Passwordless Authentication

junk-rat

2024-01-02

Was ist Passwordless Authentication? [1]

- Authentisierung ohne Wissens-Faktor
- Besitzfaktor
- Biometrie
- Fähigkeit

Beispiele

- Hardware Token
- Gesichtserkennung
- Fingerabdrucksensoren
- Unterschrift

Wozu brauchen wir Passwordless Authentication? [2] [3]

- Häufige Nutzung unsicherer Passwörter
- Angriffsfläche für Phishing wird minimiert
- Für "normalen" Internetnutzer sicheres MFA häufig zu aufwändig

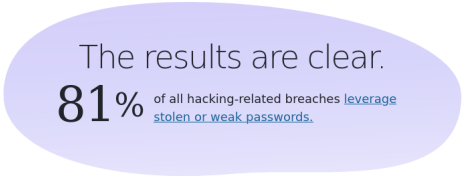

Bild: webauthn.guide

FIDO Alliance [4]

- Fast IDentity Online
- Will Abhängigkeit von Passwörtern reduzieren
- **Hauptziel:** Phishing-Resistent, Public-Key Cryptography, Sicher
- Feste Bindung des Secret Keys an Hardware (Authenticator)

Bild: fidoalliance.org

WebAuthN [5] [6]

- Public Key Verfahren mit Challenge Response
- Server sendet Client eine Challenge
- Client signiert die Challenge mit Secret Key
- Server kann mit Public Key überprüfen

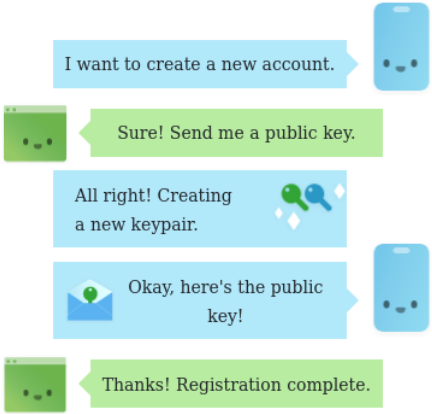

Bild: webauthn.guide

WebAuthN Demo [7]

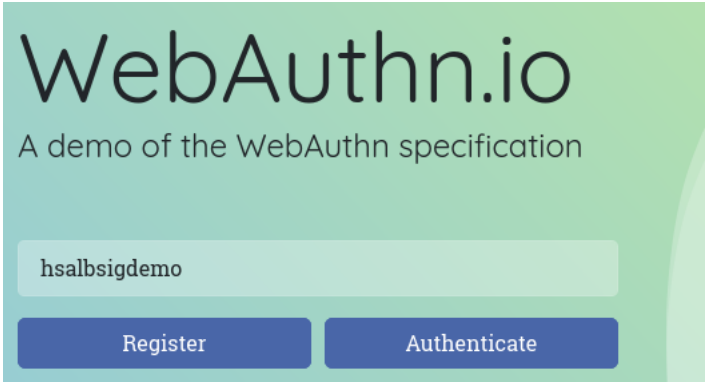

Bild: Screenshot von webauthn.io

WebAuthN Demo [7]

Bild: Screenshot von webauthn.io

WebAuthN Demo [7]

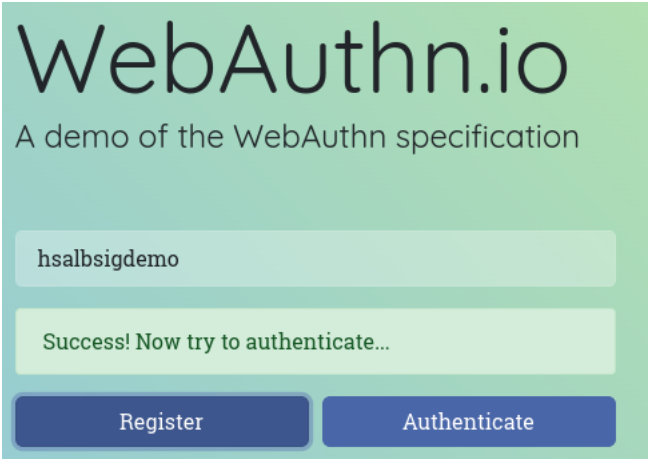

Bild: Screenshot von webauthn.io

WebAuthN Demo [7]

