Why your project should support passwordless login, FIDO2, WebAuthn

Jan Suhr, Nitrokey

- Founded in 2015, Berlin
- Open Source Security Hardware Made in Germany
- Supported use cases:
  - Data encryption
  - Cryptographic key store (HSM)
  - Two-Factor authentication (2FA)
  - Passwordless authentication

Nitrokey
secure your digital life

Nitrokey FIDO2

Nitrokey
secure your digital life

Why to use passwords

- Easy to implement
- Easy to use
- All platforms, native apps, web
- Everybody uses them

Why not to use passwords

- Low to moderately secure
- More than 10 billion passwords leaked
- Passwords don't scale (for users)
- Enables phishing attacks
- With increasing security, becoming **inconvenient**!

Nitrokey
secure your digital life

One-Time Passwords (OTP) to the Rescue

- Standardized in 2005 (HOTP)
- Widely supported by large websites
- Client: Smart phone, USB key
- Setup: Secret is shared between client and server
- Time-based OTP: `hash(secret, time)`
- Usability: mediocre
- Phishing protection: none

Nitrokey
secure your digital life

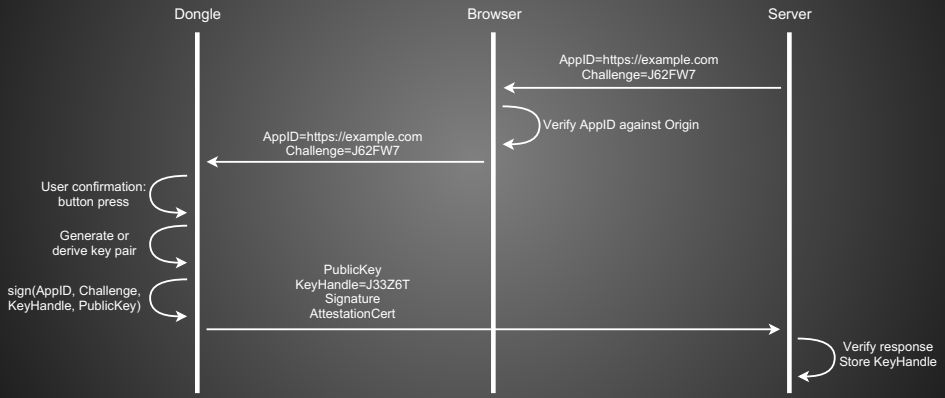
FIDO Universal 2nd Factor (U2F) (1)

- Think: "OTP version 2"
- Released in 2014
- Client: USB, BT or NFC key with confirmation button
- Uses public key cryptography (ECDSA)
- Phishing protection
- Privacy: one key-pair per service
- Option: Master key enables unlimited amount of accounts

FIDO Universal 2nd Factor (U2F) (2)

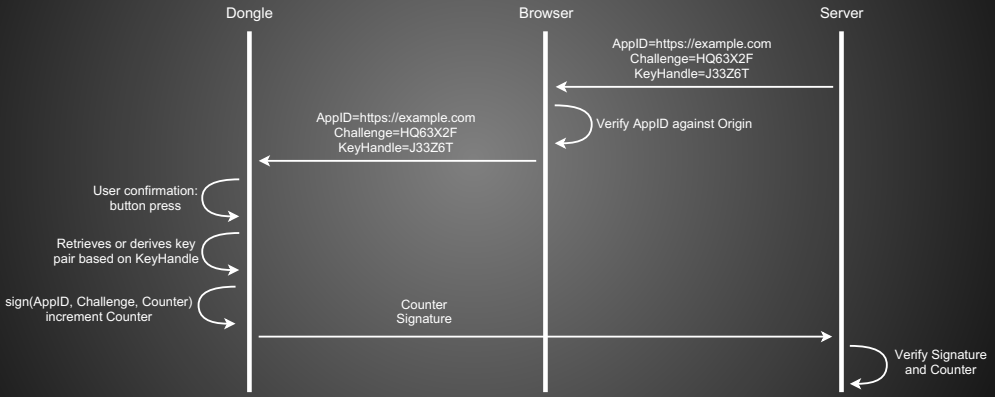
- Native browser support
- Used to be a proprietary web API
- Login: Username, password, touch of the device button
- Usability: good
- Acceptance: poor

FIDO U2F Registration



Nitrokey
secure your digital life

FIDO U2F Authentication



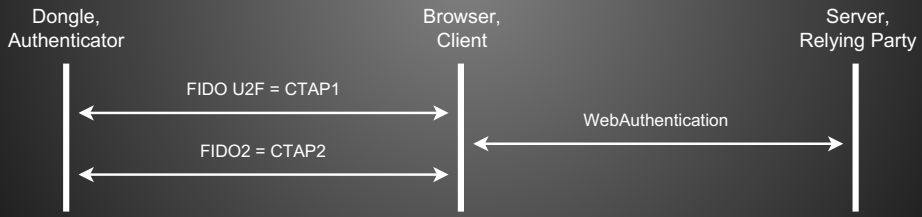
Nitrokey
secure your digital life

FIDO2

- In a nutshell: Like FIDO U2F plus:
  - Passwordless authentication: 1st and 2nd factor
  - Usernameless authentication
  - Includes TPM, biometrics (former FIDO UAF)
  - Not just for the Web
- Great usability
- Acceptance: acceptance?

