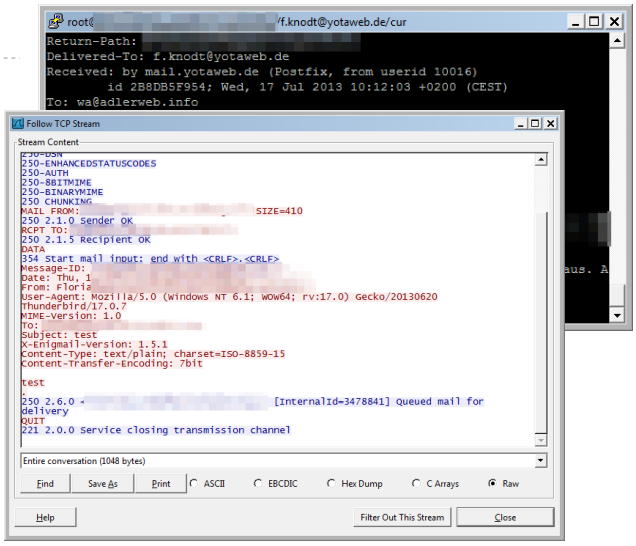
E-Mail-Verschlüsselung unter Linux

Wie sicher ist eine „normale“ E-Mail

- E-Mails werden im Internet üblicherweise unverschlüsselt übertragen
- Jeder mit Zugriff auf den Datenstrom kann die E-Mail lesen und manipulieren
  - Personen im selben Netzwerk
  - Internetprovider und Netzbetreiber zwischen Start und Ziel
  - Geheimdienste
  - etc
- SSL/TLS schützt nur auf dem Weg zwischen PC und Mailserver, zwischen und auf den Servern selbst sind die Daten meist trotzdem unverschlüsselt



Womit kann man die Inhalte verschlüsseln?

	PGP/GPG	S/MIME
Schlüsselverwaltung	Dezentrales Web-of-trust	Zentrale Cert-Authorities
Clientunterstützung(Mail)	Via Plugin	Meist Integriert
Anwendung	E-Mail, Dateien, u.v.a	Nur E-Mail
Verschlüsselung	Nur Mailinhalt, keine Metadaten	Nur Mailinhalt, keine Metadaten

Clientunterstützung

- S/MIME
  - Thunderbird: Nativ
  - Claws: nativ
  - Android Mail: DJIGZO S/MIME Plugin
  - Android K9: Nativ
  - Outlook: Nativ
  - Lotus Notes: Nativ
  - Firefox: „Gmail-SMIME“ (nur GMail)
  - Chrome: N/A

- PGP/GPG (http://www.gnupg.org/)
  - Thunderbird: Enigmail
  - Claws: GPG-Plugin / GPGME
  - Android Mail: Nicht möglich
  - Android K9: Nativ mit APG
  - Outlook: GPG4Win / „Outlook Privacy Plugin“
  - Lotus Notes: PGPNotes (kommerziell)
  - Firefox/Chrome: Mailvelope

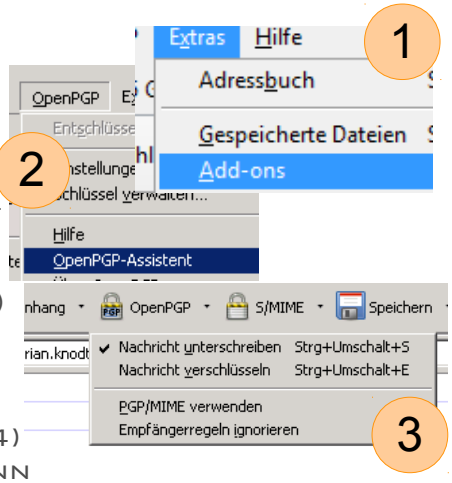
Begriffe

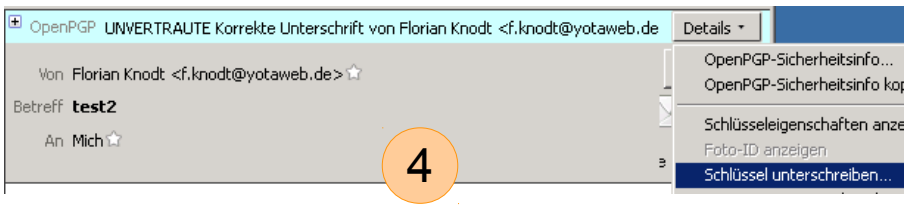
- **Certificate Authority (CA)** Zentrale Prüfstelle für öffentliche Schlüssel. Kommt u.A. bei HTTPS und S/MIME zum Einsatz
- **Metadaten** Bei E-Mail u.A. Absender, Empfänger, Betreff, verwendete Software und Datum
- **Schlüssel** Der „Ausweis“ für die Verschlüsselung. Besteht aus einem öffentlichen und einem privaten Teil – nur der Private kann entschlüssen und darf daher nicht weitergegeben werden
- **Signieren** Digitale Unterschrift – stellt sicher, dass der Text vom Schlüsselinhaber stammt und nicht verändert wurde.
  Im Zusammenhang mit PGP-Schlüsseln: Für die Identität eines fremden Schlüssels bürgen
- **Verschlüsseln** Daten werden mit Hilfe des öffentlichen Schlüssels unlesbar gemacht und können nur vom Besitzer des privaten Schlüssels gelesen werden
- **Web Of Trust (WoT)** Dezentrales System zur Verwaltung von Vertrauensstellungen. Wird u.A. bei PGP/GPG eingesetzt

Mehr Tipps & Tricks rund um Verschlüsselung im Internet: https://www.cryptoparty.in/documentation/handbook

E-Mail-Verschlüsselung Mit Thunderbird

- Über Paketmanager „GPG“ oder „GnuPG“ installieren (meist vorinstalliert)
- Im Add-on-Manager („Extras“►„Add-ons“) „Enigmail“ installieren, neu starten (1)
- Einrichtungsassistent über „OpenPGP“► „OpenPGP-Assistent“ starten (2)
- Die Fragen gemäss eigenen Wünschen auswählen
- neues Schlüsselpaar erzeugen
- Widerrufszertifikat: Hiermit kann der Schlüssel bei Verlust/Datenklau ungültig markiert werden
- Beim Senden kann über die Schaltfläche „OpenPGP“ das Verhalten angepasst werden. (3)
- Schlüssel können über „OpenPGP“►„Schlüssel verwalten“ importiert werden
- Eingehende Nachrichten werden automatisch verarbeitet, Status wird in neuer Zeile gezeigt (4)
- Über „Details“►„Schlüssel unterschreiben“ kann das Vertrauen des Absenders festgelegt werden (4)





E-Mail-Verschlüsselung Im Browser

Chrome: Im Extension-Manager
Firefox: https://github.com/toberndo/mailvelope/raw/firefox/dist/mailvelope.xpi (Beta)

- Extension/Add-On installieren
- Über die Mailvelope-Schaltfläche können Schlüssel verwaltet oder erstellt werden (1)
- Auf der Webseite des Mail-Anbieters Mailvelope-schaltfläche drücken und „Add Page“ wählen (2)
- Über die im Textfeld erscheinende Schaltfläche den Editor öffnen (3)
- Über die Schlüssel-Schaltfläche im Editor die Mail verschlüsseln
- Eingehende Nachrichten können per Klick auf das Entschlüsselungssymbol verarbeitet werden (4)
- Hinweis: Browser sind ggf. anfälliger für Angriffe