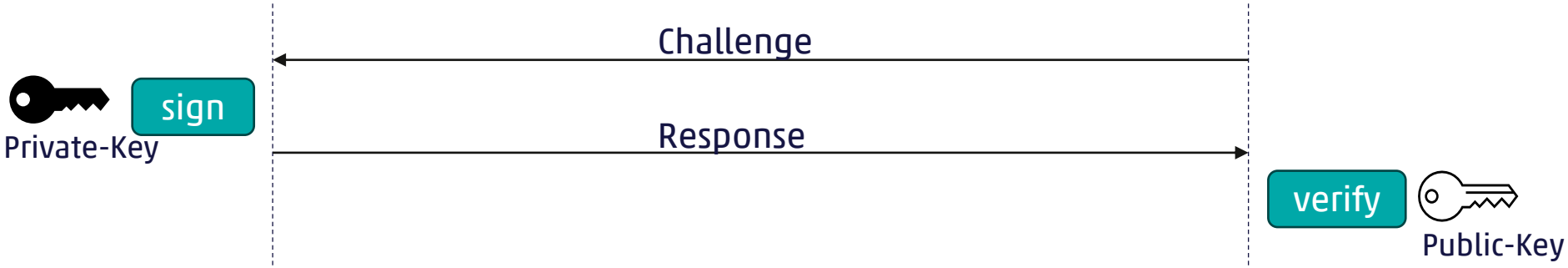
FIDO2 – Fazit

Urs Wagner

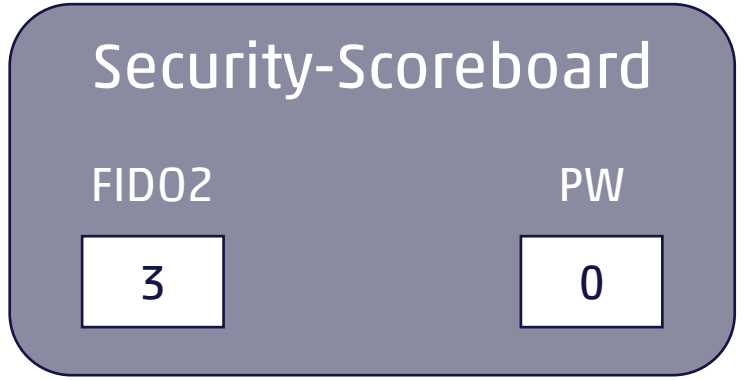
cnlab Herbsttagung 2025 – FIDO2: einfach und sicher
Gleisarena, Zürich, 3. September 2025

cnlab

FIDO2 – eine Authentisierungslösung



- Challenge-Response mit asymmetrischen Schlüsseln
- State-of-the-Art Prinzip
  - Private-Key wird nie übermittelt
  - Freshness: Response kann nicht ge-replayed werden
  - Vertraulichkeit des Public-Keys unkritisch
- FIDO2:
  - Regelt, wie dies für Anmeldungen an Online-Diensten gemacht werden kann
  - Enthält Mechanismen gegen Real-Time-Phishing
- FIDO2 gibt's schon seit 2018, weshalb ist es nicht mehr verbreitet?



Wo ist der Schlüssel – und wer hat Zugriff darauf? (Part I)

- Es braucht ein Gerät, welches:
  - den Private-Key sicher speichert
  - die Challenge beantworten kann
- Usability-Limitationen:
  - Backup
  - Verwaltung
- Deshalb Verbreitung primär:
  - im professionellen Umfeld
  - bei «Techies»

Plattformhersteller to the Rescue!

Windows Hello

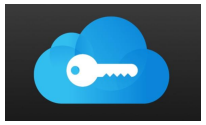
Google Password Manager

Apple KeyChain

- Keine Spezial-Geräte notwendig
- Security: Hardware-backed
- Backup und Verwaltung (teilweise) gelöst

→ macht es interessant für «Standardbenutzer»

Wo ist der Schlüssel – und wer hat Zugriff darauf? (Part II)



- Challenge: Überblick zu behalten, wann wie eingeloggt werden kann
- Relevant beim Speichern der Schlüssel auf den Plattformen:
  - Schutz der Konten (Apple, Android, Microsoft ..)
  - Einstellungen zur Synchronisation von Schlüsseln
  - Schutz der Geräte
  - Natürlich muss man den Plattformanbietern vertrauen

In der Verantwortung des Benutzers!

