

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



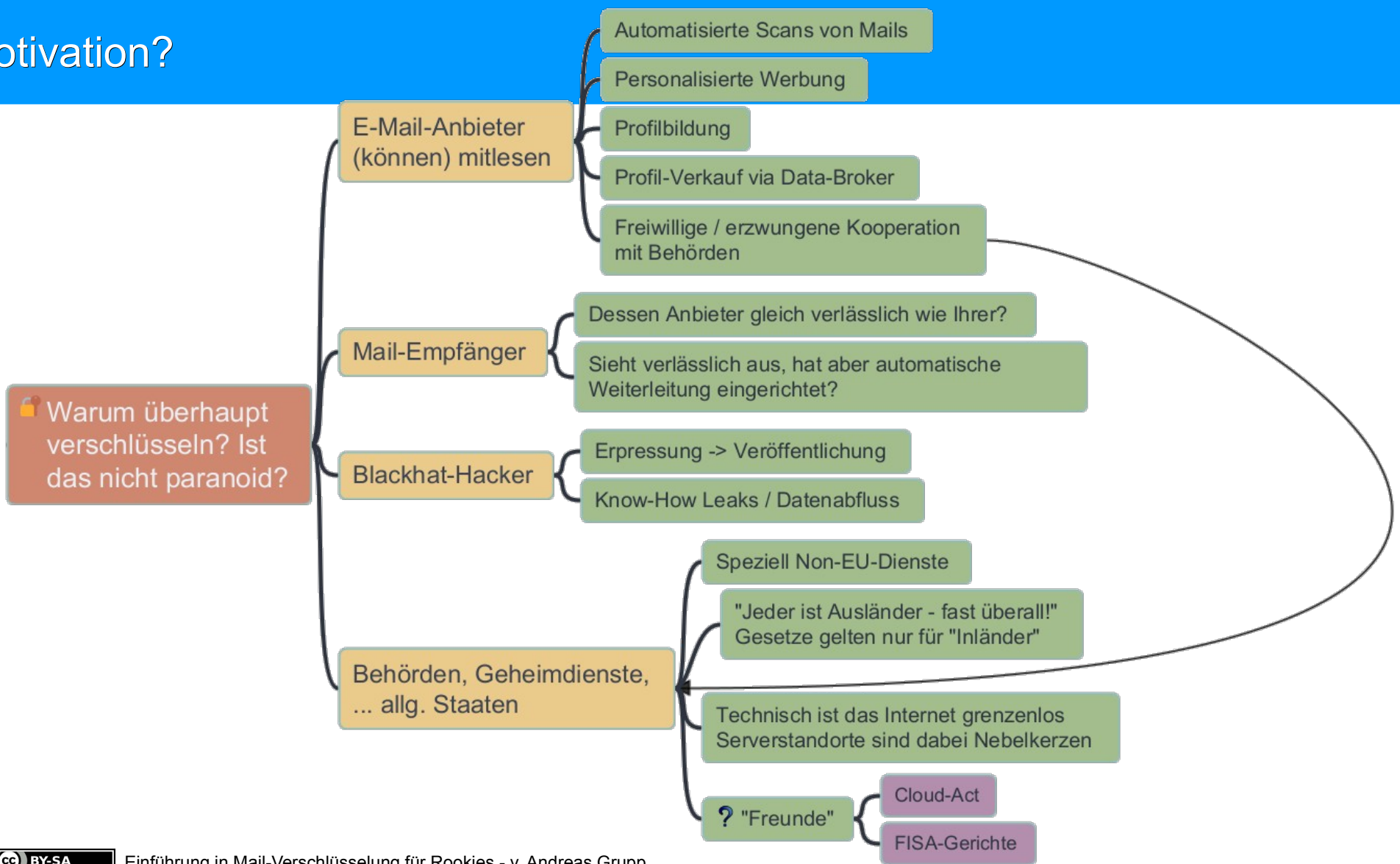
andreas@grupp-web.de

[@angry@social.tchncs.de](#)



"Einführung in Mail-Verschlüsselung für Rookies"
© 2024 by [Andreas Grupp](#) is licensed under
[Attribution-ShareAlike 4.0 International](#)

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 verschlüsselt] ...)
Ausnahme: Mailvelope erlaubt OpenPGP-Verschlüsselung im Browser



- 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



Inhalt:

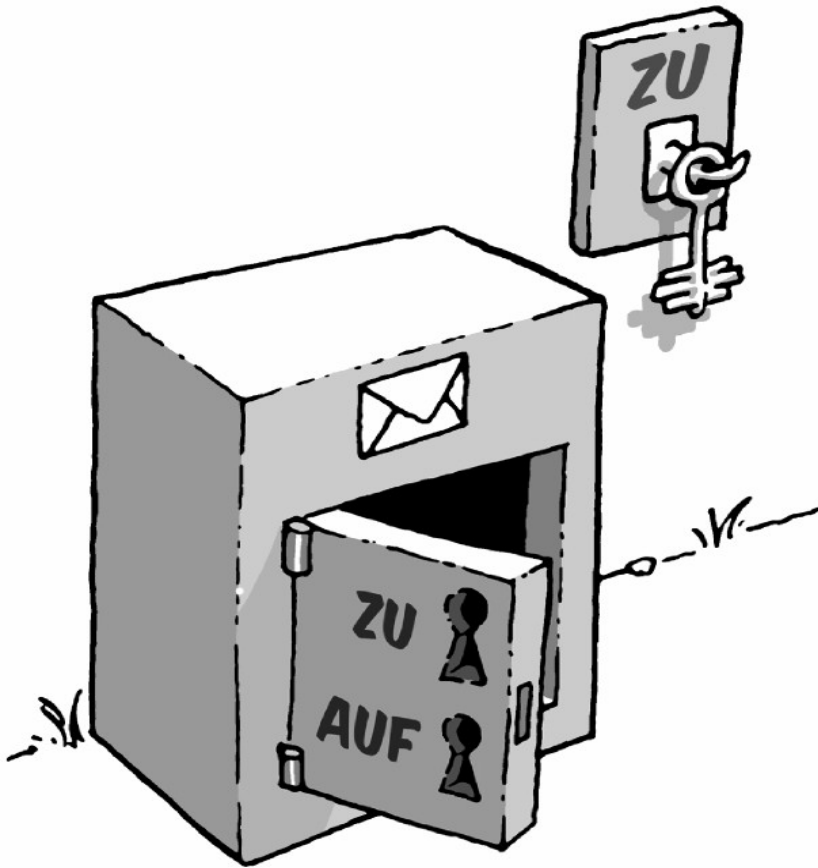
- Vorspann: SMTP/IMAP bei Providern
- Thunderbird mit Mailkonto verknüpfen
- Schlüsselpaar erzeugen

