

E-Mail-Verschlüsselung

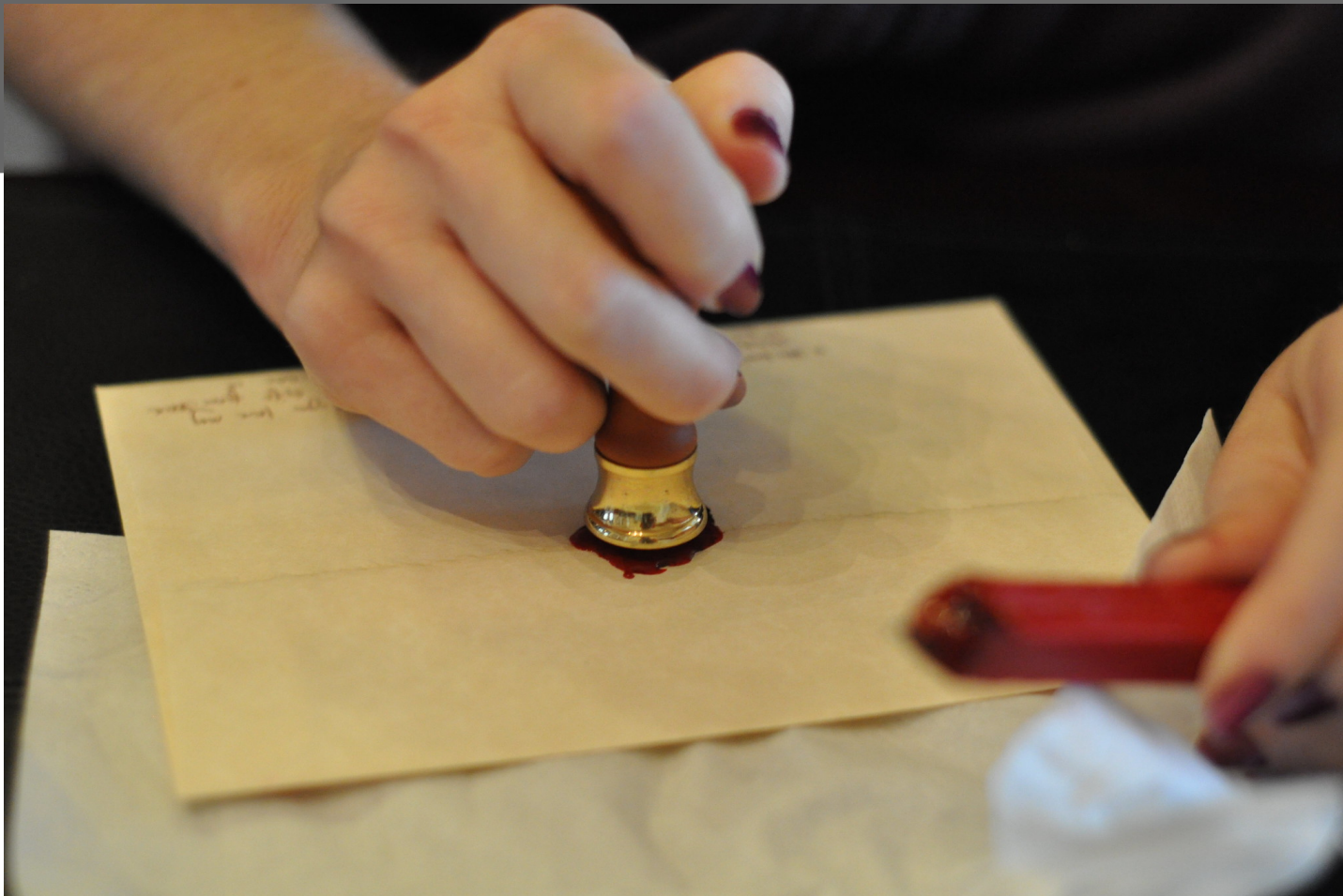


Bild: „2013-02-17 13.44.53“, S. Davis on Flickr. CC-BY-ND

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
 - ▷ Mails offline lesen, speichern, durchsuchen
 - ▷ **E-Mail-Verschlüsselung** – seit Thunderbird 78 ohne Add-on
 - ▷ Kalender verwalten, Team-Kalender nutzen, Termineinladungen
 - ▷ Adressbücher, auch Team-Adressbücher (CardDAV, LDAP), Listen
 - ▷ Add-ons bieten viele sehr nützliche Funktionen – Auswahl:
 - individualisierte Massenmails (*Mail Merge*)
 - Verhindern von Mail-Datenschutz-Pannen mit vielen Adressen in „To“ oder „Cc“ (*Limit non-BCC recipients* – einfacherer Schutz schon ohne Add-on)

