Einführung in Mail-Verschlüsselung für Rookies

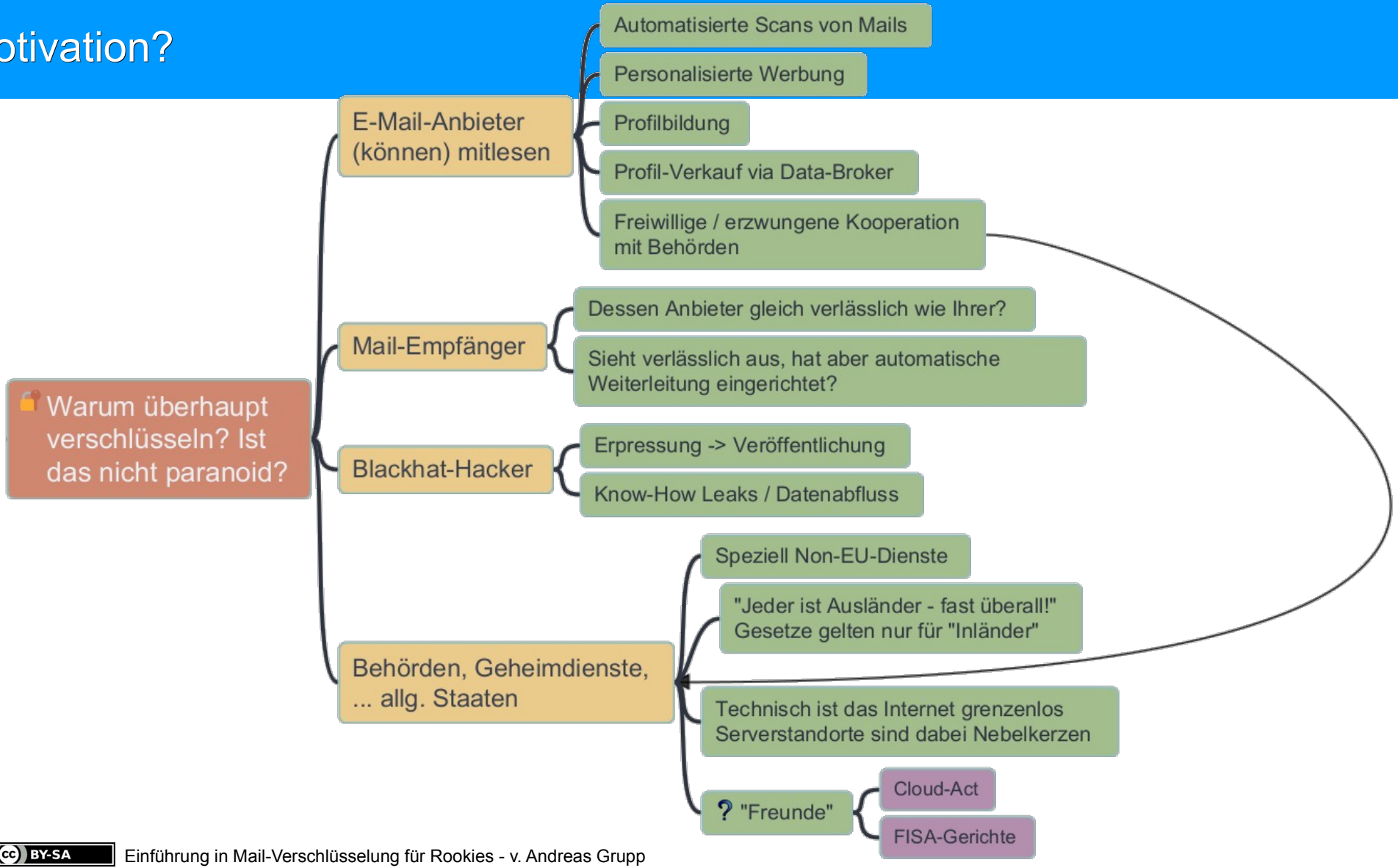
Wikipedia: "*A rookie is a person new to an occupation, profession, or hobby. In sports, a rookie is a professional athlete in their first season (or year).*"

Andreas Grupp

andreas@grupp-web.de

@angry@social.tchncs.de

Motivation?



