IT-Security Bootcamp

Michael Lück

FOSSLC e.V.

27.10.2010

Einführung Kryptographie

- Was ist das?
  - Wissenschaft der Verschlüsselung von Informationen
  - sichert Vertraulichkeit, Integrität, Authentizität von Informationen während und nach der Übertragung
  - nicht gerade einfach :-)

Einführung Kryptographie

- Was ist das?
  - Wissenschaft der Verschlüsselung von Informationen
  - sichert Vertraulichkeit, Integrität, Authentizität von Informationen während und nach der Übertragung
  - nicht gerade einfach :-)
- Wozu brauch ich das?
  - vertrauliche E-Mails schreiben
  - sicher im Internet einkaufen
  - Onlinebanking
  - ...

Einführung Kryptographie

- Was ist das?
  - Wissenschaft der Verschlüsselung von Informationen
  - sichert Vertraulichkeit, Integrität, Authentizität von Informationen während und nach der Übertragung
  - nicht gerade einfach :-)
- Wozu brauch ich das?
  - vertrauliche E-Mails schreiben
  - sicher im Internet einkaufen
  - Onlinebanking
  - ...
- Who the F*** is Alice?
  - Namen von Kommunikationspartnern in Beispielen (statt A und B)

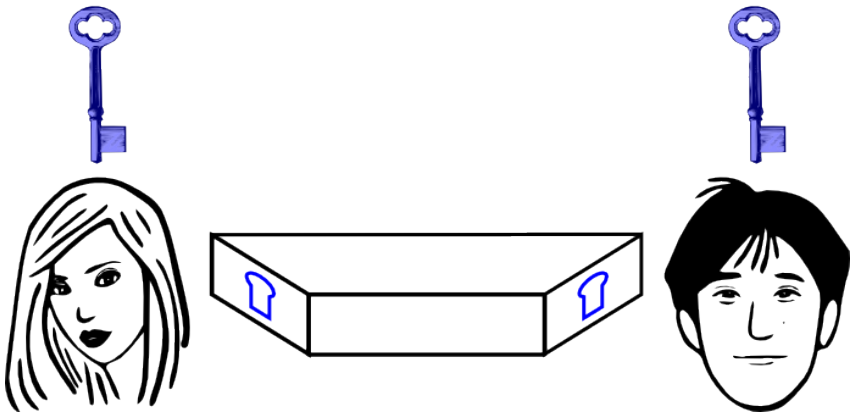

Alice

Bob

Eve

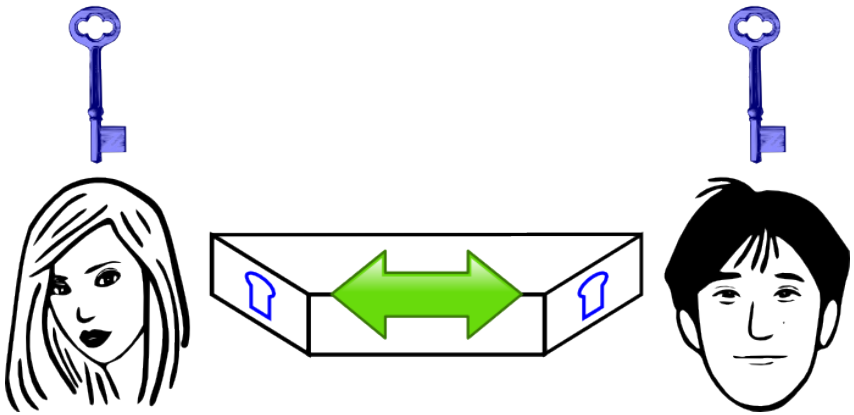
asymmetrische vs. symmetrische Verschlüsselung

