PGP (Pretty Good Privacy) Eine praktische Einführung in die Signierung und Verschlüsselung von Email

- Public Key Kryptographie
  - ⋆ Was bietet PGP
  - ⋆ Symetrische Verschlüsselung $\leftrightarrow$ Public Key Verschlüsselung
  - ⋆ Verschlüsseln/Signieren mit Public Keys
- PGP im Einsatz
  - ⋆ Schlüssel erzeugen
  - ⋆ Schlüsselverwaltung – Der Keyring
  - ⋆ Texte signieren/Verschlüsseln
  - ⋆ Signaturen checken
  - ⋆ Schlüssel invalidieren

PGP (Pretty Good Privacy) Eine praktische Einführung in die Signierung und Verschlüsselung von Email

- Schlüssel Signaturen
  - ⋆ Wieso müssen Schlüssel signiert werden
  - ⋆ Web of Trust
  - ⋆ Signing Parties
  - ⋆ CAs
- PGP Versionen und Plugins
- Software und Literatur

Was bietet PGP

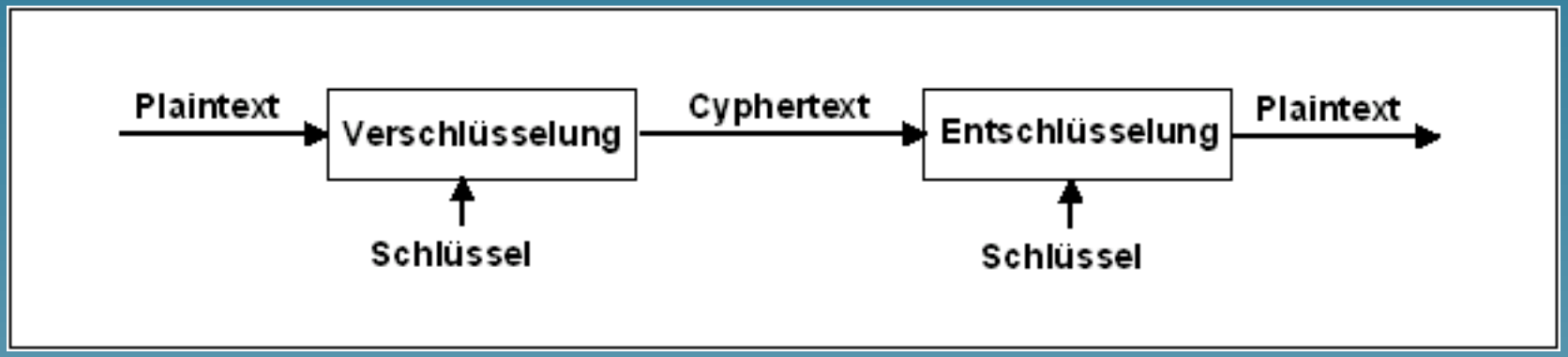
PGP bietet unter Zuhilfenahme von Public Key Kryptographie:

- Verschlüsselung von Daten.
- Digitale Unterschriften unter Dokumenten sog. digitale Signaturen zum Herkunftsnachweis und zur Verhinderung von Fälschungen.
- Schlüsselverwaltung der Schlüssel die zur Verschlüsselung und für Signaturen benötigt werden.

Das Schlüsselproblem

Arbeitsweise symetrischer Verschlüsselungsverfahren:

- Verschlüsseln/Entschlüsseln



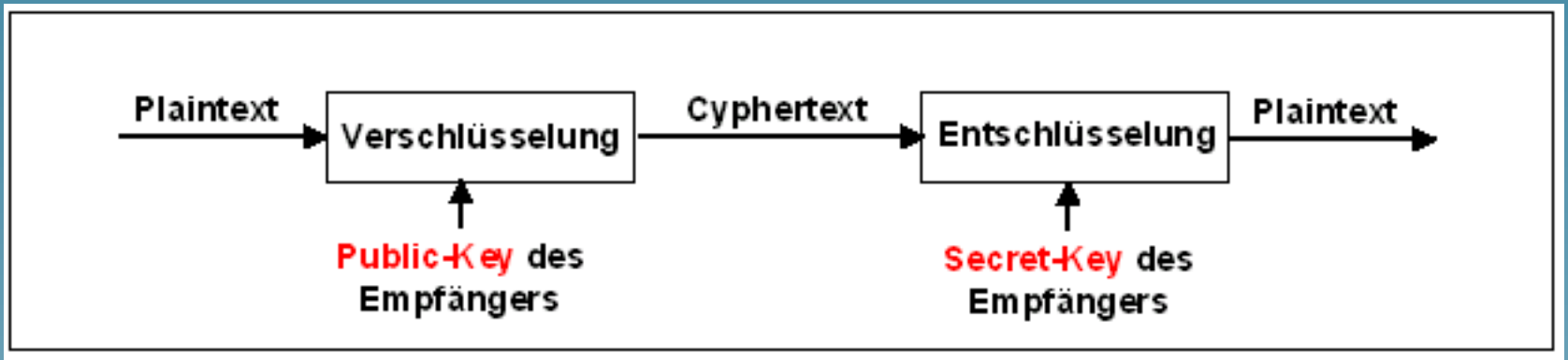
- „Normale“, symetrische Verschlüsselungsverfahren (wie z.B. DES, IDEA, Blowfish. . .) benutzen nur einen Schlüssel zum Ver- und Entschlüsseln.

- Wie wird nun der Schlüssel zum Partner transferiert, so daß er nur dem Partner bekannt wird?

Public Key Kryptographie (1)

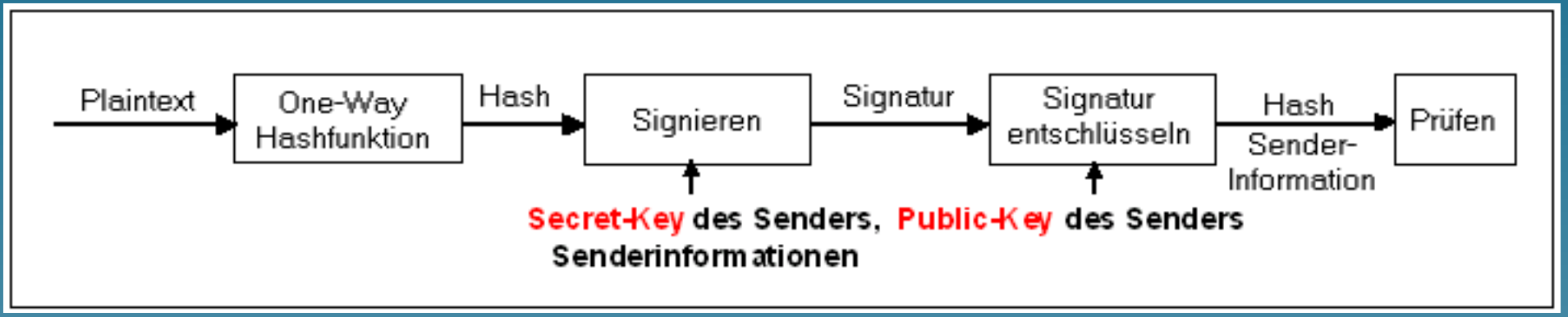
- Public Key Kryptographie arbeitet mit zwei Schlüsseln:
  - ⋆ Einem Public Key der veröffentlicht wird
  - ⋆ Einem Secret Key den nur die verschlüsselnde Partei besitzt

