Passwortlose Logins mit PassKeys

Stefan Schumacher, https://cryptomancer.de

$Id: 188-Schumacher-Passkeys-Shortpaper.adoc,v 1.11 2025/09/17 15:11:21 stefan Exp $

https://www.cryptomancer.de/posts/202503passkey/

PGP: 7B2B 45B1 330E 579E 3C3E 9B34 089D 8068 8050 ECCF

Abstract

Auf den CLT 2016 habe ich die Zwei-Faktor-Authentifizierung mit Yubikeys vorgestellt. Inzwischen hat sich in der FIDO-Welt einiges getan. So haben die FIDO-Alliance und das W3C schon 2022 sogenannte Passkeys ausgerollt. Diese sollen langfristig den Einsatz von Passwörtern überflüssig machen und Phishing-Attacken nachhaltig verhindern.

In diesem Vortrag zeige ich, wie WebAuthN bzw. FIDO2 funktionieren und erweitert wurden, um sichere passwortlose Logins zu ermöglichen. Desweiteren zeige ich, welche Hardware (Tokens, Smartphones, Secure Enclave) für Passkeys genutzt werden können und wo welche Vor- und Nachteile liegen. Besonderes Augenmerk liegt dabei auf der Kryptographie und Sicherheit des Verfahrens und auf dem versprochenen Phishing-Schutz. Außerdem diskutiere ich die Gefahr des Verlustes der digitalen Identität, wenn man seine Credentials an bestimmte Hersteller ausliefert.

Erwünschte Vorkenntnisse: Der Vortrag ist für Einsteiger geeignet.

Grundlagen der 2-Faktor-Auth findet man in meinem Vortrag »Zwei-Faktor-Authentifizierung mit Yubikeys« von 2016: https://chemnitzer.linux-tage.de/2016/de/programm/beitrag/321/

Struktur des Vortrags

1. Einführung und Motivation:
    a. Was ist Zwei-Faktor-Authentifikation
    b. Warum passwortlose Logins überhaupt?
2. Die FIDO-Alliance und FIDO2
    a. Application Layer Architecture
    b. Registrierung eines Passkeys mit Discoverable Credentials
    c. Passwortlose Logins
    d. Phishing-Resistenz von Passkeys
    e. Beglaubigte Passkeys
3. Passkeys
    a. als Datei/im Passwortmanager
    b. in mobilen Endgeräten

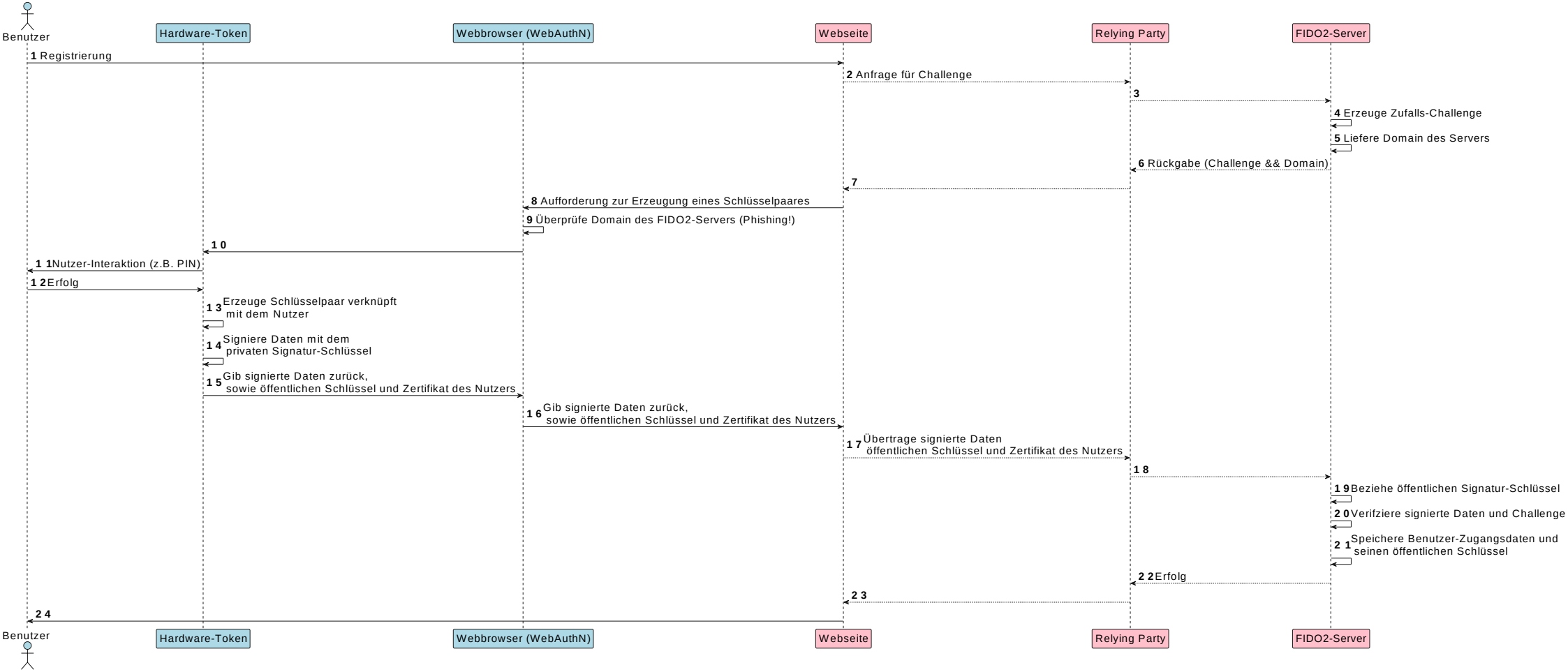
    c. als Hardware-Token
    d. Risiken und Backups von Passkey
4. Passkeys auf der Befehlszeile mit libfido2 ansprechen
5. OIDC-Provider um Passkeys im Selfhosting zu nutzen

