
  - Bsp.: Outlook, Netscape



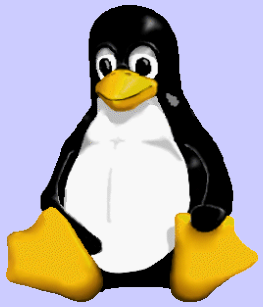
OpenPGP kann...

- Dateien und eMail :
- verschlüsseln
  - An einen oder mehrere Empfänger mit “Public Key” Kryptographie
  - Mit Passworten
- signieren
- Public Keys verwalten



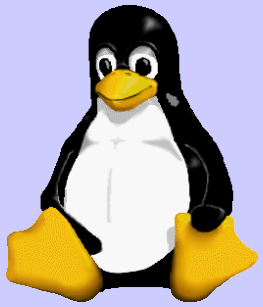
Symmetrisch...

- Symmetrische Verschlüsselung:
  - Der selbe Schlüssel wird zum ver- und ent-schlüsseln genutzt.
  - Schlüssel muss geheim gehalten werden
  - Schlüssel muss beiden Partnern bekannt sein.



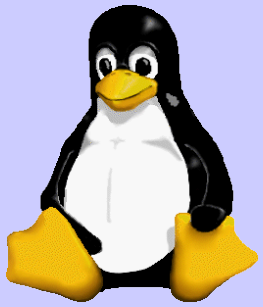
Asymmetrisch

- Asymmetrische Verschlüsselung (Public Key Verschlüsselung)
  - Zwei Schlüssel:
    - Public Key wird jedem bekannt gegeben, eignet sich nur zum Verschlüsseln
    - Secret Key muss geheim gehalten werden, eignet sich nur zum Entschlüsseln
  - Signatur:
    - Elektronische Unterschrift mit Secret Key
    - Kann mit Public Key geprüft, aber nicht gefälscht werden



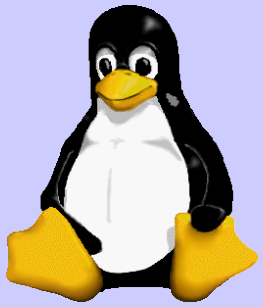
Warum der Aufwand?

- “Nur weil Du nicht paranoid bist, heißt das noch lange nicht, dass SIE Dich nicht verfolgen!”
- Jeder mit dem notwendigen Wissen kann Netzwerkverkehr mitverfolgen.
  - Email = Postkarte
- Man bedenke:
  - Warum werden Briefe in Umschläge gesteckt?
  - Warum ist Cryptographie in Diktaturen verboten?



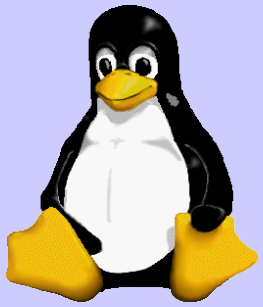
OpenPGP ist nicht:

- Firewall
- Antivirus Software
- Absicherung gegen lokale Angreifer
- Magie



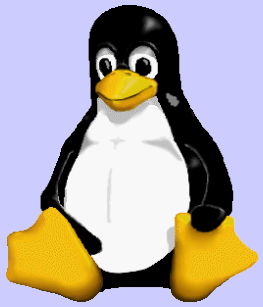
Keys

- Public Key Algorithmen:
  - RSA
  - ElGamal
  - DSA
- Ein Schlüssel enthält:
  - Key material
  - UIDs (Name + eMail-adresse)
  - Eigensignaturen
  - Signaturen