- Verschlüsseln:



Public Key Kryptographie (2)

- Signieren:



- Die digitale Signatur enthält eine Checksumme (One–Way Hash) der signierten Daten, Informationen über den Signierer (Name, EMail) und eine Erstelldatum.
- Diese Daten können nur mit dem richtigen Public Key entschlüsselt werden.
- Mit Hilfe der Checksumme kann die Authentizität der signierten Daten sichergestellt werden.
- Der Signierer ist die Person, die den passenden Secret Key besitzt.

Erzeugen eines Schlüssels mit PGP (1)

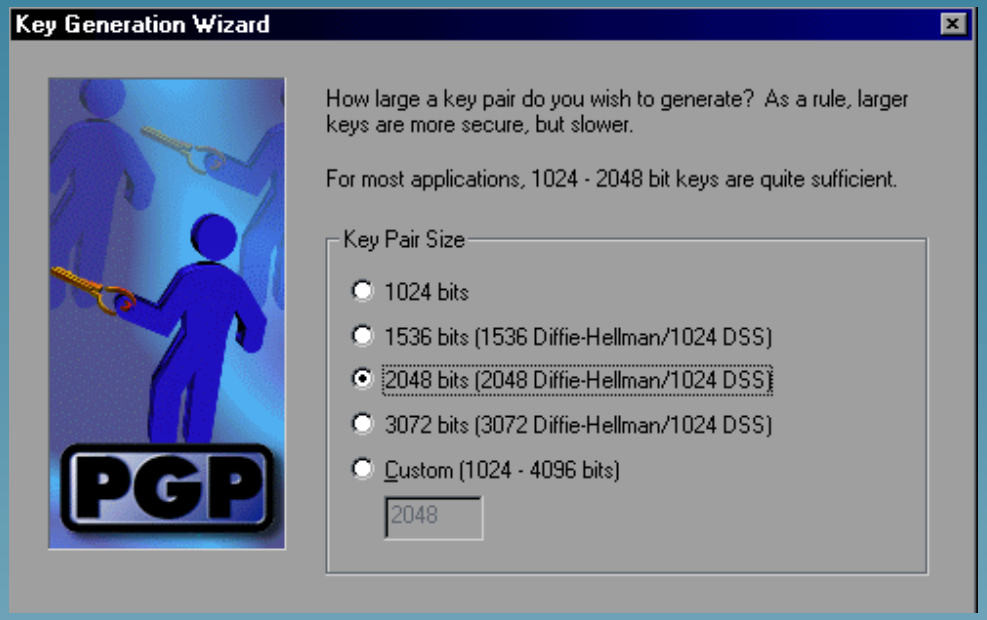
- Der Schlüssels enthält Name und Email–Adresse des Schlüsselbesitzers. Diese bilden die UserID.

Erzeugen eines Schlüssels mit PGP (2)

- PGP ab Version 5 unterstützt zwei zueinander inkompatible Schlüsselformate:
  - ⋆ Diffie Hellman/DSS mit einermn DSS (Digital Signing Standard) Signingkey und einen ElGamal Verschlüsselungskey.
  - ⋆ und das alte RSA–Format der Version 2.

Erzeugen eines Schlüssels mit PGP (3)

- Schlüssel mit ≥ 1024 bits gelten momentan als sehr sicher.
- Je länger der Schüssel, desto schwerer zu knacken und um so größer der Aufwand der Verschlüsselung.

