Passkey

Adrian Kaunas – EOSM

FIDO-Alliance:

FIDO-Alliance in Kooperation mit W3C implementieren Industriestandards:
FIDO2 Standard (WebAuthn, CTAP) und Passkey Standard

Arten von Passkeys:

- Synced Passkey: Cloud Synchronisiert
- Device-Bound Passkey: Passkey fest auf Gerät

Voraussetzung für Device-Bound Passkey

TPM – Secure Enclave

- Voraussetzung für Device-Bound Passkey
- Dedizierter Chip
- kryptografische Operationen
- Speichern von private keys

WebAuthn:

Kryptografische Grundlagen

- Kernteil von FIDO2
- Asymmetrische Kryptografie
- Challenge-Response-Verfahren
- Multi-Faktor Authentikation (MFA)
  - Identität
  - Besitz
  - Wissen

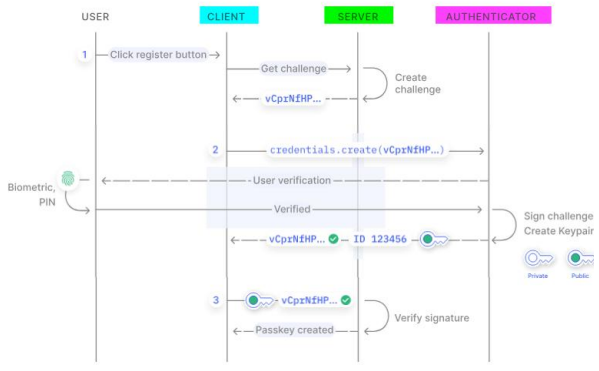
Aufbau

Relying Party (RP) / server
- Gegenüber der man sich authentifizieren möchte

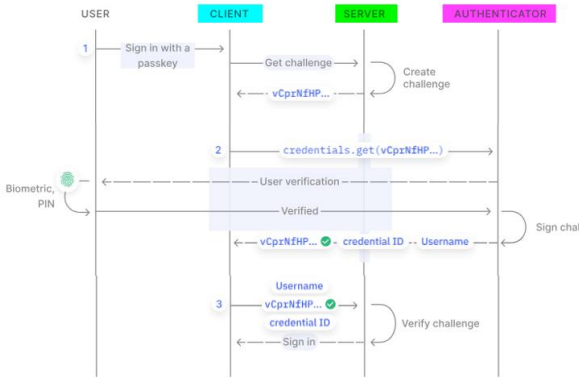
Client
- Schnittstelle zwischen RP, Authentificator und Nutzer
- Integriert in Browser oder Betriebssystem

Authenticator
- Der das benötigte Schlüsselmaterial erzeugt, nutzt und sicher verwahrt
- Benötigt TPM, Secure Enclave, Cloud

Passkey erstellen



Authentifikation mit Passkey



Gründe für und gegen die Nutzung

Vorteile	Nachteile
- Gegen Angriffe für symmetrische Krypo resistent	- WebAuthn leistungsintensiv (Server)
- Schwer zu Kompromittieren	- Höhere Kosten
- Benutzerfreundlich	- Kunden müssen sich umgewöhnen