Mail-Client benutzen! Warum denn das? Ich nehm’ Webmail!?!?

- Vorteile eines Webmailers / Mail in Browser-Oberfläche
  - Internet → Browser → Login … geht! Ist doch fein …!?
- Nachteile eines Webmailers
  - Mails, Adressbuch, Kalender, … nur online lesbar.
  - Alle Daten an jeweiligen Mailprovider gebunden – Lock-In-Effekt!
  - Mailbearbeitung: Lesen und Verfassen nur online möglich
  - Mehrere Mailprovider / -adressen
  - → mehrere verschiedene Webmail-Oberflächen
  - Verschlüsselung meist nur über vorbereiteten Datei-Anhang (z.B. VeraCrypt-Container, 7z-AES-Container, Office-Dokument mit Passwort [dadurch verschlüssel] …)

    Ausnahme: Mailvelope erlaubt OpenPGP-Verschlüsselung im Browser

Mail-Client: Thunderbird

- Freie Software & verschied. Plattformen (Linux, Mac, Windows)
- Viele Grundfähigkeiten, zusätzlich über Add-On's erweiterbar
- Auch Portable (z.B. auf USB-Stick, in verschlüsseltes VeraCrypt-Volume) installierbar
- Generelle Fähigkeiten von Mail-Clients:
  - POP3S- und IMAPS-fähig
  - Mehrere Mailkonten / -provider in **einer** Software
  - Offline-Bearbeitung von Mails
  - Mail-Provider unabhängige Adressbücher, Kalender, …
    - Können auch Mailkonten-übergreifend genutzt werden
  - Verschlüsselung von Mails & Anhängen per Default möglich

Video 1: Mailprogramm einrichten, Schlüssel erzeugen

Inhalt:
- Vorspann: SMTP/IMAP bei Providern
- Thunderbird mit Mailkonto verknüpfen
- Schlüsselpaar erzeugen

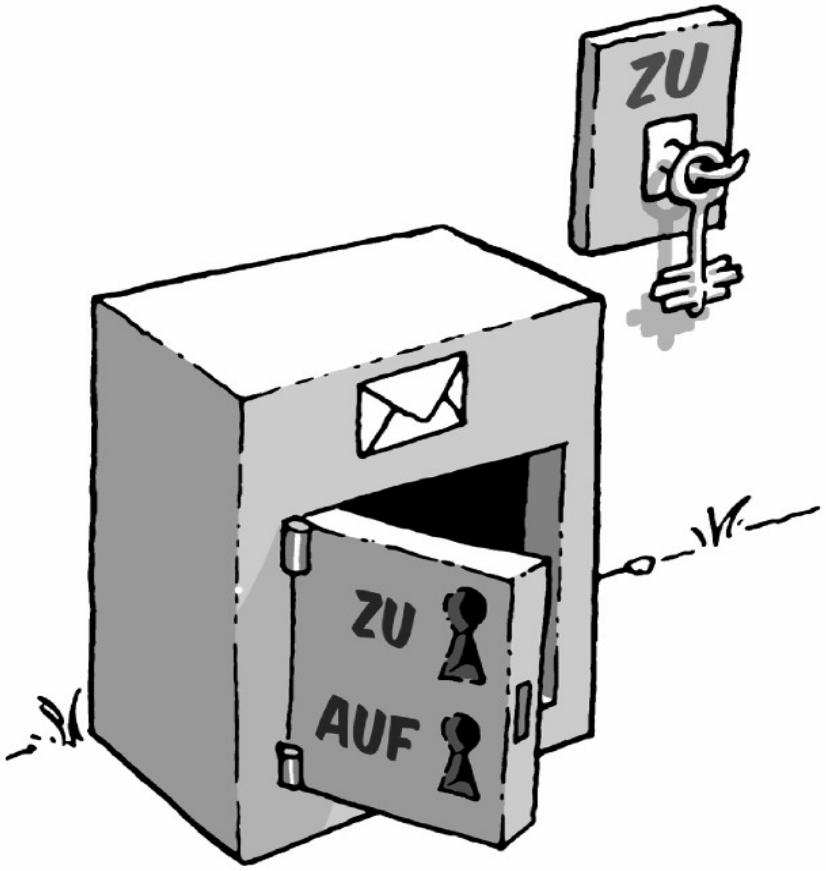
… oder in 5 Minuten können wir verschlüsselt mailen!

