Yubikey

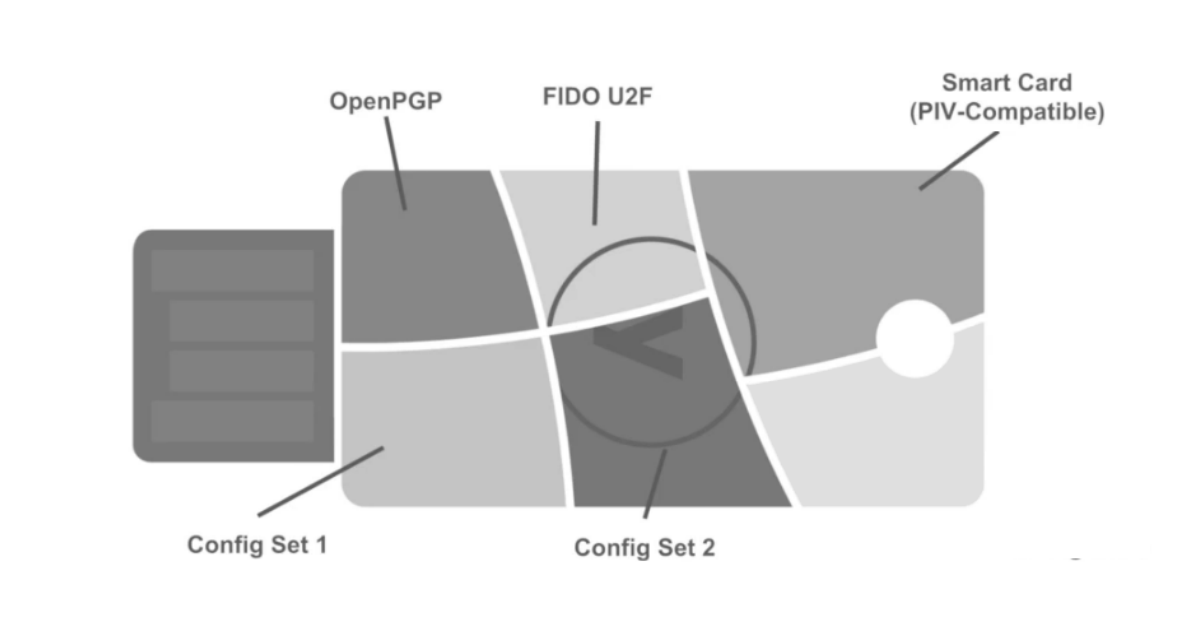
judge

20.12.2018

Hardware Security Token

- Do Crypto stuff external device
- No need for multiple keys or copying of keys to different machines
- There are many Hardware Security tokens, yubikey is a nice low cost variant

One Key to rule them all



Config Slots

- symmetric encryption
- Yubico OTP
- HOTP
- Challenge Response

PGP Smart-card

- asymmetric encryption
- Encryption
- Signing
- Authentication

PIV Smart-card

- asymmetric encryption
- 4 Slots usable for multiple purposes

Second Factor

Website Login

- Yubico OTP
- generate OTP with yubikey, gets validated against yubico cloud (they need to know the symmetric key)

Second Factor

Website Login

- Yubico OTP
- generate OTP with yubikey, gets validated against yubico cloud (they need to know the symmetric key)

Password Manager

- using challenge response
- KeepassXC (or KeepassX with Plugin)
- hash of database, as input to challenge, result gets appended to password

Second Factor

HOTP

- Google Authentication (TOTP)
- TOTP based on HTOP
- symmetric keys stored on yubikey
- generating otp is possible on all platforms

PC login

- Using PIV smart-card
- Sign Challenge with Private Key
- OpenSC + PAM
  `https://github.com/OpenSC/pam_p11`

PGP Smart-card

- Up to 3 slots for, encryption, signing, authentication
- Can configure key press for each action
- move keys to yubikey `https://roll.urown.net/desktop/secrets/yubikey_gpg.html`

SSH Authentication

- Export PGP Public key as SSH key
- Use gpg-agent als ssh-agent
- agent forwarding is possible