FIDO 2 - Passkey-Synch

René Vogt

cnlab Herbsttagung 2025 – FIDO2: einfach und sicher
Gleisarena, Zürich, 3. September 2025

cnlab

Agenda_

Google Passwort Manager

Apple iCloud Keychain

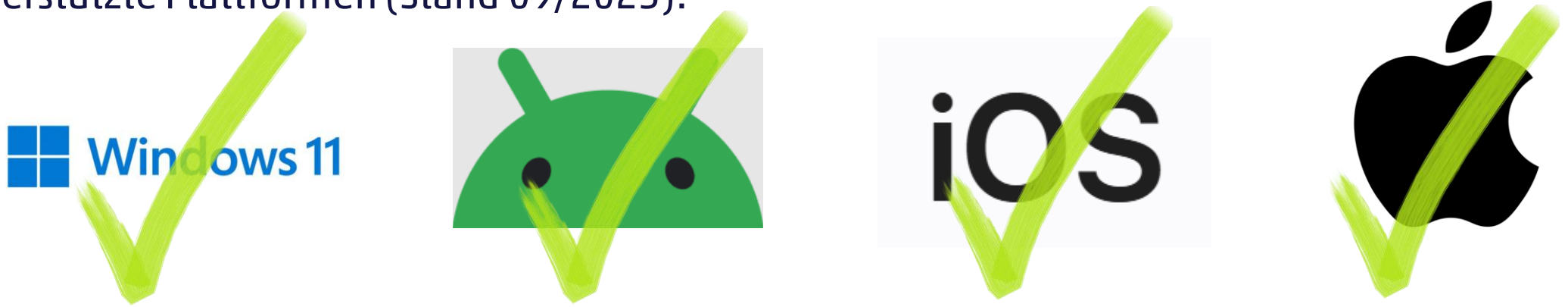
Microsoft Windows 11

Interoperabilität

Passkey-Synch - Google Password Manager

- Passkeys sind geschützt durch TPM
- Verwendung ist nur «online» möglich
- Aktivierung von neuen Geräten ist nicht Phishing-sicher (in vielen Konfigurationen). Benötigt
  - Google ID und Passwort
  - Falls 2FA aktiv: Bestätigung auf bestehendem Gerät oder TAN
  - PIN eines aktivierten Gerätes

Unterstützte Plattformen (Stand 09/2025):



Passkey-Synch - Apple iCloud Keychain

- Passkeys sind geschützt durch TPM (secure enclave)
- Zur Erstellung eines Passkeys muss iCloud-Keychain-Synchronisierung aktiv sein
- Aktivierung von neuen Geräten ist nicht Phishing-sicher (in vielen Konfigurationen). Benötigt
  - Apple ID und Passwort
  - Bestätigung auf bestehendem Gerät oder TAN
  - PIN eines aktivierten Gerätes

Unterstützte Plattformen (Stand 09/2025):

Passkey-Synch - Microsoft Windows 11

- Passkeys sind gebunden an Gerät (TPM, geschützt durch Windows Hello)
  - Anzeigen und Verwaltung unter Einstellungen → Konten → Hauptschlüssel
- Synchronisierung mit Microsoft-Account ist geplant

Unterstützte Plattformen (Stand 09/2025):

Passkey-Synch - Interoperabilität zwischen «Passkey-Universen»

Migration zwischen verschiedenen Passkey-Anbietern ist aktuell noch nicht möglich

- Spezifikation existiert als Draft (Credential Exchange Specification, CXF)

- KeePassXC kann Passkeys exportieren in ein Text-File (JSON), und umgekehrt (unverschlüsselt)

Vielen Dank für Ihre Aufmerksamkeit_

René Vogt

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland