E-Mail-Verschlüsselung

Alternativen zu „kostenlosen“ E-Mail-Anbietern

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

Vorteile

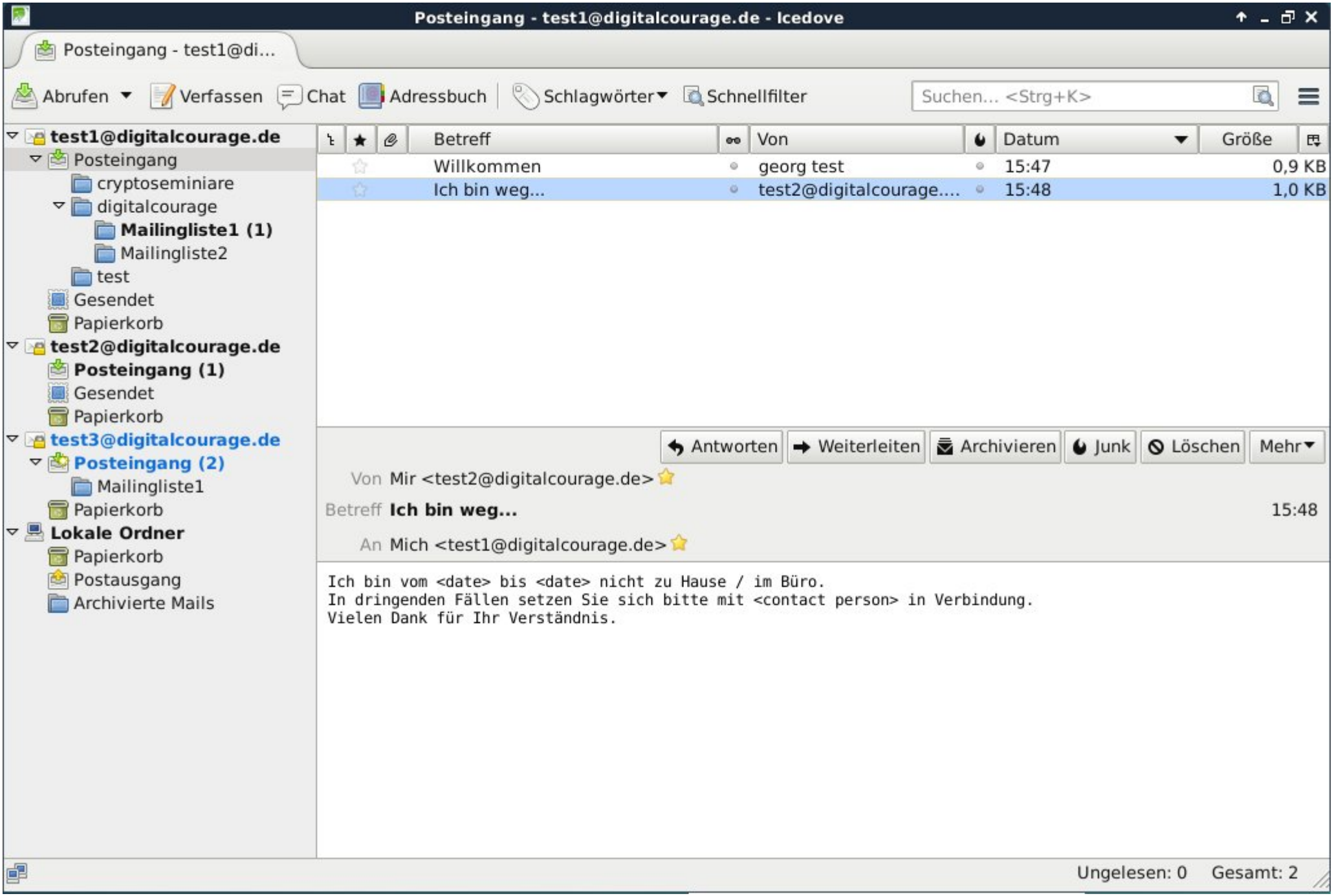
- Standort in Deutschland
- Datensparsamkeit
- keine Inhaltsanalyse
- keine Werbung
- anonyme Nutzung möglich
- Datenschutz hat Priorität

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
  - HTML abschalten möglich
  - 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 *Use Bcc Instead C*)
    - **Verschlüsselung (Enigmail)**


Posteingang - test1@digitalcourage.de - Icedove
Posteingang - test1@di...
Abrufen
Verfassen
Chat
Adressbuch
Schlagwörter
Schnellfilter
Suchen... <Strg+K>
test1@digitalcourage.de
Posteingang
cryptoseminiare
digitalcourage
Mailingliste1 (1)
Mailingliste2
test
Gesendet
Papierkorb
test2@digitalcourage.de
Posteingang (1)
Gesendet
Papierkorb
test3@digitalcourage.de
Posteingang (2)
Mailingliste1
Papierkorb
Lokale Ordner
Papierkorb
Postausgang
Archivierte Mails
Betreff
Von
Datum
Größe
Willkommen
georg test
15:47
0,9 KB
Ich bin weg...
test2@digitalcourage....
15:48
1,0 KB
Antworten
Weiterleiten
Archivieren
Junk
Löschen
Mehr
Von Mir <test2@digitalcourage.de>
Betreff Ich bin weg...
15:48
An Mich <test1@digitalcourage.de>
Ich bin vom <date> bis <date> nicht zu Hause / im Büro.
In dringenden Fällen setzen Sie sich bitte mit <contact person> in Verbindung.
Vielen Dank für Ihr Verständnis.
Ungelesen: 0
Gesamt: 2

E-Mail-Verschlüsselung (PGP / GnuPG)

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

Benötigte Software:

- E-Mail Programm: Thunderbird
- Add-on: **Enigmail**
  - **p≡p** (Pretty Easy Privacy) nutzen wir noch nicht (ggf. deaktivieren)

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

- Öffentlicher Schlüssel
  - kann und muss verteilt werden (an alle, über unsichere Kanäle)
- Privater Schlüssel
  - bleibt privat – gut schützen und sichern, niemals herausgeben!
- Zentrale Voraussetzungen
  - private Schlüssel können von niemand sonst benutzt werden
  - öffentliche Schlüssel sind unverfälscht und korrekt zugeordnet

