Passkeys, Webauthn und FIDO2

Einführung in hardwarebasierte Authentifizierung

[MS]

10. Oktober 2025

Was sind Passkeys[1]

- in der Regel Authentifizierungsverfahren
  - Ent/Verschlüsselung auch möglich
- am Ende immer public-private Schlüsselpaar, irgendwie gespeichert
  - Biometrische Systeme
  - Hardwaretokens
  - Tpm
  - Cloud
  - ...
- öffentlicher Schlüssel im Service hinterlegt
- zum Anmelden wird mit privatem Schlüssel eine Challenge signiert

[1] Gregg Lindemulder 2025.

Vorteile gegenüber Passwörtern[1]

- keine schwachen Passwörter möglich
- Abfangen von Passwörtern in Transit sinnlos
  - in der Regel ist die Challenge einzigartig
- keine Mehrfachnutzung von Credentials
  - für Webservices haben die Keys eine 1:1-Beziehung zu den Seiten
- eingebaute Fishing Abschwächungen
- nichts zu vergessen
  - Verlust dennoch möglich

[1] Bundesamt für Sicherheit in der informationstechnik (BSI) 2025.

Verbreitung von Passkeys

- von vielen Plattformen unterstützt
- Konzept in Deutschland eher unbekannt[1]
  - Bei 38 % bekannt, von 18 % genutzt
    - ★ selbst wenn bekannt oft keine unterstützten Dienste bekannt
  - viele offen für Nutzung
    - ★ neben Sicherheitsaspekten ist Usability ein wichtiger Faktor
- (Matzen u. a. 2025) fasst mögliche Endnutzerprobleme zusammen
  - zu unbekannt
  - Keine Backups möglich → Angst vor Tokenverlust
    - ★ Platformwechsel
  - kein Teilen von Tokens
  - Komplexität
  - bisher keine zentrale Invalidierung
  - inkonsistent umgesetzte Standards

[1] Bundesamt für Sicherheit in der informationstechnik (BSI) 2024.

Viele Begriffe, eine Idee

- Passkey wird als Marketingbegriff für FIDO2 Geräte und in-Software Webauthn-Lösungen genutzt[1]
- FIDO2 enthält Webauthn und CTAP2[2]
  - Webauthn ist der Kommunikationsstandard zwischen Browser und Endgerät.[3]
  - CTAP ist der Kommunikationsstandard zwischen Endgerät und Authentifizierungsgerät.[4]

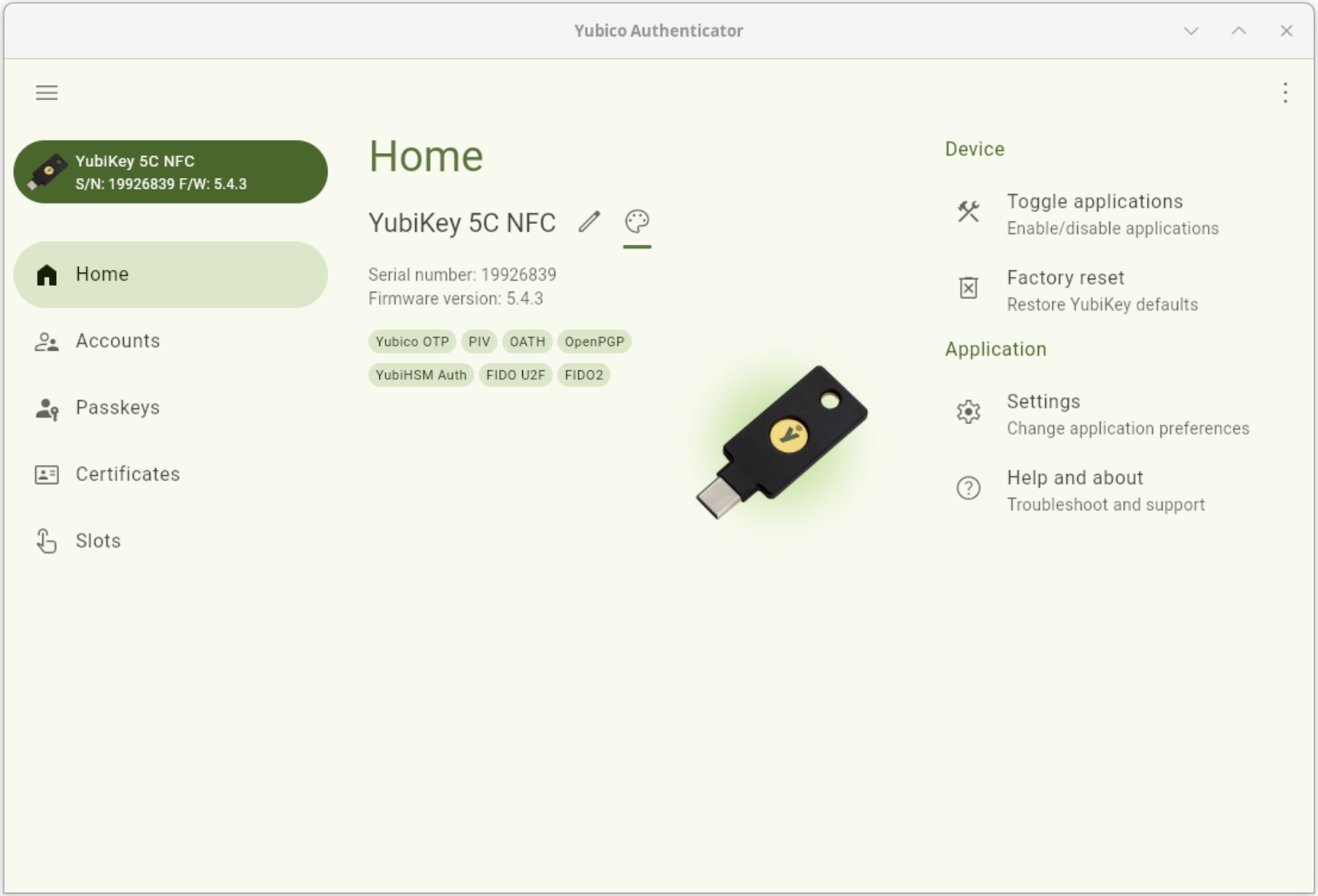
[1] Harrell 2023.
[2] Gregg Lindemulder 2025.
[3] W3C 2021.
[4] FIDO Alliance 2019b.

