

FIDO2-Standard

Martin Kaufmann

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

FIDO Alliance

- Offener Branchenverband (open industry association)
- FIDO = Fast Identity Online
- Mission der FIDO Alliance: die Abhängigkeit der Welt von Passwörtern verringern
- Fördert die Entwicklung, Verwendung und Einhaltung von Standards für die Authentisierung und Gerätebescheinigung (Attestation).



FIDO Alliance: Board Level Members

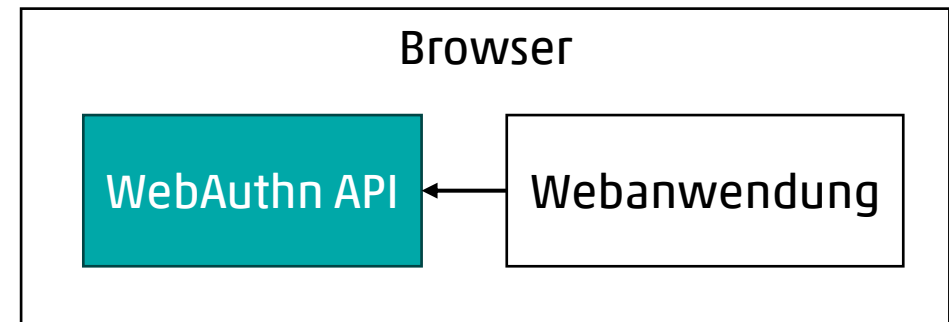
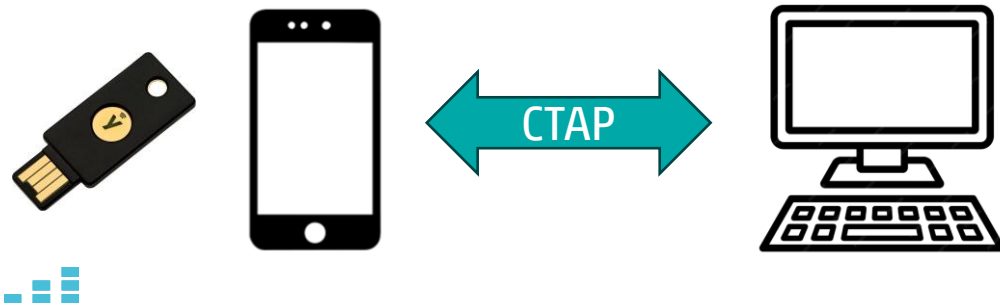
				
				
				
				
				
				
				
				
				



FIDO2

- Phishing-resistente Benutzer-Authentisierung mit Public-Key-Kryptografie
- Umfasst zwei Spezifikationen
 - Client to Authenticator Protocol, v2 (CTAP)
 - Publiziert von der Fido Alliance
 - Anwendungsprotokoll für die Kommunikation mit Roaming-Authenticators
 - Web Authentication, Level 2 (WebAuthn)
 - Publiziert vom "World Wide Web Consortium" (W3C)
 - Browser-API zur Authentisierung mit Public-Key-Kryptografie

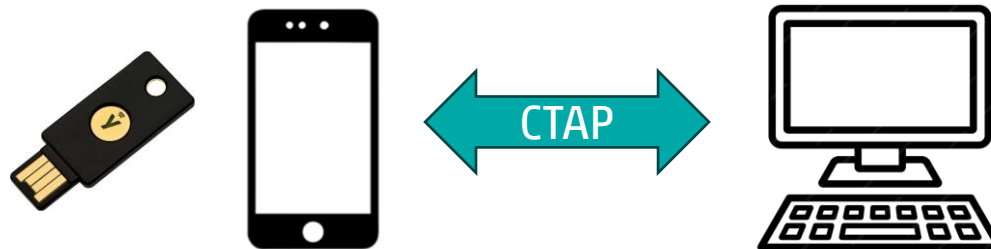
Roaming Authenticator



Client to Authenticator Protocol (CTAP)