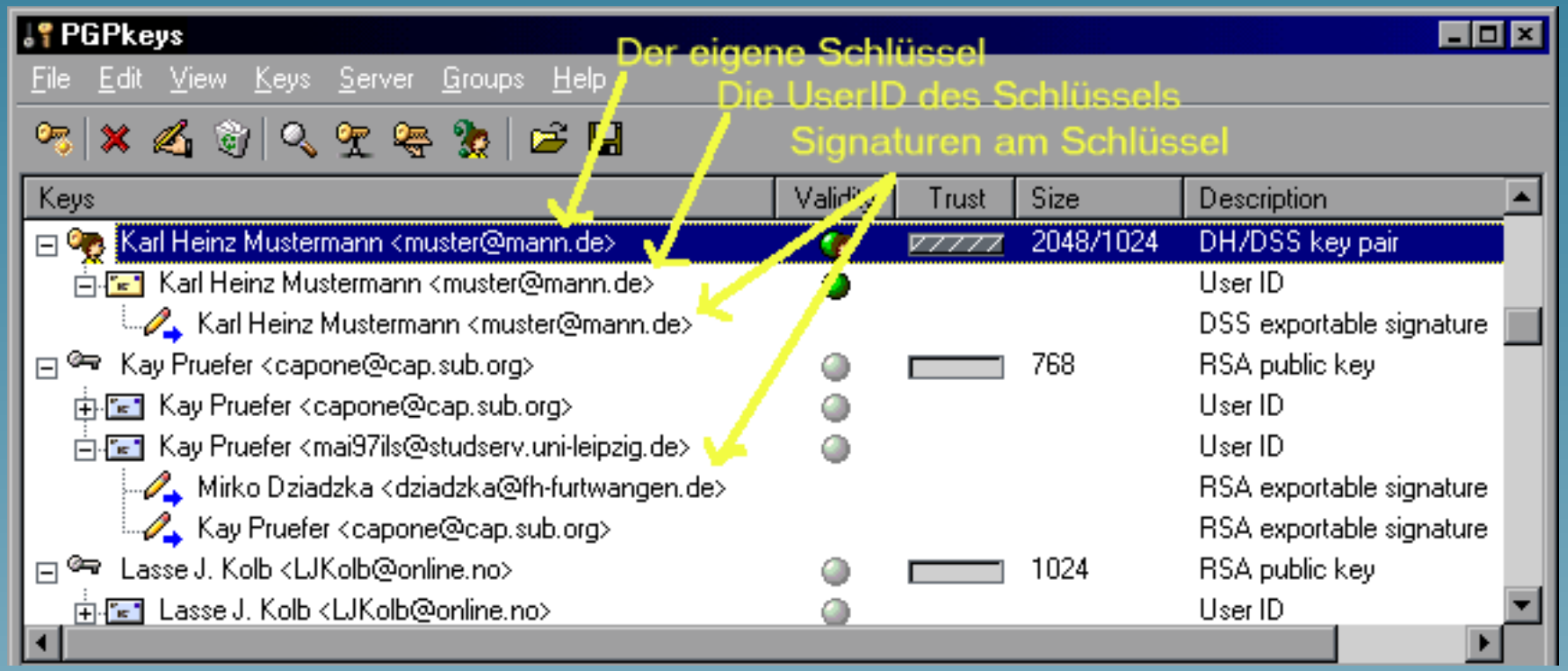


Erzeugen eines Schlüssels mit PGP (4)

- Der Secret Key wird mit einer Passphrase (Passwort) vor Mißbrauch geschützt.
- Die Passphrase sollte lang sein damit sie schwer zu erraten ist.

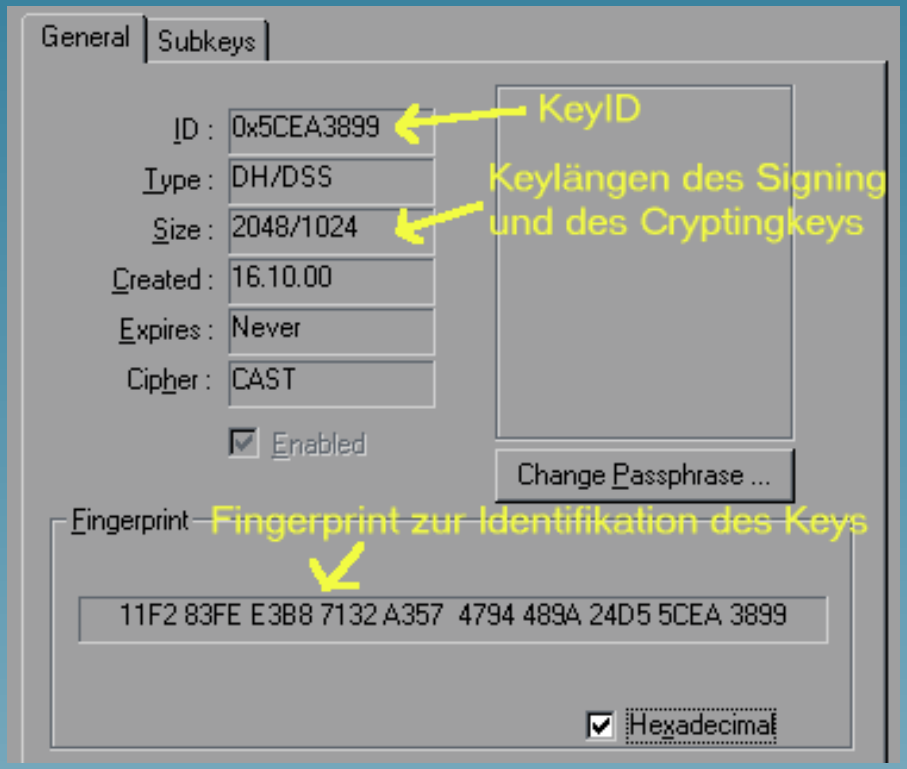
Der Keyring (1)

- Zur Verschlüsselung wird der Schlüssel des Empfängers benötig. PGP verwaltet Schlüssel in einem sog. Keyring.
- Auch der eigene Schlüssel wird in diesem Keyring verwaltet.
- PGP besitzt einen Public Keyring und einen Secret Keyring.



Der Keyring (2)

- Die einzelnen Schlüssel können im Detail betrachtet werden.
- Zur Identifizierung des Schlüssels werden Schlüssellänge und Fingerprint benötigt.