Der YubiKey

- unterstützt den FIDO2 Stack
  - Hersteller Mitglied der FIDO-Alliance
- aber auch andere Protokolle[1]
  - PIV (smart Card)
  - OATH (hardware basierte OTP)
  - OTP
  - OpenPGP
- speichert FIDO2 private keys kopiergeschützt in Hardware
  - zum Signieren der Challenge muss der Stick berührt werden

[1] Degruchy 2020.

Yubico authenticator



CLI tool

- mehr Möglichkeiten als GUI-Tool
- besser dokumentiert (Yubico 2025a)
- konnte Problem hier besser identifizieren
- analoges GUI-Programm ist bald EOL

```
lab@lab:~$ ykman fido credentials list
ERROR: Credential Management requires having a PIN. Set a PIN first.
lab@lab:~$ ykman fido credentials list
Enter your PIN:
Credential ID  RP ID                Username                          Display name
b16ba722...
```

Idee[1]

- Browser baut TLS-Verbindung zu Service auf
- Service spricht API zum Anmelden mit Token an, liefert Challenge mit
- Wenn Schlüssel für gegeben Website vorhanden:
  - Browser nutzt Hardware-Schnittstelle zum signieren der Challenge
  - Browser gibt signierte Challenge an Server zurück
  - Server validiert Signatur mit öffentlichem Schlüssel

[1] MDN contributors 2025.