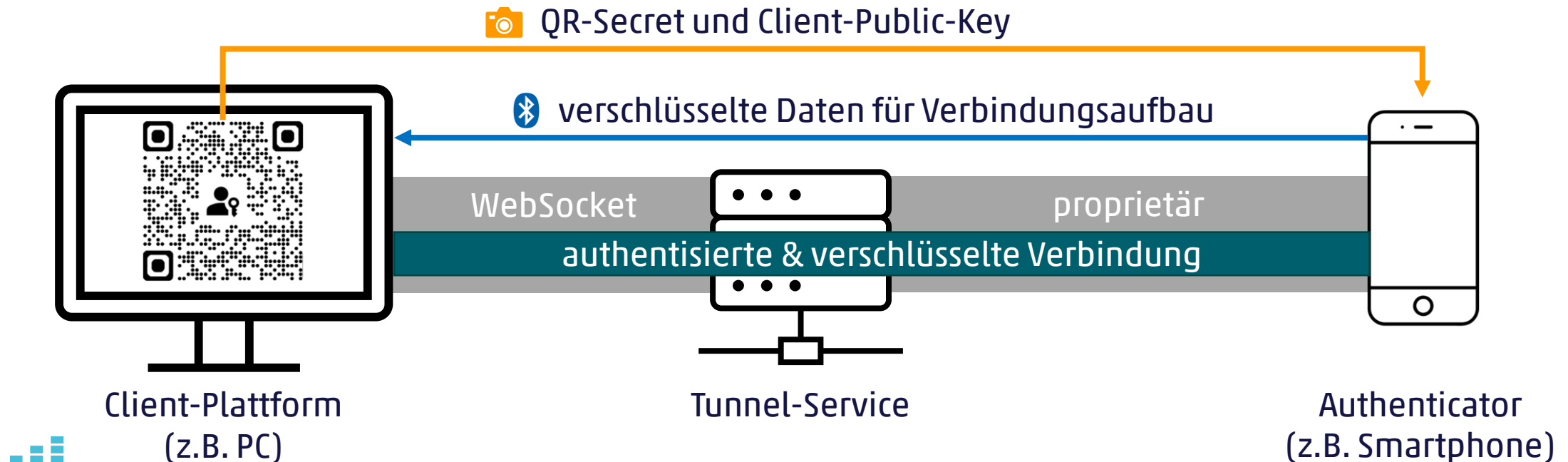
- Anwendungsprotokoll für die Kommunikation mit Roaming Authenticators
- Ziel von CTAP: Authenticator befindet sich in der Nähe des Geräts, auf dem man sich anmeldet
- Transports
 - USB Human Interface Device (USB HID)
 - Near Field Communication (NFC)
 - Bluetooth Low Energy (BLE)
 - Hybrid Transports / cloud-assisted Bluetooth Low Energy (caBLE)