symmetrisch



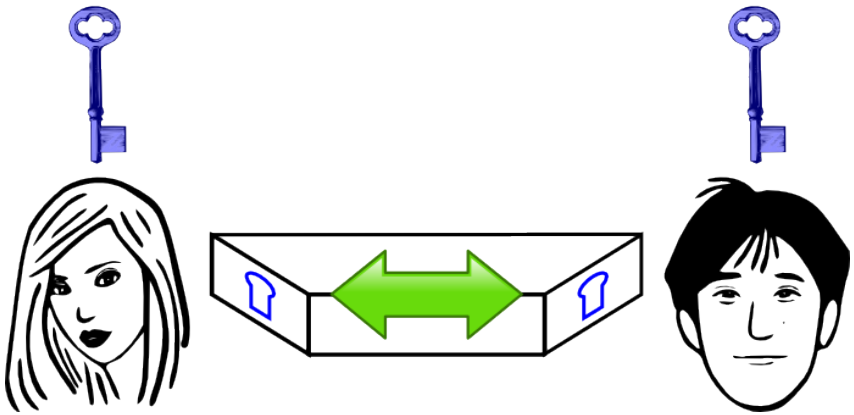
asymmetrische vs. symmetrische Verschlüsselung

symmetrisch

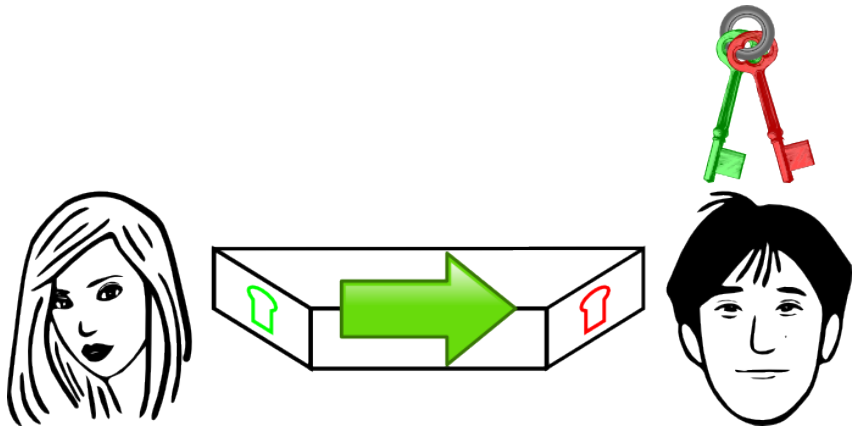


asymmetrische vs. symmetrische Verschlüsselung

symmetrisch

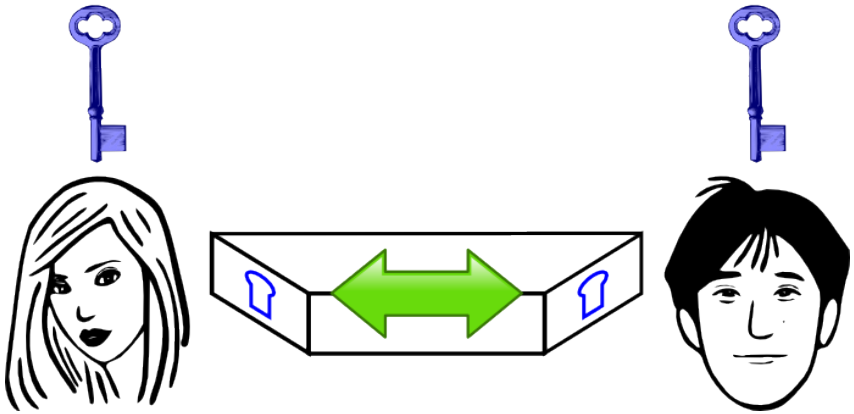


asymmetrisch

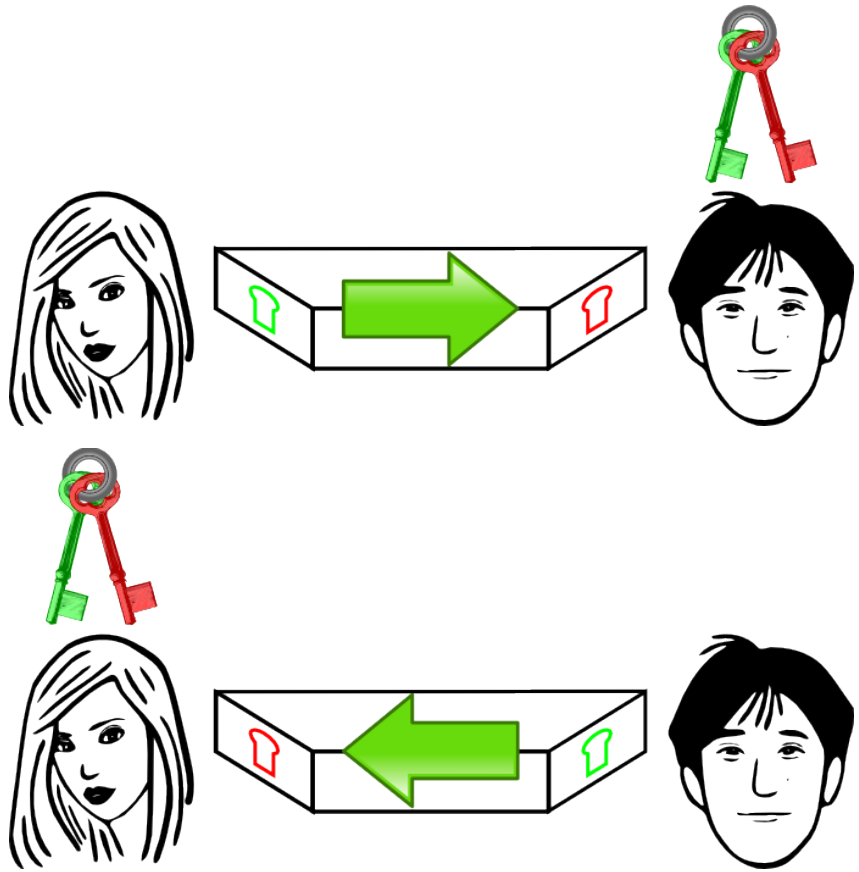


asymmetrische vs. symmetrische Verschlüsselung

symmetrisch