→ https://tube.tchncs.de/w/m72VWx7w8KbHd4UNWSb9Q7

Verschlüsselung von Mails

- Zwei Standards / Verfahren verfügbar
  - Beide technisch auf gleicher Basis (asymmetrische Verschlüsselung)
  - S/MIME – offiziell standardisiert
    - Wie bei https → X.509-Zertifikate, **kostenpflichtig, zeitlimitiert**
  - GnuPG / OpenPGP
    - existiert länger als S/MIME, IETF-Proposed-Standard, der dafür aber weltweit verbreitet und kostenfrei ist.
- Mailprogramme unterstützen meist von Haus aus S/MIME
  - Thunderbird unterstützt darüber hinaus OpenPGP
  - Outlook (die lokal installierte Variante) ist mit PGP nachrüstbar
- S/MIME de-facto nicht nutzbar
- Deshalb Konzentration auf OpenPGP-Standard

Grundprinzip der asymmetrischen Verschlüsselung (1)

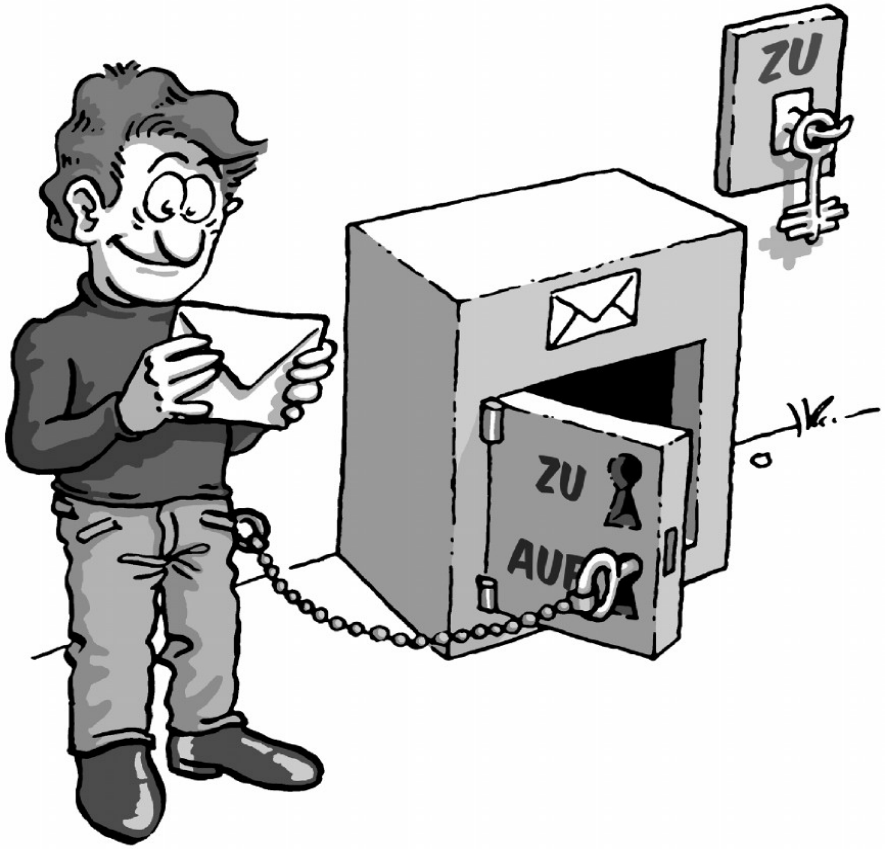


Durch den öffentlich verfügbaren „ZU“-Schlüssel kann jede Person etwas „einschließen“
→ **Verschlüsseln**

Einmal verschlüsselt kann es mit dem dafür genutzten öffentlichen Schlüssel (auch Public-Key genannt) nicht mehr entschlüsselt werden!

