E-Mail-Verschlüsselung

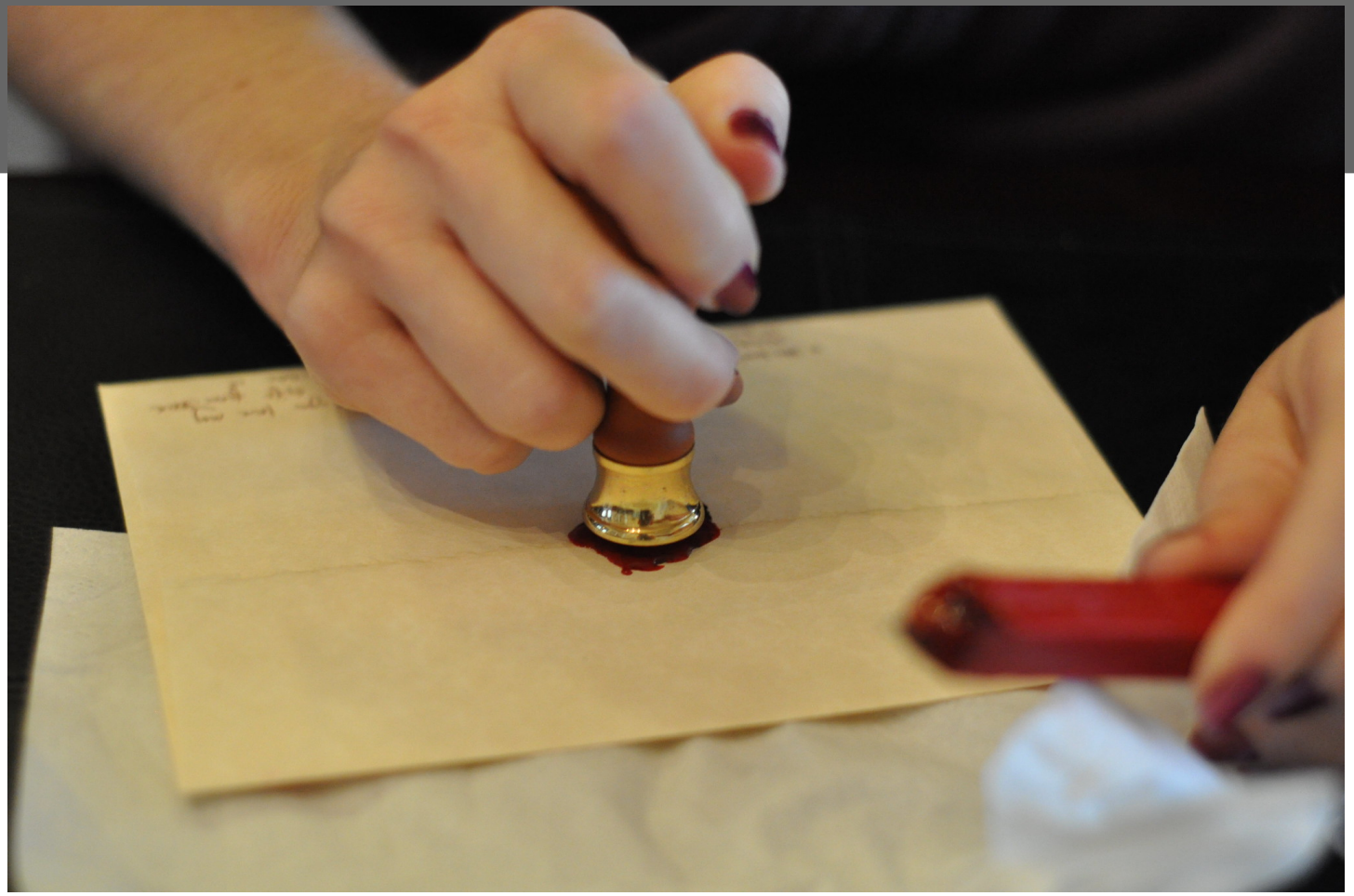


Bild: „2013-02-17 13.44.53“, S. Davis on Flickr. CC-BY-ND

Alternativen zu „kostenlosen“ E-Mail-Anbietern

- **posteo.de** oder **mailbox.org**
- 24h-Einmal-E-Mail-Adresse, gratis: anonbox.net (CA-Cert)

Vorteile

- Standort in Deutschland
- Datensparsamkeit
- keine Inhaltsanalyse
- keine Werbung
- anonyme Nutzung möglich
- Datenschutz hat Priorität