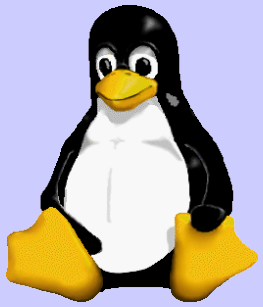
Key example

```
pub  1024D/0F4648C4 2000-05-20 Konrad Rosenbaum <konrad.rosenbaum@gmx.net>
sig         0F4648C4 2001-03-26  Konrad Rosenbaum <konrad.rosenbaum@gmx.net>
sig         98016DC7 2002-06-03  Josef Spillner <dr_maux@users.sourceforge.net>
sig         1242A6F2 2002-06-08  Simon Hausmann <hausmann@kde.org>
sig         28FA388A 2002-06-08  Matthias Kretz <kretz@kde.org>
sig         4456536A 2002-06-11  Holger Freyther (zecke) <freyther@gmx.net>
sig         0485B101 2002-06-11  Nikolas Zimmermann <wildfox@kde.org>
sig         2028C057 2002-06-10  Carsten Niehaus <cniehaus@gmx.de>
sig         30E0B9D8 2002-06-16  Ingo Klöcker <ingo.kloecker@epost.de>
sig         B3B2A12C 2002-06-26  ct magazine CERTIFICATE <pgpCA@ct.heise.de>
sig         13E290A4 2002-06-30  Eva Brucherseifer <eva@rtr.tu-darmstadt.de>
uid                              [revoked] Konrad Rosenbaum <htw6966@htw-dresden.de>
rev         0F4648C4 2002-06-10  Konrad Rosenbaum <konrad.rosenbaum@gmx.net>
sig         0F4648C4 2000-05-20  Konrad Rosenbaum <konrad.rosenbaum@gmx.net>
sig         98016DC7 2002-06-03  Josef Spillner <dr_maux@users.sourceforge.net>
```



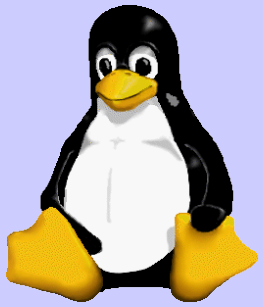
Signatures

- Eigensignatur
  - Der Besitzer des Schlüssels benutzt diese UID
- Signatur
  - Der Besitzer des signierenden Schlüssels erkennt die Verbindung zwischen Schlüssel und UID an



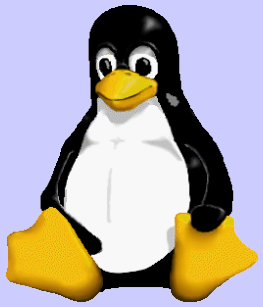
Revocation Signatures

- Eigensignatur revocation
  - Die UID wird nicht mehr benutzt, weil:
    - eMail-adresse ist ungültig
    - Der Schlüssel ist unsicher (alle UIDs werden revoziert)
    - the key has been compromised (all UIDs)
- Signatur revocation
  - Der Signierer glaubt nicht (mehr), dass die Verbindung zwischen Key und UID besteht



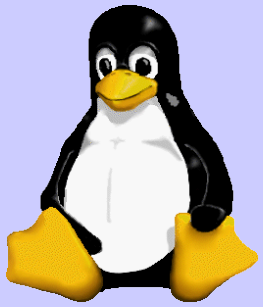
Trust/Vertrauen

- Signaturen und Identitäten werden geprüft, Vertrauen wird gegeben.
- Trust steht nicht im Schlüssel!
- Alice vertraut Bob bedeutet:
  - Alice vertraut darauf, dass alle Schlüssel und UIDs, die von Bob signiert sind korrekt sind, ohne selbst zu prüfen.



Schlüsselaustausch

- direkt: Floppy
- indirekt:
  - eMail
  - Web-seite
  - Key-Server (zB. pgp.net)
  - !der Schlüssel muss geprüft werden!



Schlüssel prüfen

- Ein Schlüssel ist identifiziert durch:
  - KeyID (zB. 0F4648C4)
  - Fingerprint (zB. B333 F8FB 644A D695 F494 7068 9BAA 4EEC 0F46 48C4)
    - MD5 (PGP2.x) or SHA-1 (neuere) Hash des key material
- Absicherung:
  1. Schlüsselbesitzer muss sich ausweisen
  2. Fingerprint vergleichen

Fragen?

?