
Hochschule Niederrhein
University of Applied Sciences

E-Mail-Verschlüsselung mit GPG. Von der Key-Erzeugung zur verschlüsselten E-Mail.

Chemnitzer Linux-Tage 2010.

13.März 2010 | Vortrag

Hochschule Niederrhein
University of Applied Sciences

Schlüssel signieren

Private Key

Key Signing Party

Key Server

E-Mail verschlüsseln

Web of Trust

Schlüsselbund

E-Mail signieren

Public Key

Verschlüsselungsverfahren

- Symetrische Verschlüsselung
  - Zum Ver- und Entschlüsseln wird der gleiche Schlüssel genutzt

- Hohe Anzahl benötigter Schlüssel (1 pro Paar)
- Problem des Schlüsselaustausches

Verschlüsselungsverfahren

- Asymmetrische Verschlüsselung
  - Verschlüsselung mit Public Key
  - Entschlüsselung mit Private Key

- Geringere Anzahl benötigter Keys (1 pro Person)
- Austausch von Schlüsseln vereinfacht

Verschlüsselungsverfahren

- **Hybride Verschlüsselung**
  - **Nachricht wird mit Zufallsschlüssel symmetrisch verschlüsselt**
  - **Schlüssel wird asymmetrisch verschlüsselt und mitgeliefert**

E-Mails verschlüsseln

Absender

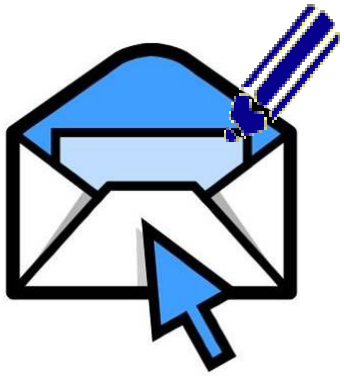
Empfänger

- Absender verschlüsselt mit Public Key des Empfängers
- Empfänger entschlüsselt mit eigenem Private Key

- Empfänger muss Private Key besitzen
- Absender muss Public Key des Empfängers haben

E-Mails signieren

Absender



Empfänger

- Absender signiert mit eigenem Private Key
- Empfänger verifiziert mit Public Key des Absenders

- Absender muss Private Key besitzen
- Empfänger muss Public Key des Absenders haben

Was braucht man für gesicherte E-Mail?

- Beide Teilnehmer der E-Mail-Kommunikation müssen einen Key besitzen

- Veröffentlicht wird nur der Public Key!
- Private Key muss geheim bleiben!

- Eigener Private Key durch „Mantra“ geschützt
  „Mantra“ ist die „Schwachstelle des Systems“, kann aber sehr lang sein

Verwaltung von Schlüsseln

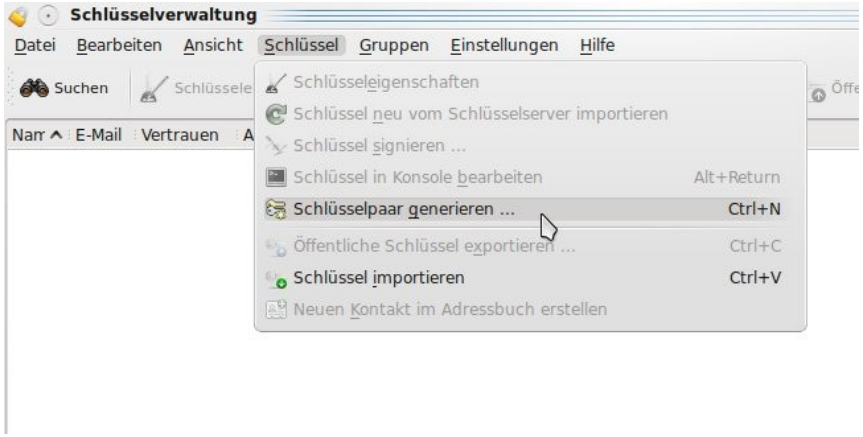
- Verwaltung der Keys im Schlüsselbund
- Steuerung über Kommandozeile oder grafische Tools

