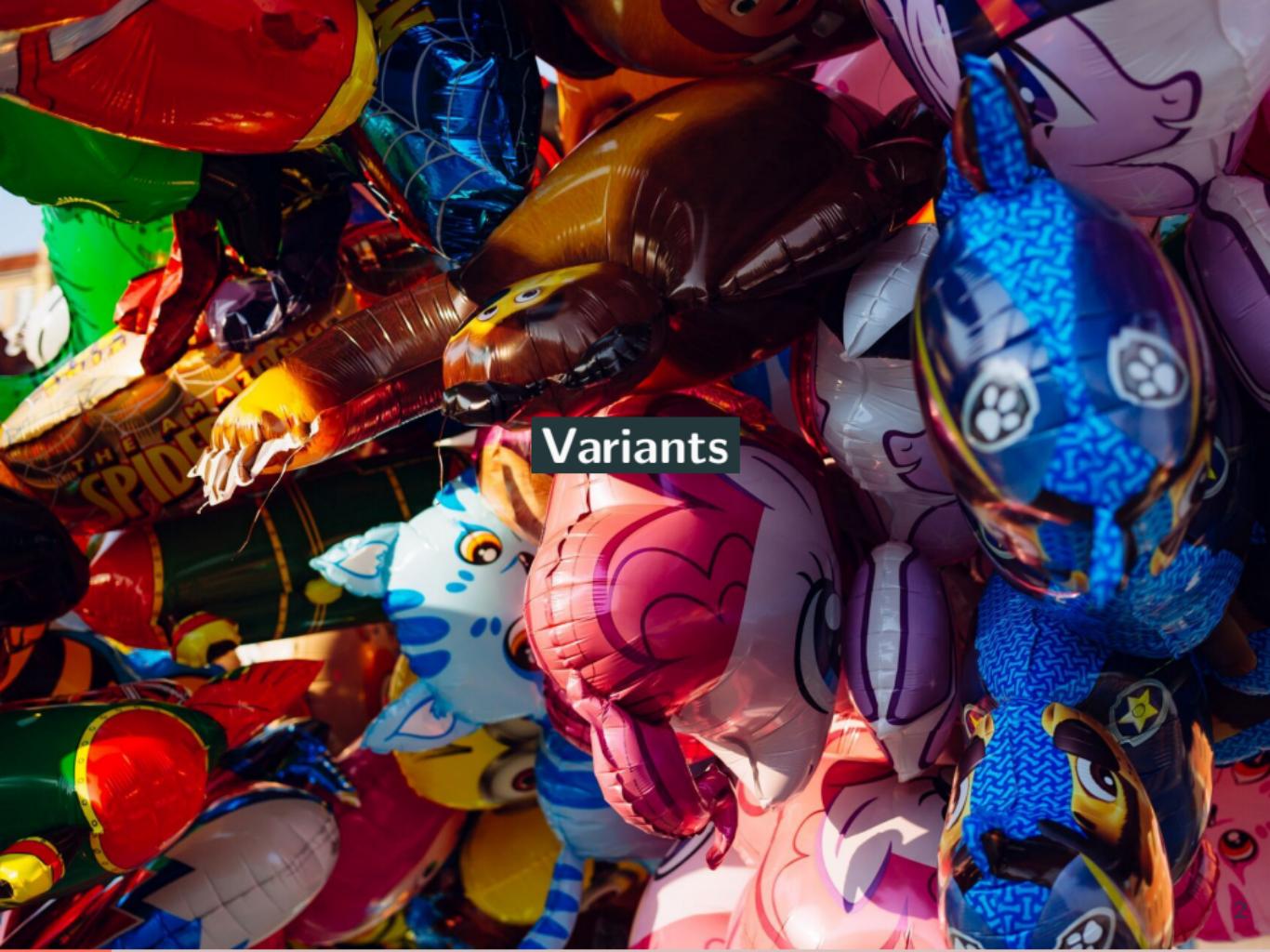


# **your Yubikey with rust**

---

Bernhard Schuster  
February 15, 2020



A vibrant, chaotic pile of various shaped and colored balloons. In the center-left, a large, multi-colored balloon features the words "WITH THE AMAZING SPIDER-MAN". To its right is a large, dark brown balloon resembling a tarantula. Below the spider balloon is a large, pink balloon with a stylized face. Other balloons include a blue unicorn-like creature, a purple and white face, and several smaller, colorful shapes.

**Variants**















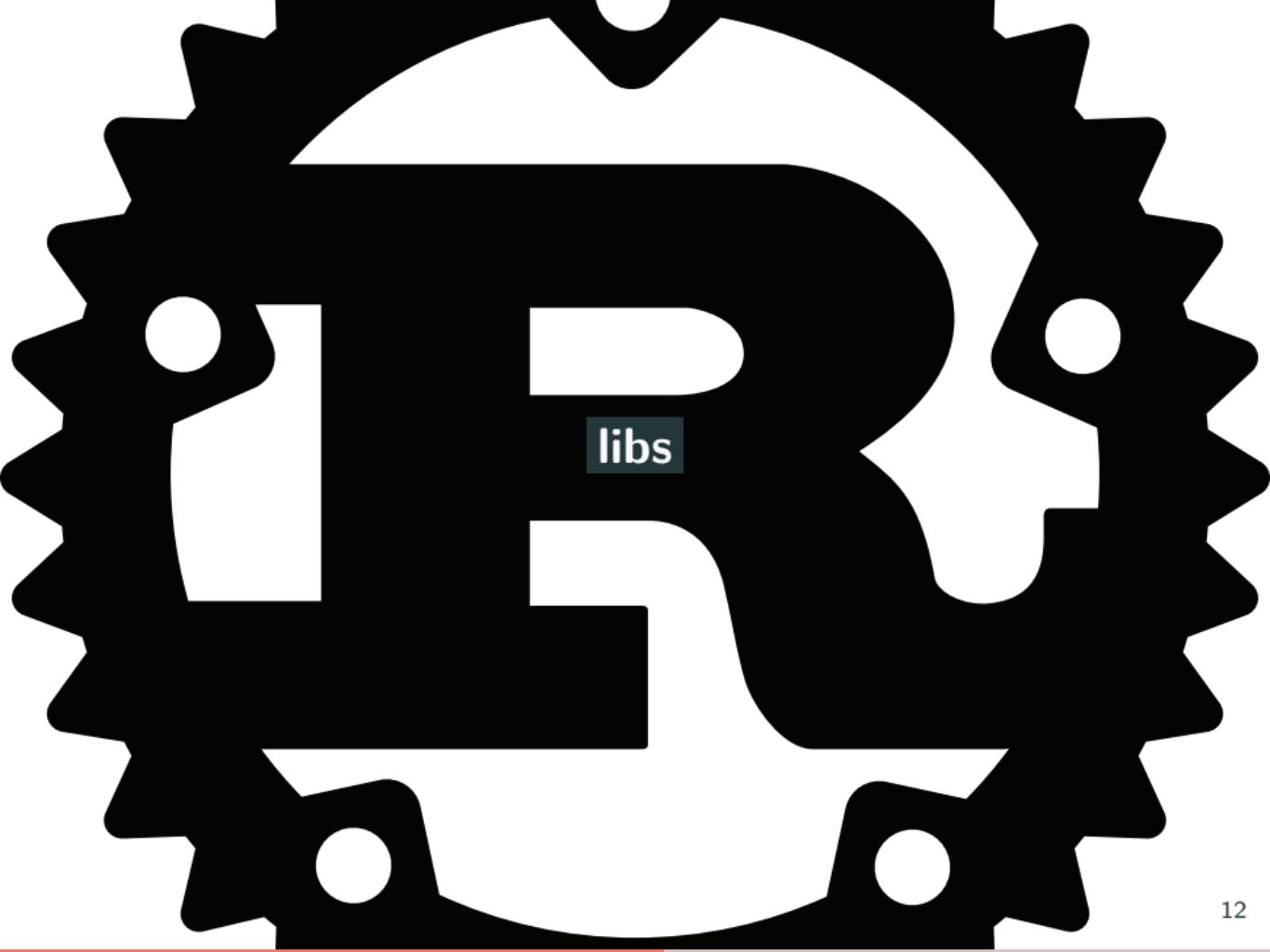
# OpenSK

## Features

- Personal Identification Verification, PIV/ PIV II (FIPS-201)
- U2F = Universal 2nd Factor
- FIDO2 = Fast IDentity Online, includes translation layer to U2F
- UAF = Universal Authentication Framework
- WebAuthn
- CTAP = Client To Authenticator Protocol, CTAP2 comes with FIDO2, CTAP1 comes with U2F
- OTP = One-time 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

- 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 verification)
- ...