asymmetrisch



asymmetrische vs. symmetrische Verschlüsselung

symmetrisch

Der Schlüssel wird zum ver- und entschlüsseln verwendet

asymmetrische vs. symmetrische Verschlüsselung

symmetrisch

Der Schlüssel wird zum ver- und entschlüsseln verwendet

asymmetrisch

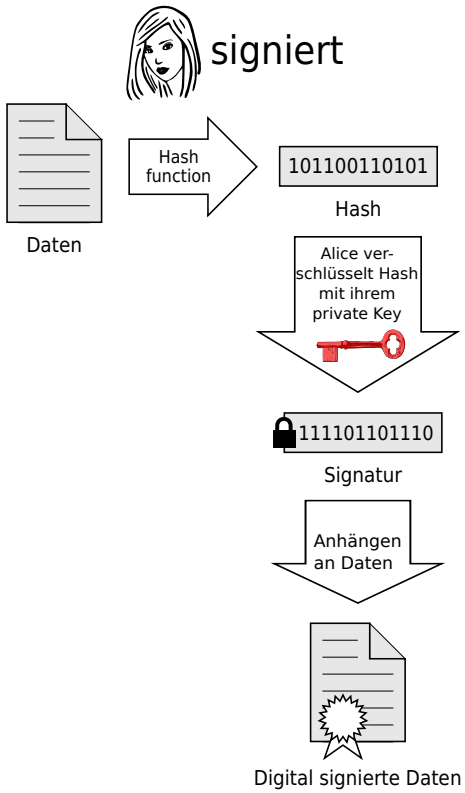
Was ein Schlüssel verschlüsselt, kann nur der andere wieder entschlüsseln

