your Yubikey with rust

Bernhard Schuster

February 15, 2020


Variants


yubico
yubico


THETIS


SoloKeys


Titan


9:00
Tuesday 7 May | 14 °C

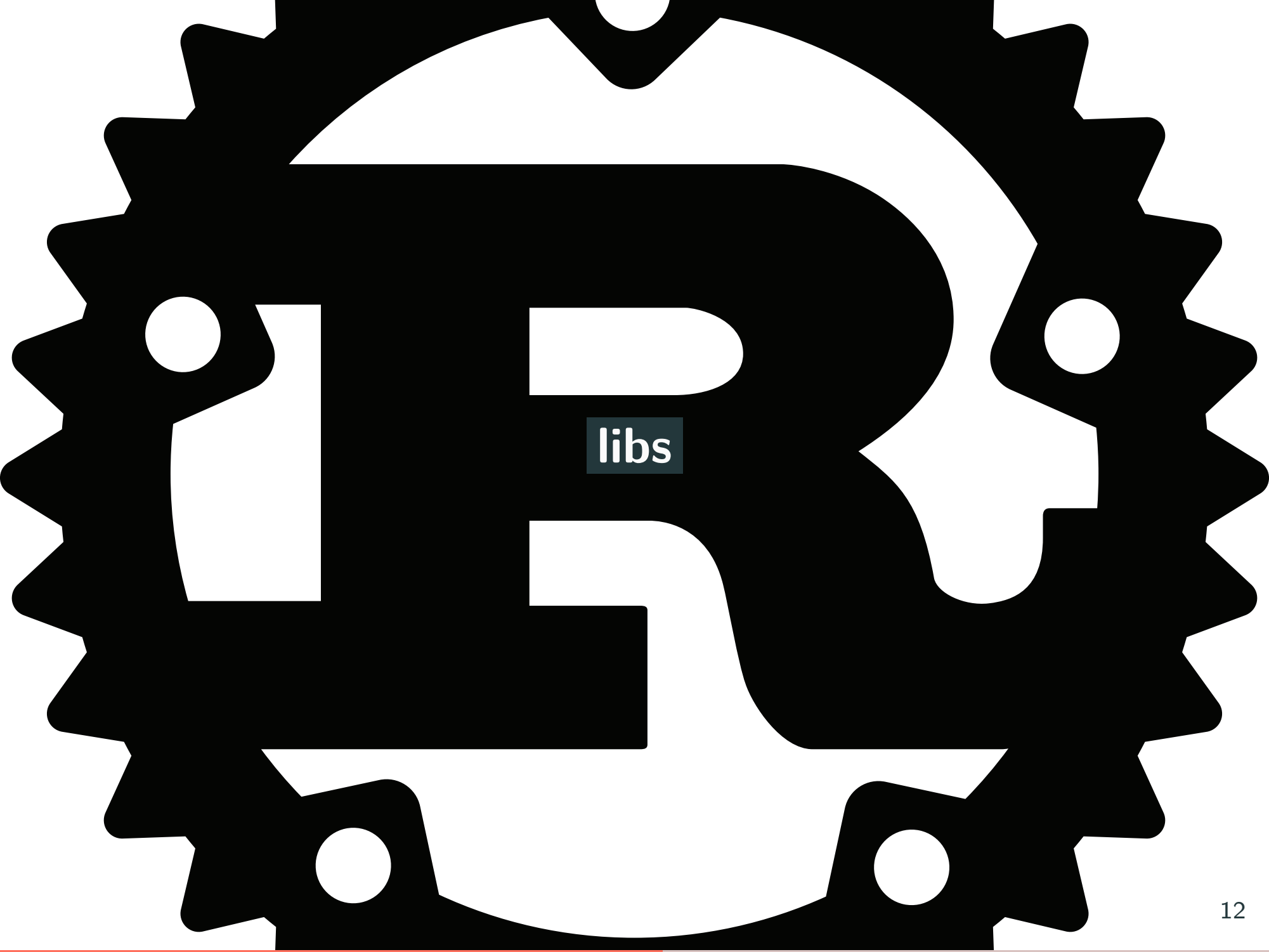
OpenSK

Features

- Personal Identification Verification, PIV/ PIV II (FIPS-201)
- U2F = Universal 2nd Factor
- FIDO2 = Fast IDentity Online, includes translation layer to U2F)
- UAF = Universal Authentification Framework
- WebAuthn
- CTAP = Client To Authenticator Protocol, CTAP2 comes with FIDO2, CTAP1 comes with U2F
- OTP = Onetime Time Password
- FIDO-Alliance = consortium specifying FIDO compat. devices and certification criteria
- OATH initiation for open authentication - specifying HOTP & TOTP (Time and HMAC OTP)
- Smart Card
- ...