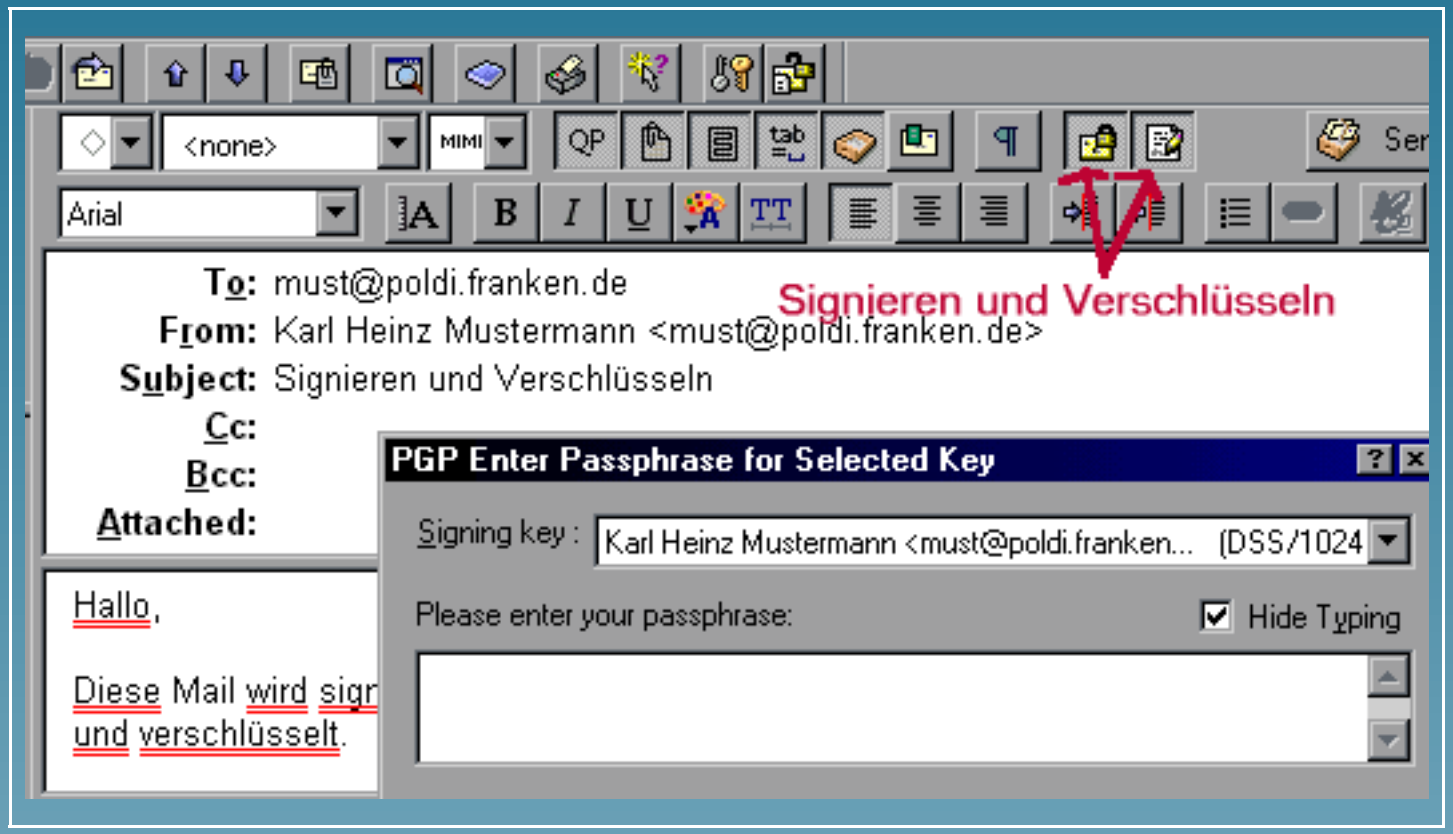
Der PGP Public Key

- Soll der Public Key verschickt werden werden, so muß er zuerst exportiert werden.
- Der Schlüssel wird im ASCII–Format (Base64–Encoding) weitergereicht.
- Ein exportierter Schlüssel hat folgendes Aussehen:

```
Type Bits/KeyID    Date       User ID
pub  1024/6969FA2D 2000/10/23 Karl Heinz Mustermann <muster@mann.de>
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i
mQCNAzn0SPkAAAEEAM8WO8a5At0Zm+1IZjoeHszPnD1CRlcHbobozsXWREkEBuGc
jiD+P8p3Ew09M441XsVDwBucegtAhqc0+ReAp2Xw503wUDIdUumVeZVM/nLoXIN5
dYQJVAE0UWBJTH1F1MSoP7mZSrbMm8sLgzQr1CNcfST7iMWR9DVmldBpafotAAUR
-----END PGP PUBLIC KEY BLOCK-----
```

Signieren mit Eudora

- Die meisten Email Programme besitzten PGP Unterstützung.
- Signaturen werden ASCII codiert im Base64 Format an die Mail angehängt.



- Beim Signieren wird nach der Passphrase gefragt. Beim Verschlüsseln muß der Schlüssel des Empfängers aus dem Keyring ausgewählt werden.

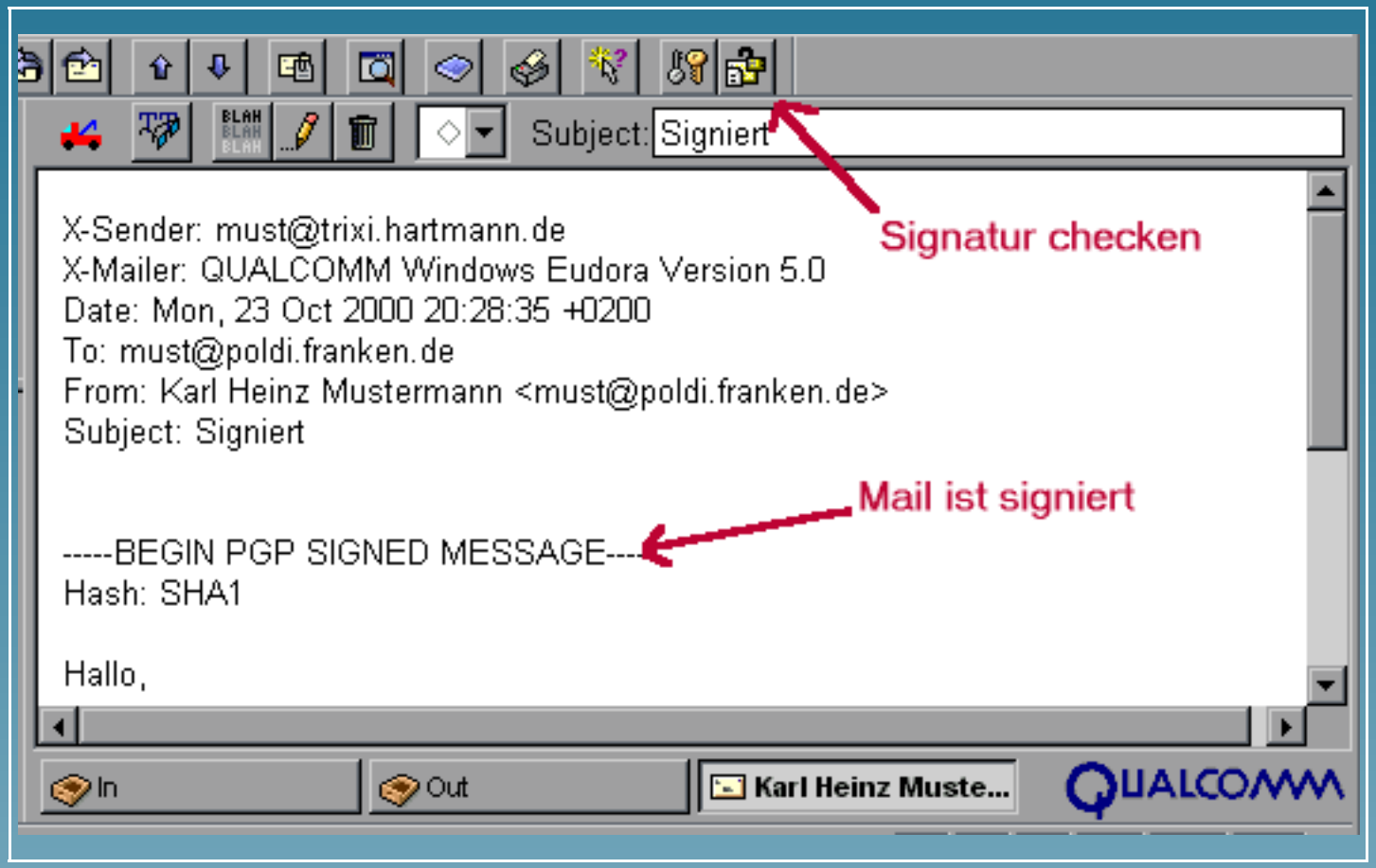
Signieren

- Die Signatur wird dem Text angehängt. Die Signatur kann auch vom Text getrennt werden (detatched Signature).
- Die Signatur wird von PGP in `BEGIN PGP SIGNED MESSAGE/END PGP SIGNATURE` eingefasst. Sie kann auch als Attachement vorliegen.