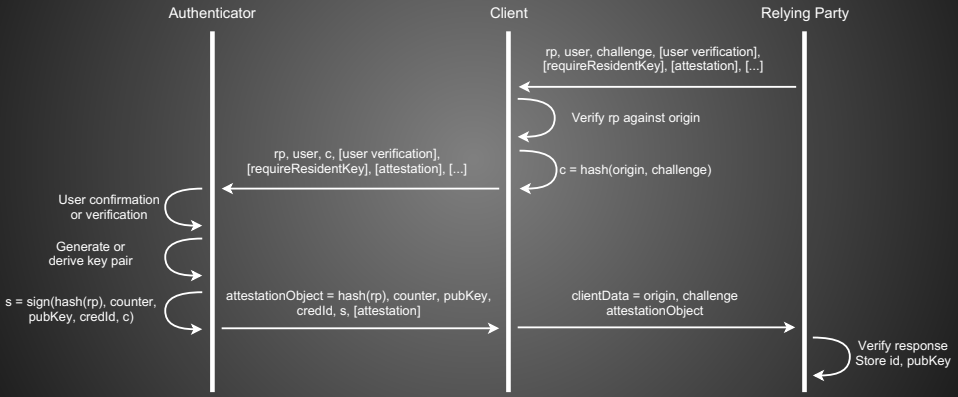
WebAuthentication (WebAuthn)

- W3C standard for browsers and web clients, 2019
- Supports FIDO U2F and FIDO2
- Supported by all major web browsers and platforms



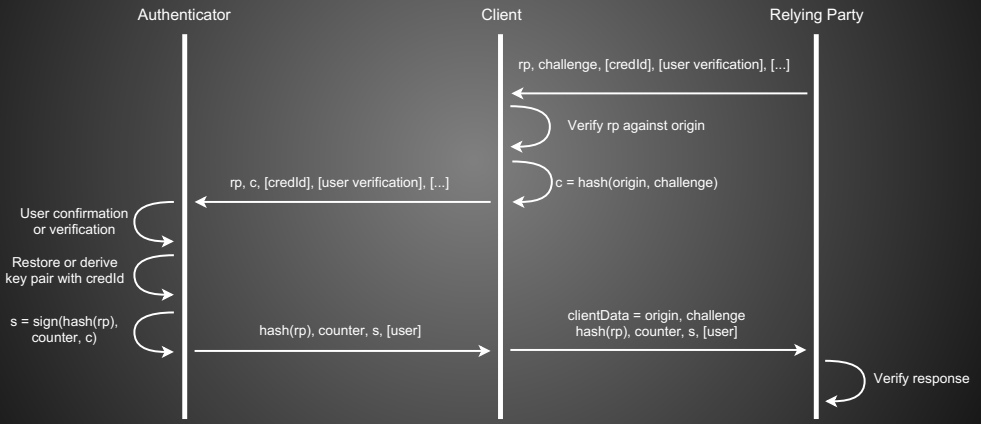
Nitrokey
secure your digital life

FIDO2 Registration



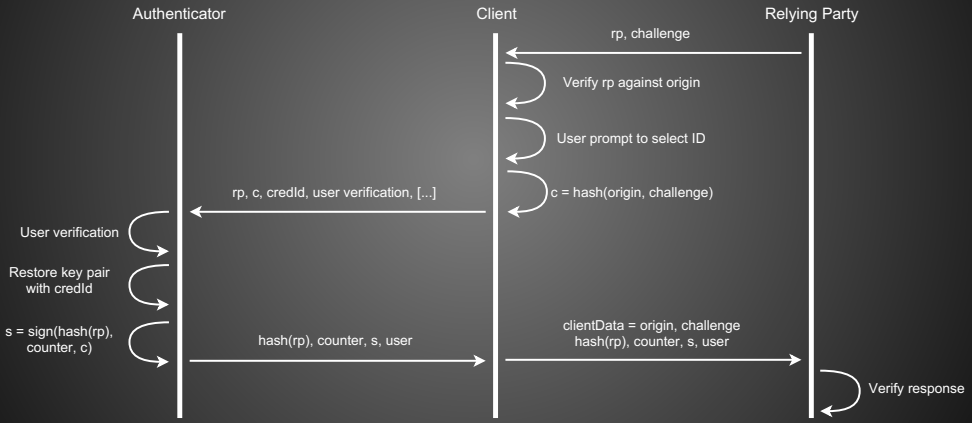
Nitrokey
secure your digital life

FIDO2 1st/2nd Factor Authentication



Nitrokey
secure your digital life

FIDO2 Username-Less Authentication



Nitrokey
secure your digital life

What to use?

- Passwords
  - Simple projects without security-focus
- OTP
  - legacy only
- WebAuthn + 2nd factor + CTAP1 (FIDO U2F)
  - serious projects, new implementations
- WebAuthn + 1st factor + CTAP2 (FIDO2)
  - serious projects, new implementations, next generation usability, pioneer to implement

Nitrokey
secure your digital life

References

- Acceptance: www.dongleauth.info
- Introduction and more: medium.com/@herrjemand/introduction-to-webauthn-api-5fd1fb46c285
- Test: webauthn.bin.coffee
- WebAuthentication: www.w3.org/TR/webauthn/
- FIDO U2F: fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-raw-message-formats-v1.2-ps-20170411.pdf
- FIDO2: fidoalliance.org/specs/fido-v2.0-id-20180227/fido-client-to-authenticator-protocol-v2.0-id-20180227.html