Yubikey

SSH

hira

```
~/.ssh
├── authorized_keys
├── config
├── hollandpark
│   ├── id_ed25519
│   └── id_ed25519.pub
├── id_ed25519_sk -> michel/id_ed25519_sk_rk_YKc-Michel
├── id_ed25519_sk.pub -> michel/id_ed25519_sk_rk_YKc-Michel.pub
├── josephs
├── known_hosts
├── known_hosts.old
├── michel
│   ├── id_ecdsa_sk-ndc_YKa-Michel
│   ├── id_ecdsa_sk-ndc_YKa-Michel.pub
│   ├── id_ed25519-Michel-automation
│   ├── id_ed25519-Michel-automation.pub
│   ├── id_ed25519_sk-ndc_YKc-Michel
│   ├── id_ed25519_sk-ndc_YKc-Michel.pub
│   ├── id_ed25519_sk-rk_YKc-Michel-automation
│   ├── id_ed25519_sk-rk_YKc-Michel-automation.pub
│   ├── id_ed25519_sk_rk_YKc-Michel
│   └── id_ed25519_sk_rk_YKc-Michel.pub
├── nsas
│   ├── id_ecdsa_sk-NSAS
│   ├── id_ecdsa_sk-NSAS.pub
│   ├── id_ed25519_sk_rk_YKc_NSAS
│   └── id_ed25519_sk_rk_YKc_NSAS.pub
├── old
│   ├── id_ecdsa_sk
│   └── id_ecdsa_sk.pub
├── schraubenscholz
├── sockets
│   └── michel@10.0.3.13:22
├── swissbit
│   ├── id_ecdsa_sk-swissbit
│   └── id_ecdsa_sk-swissbit.pub
└── test

10 directories, 27 files
```

Generating key with a yubikey

Recomendation:

```
ssh-keygen -t ed25519-sk -O application=ssh:YKc-Michel-ndc -O verify-
required -O user=michel
```

This will generate a non discoverable key that used for signing the generated (id*ed25519*sk) So in order to login to an other system, the private key (id*ed25519*sk) and the non discoverable key (on Yubikey) is needed, beside the Yubikey pin and the passphrase.

```
ssh-keygen -t ed25519-sk -O resident -O application=ssh:YKc-Michel -O
verify-required -O user=michel
```

This key can be downloaded from the Yubikey.

```
ssh-keygen -t ed25519-sk -O resident -O application=ssh:YKc-Automation-
Michel -O user=michel -O no-touch-required -C "Michel Pelzer (Automation)-
mp@nsas.de"
```

This key requires the presens of the Yubikey, but does not need to be touched. (authorized*keys) need the* no-touch-required *in front of the public key. <file plain ~/.ssh/authorized*keys> no-touch-required sk-ssh-ed25519@openssh.com AAAAGnNrLXNzaC1lZDI1NTE5QG9wZW5zc2guY29tAAAAIEawzv7L8w9eetH03oc8XHuc02gX/MCmr3sUDHH8opKVAAAAGXNzaDpZS2MtQXV0b21hdGlvbi1NaWNoZWw= </file>

~/.ssh/authorized_keys

```
no-touch-required sk-ssh-ed25519@openssh.com
AAAAGnNrLXNzaC1lZDI1NTE5QG9wZW5zc2guY29tAAAAIEawzv7L8w9eetH03oc8XHuc02g
X/MCmr3sUDHH8opKVAAAAGXNzaDpZS2MtQXV0b21hdGlvbi1NaWNoZWw=
```

Listing key on a Yubikey

```
ykman fido credentials list
```

Deleting key on a Yubikey

```
ykman fido credentials delete ssh:YKc-Automation-Michel
```

Downloading keys from a Yubikey

```
ssh-keygen -K
```

TOTP

ykman

List

```
ykman --reader yubico oath accounts
```

Add <code>ykman –reader yubico oath accounts add “NAME”<code>