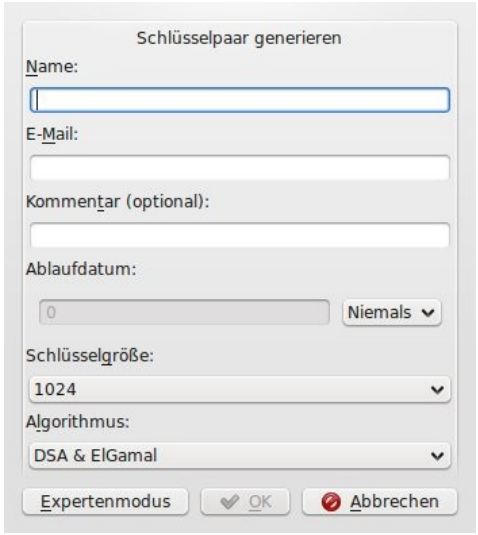
- Besteht aus
  - Eigenem Schlüssel (privat und öffentlich)
  - Fremden Schlüsseln (öffentliche)
  - Angaben zu Vertrauen und Gültigkeit

Einen Key erzeugen

- **Kommandozeile mit gpg**
  gpg --gen-key
  Schritt-für-Schritt geführte Erzeugung des Keys

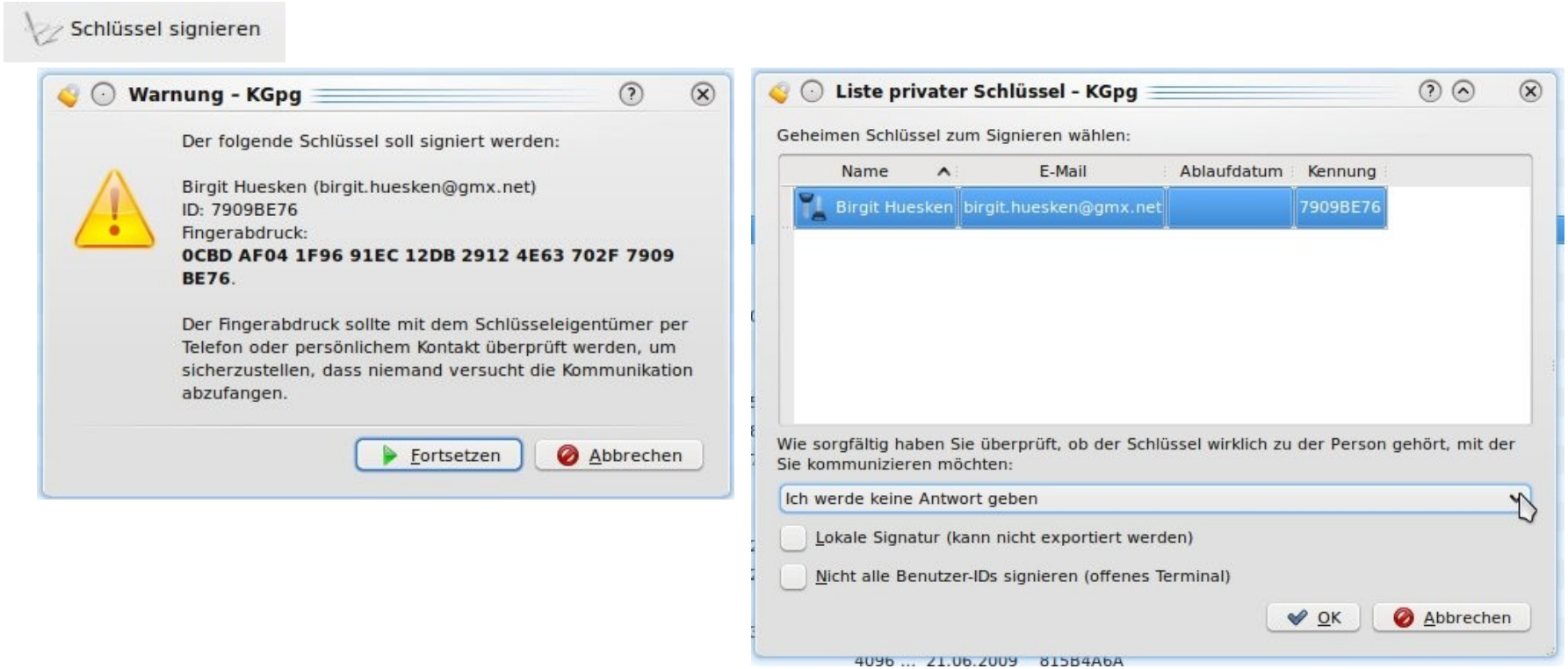
- **Grafische Tools, z.B. KGpg**





Was dann?