Screenshot Mozilla Thunderbird

The screenshot displays the Mozilla Thunderbird email client interface. The window title is "Posteingang - Test-Account 1 - Mozilla Thunderbird". The left sidebar shows the folder structure for "Test-Account 1" and "Test-Account 2". The main pane shows an email message with the following details:

- From:** Test 2 <testsl2@digitalcourage.de> ★
- Subject:** Re: eine unverschlüsselte Mail
- Date:** 29.11.20, 21:00
- To:** Test 1 <testsl1@digitalcourage.de> ★

The email body contains the following text:

Danke für die Informationen!

Wolltest du dich schon immer mal Themen der digitalen Selbstverteidigung beschäftigen, hast aber noch keine passende Gelegenheit gefunden? In deiner Nähe findet keine CryptoParty statt oder die Termine sind wegen Corona ausgefallen? Dann nimm ab dem 25. November an den Online-Workshops unseres Crypto-Seminars teil, das als Kooperation der Digitalcourage-Hochschulgruppe Bielefeld mit dem Fachbereich Sozialwesen der Fachhochschule Bielefeld stattfindet! Über zwei Wochen verteilt werden wir uns vier Themenblöcken der digitalen Selbstverteidigung widmen:

25.11. (Mi), 18-20 Uhr: Passwörter und Dateiverschlüsselung

At the bottom right of the window, it shows "Ungelesen: 0 Gesamt: 1".

Komponenten

E-Mail-Verschlüsselung (PGP/GnuPG)

- ▶ früher: mehrere Komponenten
 - ▷ Verschlüsselung: **GnuPG**, systemweit installiert
 - ▷ E-Mail Programm: **Thunderbird**
 - ▷ Add-on zur komfortablen Bedienung: **Enigmail**
 - **p≡p** (Pretty Easy Privacy) war Zusatzfunktion in Enigmail
- ▶ seit Sommer 2020: neue Add-on-Technik, Thunderbird 78+
 - ▷ viele alte Add-ons funktionieren nicht mehr, auch Enigmail
 - ▷ für Verschlüsselung **alle Komponenten integriert**
 - weder zugrundeliegendes GnuPG noch Add-on nötig
 - eigener Schlüsselvorrat im Thunderbird-Profil
 - Enigmail war noch Assistent für Import bzw. Migration von früheren Versionen
 - p≡p evtl. als Add-on für mehr Komfort („opportunistische Verschlüsselung“)

Vorteile und Nachteile E-Mail-Verschlüsselung

Vorteile

- ▶ Inhalt Ende-zu-Ende-verschlüsselt
- ▶ Absender¹ & Empfängerin werden eindeutig
(¹ mit PGP-Signatur)

Nachteile

- ▶ Metadaten (von, an, Betreff² etc). bleiben unverschlüsselt
(² Thunderbird kann den Betreff verschlüsseln, dadurch entstehen jedoch Probleme mit anderer Mail-Software)
- ▶ Absender & Empfängerin müssen PGP nutzen

Verschlüsselung – was ist das eigentlich?