Roaming Authenticator

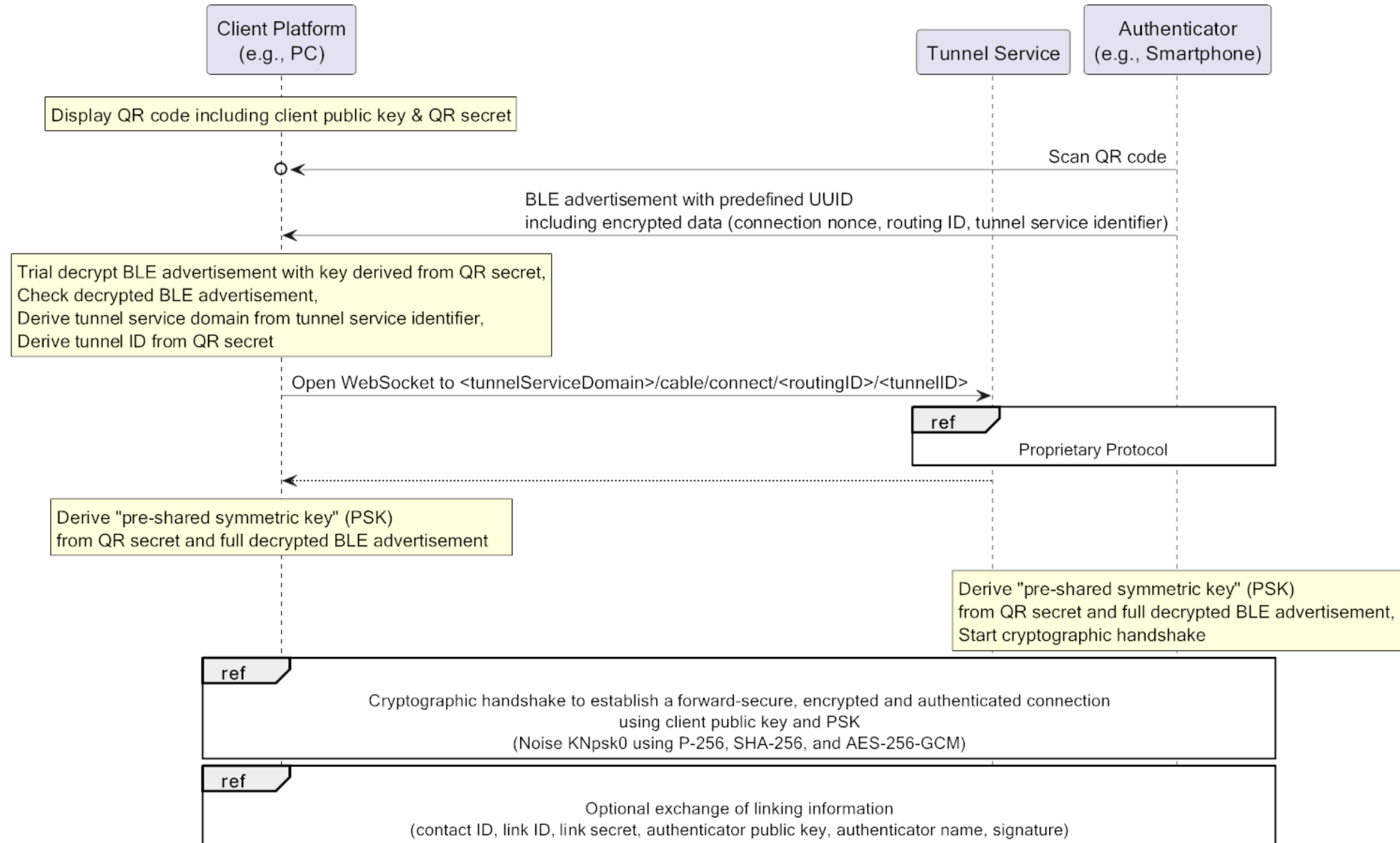


cloud-assisted Bluetooth Low Energy (caBLE)

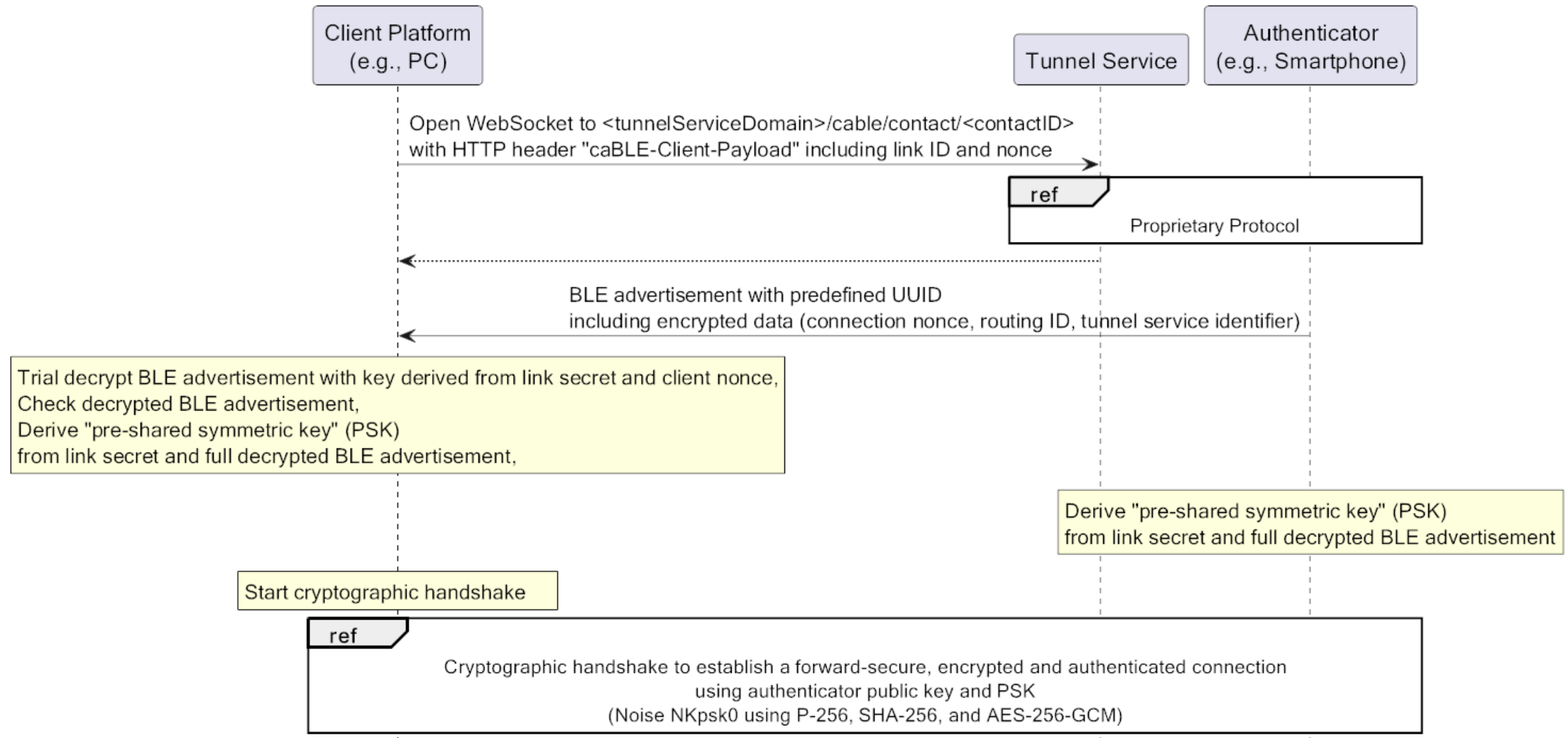
- zur Verbindung einer Client-Plattform (z.B. PC) mit einem Authenticator mit Kamera (z.B. Smartphone)
 - Client-Plattform zeigt QR-Code an (enthält QR-Secret und Client-Public-Key)
 - Benutzer scannt QR-Code mit Authenticator
 - Authenticator sendet verschlüsselte Daten für Verbindungsaufbau via BLE an Client-Plattform
 - Client-Plattform und Authenticator bauen Verbindung über Tunnel-Service auf
- "Linking" von Client-Plattform und Authenticator für zukünftigen Verbindungsaufbau ohne QR-Code