Programme

- libfido2: https://github.com/Yubico/libfido2
- PocketID: https://pocket-id.org/
- Authentik: https://goauthentik.io/
- Authelia: https://www.authelia.com/
- KanIDM: https://kanidm.com/
- Keycloak: https://www.keycloak.org/
- KeePassium (iOS): https://keepassium.com/
- KeePassXC: https://keepassxc.org/
- Bitwarden: https://bitwarden.com/de-de/

Verweise und Literatur

- https://fidoalliance.org/fido-alliance-publishes-new-specifications-to-promote-user-choice-and-enhanced-ux-for-passkeys/
- CCC2004: Einführung in die Kryptographie https://events.ccc.de/congress/2004/fahrplan/event/41.en.html
- CLT2008: Sichere Passwörter https://chemnitzer.linux-tage.de/2008/vortraege/detail.html.113.html
- CLT2016: Zwei-Faktor-Authentifizierung mit Yubikeys https://chemnitzer.linux-tage.de/2016/de/programm/beitrag/321/
- Stratfor-Passwörter cracken: https://www.youtube.com/watch?v=fXsggaDNrcU
- CLT2024: Sichere Datenhaltung und Backup in der Cloud: https://chemnitzer.linux-tage.de/2024/de/programm/beitrag/211
- BSI: Technische Betrachtung: Wie sicher sind die verschiedenen Verfahren der 2FA? https://www.bsi.bund.de/dok/1032220
- schumacher-crypt
- S. Schumacher, “Zwei-Faktor-Authentifizierung mit Yubikey-Token,” *UpTimes*, no. 2, pp. 16–27, 2018, Accessed: Feb. 01, 2019. [Online]. Available: https://www.guug.de/uptimes/2018-2/uptimes_2018-02.pdf.


FIDO2: Registrierung eines Passkey mit Discoverable Credentials
Benutzer
Hardware-Token
Webbrowser (WebAuthN)
Webseite
Relying Party
FIDO2-Server
1 Registrierung
2 Anfrage für Challenge
3
4 Erzeuge Zufalls-Challenge
5 Liefere Domain des Servers
6 Rückgabe (Challenge && Domain)
7
8 Aufforderung zur Erzeugung eines Schlüsselpaares
9 Überprüfe Domain des FIDO2-Servers (Phishing!)
10
11 Nutzer-Interaktion (z.B. PIN)
12 Erfolg
13 Erzeuge Schlüsselpaar verknüpft mit dem Nutzer
14 Signiere Daten mit dem privaten Signatur-Schlüssel
15 Gib signierte Daten zurück, sowie öffentlichen Schlüssel und Zertifikat des Nutzers
16 Gib signierte Daten zurück, sowie öffentlichen Schlüssel und Zertifikat des Nutzers
17 Übertrage signierte Daten öffentlichen Schlüssel und Zertifikat des Nutzers
18
19 Beziehe öffentlichen Signatur-Schlüssel
20 Verifziere signierte Daten und Challenge
21 Speichere Benutzer-Zugangsdaten und seinen öffentlichen Schlüssel
22 Erfolg
23
24
Benutzer
Hardware-Token
Webbrowser (WebAuthN)
Webseite
Relying Party
FIDO2-Server