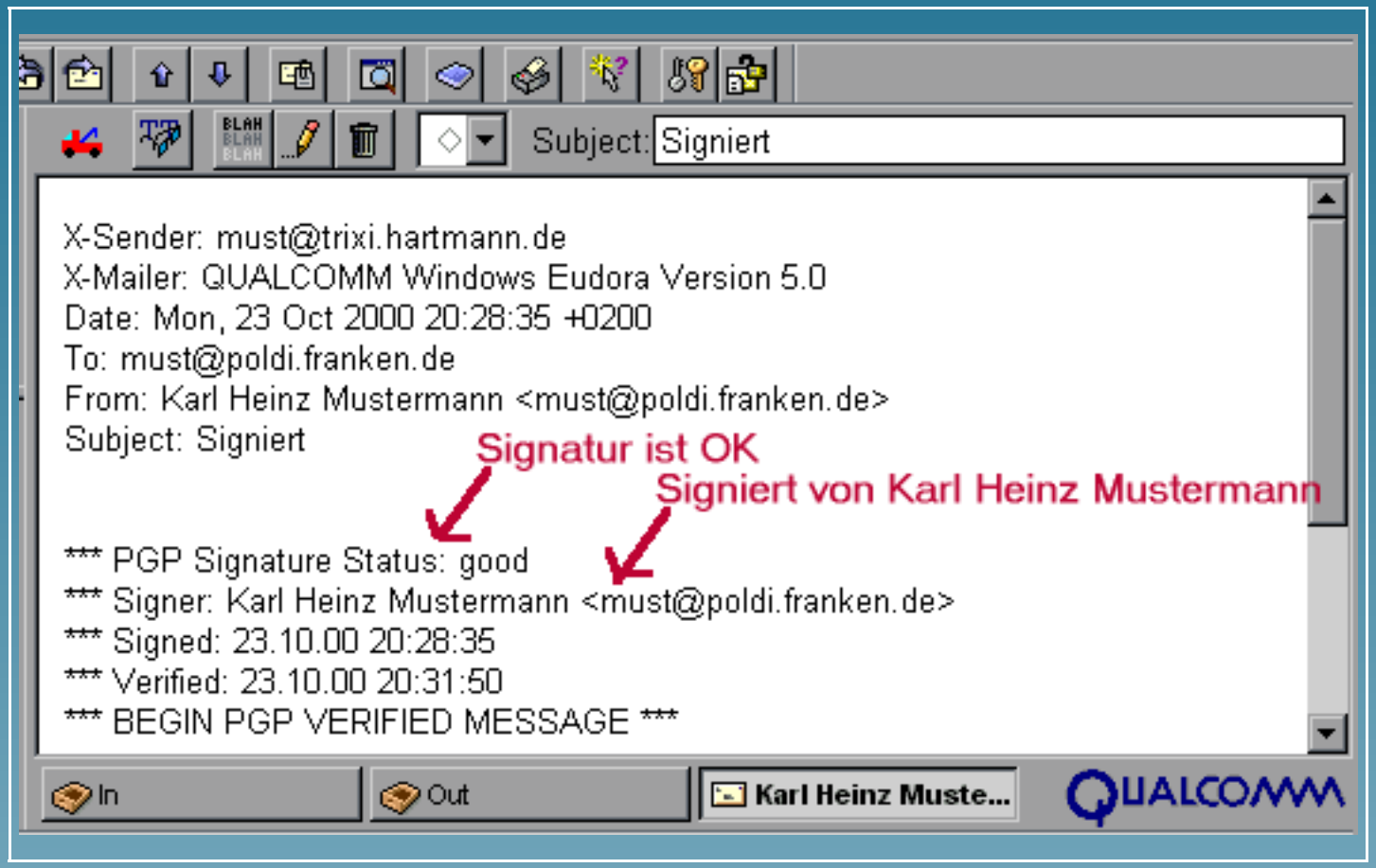
Mail mit Signatur:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hallo,
Dies ist eine Testmessage.
cu Karl
-----BEGIN PGP SIGNATURE-----
Version: 2.6.3i
Charset: noconv
iQCVAwUBOfiGPaj4ha4jWKV1AQFsCAP/ec5Rgb73mgf+UPaUZ5OnkDWPvOxEuXQd
7UMD97tWX/SQZOT4bacoaVy0Jw/fPsxL0dhfG4pedg6suxtutVAo27D3WFNNMAlu
=3itF
-----END PGP SIGNATURE-----
```

Signatur überprüfen (1)

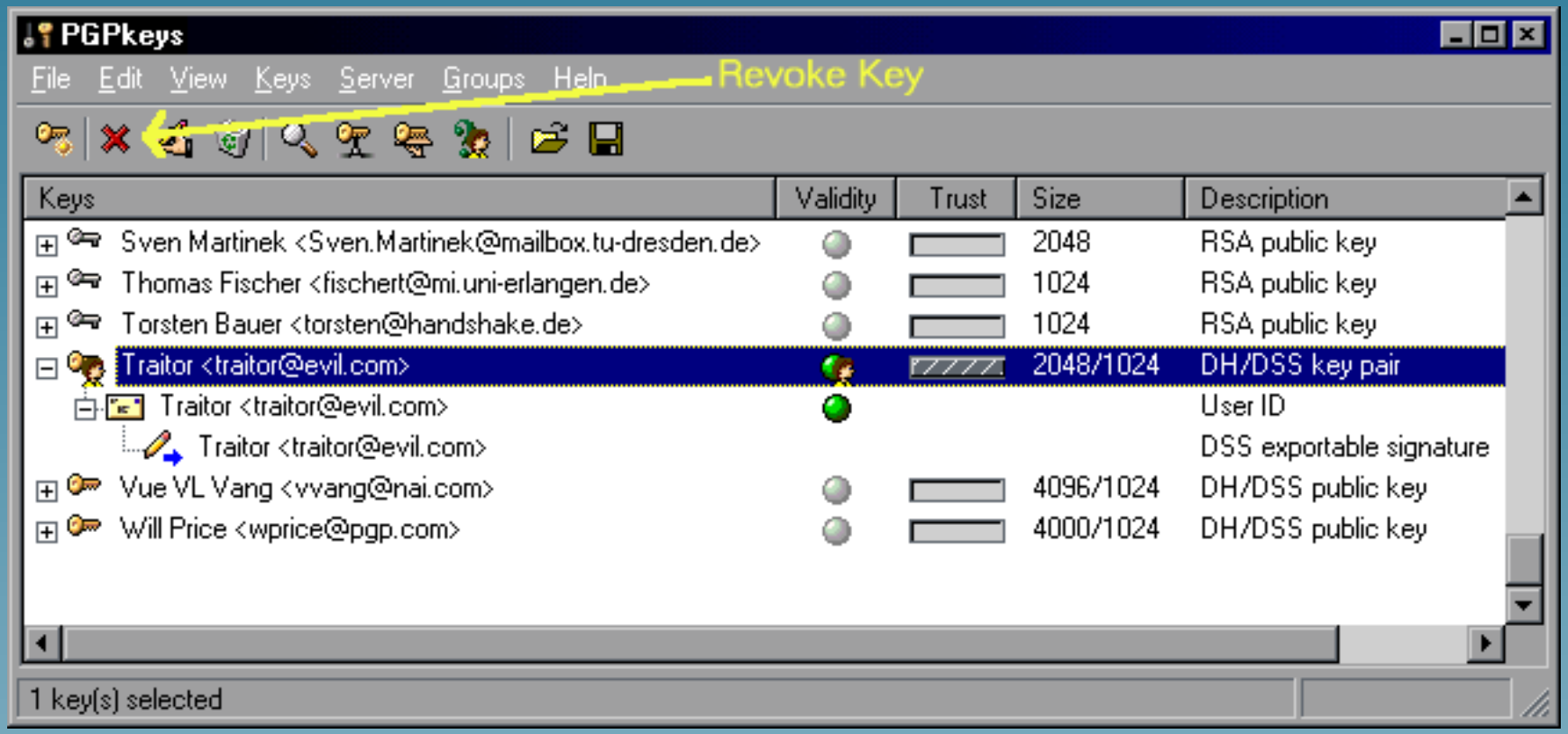


Signatur überprüfen (2)



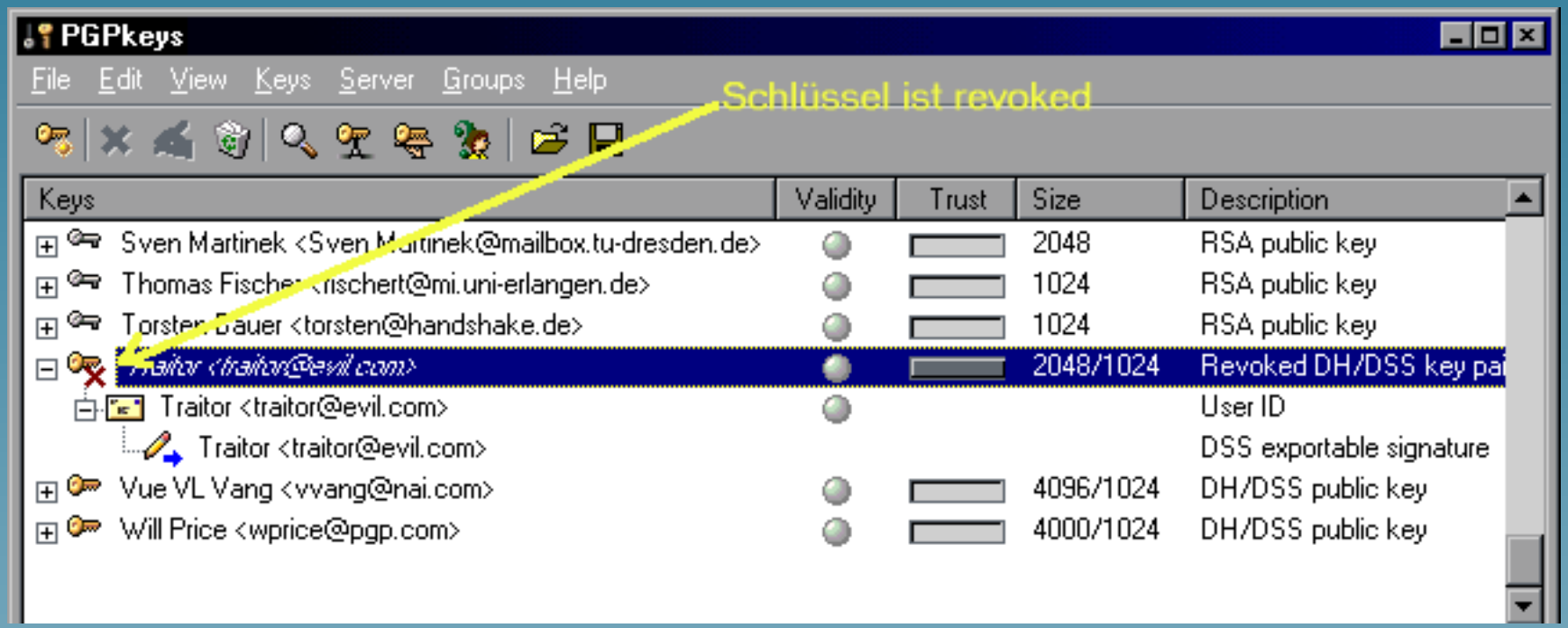
Schlüssel invalidieren (1)

- Soll ein Schlüssel nicht mehr eingesetzt werden oder wurde er korrumpiert, so kann er invalidiert (das sog. Keyrevoking) werden.



Schlüssel invalidieren (2)

- Der Schlüssel wird als revoked markiert. Er kann nicht mehr reaktiviert werden.
- Der orginale Schlüssel muß auf allen Keyservern durch den revoked–markierten ersetzt werden.



