PGP

Pretty Good Privacy

Warum Kryptografie

- **Vertraulichkeit**
  Mails nur vom Empfänger lesbar

- **Integrität**
  Keine Veränderung der Daten

- **Authentizität**
  Richtiger Absender bekannt

Geschichte

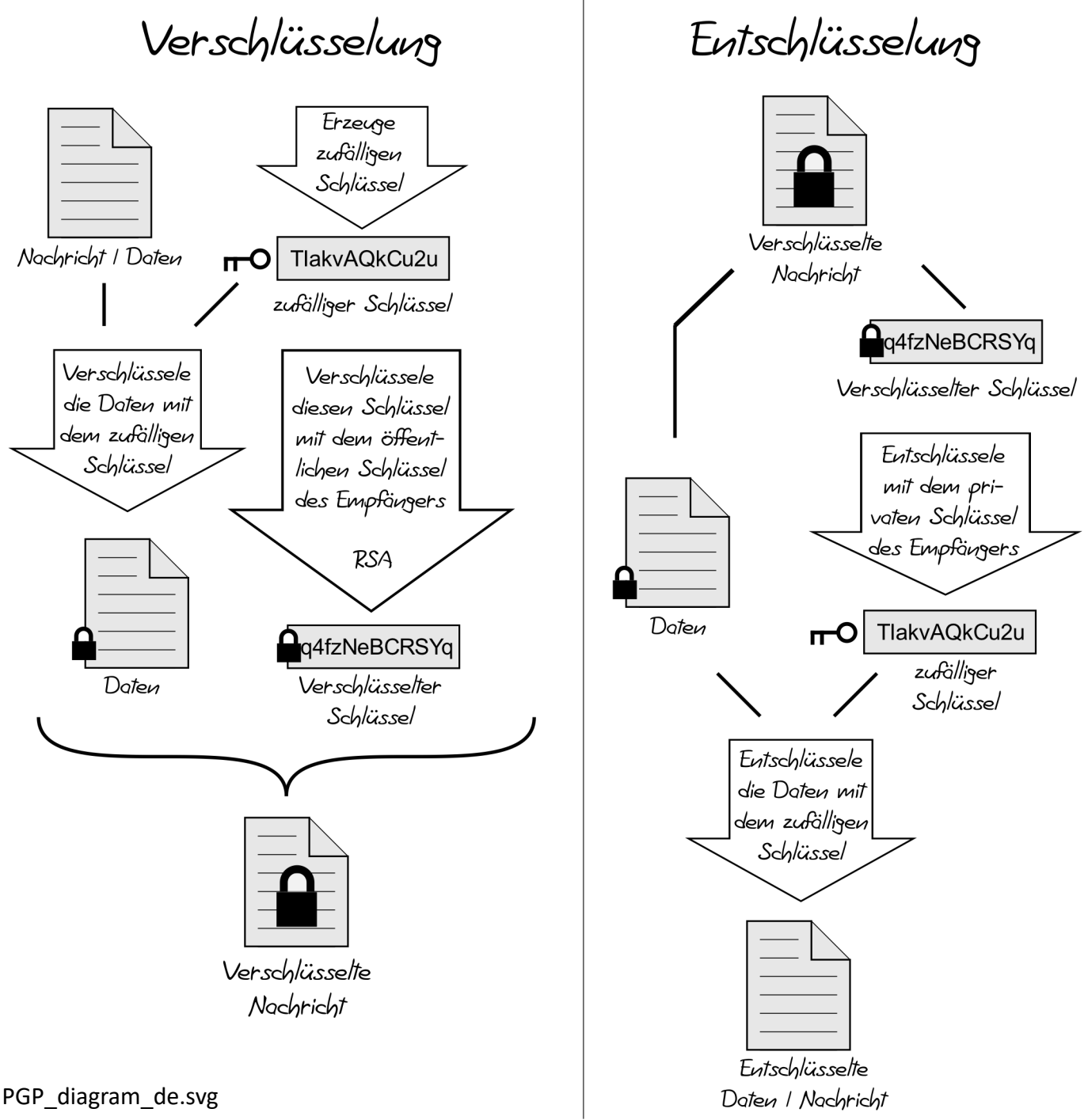
- Entwickelt von Phil Zimmermann
  - Schutz von Bürgern und Bürgerrechtsbewegungen
- Erste Version 1991 veröffentlicht
- Internationale Version 1995 per Buch veröffentlicht
- Verschiedene Firmen: ViaCrypt, PGP Inc., Network Associates (McAfee), PGP Corporation
- Viele parallele Versionen: PGP / PGPi, diverse Versionen

OpenPGP

- RFC 1991, RFC 2440, RFC 4880
- Freie Algorithmen
- Verschieden Programme
  - GnuPG [Linux/Unix]
  - gpg4win [Windows]
  - GPG Suite [macOS]
  - Enigmail [Thunderbird]

Verfahren - Verschlüsselung

- PGP nutzt ein Hybrides Verschlüsselungssystem
- Symmetrische Nachrichtenschlüssel
  - Sichere Schlüssel: 128 bit oder mehr
  + Schnell
  – Schlüsselverteilung
- Asymmetrische Userschlüssel
  - Sichere Schlüssel: 2048 – 4096 bit
  + Öffentliche Schlüssel
  – langsam