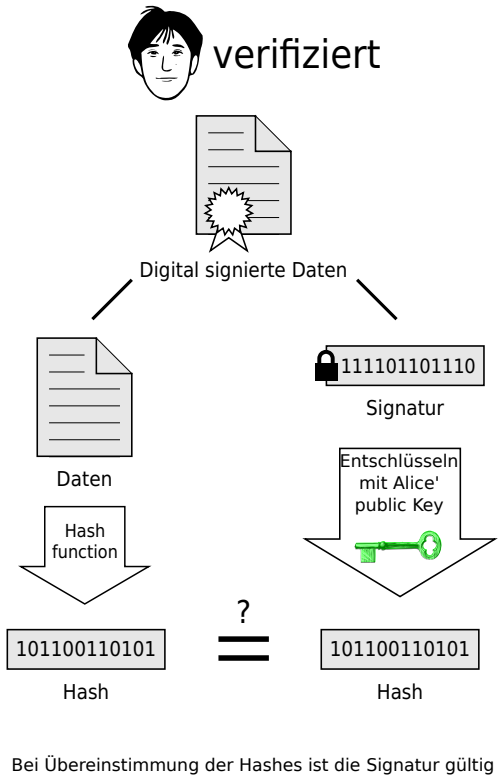
Digitale Signatur

- nur sinnvoll mit asymmetrischer Kryptographie

Digitale Signatur

- nur sinnvoll mit asymmetrischer Kryptographie

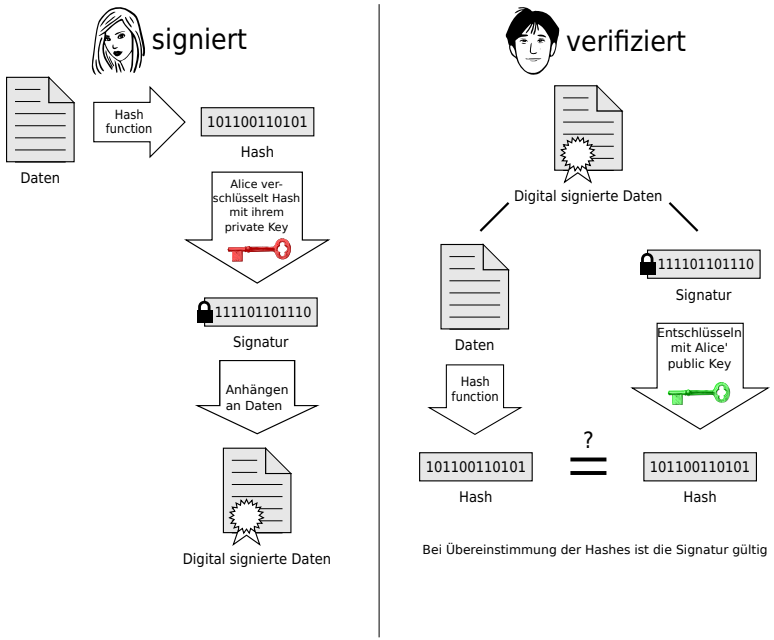




Base on [Acd08]

Digitale Signatur

- nur sinnvoll mit asymmetrischer Kryptographie

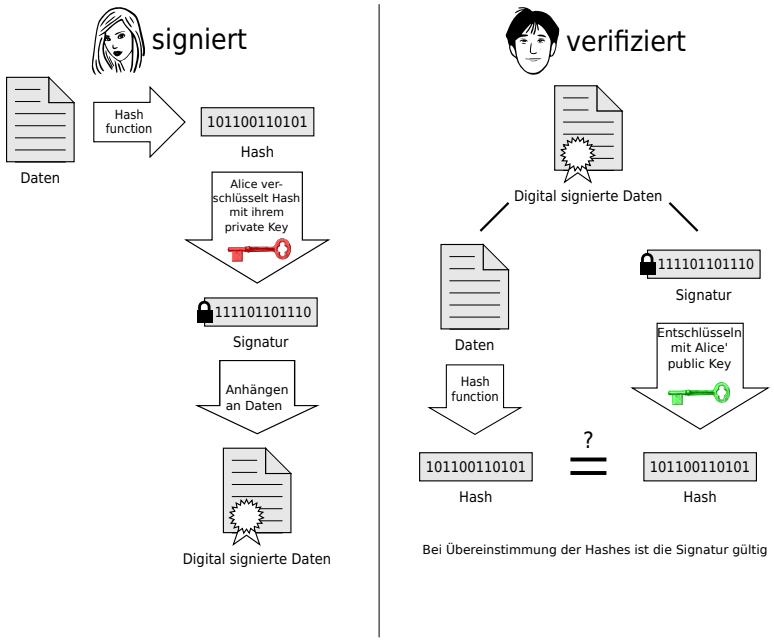


Base on [Acd08]