PGP Public–Keyserver

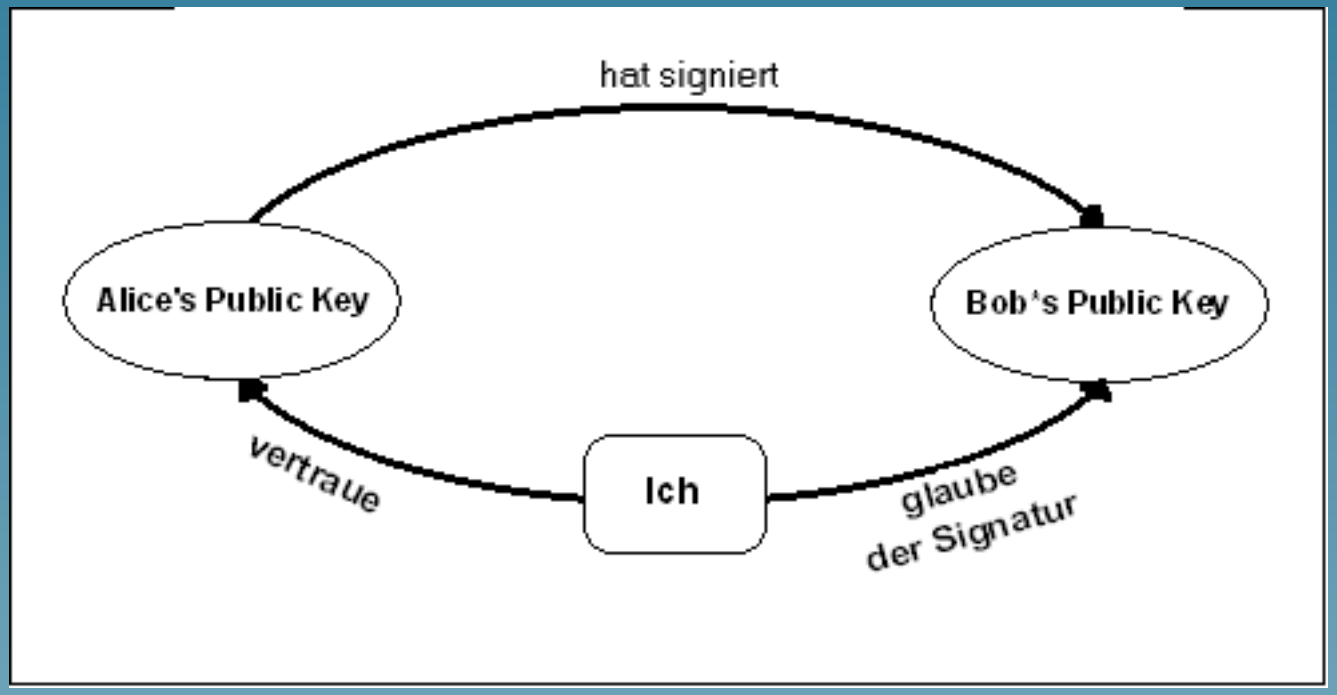
- Public Keys bekommt man im Internet von sog. PGP Public–Keyservern.
- Keyserver sind per Web, Email oder LDAP zu erreichen.
- Kleine Auswahl an Keyservern:
  - *http://www.keyserver.net*
  - *http://math-www.uni-paderborn.de/pgp*
  - *http://www.openpgp.net/pgpsrv.html*

Das Schlüsselproblem bei PGP

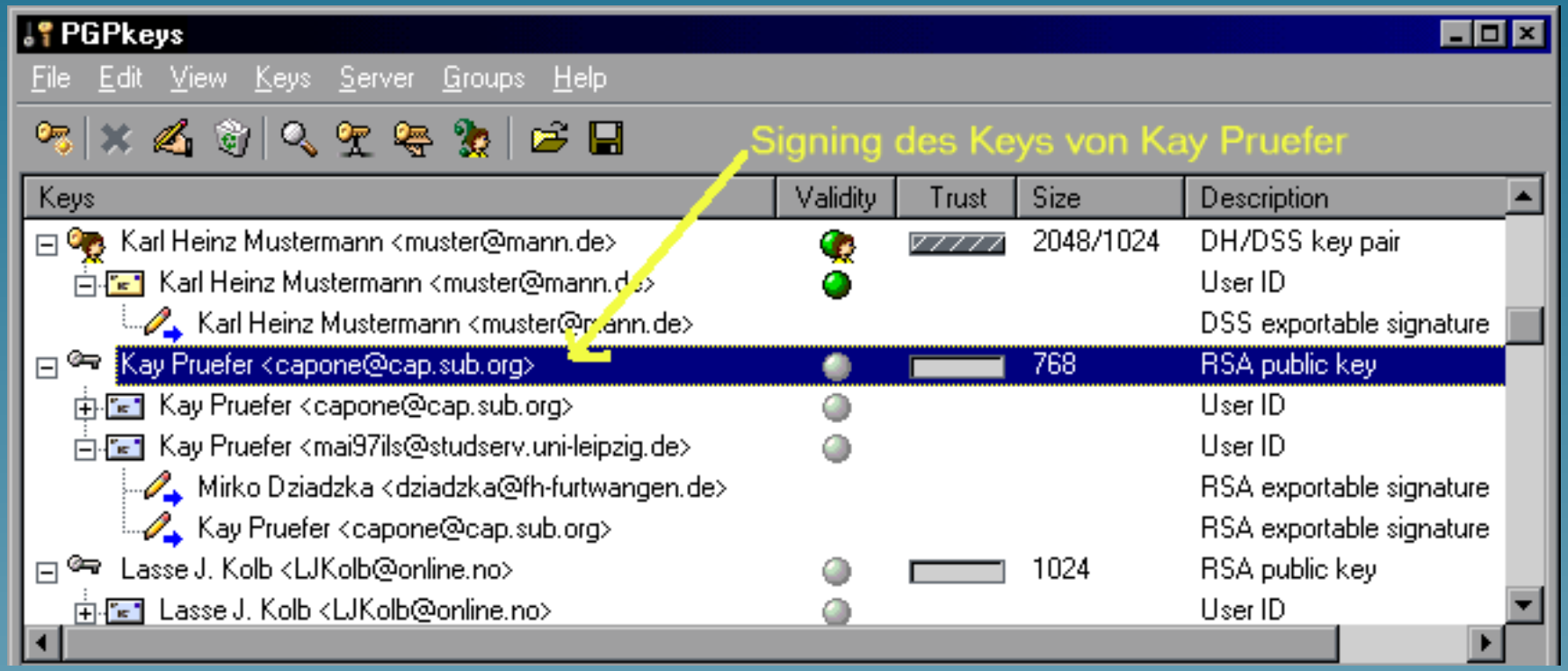
- Public Keys werden über Keyserver oder per Email verteilt.
- Schlüssel mit beliebigen UserIDs können von jedem erzeugt werden.
- Wie kann ich einen Public Key einer Person zuordnen? Wie kann ich sichergehen, daß ein Schlüssel nicht gefältscht wurde?

Das Web of Trust

- Woher weiß ich, daß der Public Key nicht gefälscht wurde:
  1. Von dem Schlüsselbesitzers persönlich erhalten