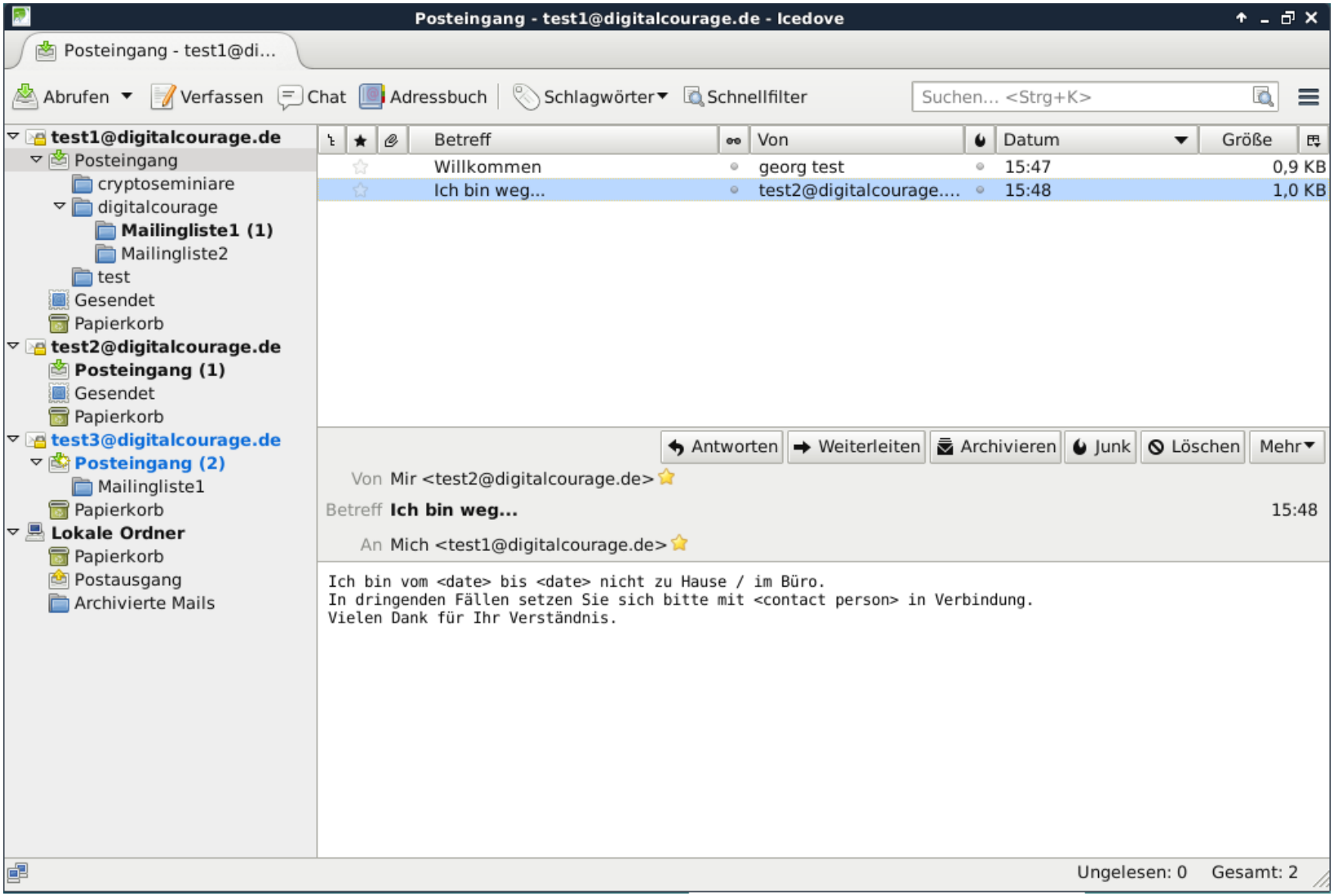
Nachteile

- posteo.de und mailbox.org kosten 1 € pro Monat

E-Mail-Verwaltung

- Software: Mozilla Thunderbird
  - Freie Software
  - mehrere Mail-Konten möglich
  - Verwaltung mit Filtern und Ordnern
  - Schutz gegen Ausspähen und Angriffe (etwa HTML abschalten)
  - Mails offline lesen, speichern und durchsuchen
  - Add-ons bieten viele sehr nützliche Funktionen – Auswahl:
    - Kalender (*Lightning* – ist schon bei Installation von Thunderbird enthalten)
    - Massenmails (*Mail Merge*)
    - Verhindern von Mail-Datenschutz-Pannen mit vielen Adressen in den Feldern „Empfänger“ oder „Kopie“ – Add-on schlägt vor, in „Blindkopie“ umzuwandeln (*Use Bcc Instead* bzw. für neue Thunderbird-Versionen *Use Bcc Instead C*)
    - **Verschlüsselung (*Enigmail*)**