- eine Übereinstimmung bedeutet:

Digitale Signatur

- nur sinnvoll mit asymmetrischer Kryptographie

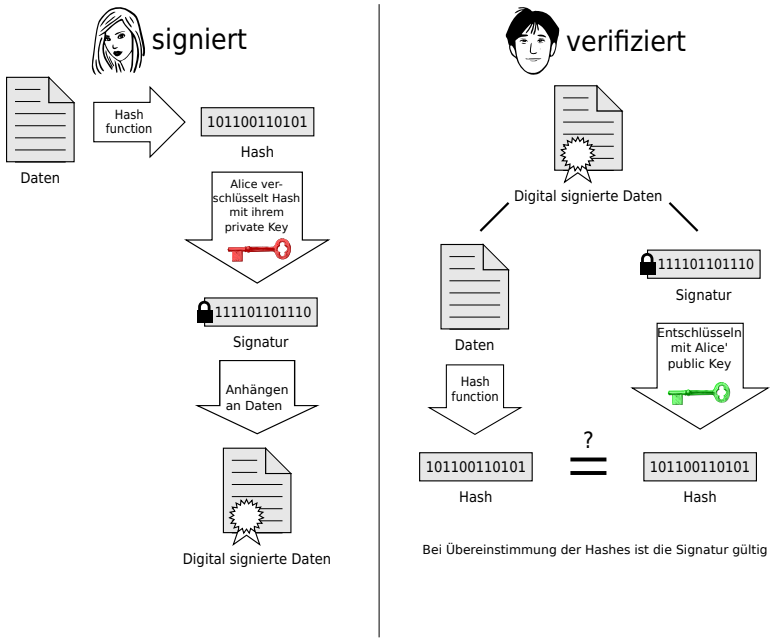


Base on [Acd08]

- eine Übereinstimmung bedeutet:
  - nur mit Alice private key kann Signatur erzeugt worden sein

Digitale Signatur

- nur sinnvoll mit asymmetrischer Kryptographie



Base on [Acd08]

- eine Übereinstimmung bedeutet:
  - nur mit Alice private key kann Signatur erzeugt worden sein
  - das Dokument wurde nach Erzeugung der Signatur nicht verändert

PGP/OpenPGP

- **P**retty **G**ood **P**rivacy

PGP/OpenPGP

- **P**retty **G**ood **P**rivacy
- Implementierung eines asymmetrischen Kryptographiesystems

PGP/OpenPGP

- **P**retty **G**ood **P**rivacy
- Implementierung eines asymmetrischen Kryptographiesystems
  - ermöglicht Verschlüsselung und Signierung (s.u.)

PGP/OpenPGP

- **P**retty **G**ood **P**rivacy
- Implementierung eines asymmetrischen Kryptographiesystems
  - ermöglicht Verschlüsselung und Signierung (s.u.)
- Schlüsselpaar wird erzeugt für eine ID

PGP/OpenPGP

- **P**retty **G**ood **P**rivacy
- Implementierung eines asymmetrischen Kryptographiesystems
  - ermöglicht Verschlüsselung und Signierung (s.u.)
- Schlüsselpaar wird erzeugt für eine ID
  - Name & E-Mailadresse
  - weitere IDs können später hinzugefügt werden

PGP/OpenPGP

- **P**retty **G**ood **P**rivacy
- Implementierung eines asymmetrischen Kryptographiesystems
  - ermöglicht Verschlüsselung und Signierung (s.u.)
- Schlüsselpaar wird erzeugt für eine ID
  - Name & E-Mailadresse
  - weitere IDs können später hinzugefügt werden
- Public Key kann von anderen signiert werden

PGP/OpenPGP

- **P**retty **G**ood **P**rivacy
- Implementierung eines asymmetrischen Kryptographiesystems
  - ermöglicht Verschlüsselung und Signierung (s.u.)
- Schlüsselpaar wird erzeugt für eine ID
  - Name & E-Mailadresse
  - weitere IDs können später hinzugefügt werden
- Public Key kann von anderen signiert werden
  - Signatur drückt Vertrauen aus, dass