- ▶ Alice schreibt an Bob, Eve will mithören (eavesdrop) / Mallory (malicious) will manipulieren → person 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 Kryptographie entsteht dann, wenn 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 **verschlüsselt**, muss mit dem **anderen** Schlüssel **entschlüsselt** 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)

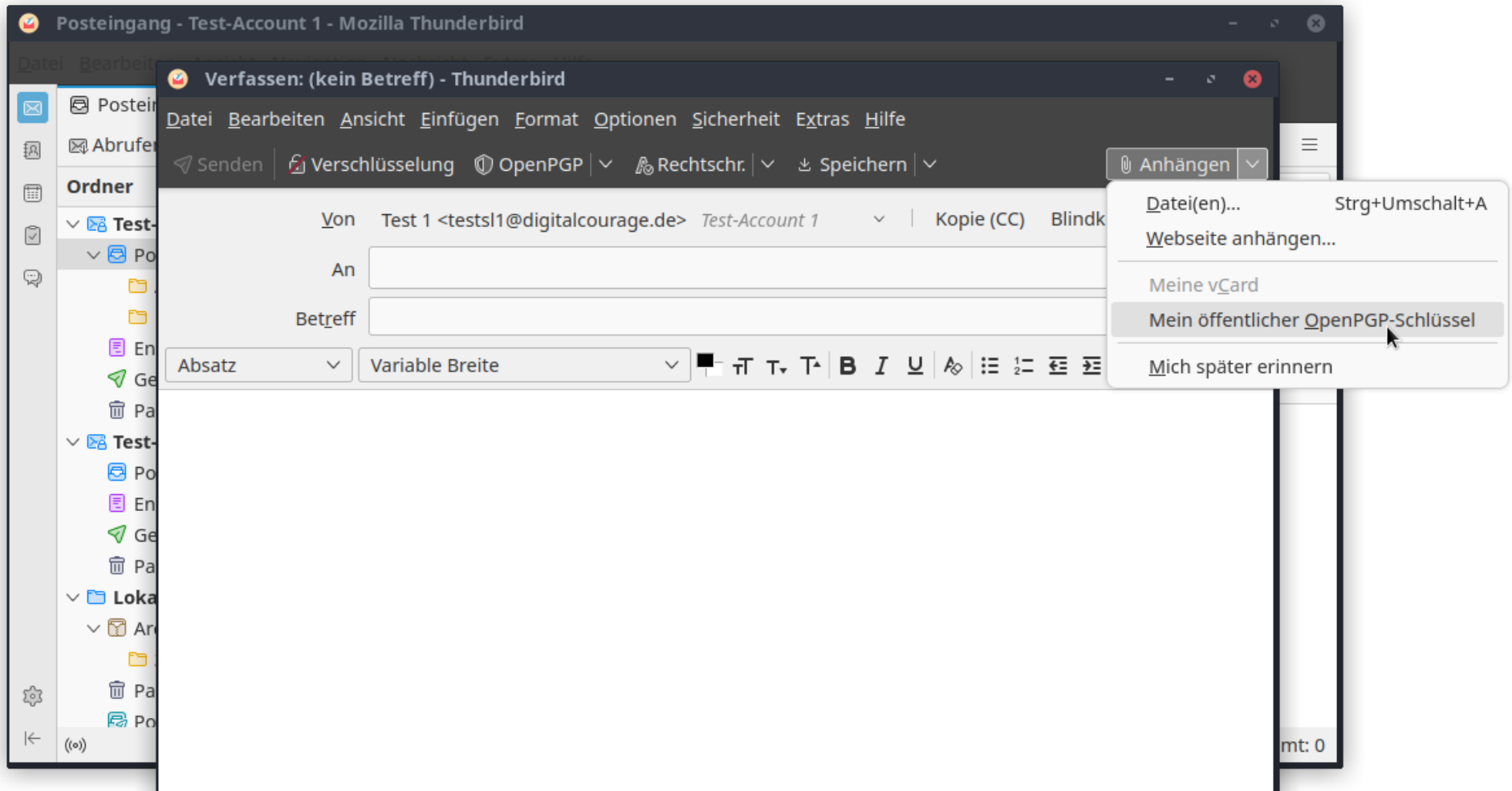
▶ Verschlüsseln und Signieren sind unabhängig voneinander