Passkeys

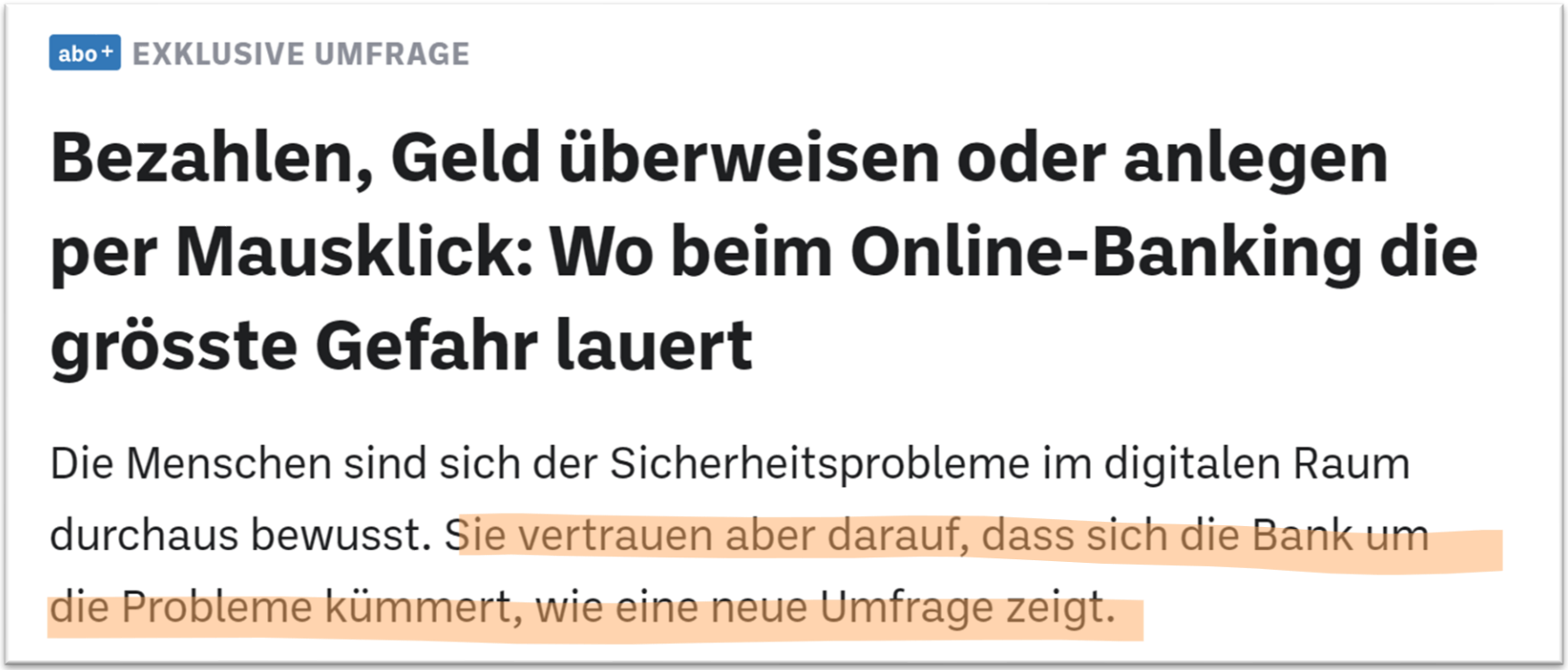
With passkeys, you can securely log in to your SwissID account using just your fingerprint, face or screen lock.

We suggest trying SwissID passkeys with the following:

- **Google Password Manager**
- **iCloud Keychain on Apple devices**
- **Chrome or Safari browser**

Since passkeys are strictly personal, make sure to keep your device's screen lock private and use a code that is difficult to guess. Also make sure your passkey is not synchronised with devices that others have access to, such as a family tablet.

Viel Verantwortung beim Benutzer – ein Problem?



abo+ EXKLUSIVE UMFRAGE

Bezahlen, Geld überweisen oder anlegen per Mausklick: Wo beim Online-Banking die grösste Gefahr lauert

Die Menschen sind sich der Sicherheitsprobleme im digitalen Raum durchaus bewusst. Sie vertrauen aber darauf, dass sich die Bank um die Probleme kümmert, wie eine neue Umfrage zeigt.

Zeitungen der CHMedia, 18.6.2025

Fazit

Soll ich auf Passkeys umsteigen?

- Als Ersatz für Passwörter: ja
- Für starke Authentisierung:
  - Mit speziellen FIDO2-Tokens: ja
  - Mit den Plattformanbietern: ja, wenn ich meine Geräte und Konten im Griff habe und den Plattformanbietern vertraue (es gibt aber viele «ifs»)

Können Banken und Anbieter ähnlich kritischer Anwendungen die Anmeldung mittels Plattform-Passkeys erlauben?

- Als Ersatz für das Passwort: ja
- Als starke Authentisierung für das breite Publikum: empfehlen wir nicht

Und wie ist's mit dem neuen Standard für Zahlungsbestätigungen?

- Noch nicht so weit, um Transaktionsbestätigungen im Banking abzulösen
- Schlüsselfrage auch nicht zufriedenstellend gelöst (Device-PIN)

Vielen Dank für Ihre Aufmerksamkeit_

Urs Wagner

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

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

cnlab