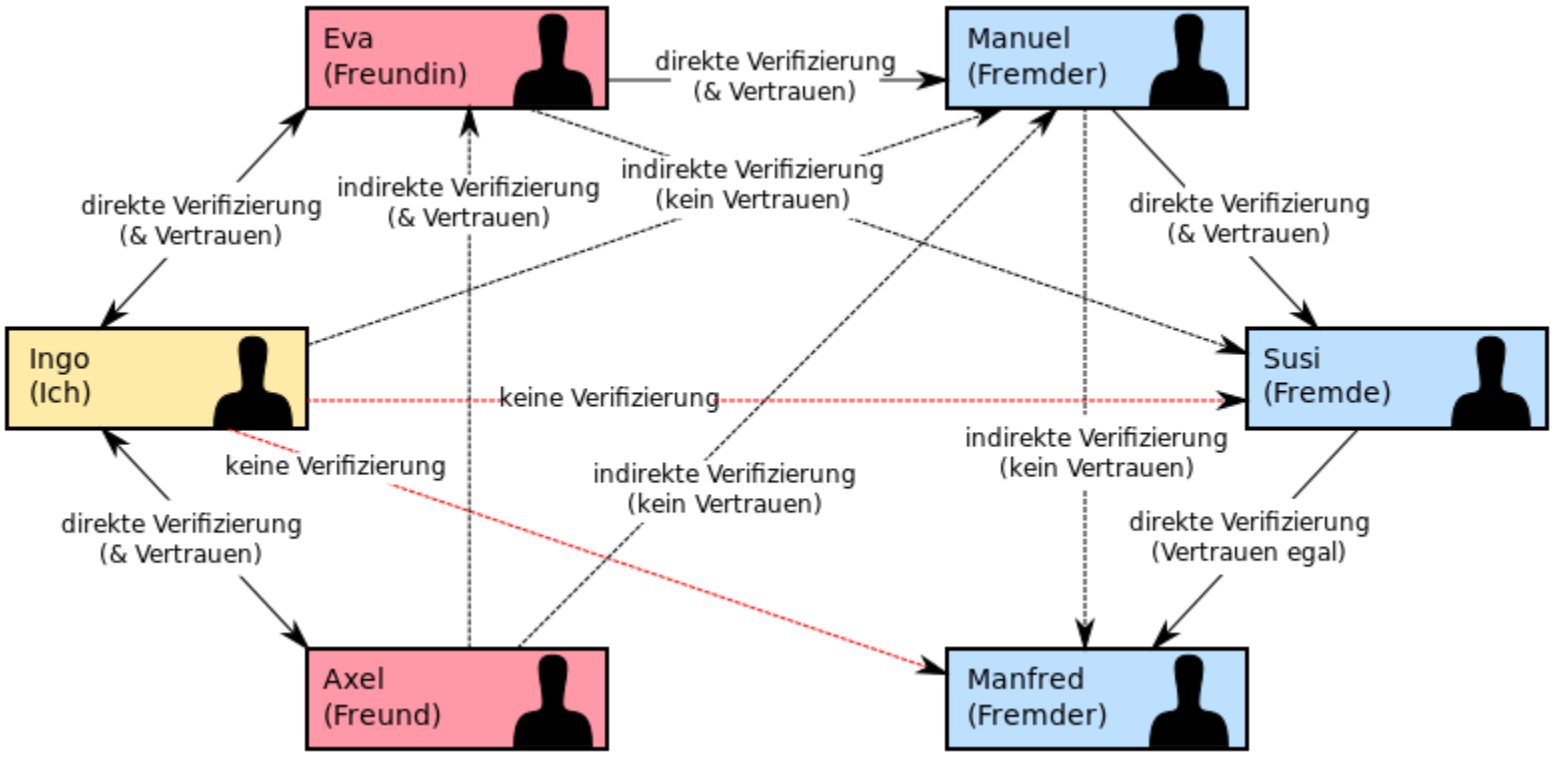
E-Mails verschlüsseln und signieren

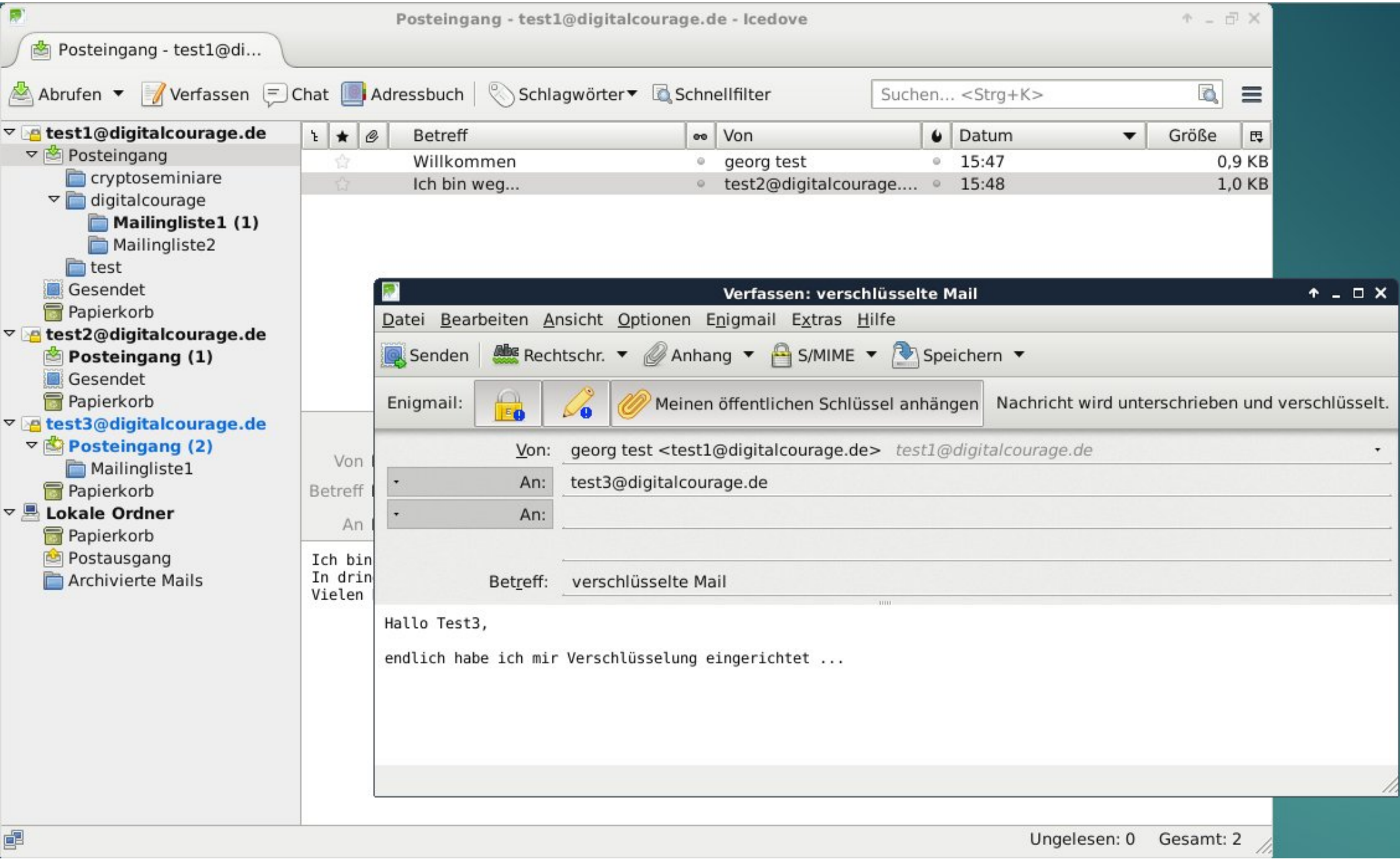
- Verschlüsseln
  - sichert Vertraulichkeit der Nachricht
  - verwendet den **öffentlichen Schlüssel des Empfängers**
    (nur der Empfänger kann mit privatem Schlüssel entschlüsseln)
- Signieren
  - sichert Unverfälschtheit der Nachricht und wer sie verfasste
  - nicht verwechseln mit Unterschrift und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

Web of Trust




Posteingang - test1@digitalcourage.de - Icedove
Posteingang - test1@di...
Abrufen
Verfassen
Chat
Adressbuch
Schlagwörter
Schnellfilter
Suchen... <Strg+K>
test1@digitalcourage.de
Posteingang
cryptoseminiare
digitalcourage
Mailingliste1 (1)
Mailingliste2
test
Gesendet
Papierkorb
test2@digitalcourage.de
Posteingang (1)
Gesendet
Papierkorb
test3@digitalcourage.de
Posteingang (2)
Mailingliste1
Papierkorb
Lokale Ordner
Papierkorb
Postausgang
Archivierte Mails
Betreff
Von
Datum
Größe
Willkommen
georg test
15:47
0,9 KB
Ich bin weg...
test2@digitalcourage....
15:48
1,0 KB
Verfassen: verschlüsselte Mail
Datei Bearbeiten Ansicht Optionen Enigmail Extras Hilfe
Senden
Rechtschr.
Anhang
S/MIME
Speichern
Enigmail:
Meinen öffentlichen Schlüssel anhängen
Nachricht wird unterschrieben und verschlüsselt.
Von:
georg test <test1@digitalcourage.de>
test1@digitalcourage.de
An:
test3@digitalcourage.de
An:
Betreff:
verschlüsselte Mail
Hallo Test3,
endlich habe ich mir Verschlüsselung eingerichtet ...
Ungelesen: 0
Gesamt: 2

– Ende E-Mail-Verschlüsselung –