öffentliche PGP-Schlüssel austauschen

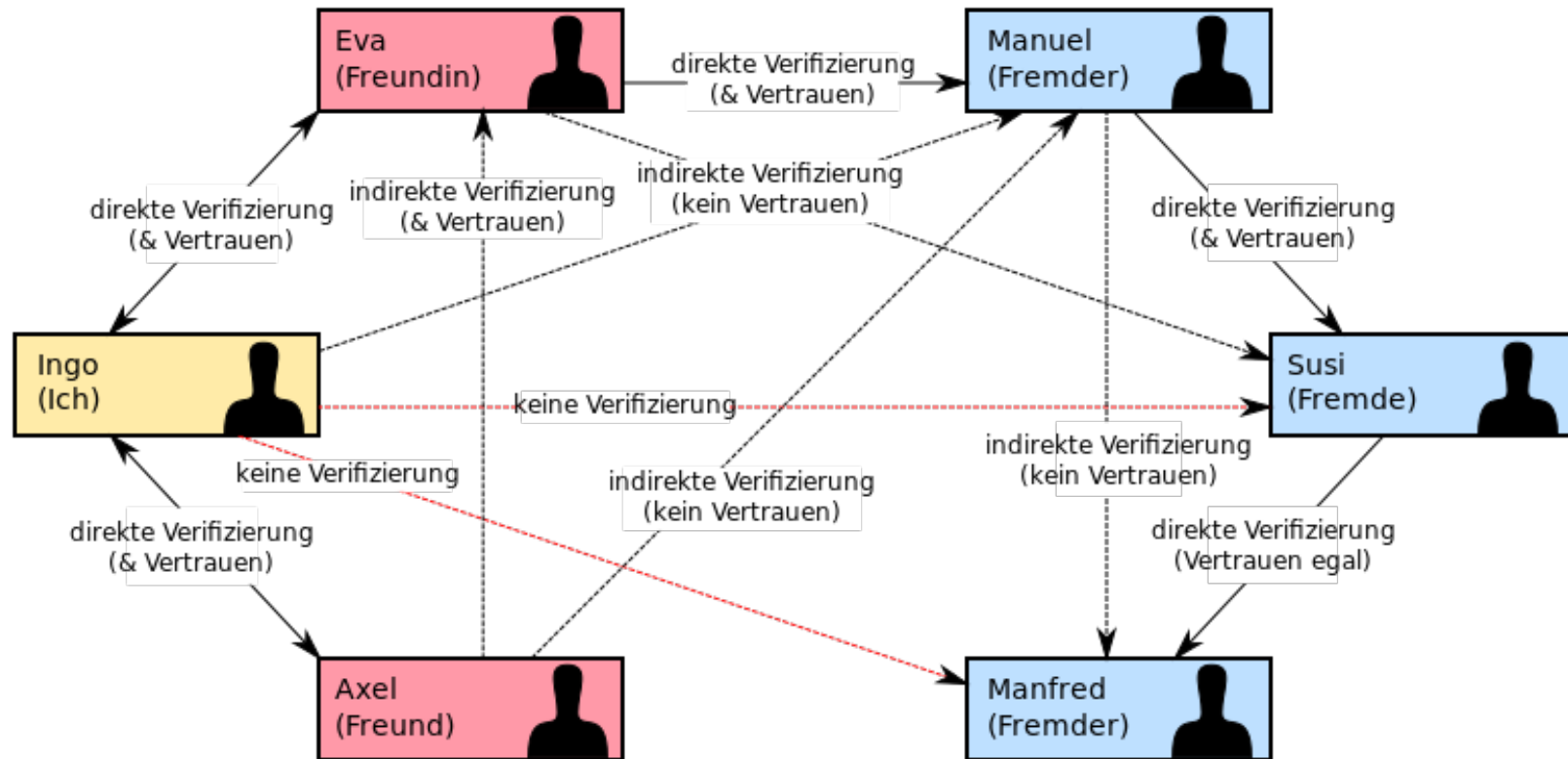
- ▶ E-Mail-Anhang
 - ▷ zur Verteilung im privaten Kreis
- ▶ Key-Server
 - ▷ bequem durchsuchbar
 - ▷ E-Mail-Adresse öffentlich einsehbar
- ▶ Habe ich den richtigen Schlüssel bekommen?
 - ▷ komplexes Thema → Schlüssel signieren, „Web of Trust“
 - Web of Trust von Thunderbird 78+ nicht unterstützt → Schlüssel „akzeptieren“
 - ▷ 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 Thunderbird



Web of Trust



CC-BY-SA Ogmios (Wikimedia Commons)

– Ende E-Mail-Verschlüsselung –