... oder in 5 Minuten können wir verschlüsselt mailen!

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

- 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

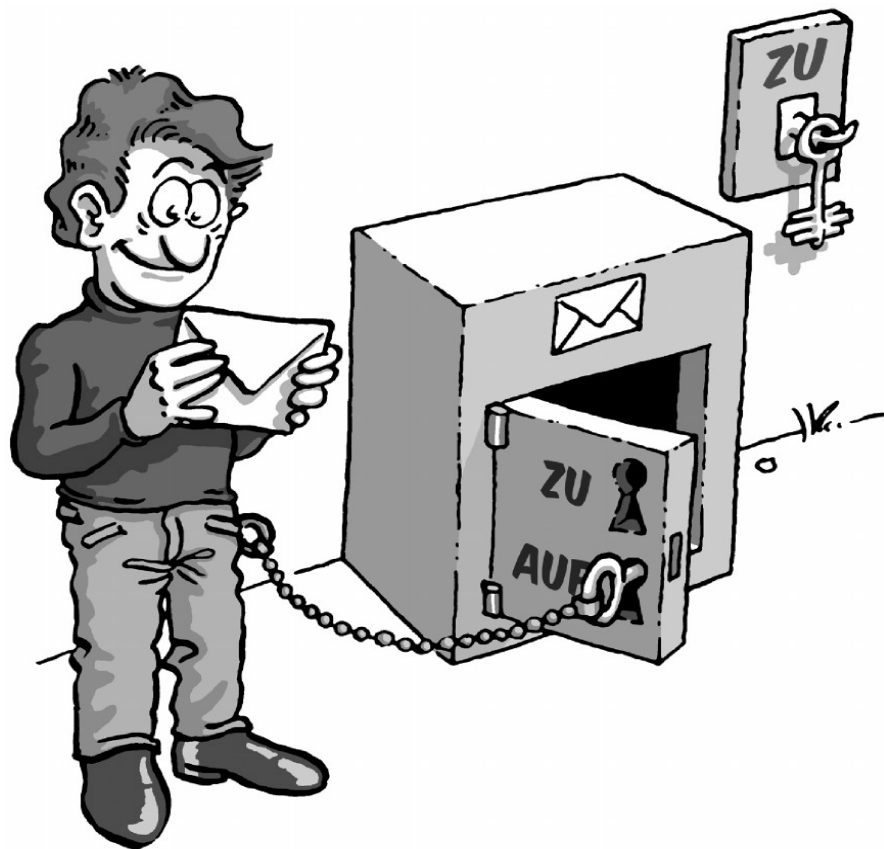
<http://www.gpg4win.org/doc/de/gpg4win-compendium.html>

Copyright c 2002 Bundesministerium für Wirtschaft und Technologie

Copyright c 2005 g10 Code GmbH

Copyright c 2009, 2010 Intevation GmbH

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>

Copyright c 2002 Bundesministerium für Wirtschaft und Technologie

Copyright c 2005 g10 Code GmbH

Copyright c 2009, 2010 Intevation GmbH

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



Inhalt:

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

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

- 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 vergessener Passphrase



Inhalt:

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

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

- 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 Browser
 - OX Guard für Open-Xchange
 - Voll in die Web-Anwendung integriertes Add-On
 - Key, auch privater Schlüssel, auf Server!
 - Vor- und Nachteile

- Suche nach Mails mit bestimmten Inhalten, Wörtern, ...
 - TB speichert derzeit verschlüsselte Mails in diesem Zustand
 - Suchfunktion durchsucht diese Mails nicht!
 - Suche nicht einmal dann wenn Mails vorher entschlüsselt werden!
 - https://bugzilla.mozilla.org/show_bug.cgi?id=1562737
- Lösungsansatz (Stand 20.4.24 bei erstem Test **nicht funktioniert**)
 - Betterbird - <https://www.betterbird.eu/>
 - „*Betterbird is a fine-tuned version of Mozilla Thunderbird, Thunderbird on steroids, if you will*“
 - Betterbird hat offenbar Suche für OpenPGP- und S/MIME-verschlüsselte Mails implementiert
 - Parallelinstallation beider Anwendungen möglich!

- 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!

```
andreas@r-saentis:~> qr --error-correction=H \  
> https://grupp-web.de/cms/2024/03/16/e-mail-verschluesselung-fuer-rookies/
```



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