PGP/OpenPGP

- **P**retty **G**ood **P**rivacy
- Implementierung eines asymmetrischen Kryptographiesystems
  - ermöglicht Verschlüsselung und Signierung (s.u.)
- Schlüsselpaar wird erzeugt für eine ID
  - Name & E-Mailadresse
  - weitere IDs können später hinzugefügt werden
- Public Key kann von anderen signiert werden
  - Signatur drückt Vertrauen aus, dass
    - der signierte Schlüssel dem Besitzer der Mailadresse gehört
    - der Inhaber des Schlüssels diesen vor Missbrauch schützt

PGP/OpenPGP

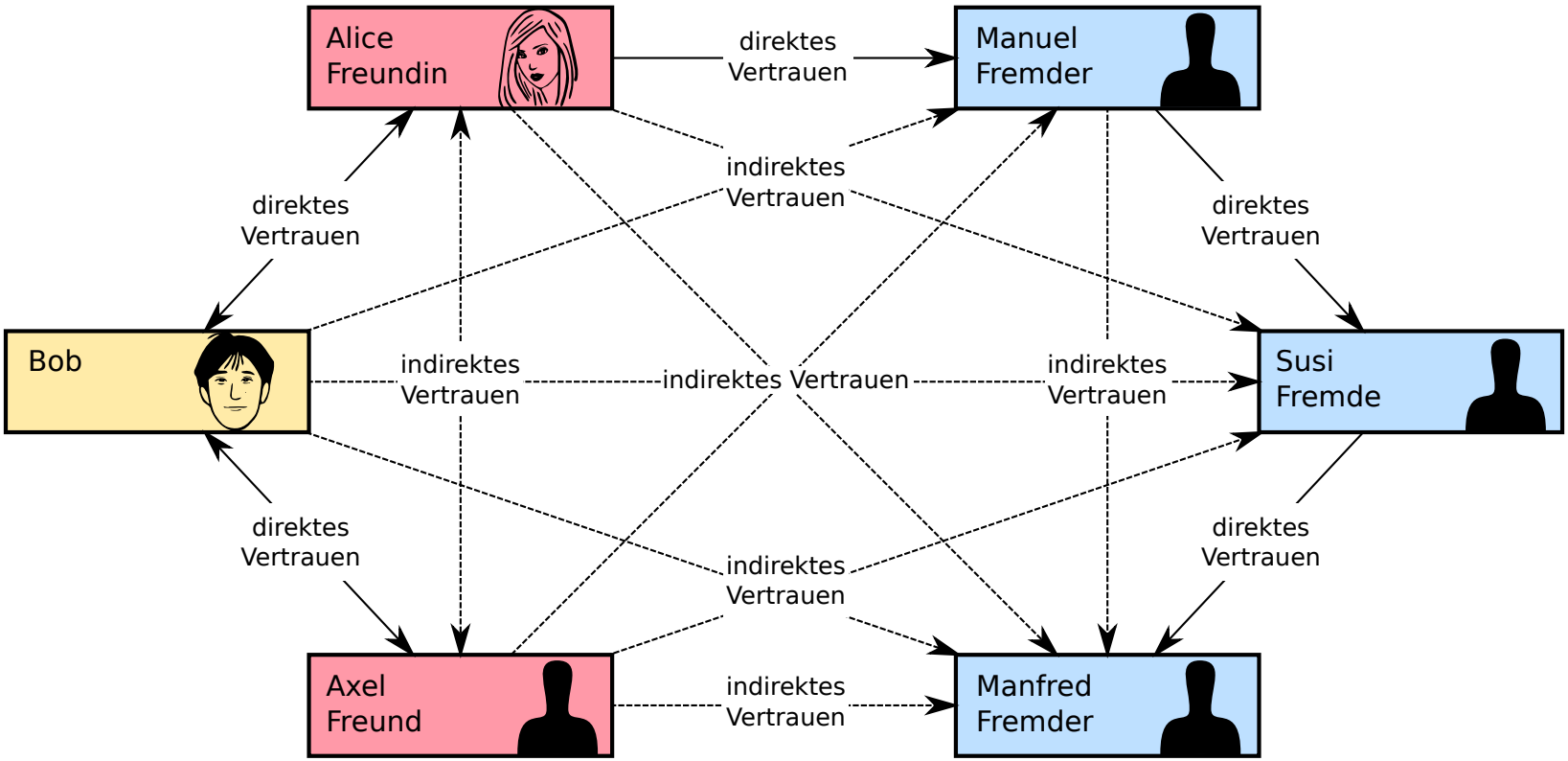
- **P**retty **G**ood **P**rivacy
- Implementierung eines asymmetrischen Kryptographiesystems
  - ermöglicht Verschlüsselung und Signierung (s.u.)
- Schlüsselpaar wird erzeugt für eine ID
  - Name & E-Mailadresse
  - weitere IDs können später hinzugefügt werden
- Public Key kann von anderen signiert werden
  - Signatur drückt Vertrauen aus, dass
    - der signierte Schlüssel dem Besitzer der Mailadresse gehört
    - der Inhaber des Schlüssels diesen vor Missbrauch schützt
  - Signatur wird zusammen mit Schlüssel gespeichert (gehört zum Schlüssel)