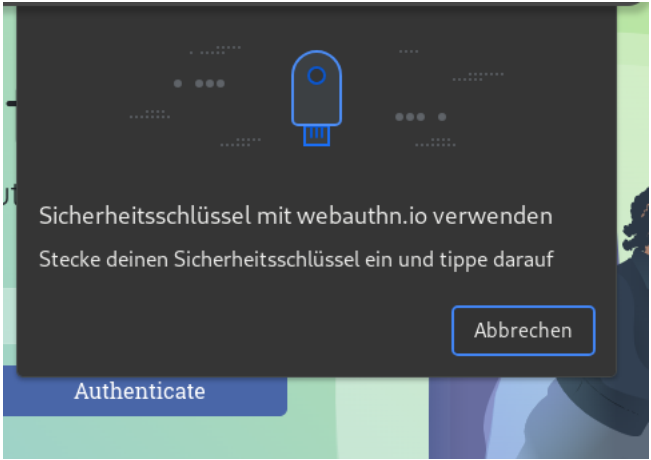

Bild: Screenshot von webauthn.io

WebAuthN Demo [7]

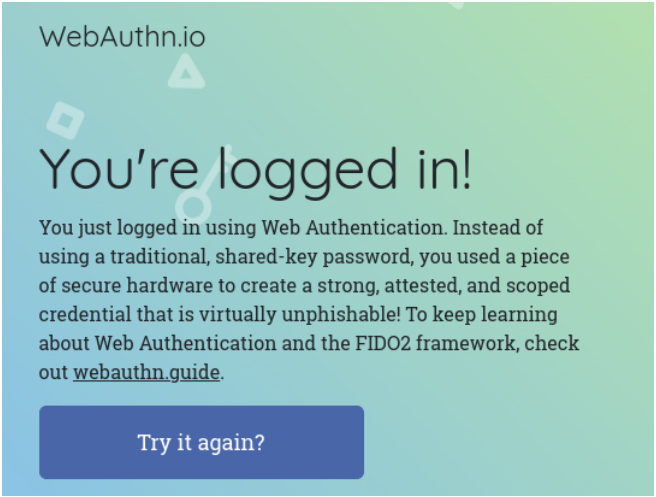

Bild: Screenshot von webauthn.io

Nachteile von WebAuthN [5]

- Mehr Kosten für Security-Token
- Schlüssel werden auf gleichem Gerät gespeichert, mit dem man sich authentisiert
- Für jedes Gerät auf dem man sich anmelden will, braucht man ein neues Schlüsselpaar

Passkeys [8] [9] [10]

- **Problem:** Was passiert, wenn man das Gerät verliert? Backups?
- Schlüssel sind zurücksetzbar (Synchronisation mit Cloud)
- Schlüssel verlässt sicheren Hardware Bereich
- Schutz nur noch so gut, wie Schutz bei Cloudanbieter

Fazit

Pro

- Passkeys bieten "normalen" Nutzern ein relativ hohes Sicherheitslevel
- Einfach zu benutzen
- Phishing wird verhindert
- Durch Passkeys wird "normales" WebAuthN mehr unterstützt

Contra

- Schlüssel zurücksetzen
- Abhängigkeit von einem Cloud-Anbieter
- Passwörter werden immer noch für z.B. Google Account benötigt

Quellen

- [1] Kinzer, K. (2023, July 24). Passwordless authentication methods and examples. JumpCloud. https://jumpcloud.com/blog/passwordless-authentication-methods-examples (Abgerufen am 01.01.2024)
- [2] Schneider, T. (2022, August 24). 5 Dinge, die Sie über die passwortlose Authentifizierung wissen sollten. Ping Identity. https://www.pingidentity.com/de/resources/blog/post/what-to-know-about-passwordless-authentication.html (Abgerufen am 01.01.2024)
- [3] Guide to web Authentication. (n.d.). Guide to Web Authentication. https://webauthn.guide/ (Abgerufen am 01.01.2024)
- [4] FIDO Alliance. (2024, January 5). FIDO Alliance. https://fidoalliance.org/ (Abgerufen am 01.01.2024)
- [5] Curity. (2021, April 29). An overview of WebAuthn. https://curity.io/resources/learn/webauthn-overview/ (Abgerufen am 01.01.2024)
- [6] Guide to web Authentication. (n.d.-b). Guide to Web Authentication. https://webauthn.guide/ (Abgerufen am 01.01.2024)
- [7] A demonstration of the WebAuthn specification. (n.d.). WebAuthn.io. https://webauthn.io/ (Abgerufen am 01.01.2024)
- [8] Eikenberg, R. (2023, May 19). Passkeys: Wie ein Account ohne Passwort funktioniert. C't Magazin. https://www.heise.de/hintergrund/Bestandsaufnahme-Passwort-Nachfolger-Passkeys-9048722.html (Abgerufen am 01.01.2024)
- [9] Passkeys: the web authentication standard. (n.d.). https://www.passkeys.com/ (Abgerufen am 01.01.2024)
- [10] Grauer, Y. (2023, May 24). Should you use passkeys instead of passwords? Consumer Reports. https://www.consumerreports.org/electronics/digital-security/should-you-use-passkeys-instead-of-passwords-a1201817243/ (Abgerufen am 01.01.2024)