Registrieren mit Webauthn

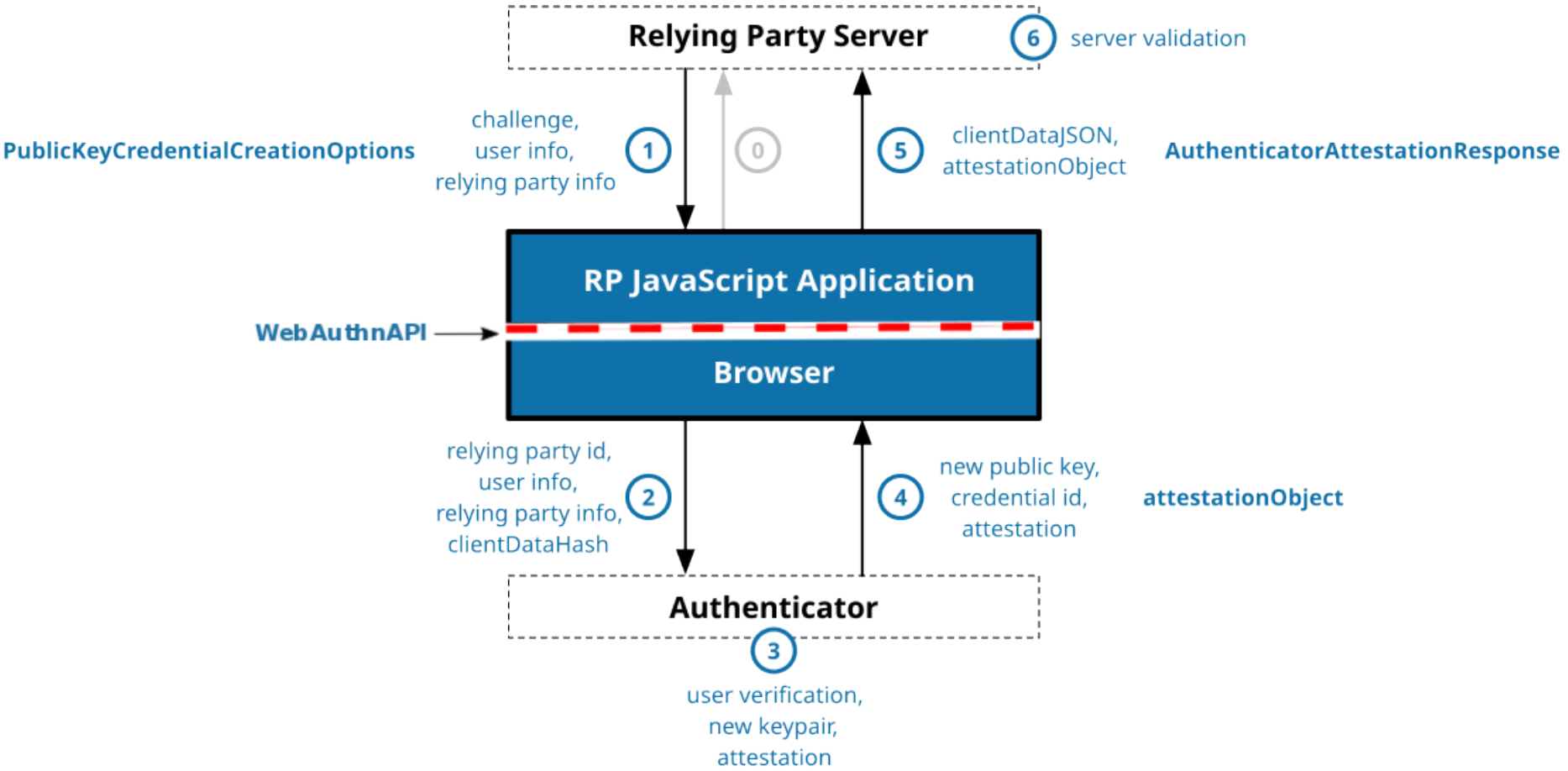


Abbildung: Registrierung mit Webauthn (W3C 2021)

Anmelden mit Webauthn

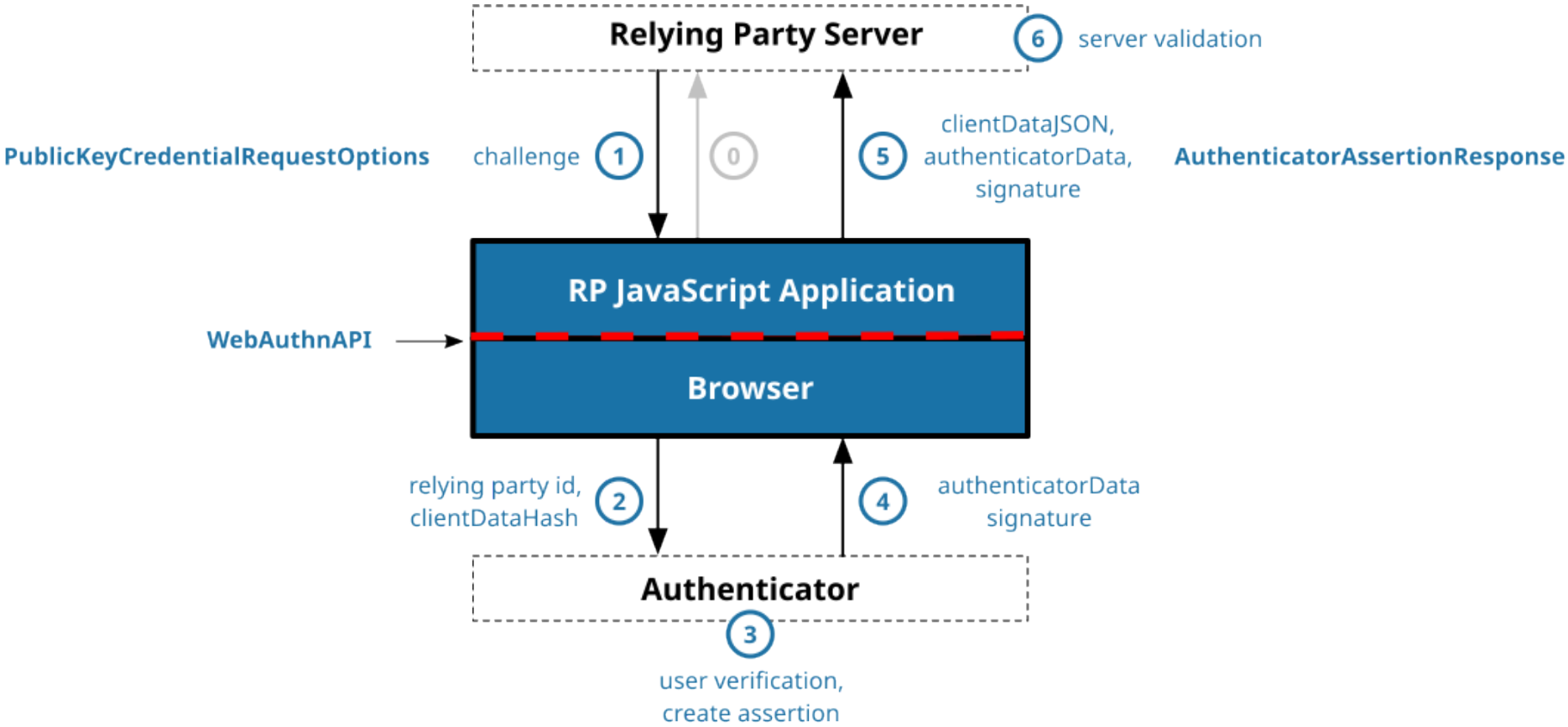
