Yubikey

SSH

hira

```
~/.ssh
/home/michel/.ssh
├── authorized_keys
├── conf.d
│   ├── hetzner.conf
│   ├── hollandpark.conf
│   ├── nsas.conf
│   ├── other.conf
│   └── swissbit.conf
├── 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
├── swissbit
│   ├── id_ecdsa_sk-swissbit
│   └── id_ecdsa_sk-swissbit.pub
│
```

```
└── test
```

~/.ssh/config

```
#=============================================================================
=
# Global
#=============================================================================
=
include ~/.ssh/conf.d/nsas.conf
include ~/.ssh/conf.d/hetzner.conf
include ~/.ssh/conf.d/hollandpark.conf
include ~/.ssh/conf.d/swissbit.conf
include ~/.ssh/conf.d/other.conf
#=============================================================================
=
# Global
#=============================================================================
=
Host *
    LogLevel QUIET
    ControlMaster auto
    ControlPath ~/.ssh/sockets/%r@%h:%p     # automatically add ssh
keys to running ssh agent (mkdir -p ~/.ssh/sockets)
    ControlPersist yes              # keep connections open
indefinitely, even after logging out
    ForwardAgent yes                # ssh -A host # on the command line
    VerifyHostKeyDNS no             # Specifies whether to verify the
remote key using DNS and SSHFP
    AddKeysToAgent yes
    TCPKeepAlive yes
    Compression yes
    StrictHostKeyChecking no
    VersionAddendum none
    UpdateHostKeys yes
    # IdentitiesOnly yes
    PreferredAuthentications publickey,password
    # HostKeyAlgorithms +ssh-rsa
    # PubkeyAcceptedKeyTypes +ssh-rsa
    # Ensure KnownHosts are unreadable if leaked - it is otherwise
easier to know which hosts your keys have access to.
    HashKnownHosts yes
    # Host keys the client accepts - order here is honored by OpenSSH
    HostKeyAlgorithms ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-
v01@openssh.com,ssh-ed25519,ssh-rsa,ecdsa-sha2-nistp521-cert-
v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-
nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp521,ecdsa-sha2-
nistp384,ecdsa-sha2-nistp256
    KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-
sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
    MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-
```

```
etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-
sha2-256,umac-128@openssh.com
    Ciphers chacha20-poly1305@openssh.com,aes256-
gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
```

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

```
ykman --reader yubico oath accounts add "NAME"
```