- **Schlüssel selbst signieren, um Echtheit des Schlüssels sicherzustellen**
  gpg --edit-key Key-ID sign

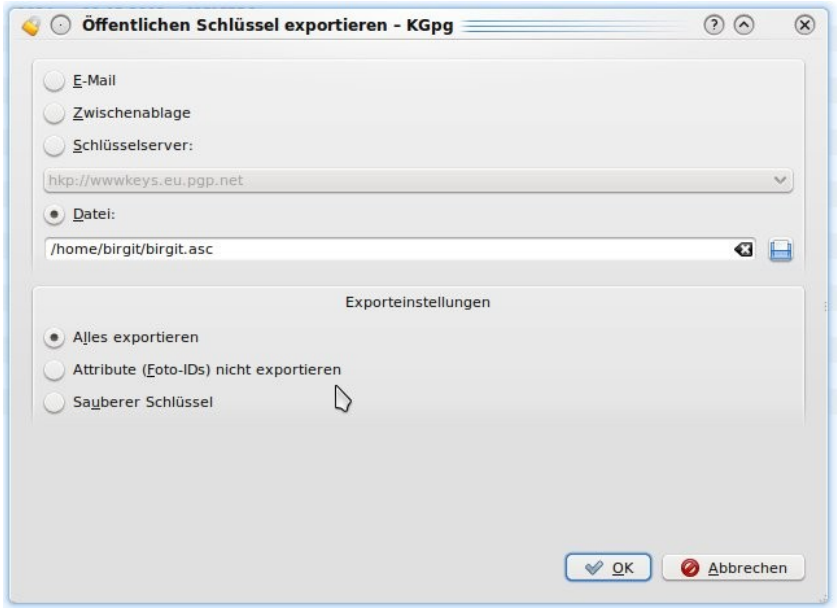


Was dann?

- **Schlüssel selbst signieren, um Echtheit des Schlüssels sicherzustellen**
- **Widerrufsurkunde erstellen**
  gpg --output revoke.asc --gen-revoke Key-ID

Was dann?

- **Schlüssel selbst signieren, um Echtheit des Schlüssels sicherzustellen**
- **Widerrufsurkunde erstellen**
- **Key exportieren**
  gpg --armor --export Key-ID



Was dann?

- Schlüssel selbst signieren, um Echtheit des Schlüssels sicherzustellen
- Widerrufsurkunde erstellen
- Key exportieren
- Fingerprint und Key-ID bekannt machen

Einen Key veröffentlichen

- Persönliche Weitergabe
- Veröffentlichung auf eigener Homepage, als Text oder Download
- Auf Key-Servern, z.B.
  - wwwkeys.de.pgp.net
  - wwwkeys.eu.pgp.net
  - gpg-keyserver.de

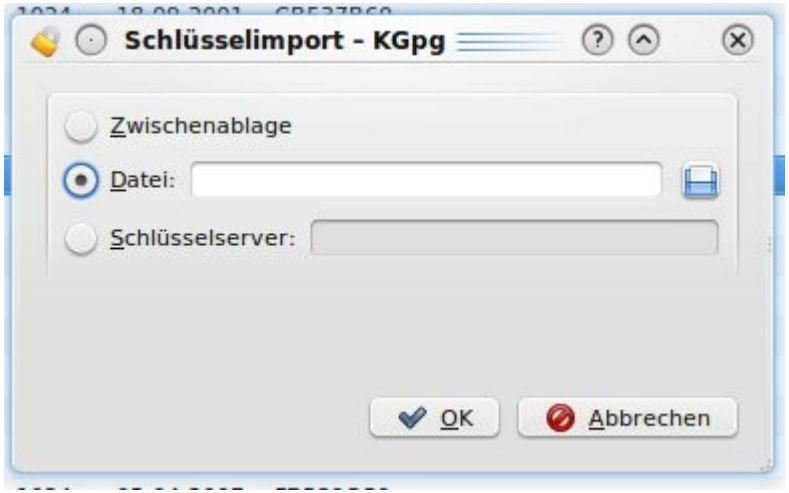
  Die Keyserver synchronisieren sich untereinander!

Andere Keys suchen, finden und importieren

- **Suche nach Key-ID oder nach Namen auf Keyservern**

- **Direkter Import von persönlich erhaltenen oder von Webseiten importierten Keys**
  gpg --search-keys Key-ID
  gpg --recv-keys Key-ID