Usecases

- gpg / git sign
- ssh auth
- pam login
- web service auth / 2nd factor
- cryptsetup / luks 2nd factor
- ...


libs

rustlibs

- libreauth (formerly r2fa)
- yubikey-piv
- authenticator (firefox, hid, CTAP)
- slauth (HOTP, TOTP server, client, no-hid)
- fido2luks (disk encryption related)
- yubico (HTOP, TOTP, client API only)
- u2f-rs (server side verfication)
- ...


Bugs

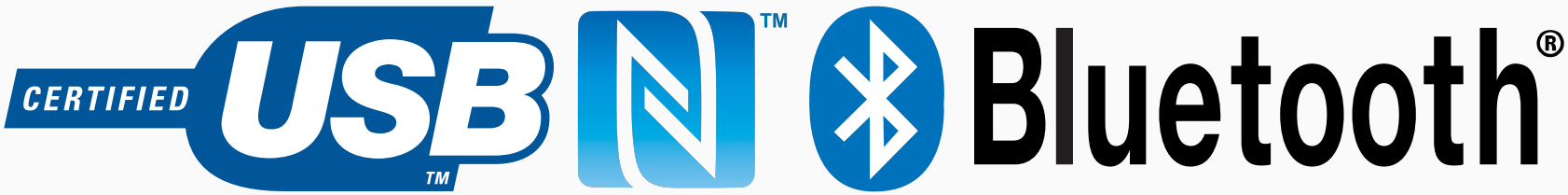
Lack of Documentation

PIV Attestation


NOPE


U2F
•UNIVERSAL 2ND FACTOR•

Transports



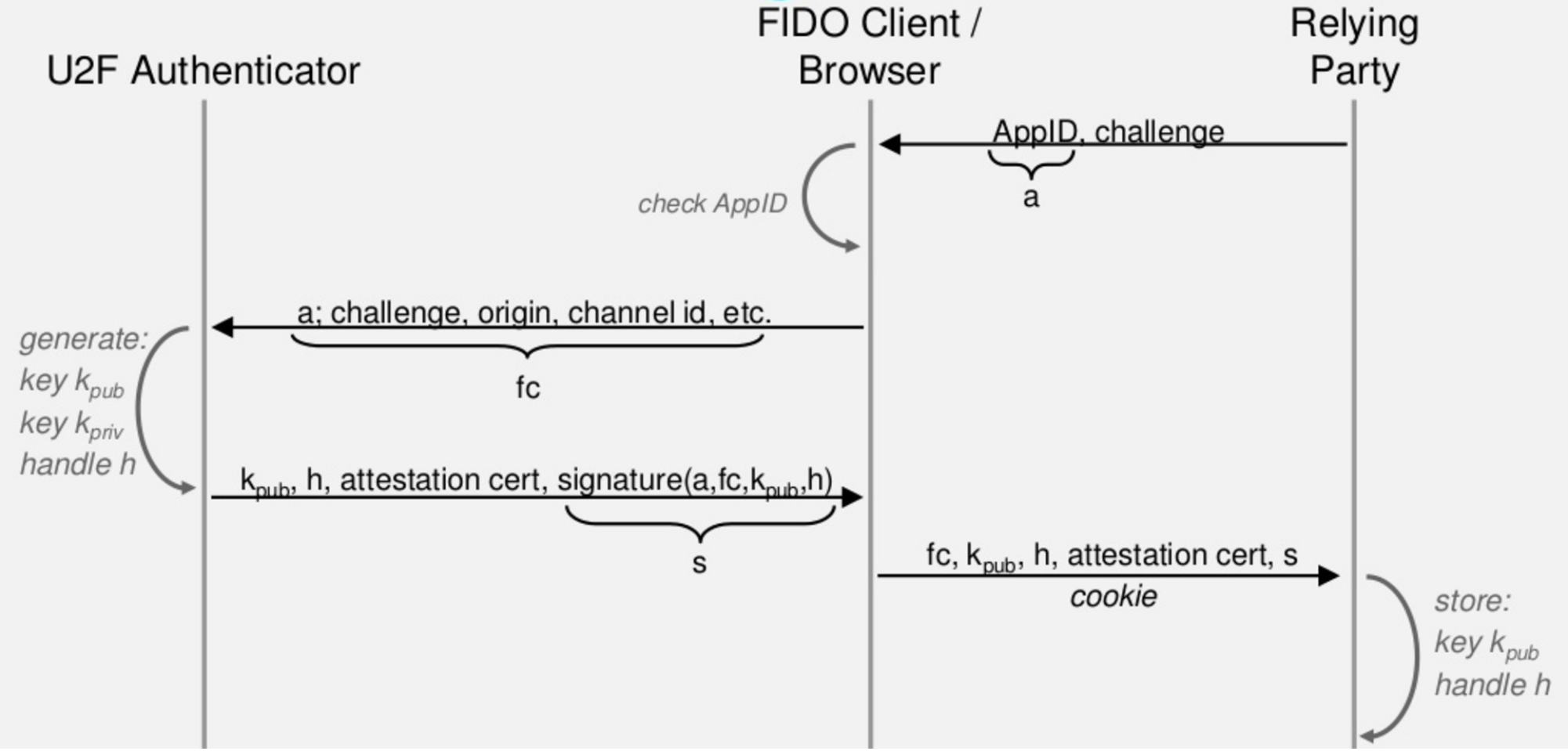
Two Stages

- Registration

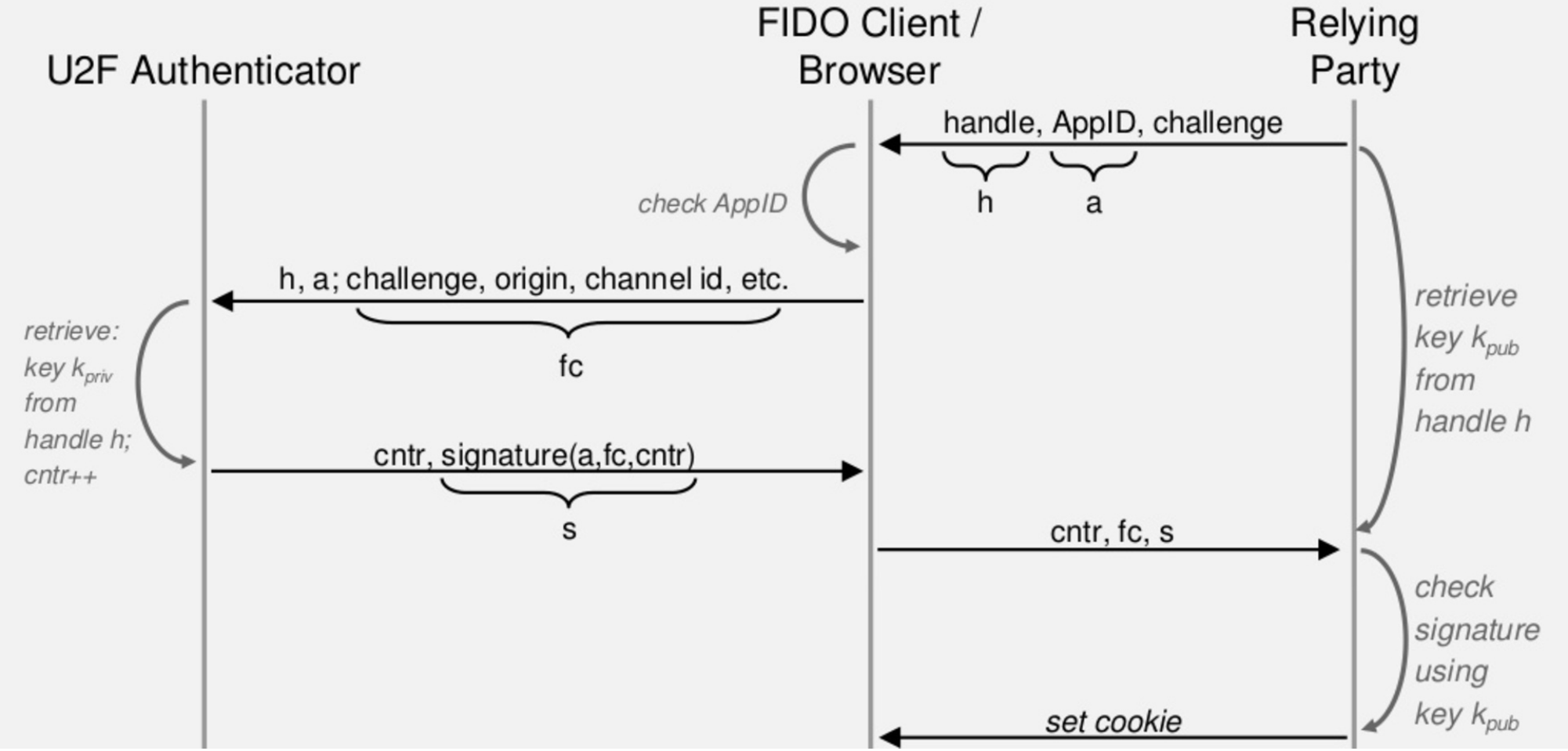
Two Stages

- Registration
- Identity Verification (often called Authentication)

U2F Registration



U2F Authentication



code to write, code written

code to write, code written u2f-rs already contains an exquisite example

code to write, code written u2f-rs already contains an exquisite example

- server in rust with rocket
- web client uses u2f-api.js


Scarlet BANDIT
CHECKER SCHUCK'S KRAGEN AUTO PARTS
FRAM
HUGHES
demo time

Questions?

Questions?
Ask me now! or bernhard@ahoi.io

Credits

Presentation by Bernhard Schuster - ahoi.io
Theme by Matze Vogelsang and contributors - bloerg.net

ArchLinux Wiki, Yubico Linux Compat, Yubico Developers - U2F, Yubico Webinars, EFF Pub Priv