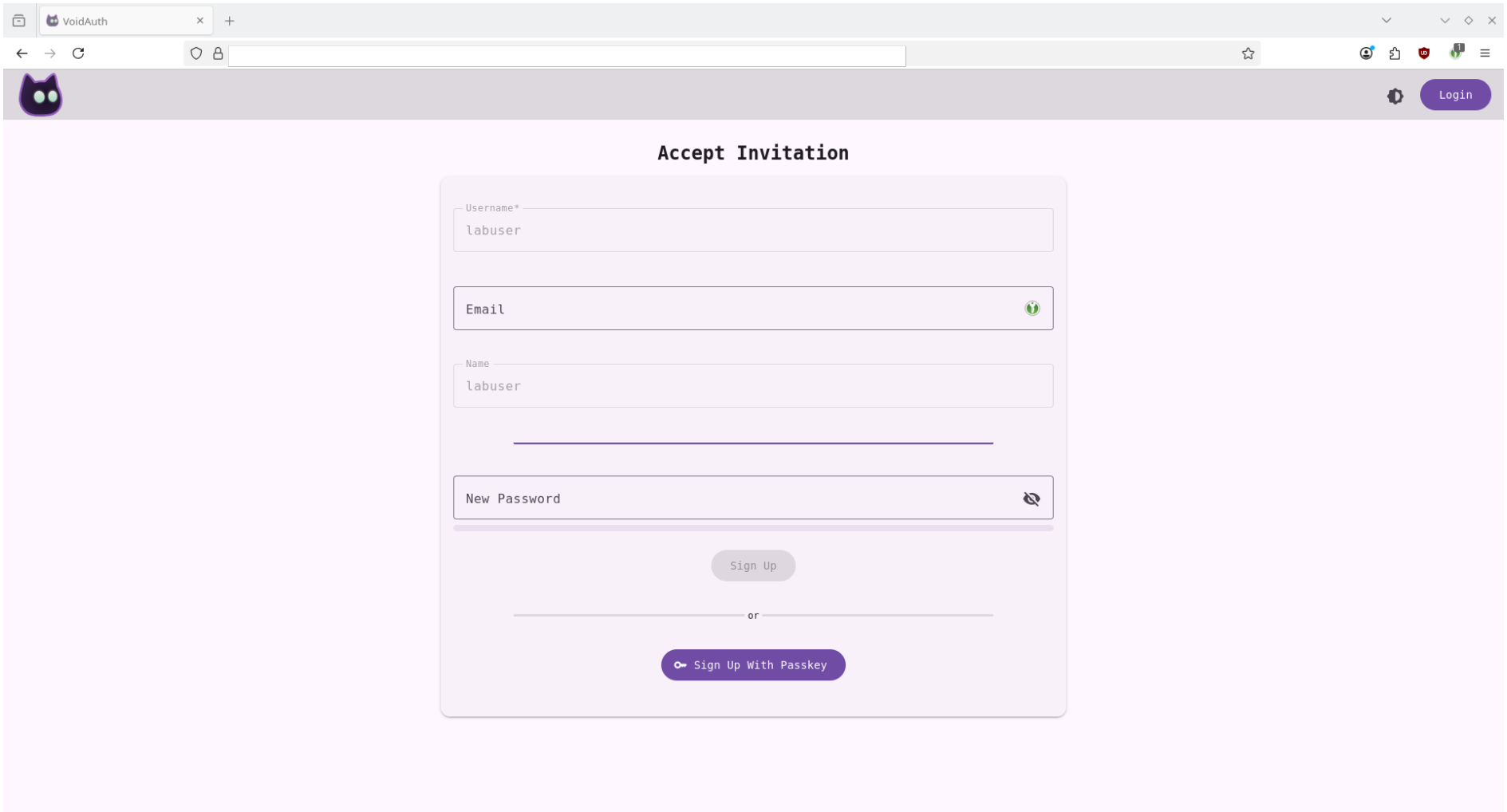
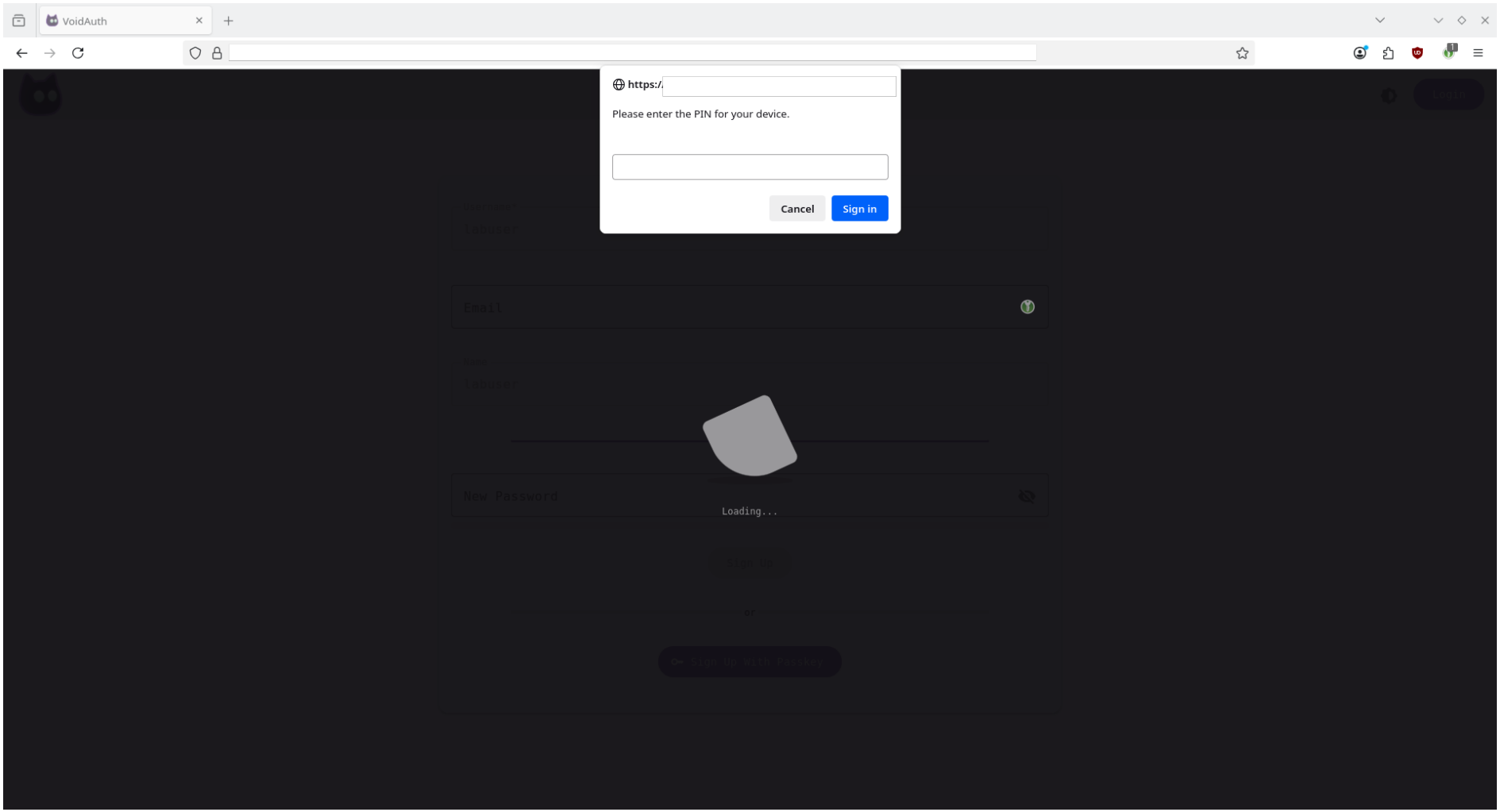


