# YubiKey

## Einleitung


## Vergleich mit GnuPG Karte


## GnuPG Karte und YubiKey gleichzeitig

Vorraussetzung: Es wurden bereits Keys erzeugt und auf die Karte verschoben. Im Verzeichnis

```
~/.gnupg/private-keys-v1.d/
```

liegen dann nur „Stubs“, also Verweise dass die Keys auf der Karte zu finden sind.

Von den vollen privaten Keys liegt ein Backup vor, z.B. auf USB Tails-Livesystem im verschlüsselten persistent Storage.

1. Eine Kopie des Backups machen, um damit den YubiKey zu bespielen. Am besten auf dem Tails-Livesystem, oder in einer Ramdisk (sudo mount -t tmpfs -o size=1g tmpfs /pfad/zum/backup)

2. Keys auf YubiKey spielen, selbe schritte wie bei der Karte, aber alle Befehle mit `–home-dir /pfad/zum/backup` ausführen. Hinweis: Es kann nötig sein, den gpg-agent vorher zu killen, damit der Yubikey „freigegeben“ wird. In /pfad/zum/backup/private-keys-v1.d verbleiben Key Stubs.

3. Es gibt nun also zwei Sets von Key Stubs, die gegeneinander getauscht werden können, je nach dem ob die Karte oder der Yubikey genutzt werden sollen. Eine Möglichkeit ist, Symlinks zu nutzen.

a) bisherige Key Stubs (Karte) umbenennen

```
cd ~/.gnupg/private-keys-v1.d/
for f in *.key; do mv $f $f.card-00012345; done # card-ID einsetzen
```

b) Key Stubs für Yubikey reinkopieren

```
cd /pfad/zum/backup/private-keys-v1.d/
for f in *.key; do cp $f ~/.gnupg/private-keys-v1.d/$f.yubikey-12345; done #
yubikey serial-nr einsetzen
```

c) Symlinks setzen

```
cd ~/.gnupg/private-keys-v1.d/
for f in *.yubikey*; do ln -s $f ${f%.*}; done
```

Am Ende sieht es so aus:

```
lrwxrwxrwx  1 steppert ldapusers   61 May 23 11:44 D0E019<snip>D032.key ->
D0E019<snip>D032.key.yubikey-012345
-rw-------+ 1 steppert ldapusers 1174 May  9 16:34
D0E019<snip>D032.key.card-0012345
-rw-------+ 1 steppert ldapusers 1199 May 23 11:40
D0E019<snip>D032.key.yubikey-012345
lrwxrwxrwx  1 steppert ldapusers   61 May 23 11:44 D329B7<snip>C811.key ->
D329B7<snip>C811.key.yubikey-012345
-rw-------+ 1 steppert ldapusers 1174 May  9 16:34
D329B7<snip>C811.key.card-0012345
-rw-------+ 1 steppert ldapusers 1199 May 23 11:40
D329B7<snip>C811.key.yubikey-012345
lrwxrwxrwx  1 steppert ldapusers   61 May 23 11:44 E1C58A<snip>3911.key ->
E1C58A<snip>3911.key.yubikey-012345
-rw-------+ 1 steppert ldapusers 1174 May  9 16:34
E1C58A<snip>3911.key.card-0012345
-rw-------+ 1 steppert ldapusers 1199 May 23 11:40
E1C58A<snip>3911.key.yubikey-012345
```

Wenn die Karte genutzt werden soll, werden die Symlinks stattdessen auf die Karte gesetzt:

```
cd ~/.gnupg/private-keys-v1.d/
for f in *.card*; do ln -sf $f ${f%.*}; done
```

Das lässt sich als Alias z.B. in die `.bash-aliases` eintragen:

```
alias gpg-use-card='(cd $HOME/.gnupg/private-keys-v1.d/; for f in *.card*;
do ln -sf $f ${f%.*}; done)'
alias gpg-use-yubikey='(cd $HOME/.gnupg/private-keys-v1.d/; for f in
*.yubikey*; do ln -sf $f ${f%.*}; done)'
```