

SÄKRARE SSH MED YUBIKEY

Viktor Ahlqvist

2020-02-07

Omegapoint kompetensdag

- Inga nycklar på datorn
- Möjlighet att ta med nycklarna
- Möjliggör lättare backup, skriptad installation, ...

- Master key
 - Skapa nycklar
 - Signera/certifiera nycklar
 - Visa att du äger nycklar
- Subkeys
 - Används för signering, kryptering och/eller autentisering
 - Nycklarna som används vardagligen
- Nycklar kan genereras på Yubiken eller tas in

- Konfigurera med Yubikey manager (ykman)
 - Stäng av OTP

```
$ ykman config usb --disable OTP
```
 - Aktivera touch

```
$ ykman openpgp set-touch aut on
```
 - Byt pin

```
$ gpg --change-pin
```

- Generera på Yubikey eller för in nyckel
- Generera nycklar
generate
- Om intresse: byt nyckeltyp/längd
key-attr

```
$ gpg --card-edit
Reader .....: 1050:04
...
gpg/card> admin
...
gpg/card> key-attr
...
gpg/card> generate
```

- GPG agenten för SSH agenten
- *pinentry* program för att mata in pinkoden
- `$ ssh-add -L` bör visa en `cardno:-nyckel`
- Ladda upp på Github (eller motsv)
- Testa med `$ ssh -v git@github.com`

- Lista kända nycklar
`$ gpg --list-secret-keys --keyid-format LONG`
- Exportera publika nyckeln
`$ gpg --armor --export KEYID`
- Ladda upp på Github (eller motsv)
- Konfigurera git att använda en specifik nyckel
`$ git config --global user.signingkey KEYID`
- Signera commits med -s och taggar med -s
`$ $ git commit -S -a -v`
`$ git tag -a '1.0.0' -m 'First release' -s`

- Presentation och mina instruktioner på
<https://github.com/Omegapoint/yubikey-kompetensdag-2020/>
- Fyll gärna på med egna instruktioner, labbande, lärdomar

- drduhs Yubikey-Guide
<https://github.com/drduh/YubiKey-Guide/>
- Debians information om subkeys:
<https://wiki.debian.org/Subkeys>
- esev <https://www.esev.com/blog/post/2015-01-pgp-ssh-key-on-yubikey-neo/>
- florin (Mac OS) <https://florin.myip.org/blog/easy-multifactor-authentication-ssh-using-yubikey-neo-tokens>
- ixdy (tillägg till florin) <https://gist.github.com/ixdy/6fdd1ecea5d17479a6b4dab4fe1c17eb>