Screenshot
Mozilla Thunderbird



Komponenten
E-Mail-Verschlüsselung (PGP/GnuPG)

- Verschlüsselung: **GnuPG**
- E-Mail Programm: **Thunderbird**
- Add-on zur komfortablen Bedienung: **Enigmail**
  - **p≡p** (Pretty Easy Privacy) nutzen wir (noch?) nicht, ggf. deaktivieren
- Wichtige Veränderungen ab Sommer 2020 (Juli/August): Thunderbird 78.x ändert die Technologie für Add-ons
  - viele Add-ons werden nicht mehr funktionieren, auch Enigmail(!)
  - ab 78.2: für Verschlüsselung **alle Komponenten integriert**
    - weder zugrundeliegendes GnuPG noch Add-on nötig (p≡p evtl. als Add-on)
    - nicht auf 78.0/78.1 aktualisieren (soll nicht automatisch angeboten werden)
    - genaue Funktionen, Speicherorte, Klickwege leider noch unbekannt

Vorteile und Nachteile E-Mail-Verschlüsselung

Vorteile

- Inhalt Ende-zu-Ende-verschlüsselt
- Absender[1] & Empfängerin werden eindeutig
  ([1] mit PGP-Signatur)

Nachteile

- Metadaten (von, an, Betreff[2] etc). bleiben unverschlüsselt
  ([2] Enigmail ab 2.0 kann Betreff verschlüsseln)
- Absender & Empfängerin müssen PGP nutzen

Verschlüsselung – was ist das eigentlich?

- Alice schreibt an Bob, Eve will mithören (eavesdrop) / Mallory (malicious) will manipulieren → man in the middle
- Beispiele und Grundprinzipien
  - meist gibt es ein **Verfahren** mit **Schlüssel**
  - Caesar-Verschlüsselung: einheitliche Verschiebung, 3 Positionen – wurde tatsächlich von Caesar und lange danach eingesetzt
  - ab 16. Jahrhundert komplexere Verfahren, noch im 1. Weltkrieg handschriftlich, 2. Weltkrieg Enigma – entscheidende Misserfolge
  - Vertrauen in moderne Kryprographie beruht darauf, dass das **Verfahren offen**, der **Schlüsselraum sehr groß** und als Angriff eigentlich **nur brute force** (alle Schlüssel probieren) bekannt ist

Unterschied symmetrische / asymmetrische Verschlüsselung

- Symmetrische Verschlüsselung
  - **derselbe Schlüssel** zum Ver- und Entschlüsseln
  - alle Beteiligten brauchen diesen (geheimen) Schlüssel
  - Problem: um Nachrichten (auf unsicheren Kanälen) zu senden, muss zuerst der Schlüssel (auf sicherem Kanal) verteilt werden

Unterschied symmetrische / asymmetrische Verschlüsselung

- Asymmetrische Verschlüsselung → PGP
  - **Schlüsselpaar:** was **ein** Schlüssel **ver**schlüsselt, muss mit dem **anderen** Schlüssel **ent**schlüsselt werden
  - Alle Beteiligten erzeugen ein eigenes Schlüsselpaar
- Verschiedene Rollen für die beiden Schlüssel
  - **öffentlicher Schlüssel:** kann und muss verteilt werden (an alle, über unsichere Kanäle)
  - **privater Schlüssel:** bleibt privat – gut schützen, datensichern, niemals herausgeben!
- Zentrale Voraussetzungen
  - private Schlüssel können von niemand sonst benutzt werden
  - öffentliche Schlüssel sind unverfälscht und korrekt zugeordnet