Quelle: https://de.wikipedia.org/wiki/Datei:PGP_diagram_de.svg

Verfahren - Signatur

1. Hash / Prüfsumme von Nachricht berechnen (bspw. SHA-256)
2. Mit eigenem privaten Schlüssel verschlüsseln
3. Verschlüsselten Hash an Nachricht anhängen == Signatur
4. Überprüfung vom Empfänger
   - öffentlicher Schlüssel vom Absender
   - selbst berechnetem Hash-Wert der Empfangenen Nachricht

Warum Kryptografie

- **Vertraulichkeit**
  Mails nur vom Empfänger lesbar
- **Integrität**
  Keine Veränderung der Daten
- **Authentizität**
  Richtiger Absender bekannt

Signieren

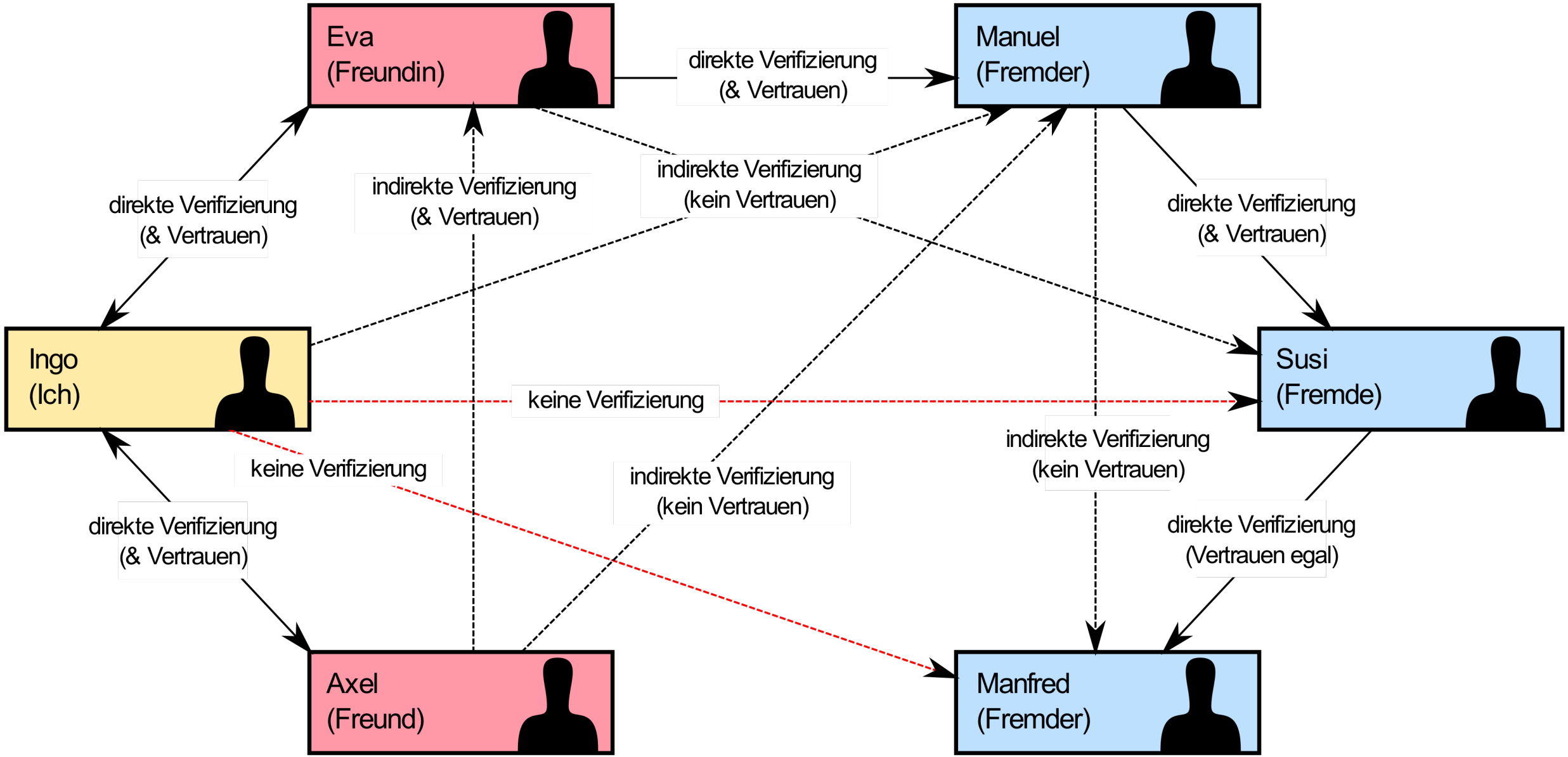
Signieren + Verschlüsseln

Web of Trust

Wikipedia:

> **Netz des Vertrauens** bzw. **Web of Trust (WOT)** ist in der Kryptologie die Idee, die Echtheit von digitalen Schlüsseln durch ein Netz von gegenseitigen Bestätigungen (Signaturen), kombiniert mit dem individuell zugewiesenen Vertrauen in die Bestätigungen der anderen („Owner Trust“), zu sichern.
> Es stellt eine dezentrale Alternative zum hierarchischen PKI-System dar.

Öffentliche Keyserver als Verzeichnis für öffentliche Schlüssel inklusive Signaturen



Quelle: https://commons.wikimedia.org/wiki/File:Web_of_Trust_2.svg