  gpg --import Key-File



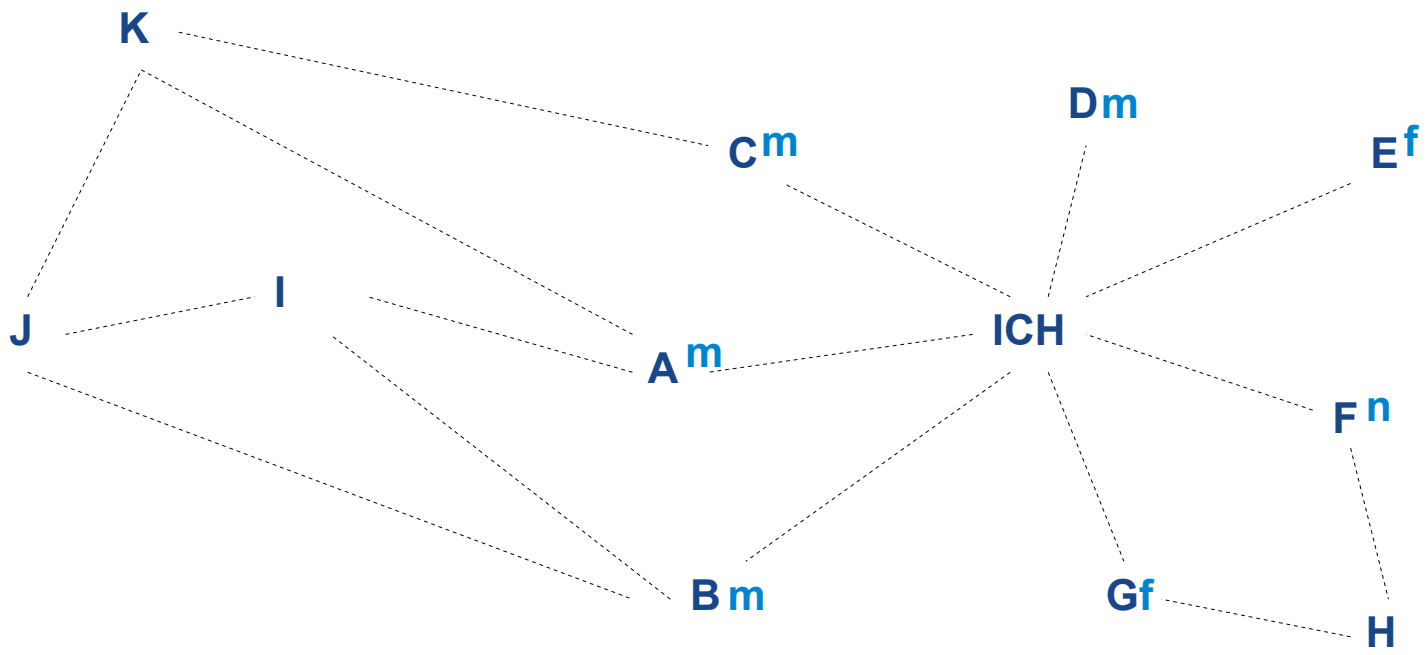
Das „Web of Trust“

- Importierte Schlüssel können signiert werden

- Jedem Schlüssel kann eine (Eigentümer-)Vertrauensstufe zugewiesen werden:
  - Unbekannt (q)
  - Kein Vertrauen (n)
  - Teilweises Vertrauen (m)
  - Volles Vertrauen (f)

- Davon abhängig ist das Vertrauen in den Schlüssel selbst
  Vertrauen ist vollständig, wenn
  - Der Schlüssel selbst ***oder***
  - Von einem Schlüssel vollsten Vertrauens ***oder***
  - Von min. 3 Schlüsseln teilweisen Vertrauens unterzeichnet wurde **und**
  - Die so entstandene Kette nicht zu lang ist (5 Schritte)

Das „Web of Trust“



Andere Keys signieren

- **Wichtig!** Eigentümer authentifizieren
  - Über Fingerprint
  - Über Ausweisdokumente

  z.B. bei Key-Signing-Partys

- Signierten Key an Eigentümer zurückgeben

  Veröffentlichung sollte durch Eigentümer selbst erfolgen!

E-Mails verschlüsseln und signieren

- Text auf Kommandozeile verschlüsseln und als E-Mail versenden

- Verschiedene Hilfsprogramme zur Signierung und Verschlüsselung, z.B.
  - Kmail / Kontact (KDE) → Kgpg
  - Gnome → Seahorse
  - Thunderbird → enigmail
  - Div. Webmailer → Browser Add-Ons, wie FireGPG für Firefox

Fragen? Anmerkungen?

Danke für die Aufmerksamkeit!

Folien bei Slideshare
http://www.slideshare.net/birgithuesken

Impressum

Birgit Hüsken
HS Niederrhein
KIS – IT Servicemanagement
Reinarzstr.49
47805 Krefeld

E-Mail birgit.huesken@hs-niederrhein.de
Tel. +49-2151-822-3225
Fax +49-2151-822-85-3225


Hochschule Niederrhein
University of Applied Sciences