

Allgemein

Allgemein gültige Tutorials

- [Yubikey Nutzung](#)
- [E-Mail Verschlüsselung mit OpenPGP](#)
- [Archiv komprimieren mit Tar und Gzip](#)
- [Daten Größen auflisten](#)
- [Latex und VS-Code](#)
- [Battery Status Laptop](#)
- [ZSH mit Theme](#)
- [Windows Virtualization with Gnome-Boxes](#)

Yubikey Nutzung

- [Mit Yubikey unter Arch Linux einloggen \(Challenge-Response, offline\)](#)

Yubikey GPG

Zu PGP siehe [E-Mail Verschlüsselung mit OpenPGP](#)

- [importing Keys](#)
- [PGP Walk-Through](#)
- [ausführliches doc hier](#)

E-Mail 2 Yubikeys

Having created two (or more Yubikeys) with the same GPG key (as described above) where the stubs are pointing to the second Yubikey.

Insert the first Yubikey (which has a different serial number) and run the following command:

```
$ gpg-connect-agent "scd serialno" "learn --force" /bye
```

GPG will then scan your first Yubikey for GPG keys and recreate the stubs to point to the GPG keyID and Yubikey Serial number of this first Yubikey. To return to using the second Yubikey just repeat (insert other Yubikey and re-run command).

E-Mail Verschlüsselung mit OpenPGP

Tiefere Infos unter gnupg.org. GnuPG (GPG) implementiert den OpenPGP Standard.

- [Cheat Sheet Commands](#)
- [one key 2 e-mails](#)
- [keys mit Smartcard \(yubikey\)](#)
- [Key setup](#)

Clients

Um verschlüsselte E-Mails versenden zu können benötigt man einen Client zum verwalten der **Schlüssel**, sowie einen E-Mail Client, welcher fähig ist verschlüsselte Mails zu senden und zu empfangen. Eine **Liste an E-Mail Clients** kann [hier](#) gefunden werden. Für Desktop empfehle ich Thunderbird, für Android FairMail, sowie OpenKeychain zum verwalten der Schlüssel.

Schlüssel erstellen

Ein Schlüssel Paar bestehen aus Privatem und Öffentlichem Key kann einfach in Thunderbird erstellt werden: **Extras --> OpenPGP-Schlüssel verwalten --> Erzeugen --> Neues Schlüsselpaar** Anschließend die E-mail auswählen und mit den Standardeinstellungen erzeugen.

Schlüssel verteilen

Wichtig niemals den privaten Schlüssel weitergeben!!

Privaten Schlüssel

Der Private Schlüssel kann in Thunderbird mit der Option **Datei --> Sicherheitskopie für geheimen Schlüssel erstellen** als Datei gespeichert werden. Diese Datei sollte dann über einen Sicheren Weg (z.B unsere Nextcloud) auf die anderen Clients(z.B. dein Handy), von denen du verschlüsselte Mails senden möchtest verteilt werden.

Öffentlicher Schlüssel

Um deinem E-Mail Empfänger deinen Öffentlichen Schlüssel zugänglich zu machen, sollte dieser auf einem Key-Server hochgeladen werden. key.openpgp.org wird als Standard von den meisten Clients verwendet. Der Öffentliche Schlüssel kann über das [Webinterface](#) hochgeladen werden.

Schlüssel eines Anderen suchen

Über Thunderbird sowie allen anderen Clients kann über eine Option wie z.B in Thunderbird **OpenPGP-Schlüssel verwalten --> Schlüsselservers --> Schlüssel online finden** der Öffentliche Schlüssel andere Leute importiert werden.

Verschlüsselte E-mails senden/empfangen/unterschreiben

Wichtig in Thunderbird muss möglicherweise unter den Konteneinstellungen den jeweiligen Identitäten unter "**Ende-zu-Ende-Verschlüsselung**" der richtige Schlüssel zugeordnet werden.

Senden

Zum Senden kann in den Mailclients mit einer Funktion, wie z.B. in Thunderbird **OpenPGP --> Verschlüsseln** beim verfassen der Mail diese verschlüsselt werden. Anschließend einfach Senden. **Wichtig** zum Senden einer verschlüsselten Mail wird der Öffentliche Schlüssel des Empfängers benötigt!

Empfangen

Beim Empfangen sollten die verschlüsselten Mails automatisch entschlüsselt werden.

Unterschreiben

E-mails können mit einem OpenPGP Schlüssel unterschrieben werden, sodass der Empfänger sicherstellen kann, dass diese nicht verändert wurde (Man-in-the-Middle). Um eine empfangene unterschriebene Mail als authentisch zu erkennen, wird der Öffentliche Schlüssel des Senders benötigt.

Archiv komprimieren mit Tar und Gzip

Archiv komprimieren mit Tar und Gzip

Archiv **extrahieren**:

```
sudo tar -xvzf documents.tar.gz
```

oder mit **Zielordner**:

```
sudo tar -xvzf documents.tar.gz -C /opt/containers
```

now Variable erstellen:

```
now=`date +"%Y-%m-%d"`
```

Inhalt eines Ordner **komprimieren**:

```
cd /opt  
sudo tar -cvzf containers_${now}.tar.gz containers
```

Daten Größen auflisten

Mit dem commandline tool `ncdu` kann aufgelistet werden wo welche daten und wie groß gespeichert sind

```
sudo pacman -S ncdu
```

Latex und VS-Code

Hier gibts das Tutorial für Latex und VS-Code: mathjiajia.github.io

Battery Status Laptop

Mit folgendem Command können sie alle möglichen Informationen über ihre Laptopbattery bekommen:

```
sudo tlp-stat -b
```

ZSH mit Theme

- Empfehlenswert alle zsh sachen mit [oh-my-zsh](#) zu machen
 - change to zsh shell: `chsh -s /bin/zsh username`
 - zsh-syntax-highlighting
 - zsh-autosuggestions
 - zsh-history-substring-search
 - [Powerlevel 10K Theme](#)
 - Da Powerlevel 10K nicht mehr maintend wird gibt es [Starship](#) als alternative. Ich kann empfehlen seine shell initial mit einem [Preset](#) zu stylen

Link zu meiner (Michi) .zshrc Konfig [hier](#)

Windows Virtualization with Gnome-Boxes

For easy virtualisation i recommend gnome-boxes. Any Linuxdistro is easy to virtualize Windows is a little harder. There are two guides Win 10 i tryed and it worked. The Win 11 guide i haven't tried yet:

- [Windows 10](#)
- [Windows 11](#)