Bugs



**Lack of Documentation**

# **PIV Attestation**





# Transports



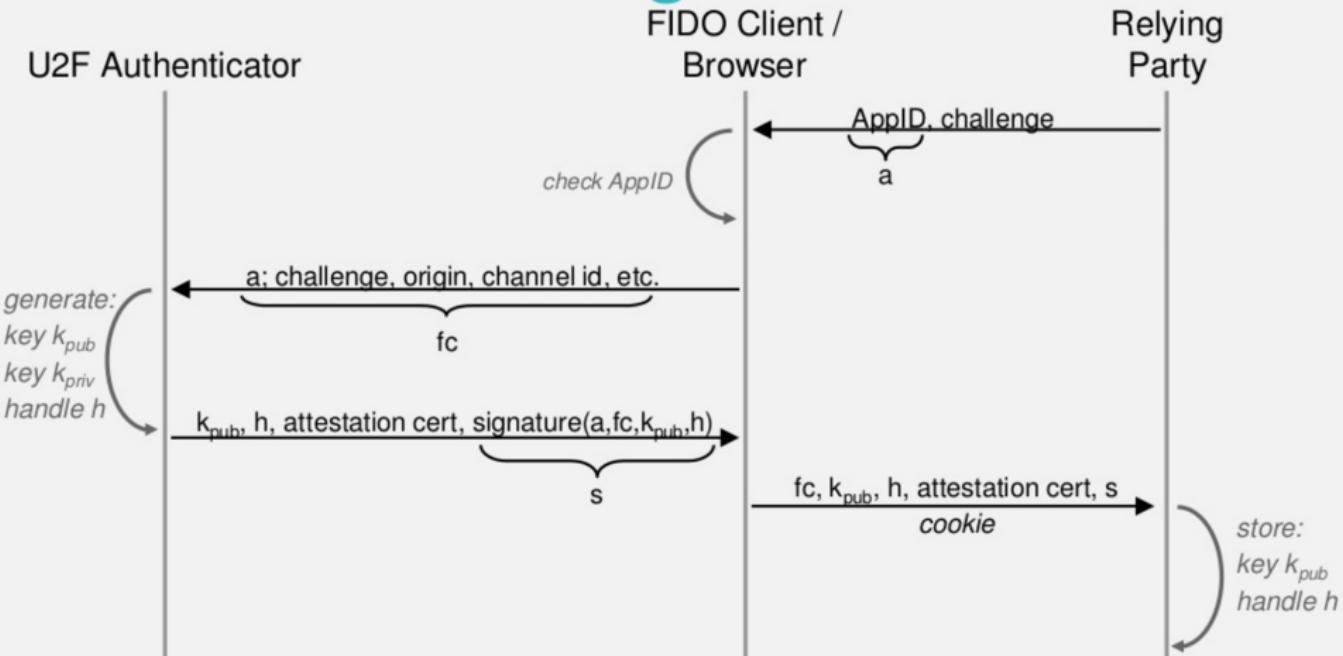
## Two Stages

- Registration

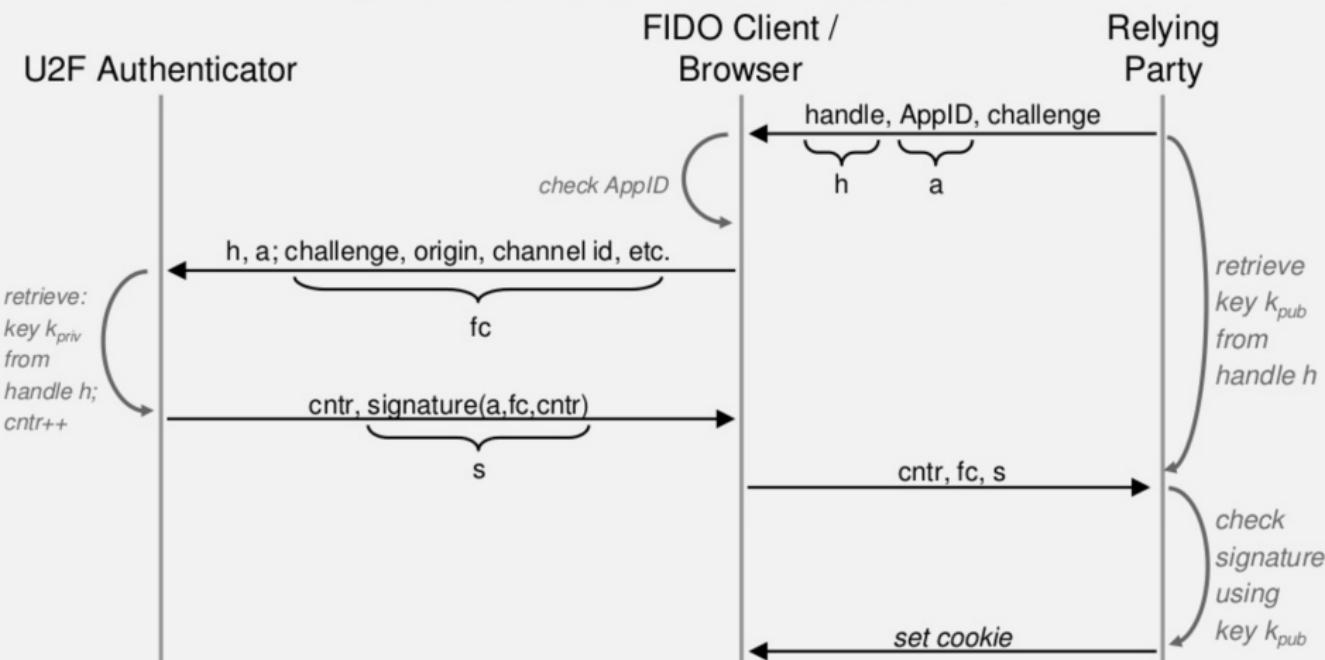
## Two Stages

- 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**



demo time

**Questions?**

**Questions?  
Ask me now! or [bernhard@ahoi.io](mailto:bernhard@ahoi.io)**

# Credits

Presentation by Bernhard Schuster - ahoi.io

Theme by Matze Vogelsang and contributors - bloerg.net

The theme *itself* is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

The images which taken from *unsplash* and are free to use for whatever you want, all others remain under control of their respective owners with all their rights reserved.

Font Awesome icons SIL OFL 1.1

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