  2. Von vertrauenswürdiger Person bestätigt
- Eine Bestätigung geschieht durch das Signieren eines Public Keys:

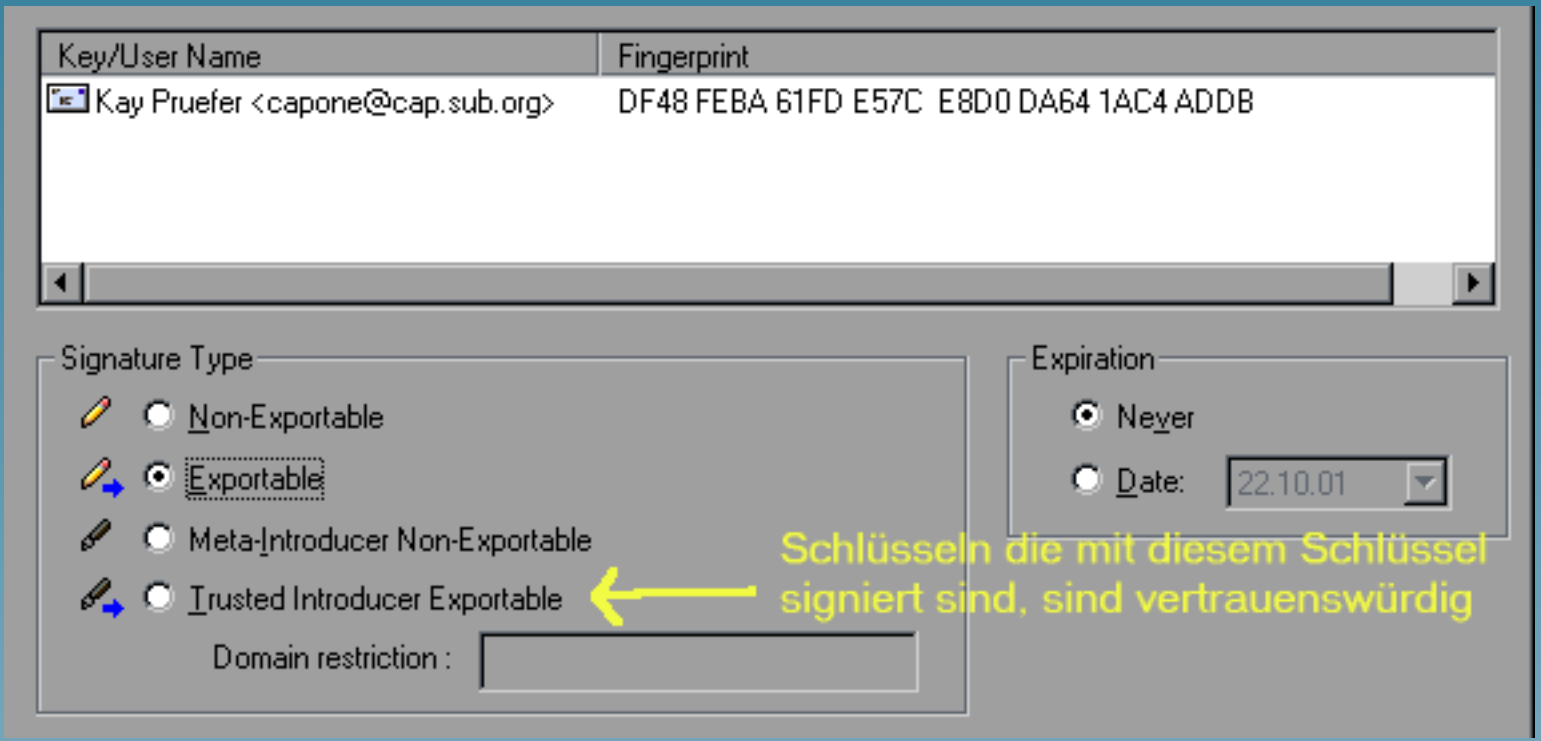


Schlüssel signieren (1)



Schlüssel signieren (2)

- Bei der Schlüsselsignatur kann das Vertrauen in den Schlüssel angegeben werden:
  - ⋆ **Exportable**: Der Schlüsselinhaber wurde überprüft. Auch andere können sich auf die Wertung verlassen.
  - ⋆ **Trusted Introducer**: Man vertraut dem Schlüsselinhaber soweit, daß er nur überprüfte Schlüssel unterschreibt. Von ihm unterschriebene Schlüssel wertet man als vertrauenswürdig.



Signingparties

- Auf Kongressen besteht die Möglichkeit Public Keys von Angesicht zu Angesicht zu tauschen.
- Am Kongress werden nur die Fingerprints getauscht.
- Für eine Signingparty muß man mitbringen:
  1. Personalausweis
  2. Vollständigen Fingerprint seines Schlüssels:

```
type Bits/KeyID    Date       User ID
pub  1024/GH75T441 1999/11/12 Karl Heinz Mustermann <muster@mann.de>
Key fingerprint = 5C 61 22 89 09 3B 55 5F  D9 2B 1F 57 B0 E0 F6 29
Karl Heinz Mustermann <muster@mann.de> (SIGN IN-CA:franken.de)
```

CA (Certification Authority)

- Eine CA ist eine Institution, die Schlüssel nach strengen Richtlinien unterschreibt.
- Die Richtlinien können öffentlich eingesehen werden.
- Dadurch ist es möglich, den Signaturen einer CA größeres Vertrauen zu schenken als Signaturen anderer Leute.
- Eine CA hat gegenüber Einzelpersonen einen größeren Wirkungsbreich.
- Der Public–Key der CA wird so veröffentlich, daß er nur schwer zu fälschen ist. Der Fingerprint der c't CA wird z.B. direkt in der c't veröffentlicht.

PGP Versionen und Plugins

- PGP gibt es in drei Varianten. PGP2, PGP5 und GnuPG. PGP5 kann mit PGP2 Schlüsseln arbeiten. GnuPG ist weitestgehend kompatibel zu PGP5.

- PGP–Unterstützung wird für die gebräuchlichsten Emailprogramme angeboten: mutt (Unix), Pine (Unix), Netscape (Unix/Windows), Eudora (Windows), Outlook (Windows), Lotus Notes (Windows).

Software und Literatur

- PGP: Pretty Good Privacy von Simon Garfinkel, O'Reilly & Associates, Inc., 1995
- The International PGP Homepage *http://www.pgpi.org*
- PGP für die USA *http://www.pgp.com*
- GNU Privacy Guard *http://www.gpg.org*
- PGP beim KNF, Regionale IN–CA Franken.de *http://www.franken.de/crypt/index.html*