PGP/OpenPGP

- **P**retty **G**ood **P**rivacy
- Implementierung eines asymmetrischen Kryptographiesystems
  - ermöglicht Verschlüsselung und Signierung (s.u.)
- Schlüsselpaar wird erzeugt für eine ID
  - Name & E-Mailadresse
  - weitere IDs können später hinzugefügt werden
- Public Key kann von anderen signiert werden
  - Signatur drückt Vertrauen aus, dass
    - der signierte Schlüssel dem Besitzer der Mailadresse gehört
    - der Inhaber des Schlüssels diesen vor Missbrauch schützt
  - Signatur wird zusammen mit Schlüssel gespeichert (gehört zum Schlüssel)

$\rightarrow$ Web Of Trust

Web Of Trust



based on [Ogm09]

PGP/OpenPGP 2

- Public Keys werden auf Keyserver gespeichert

PGP/OpenPGP 2

- Public Keys werden auf Keyserver gespeichert
  - stehen somit jedem zur Verfügung

PGP/OpenPGP 2

- Public Keys werden auf Keyserver gespeichert
  - stehen somit jedem zur Verfügung
  - Update auf Server nach Signatur notwendig

PGP/OpenPGP 2

- Public Keys werden auf Keyserver gespeichert
  - stehen somit jedem zur Verfügung
  - Update auf Server nach Signatur notwendig
- eigenes Schlüsselpaar und heruntergeladene Public Keys werden lokal gespeichert

PGP/OpenPGP 2

- Public Keys werden auf Keyserver gespeichert
  - stehen somit jedem zur Verfügung
  - Update auf Server nach Signatur notwendig
- eigenes Schlüsselpaar und heruntergeladene Public Keys werden lokal gespeichert
  - passwort-geschützt in sogenannten keyrings

PGP/OpenPGP 2

- Public Keys werden auf Keyserver gespeichert
  - stehen somit jedem zur Verfügung
  - Update auf Server nach Signatur notwendig
- eigenes Schlüsselpaar und heruntergeladene Public Keys werden lokal gespeichert
  - passwort-geschützt in sogenannten keyrings
- Und jetzt Übung ...
  - Schlüssel generieren: `gpg --gen-key`
  - Schlüssel anzeigen: `gpg --list-keys`
  - Schlüssel auf keyserver laden:
    `gpg --send-keys <key-ID> --keyserver ldap://fosslc.lan`
  - E-Mail senden mit Thunderbird + Enigmail

ACDX:
Digital Signature Diagram.
In: *wikipedia* (2008).
http://de.wikipedia.org/wiki/Datei:Digital_Signature_diagram.svg. –
CC by SA

OGMOIS:
Web Of Trust.
In: *Wikipedia* (2009).
http://de.wikipedia.org/w/index.php?title=Datei:Web_of_Trust.svg&filetimestamp=20091016131430. –
CC by SA