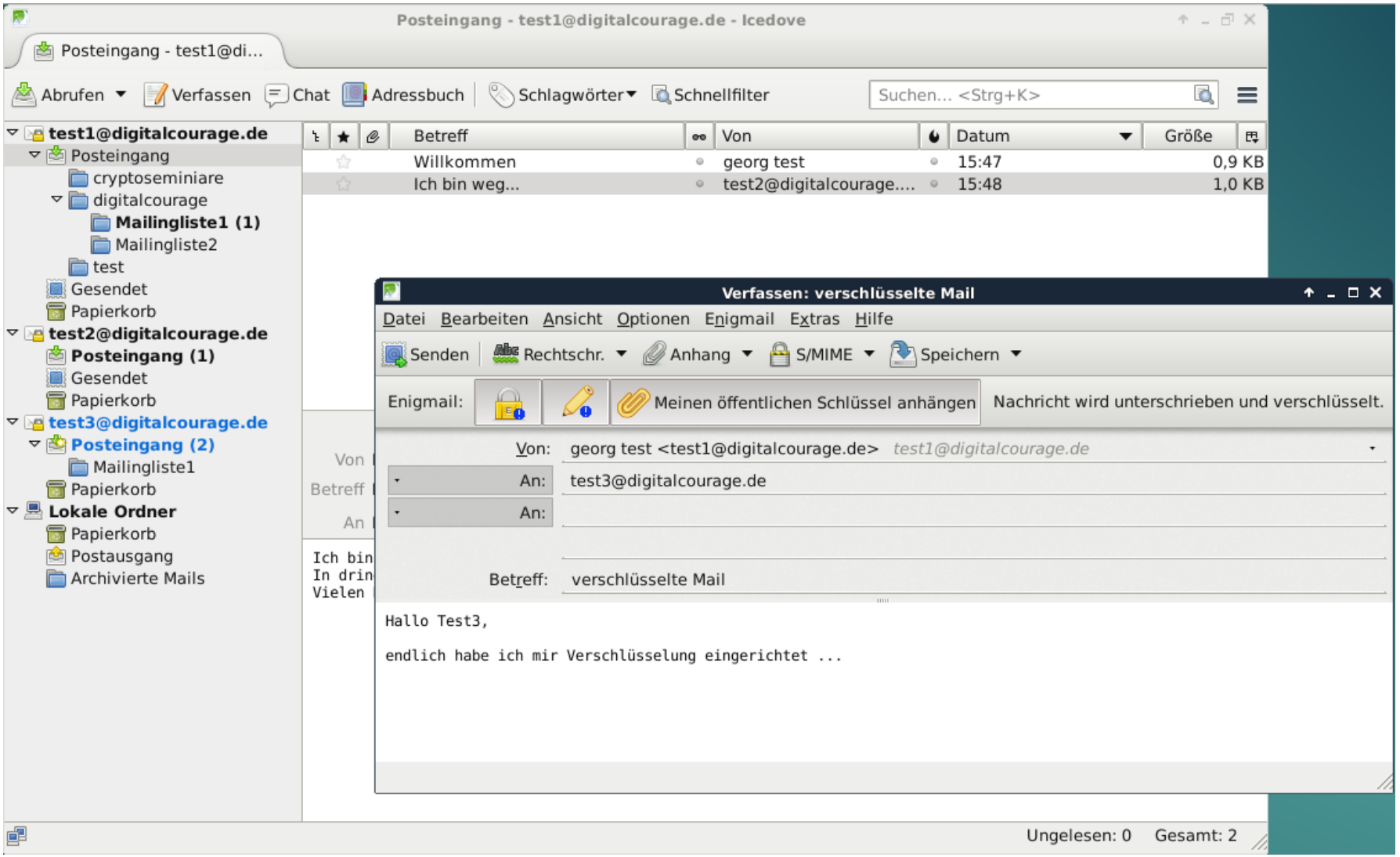
E-Mails verschlüsseln und signieren

- Verschlüsseln
  - verwendet den **öffentlichen Schlüssel des Empfängers**
  - sichert Vertraulichkeit der Nachricht
    (nur Empfänger kann mit privatem Schlüssel entschlüsseln)
- Signieren
  - verwendet den **privaten Schlüssel der Absenderin**
  - nicht verwechseln mit Unterschrift und Fußzeile („Signatur“)
  - ein Fingerabdruck der Nachricht wird verschlüsselt und angehängt
  - sichert Unverfälschtheit der Nachricht und wer sie verfasste
    (nur Absenderin konnte mit diesem Schlüssel signieren)
- Verschlüsseln und Signieren sind unabhängig voneinander