Abbildung: Anmelden mit Webauthn (W3C 2021)

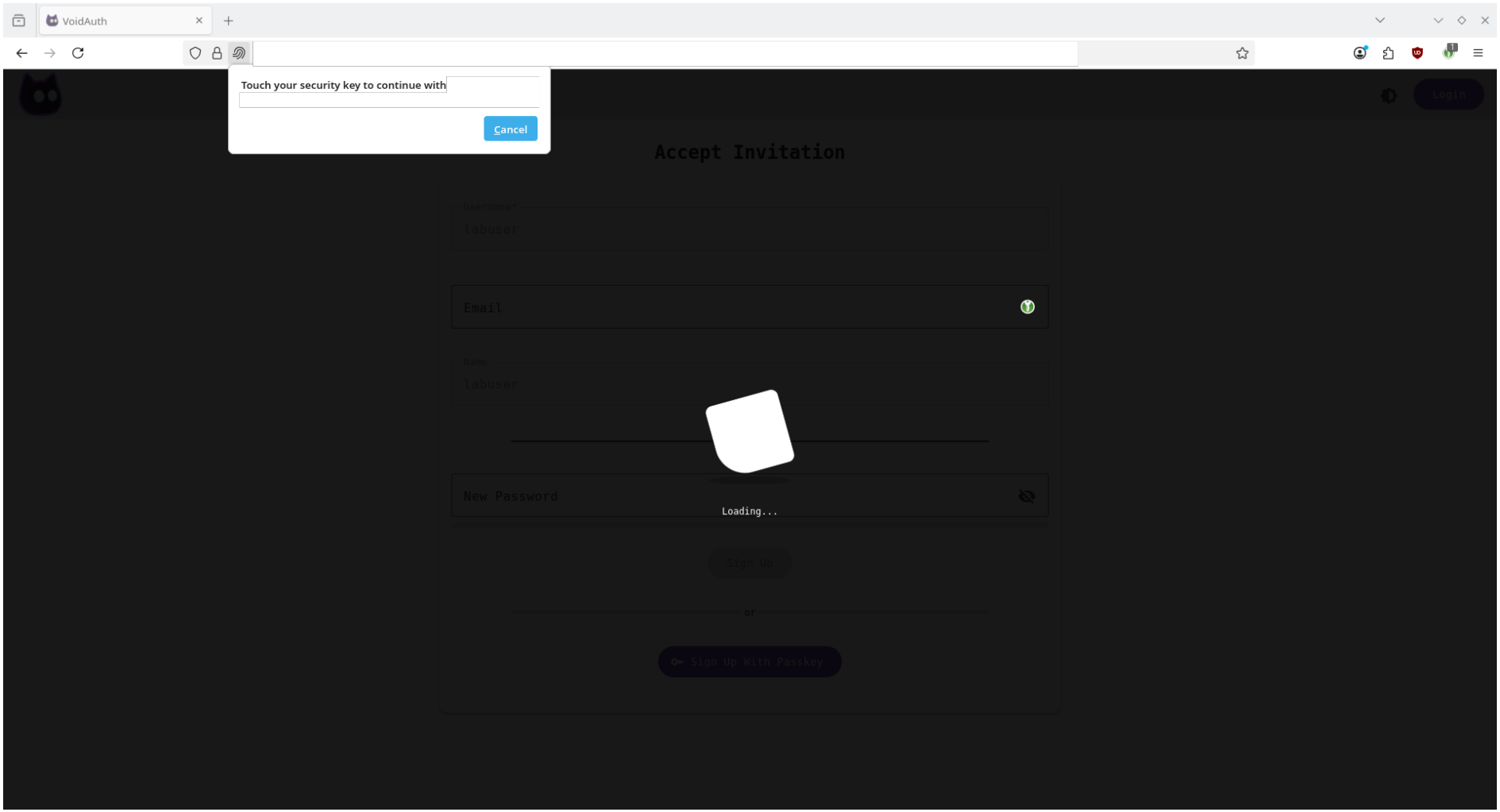
Registrierung in Voidauth



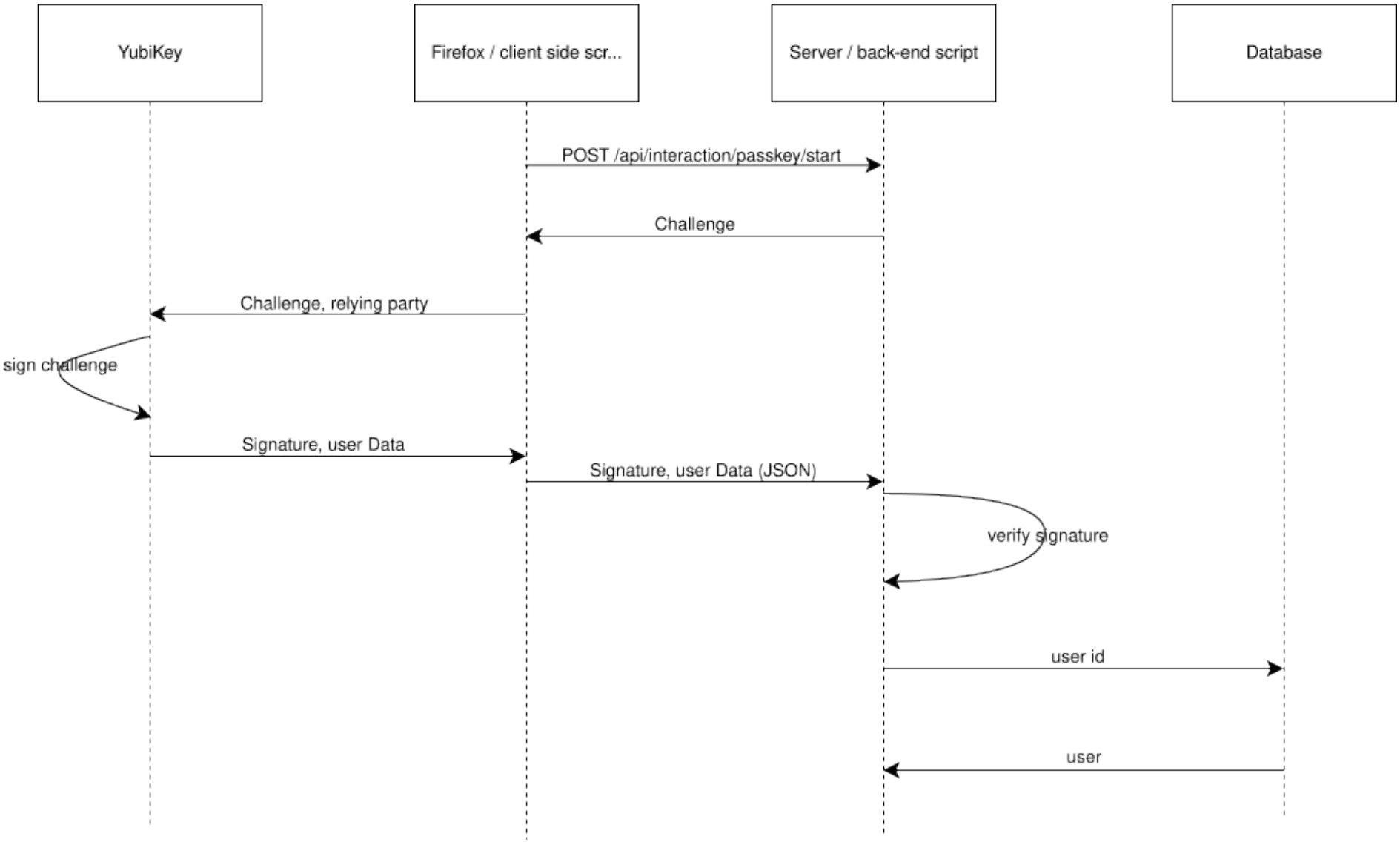
Registrierung in Voidauth



Registrierung in Voidauth



Theorie



[in dem Vortrag war hier ein live Showcase des Anmeldeflows und der Pakete in Wiregurard]

KeepassXC

- KeepassXC unterstützt Entschlüsselung per YubiKey[1]
- Keepass2 auch, aber anders
- basierend auf der Passwortdatei wird eine Challenge generiert und mit der Response die Datenbank verschlüsselt
- Challenge-Response nicht mit über FIDO-Protokoll, sondern über inoffizielle Extension
  - FIDO-Protokoll unterstützt aber identisches Verfahren (HMAC) mit anderem Hash (SHA-256 statt SHA-1)[2]
  - Implementierung des FIDO-Standards in Diskussion[3]

[1] *KeepassXC Documentation - YubiKey 2FA FAQ* 2025.
[2] FIDO Alliance 2019a.
[3] ashleysommer auf github.com 2025.

PAM (Linux Authentifizierung)

- über ein PAM-Modul u.a. in Debian möglich[1]
- nutzt älteren U2F Standard
- Ich hatte Probleme mit PAM-Konfigurationen
  - parallel-Betrieb von Tokens und Passwörtern lief mittelmäßig
  - die UI ist oft nicht auf Logins ohne Passwort ausgelegt
  - KDE-spezifisch: der Lockscreen hat standardmäßig keine eigene PAM-config[2]
  - Login hat zuletzt nicht funktioniert
- sudo funktionierte recht zuverlässig

[1] *Security/U2F* 2025.

[2] mcendu@askubuntu 2024.