Grafik-Quelle: Gpg4win-Kompendium
http://www.gpg4win.org/doc/de/gpg4win-compendium.html

Grundprinzip der asymmetrischen Verschlüsselung (2)



Öffnen kann nur die Person die den „AUF“-Schlüssel hat
→ **Entschlüsseln**

Dieser private Schlüssel (auch Secret-Key genannt) wird nie „aus der Hand“ gegeben!

Grafik-Quelle: Gpg4win-Kompendium
http://www.gpg4win.org/doc/de/gpg4win-compendium.html

Was benötigen wir somit für Mail-Verschlüsselung?

- Mail-Software …
  - die den OpenPGP-Standard eingebaut hat
  - die per Plugin OpenPGP nachrüstet (Outlook mit Gpg4win)
  - Web-Mailer-Software mit passender Unterstützung
- Jede Person benötigt …
  - Ein persönliches Schlüsselpaar, bestehend aus
    - öffentlichem Schlüssel (Public-Key)
    - privatem Schlüssel (Secret-Key)
  - Für jede/n Kommunikationspartner:in mit der/dem verschlüsselte Mails ausgetauscht werden sollen
    - deren öffentlicher Schlüssel / deren Public-Key

Video 2: Mailverschlüsselung einrichten

Inhalt:

- Erster Versuch verschlüsselt zu mailen
- Automatische Lösung mit Autocrypt
- Ein erster Blick in die Schlüsselverwaltung

→ https://tube.tchncs.de/w/o7JcmKQ8rV6LPxD5UPdPFz

Schlüssel-Management – die Kür, aber ein auf Dauer wichtiger Teil!

- Persönliche Schlüsselpaare immer sichern & für immer aufbewahren!
  - Übertragung auf andere Endgeräte
  - Abgelaufene, private Schlüssel → z.B. für Mailsausgang WICHTIG!
  - Defekte Datenträger
  - …
- Öffentliche Schlüssel
  - als Mailanhang für Mail-Clients ohne Autocrypt
  - auf Schlüssel-Server exportieren
- Widerrufs-Zertifikat
  - für kompromitierte Schlüssel
  - für Schlüssel bei vergessenem Passphrase

Video 3: Schlüssel-Management

Inhalt:

- Datei-Export des öffentlichen Schlüssels
- Verschlüsselter Datei-Export/-Sicherung des privaten Schlüssels
- Widerrufs-Zertifikat
- Bereitstellung des öffentlichen Schlüssels über einen Schlüsselserver

→ https://tube.tchncs.de/w/xskei1jMBNKN7nT6gxSBAi

Noch mal zu Web-Mailern und OpenPGP

- Web-Mail, je nach eingesetzter Web-Anwendung …
  - Mit Browser-AddOn Mailvelope - https://mailvelope.com/de - aktiv von vielen Webmail-Anwendungen bzw. Mail-Providern unterstützt
    - JavaScript und speichert Schlüsselmaterial im Browse
  - OX Guard für Open-Xchange
    - Voll in die Web-Anwendung integriertes Add-On
    - Key, auch privater Schlüssel, auf Server!
      - Vor- und Nachteile

Ausblick

- PGP / GnuPG / … als eigenständiges Werkzeug
  - Über erweiterte Einstellungen in Thunderbird möglich
- Gpg4win (Windows, Outlook, …) - https://www.gpg4win.de/
- „*Niemand aus meinen Kreisen nutzt / unterstützt / kann das*“:
  - Nun … ja … wie immer … verbreitet die Botschaft, seid Ambassadors
  - Die Videos dauern rund 20 Minuten, dann ist man fertig!
- S/MIME organisationsintern nutzen – wenn man’s unbedingt will
  - Public Key Infrastructure (PKI) mit z.B. langer Laufzeit
  - Organisationsinterne S/MIME-Zertifikate mit langer Laufzeit

So … Fragen … schießt los!

Videos als Playlist https://tube.tchncs.de/w/p/hX9zVEpik6rksw2VNvvbkT

```
andreas@r-saentis:~> qr --error-correction=H \
> https://tube.tchncs.de/w/p/hX9zVEpik6rksw2VNvvb
```