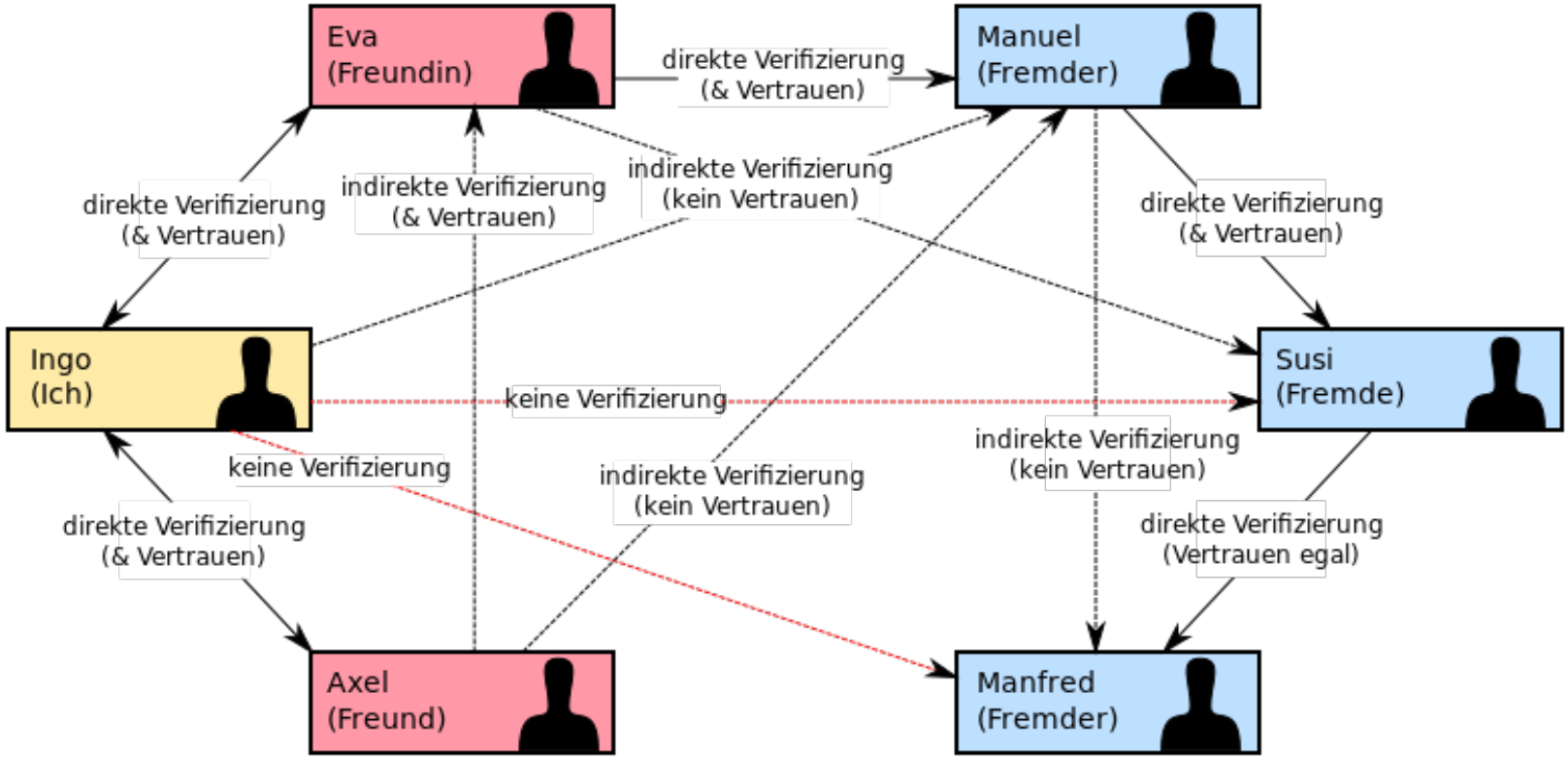
öffentliche PGP-Schlüssel austauschen

- E-Mail-Anhang
  - zur Verteilung im privaten Kreis
- Key-Server
  - bequem durchsuchbar
  - E-Mail-Adresse öffentlich einsehbar
- Habe ich den richtigen Schlüssel bekommen?
  - komplexes Thema → Schlüssel signieren, „Web of Trust“
  - pragmatische Lösung: Schlüssel auf mehreren Wegen finden (z.B. von persönlicher Website); Fingerprints austauschen und vergleichen (Visitenkarte, Telefon, Website, „Signatur“ unter Mails)

Screenshot
Schlüsselaustausch mit Enigmail



Web of Trust



– Ende E-Mail-Verschlüsselung –