ssh

- ssh wird auch ohne relyingParty nativ in FIDO2 unterstützt
- Einrichten mit Openssh dementsprechend einfach
- in (Yubico 2025b) gut dokumentiert
- anstatt des typischen private keys wird im .ssh Ordner eine Referenz zum resident key im FIDO-Token hinterlegt
- mit der Option '-O verify-required' kann das Eingeben der Pin vorausgesetzt werden

LUKS

- FIDO möglich, ähnliches Verfahren wie bei Keepass
- Challenge bleibt aber konstant und ist im LUKS-Header gespeichert
- Entschlüsselung im Bootprozess möglich
  - initramfs-cryptsetup unterstützt noch keine FIDO-Entschlüsselung[1]
  - mit Dracut wohl möglich
- (Garcia 2025) stellt Skript zur Entschlüsslung mit FIDO und initramfs-cryptsetup zur Verfügung
  - funktioniert
  - Vertrauenswürdigkeit nicht näher unetrsucht

[1] Rutenberg 2023.

Andere Services

- auch andere SSO-Services bieten Authentifizierung mit Passkeys an
  - Keykloak habe ich nicht zum Laufen bekommen
  - bei Authentik habe ich mich ausgesperrt
- Nextcloud unterstützt auch die Anmeldung mit Passkeys
- NGINX unterstützt Passkeys zum Anmelden[1], auch den Schutz von Hosts mit Passwort[2]. Zu Passkeys konnte ich aber nichts finden.
  - Apache unterstützte es wohl auch nicht
  - Sinn dort fragwürdig[3]

[1] *Configuring WebAuthn with Nginx* 2025.
[2] *Restricting Access with HTTP Basic Authentication* 2025.
[3] Zandbelt 2022.

Fragen?

ashleysommer auf github.com (1. Juni 2025). *Implementation of FIDO2 hmac-secret extension in KeePassXC*. (Besucht am 26. 10. 2025).

Bundesamt für Sicherheit in der informationstechnik (BSI) (1. Okt. 2024). *Verbraucherbefragung zur passwortlosen Authentisierung mit Passkeys*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/passwortlose-authentisierung-bericht.html?nn=1107468 (besucht am 09. 10. 2025).

— (2025). *Schafft die Passwörter ab?! Anmelden ohne Passwort mit Passkey*. URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Passkeys/passkeys-anmelden-ohne-passwort_node.html#doc1107470bodyText1 (besucht am 08. 10. 2025).

Configuring WebAuthn with Nginx (2025). URL: https://nginxui.com/guide/config-webauthn (besucht am 09. 10. 2025).

- Degruchy, Clay (Sep. 2020). *YubiKey 5 NFC*. URL: https://support.yubico.com/hc/en-us/articles/360016649339-YubiKey-5C-NFC (besucht am 08. 10. 2025).
- FIDO Alliance (2019a). „12.5. HMAC Secret Extension (hmac-secret)“. In: *FIDO Client to Authenticator Protocol (CTAP) v2.0*. FIDO Alliance. URL: https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html#sctn-hmac-secret-extension (besucht am 26. 10. 2025).
- — (Jan. 2019b). *FIDO Client to Authenticator Protocol (CTAP) v2.0*. Hrsg. von Christiaan Brand et al. URL: https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html (besucht am 08. 10. 2025).
- Garcia, Alberto (2025). *Unlock LUKS volumes at boot time using a FIDO2 token and initramfs-tools*. URL: https://github.com/bertogg/fido2luks (besucht am 09. 10. 2025).

- Gregg Lindemulder, Matthew Kosinski (2025). *Was ist FIDO2?* URL: https://www.ibm.com/de-de/think/topics/fido2 (besucht am 08. 10. 2025).
- Harrell, Christopher (2023). *A Yubico FAQ About Passkeys*. URL: https://www.yubico.com/blog/a-yubico-faq-about-passkeys/ (besucht am 08. 10. 2025).
- *KeepassXC Documentation - YubiKey 2FA FAQ* (2025). URL: https://keepassxc.org/docs/#faq-yubikey-2fa (besucht am 09. 10. 2025).
- Matzen, Alexander u. a. (2025). „Challenges and Potential Improvements for Passkey Adoption—A Literature Review with a User-Centric Perspective“. In: *Applied Sciences* 15.8. ISSN: 2076-3417. DOI: 10.3390/app15084414. URL: https://www.mdpi.com/2076-3417/15/8/4414.
- mcendu@askubuntu (Feb. 2024). *PIN on Kubuntu lockscreen KDE Plasma 5.27.8*. URL: https://askubuntu.com/questions/1502485/pin-on-kubuntu-lockscreen-kde-plasma-5-27-8 (besucht am 09. 10. 2025).

- MDN contributors, Hrsg. (11. Juli 2025). *Web Authentication API*. URL: https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API (besucht am 09. 10. 2025).
- *Restricting Access with HTTP Basic Authentication* (2025). URL: https://docs.nginx.com/nginx/admin-guide/security-controls/configuring-http-basic-authentication/ (besucht am 09. 10. 2025).
- Rutenberg, Guy (2023). *Debian Bug report logs - #1023700. cryptsetup: Option fido2-device unknow*. URL: https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1023700 (besucht am 09. 10. 2025).
- *Security/U2F* (2025). *Using U2F keys in Debian*. URL: https://wiki.debian.org/Security/U2F (besucht am 09. 10. 2025).
- W3C (Apr. 2021). *Web Authentication: An API for accessing Public Key Credentials Level 2*. Hrsg. von Jeff Hodges et al. W3C. URL: https://www.w3.org/TR/2021/REC-webauthn-2-20210408/ (besucht am 08. 10. 2025).


Yubico (2025a). *YubiKey Manager (ykman) CLI User Guide*. URL: https://docs.yubico.com/software/yubikey/tools/ykman/index.html (besucht am 09. 10. 2025).


— (2025b). *Securing SSH Authentication with FIDO2 Security Keys*. URL: https://developers.yubico.com/SSH/Securing_SSH_with_FIDO2.html (besucht am 09. 10. 2025).


Zandbelt, Hans (2022). *A WebAuthn Apache Module?* URL: https://hanszandbelt.wordpress.com/2022/05/05/a-webauthn-apache-module/ (besucht am 09. 10. 2025).