caBLE: Initialer Verbindungsaufbau

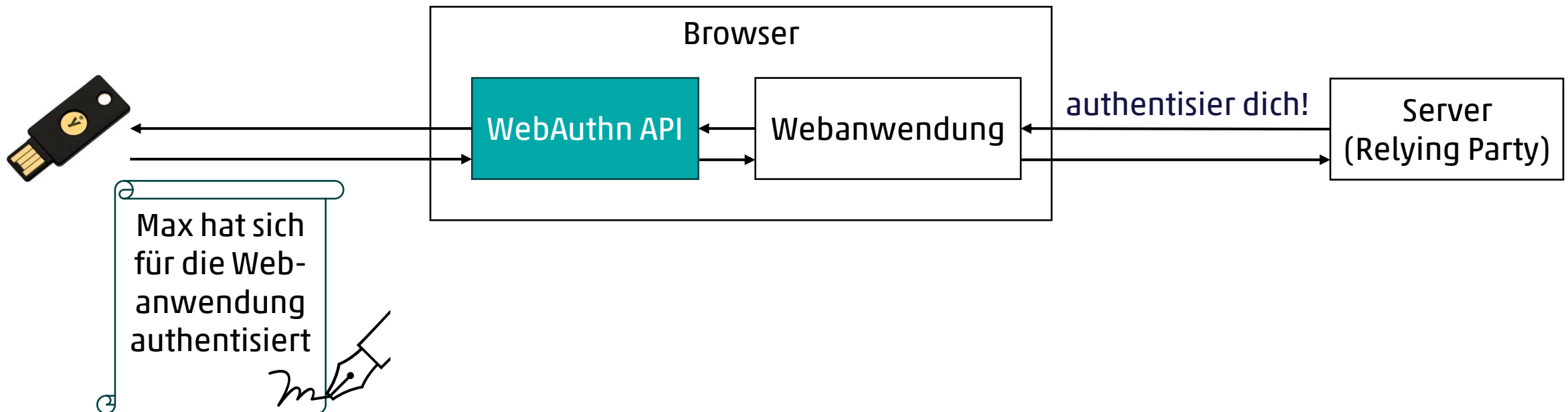


caBLE: Verbindungsaufbau nach Linking

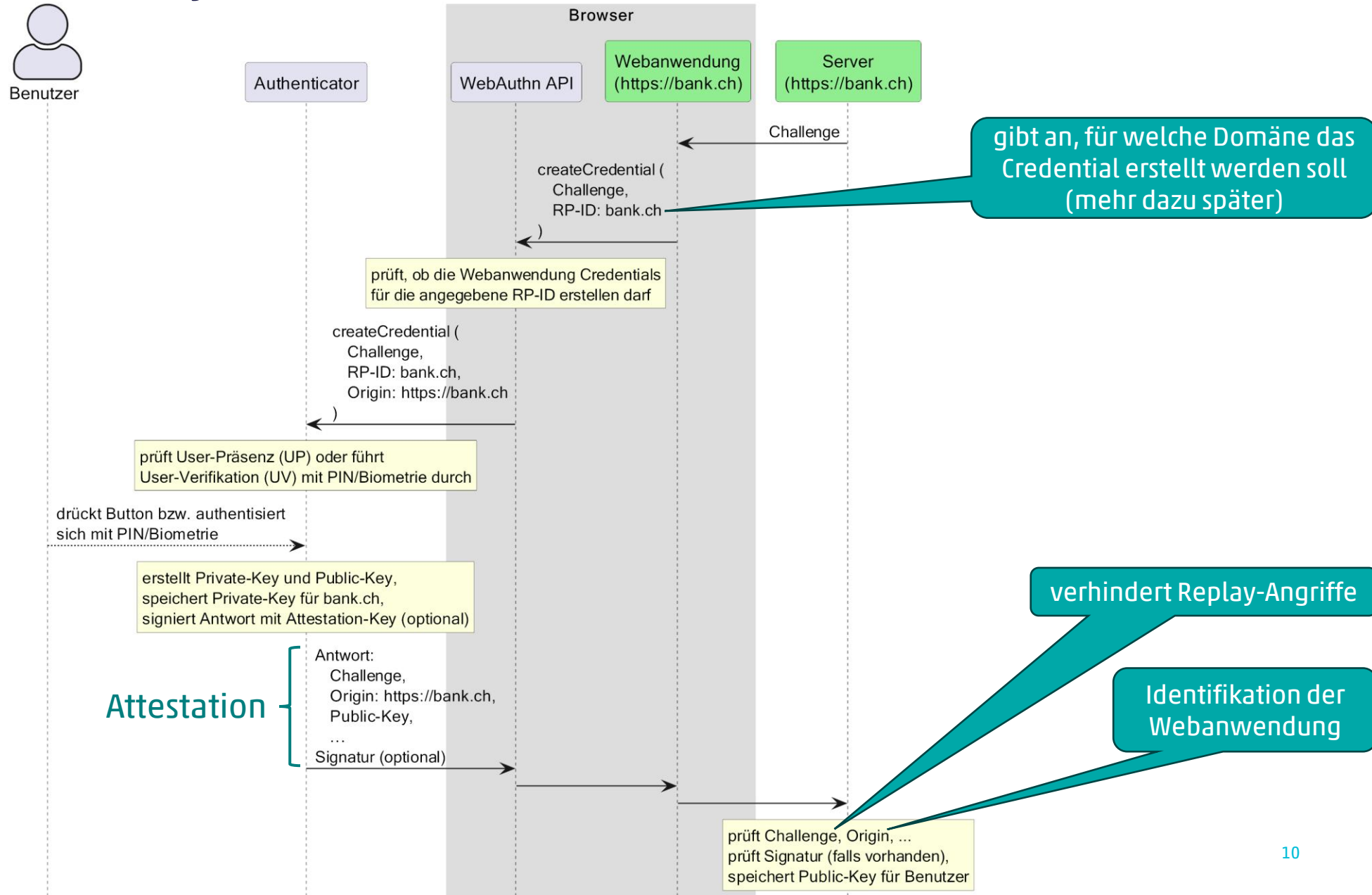


WebAuthn

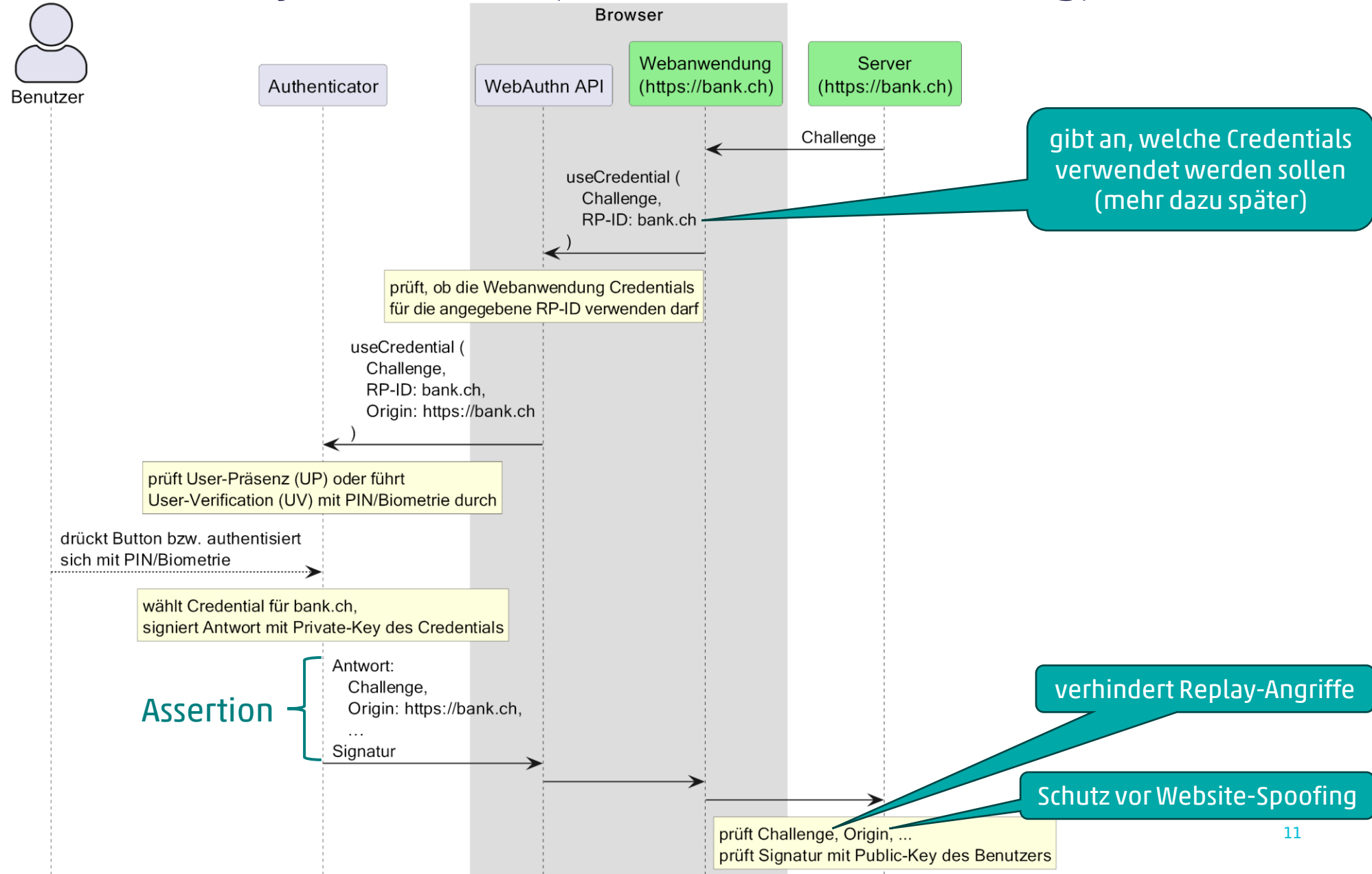
- Browser-API zur Authentisierung mit Public-Key-Kryptografie
- Hauptfunktionen
 - Erstellen eines Public-Key-Credentials
 - Verwenden eines Public-Key-Credentials (Benutzer-Authentisierung)



Erstellen eines Public-Key-Credentials



Verwenden eines Public-Key-Credentials (Benutzer-Authentisierung)



Berechtigung zum Erstellen und Verwenden von Credentials (RP-ID)

- Eine Webanwendung (z.B. <https://www.ebanking.bank.ch>) kann Credentials erstellen für
 - ihre effektive Domäne
 - www.ebanking.bank.ch
 - einen registrierbaren Domänen-Suffix ihrer Domäne
 - [ebanking.bank.ch](https://www.ebanking.bank.ch)
 - [bank.ch](https://www.ebanking.bank.ch)
 - beliebige andere Domänen, falls diese das erlauben (im File unter `"/.well-known/webauthn"`)
- dasselbe gilt für das Verwenden von Credentials
- wird durch den Browser sichergestellt



Vorteile von FIDO2

- Phishing-Schutz
 - Private-Key bleibt im Authenticator
 - Authenticator „muss“ in der Nähe des Geräts sein, auf dem man sich anmeldet
 - Browser übergibt dem Authenticator die Origin der Webanwendung. Origin ist Teil der signierten Assertion und wird vom Server geprüft. (Schutz vor Website-Spoofing)
- Einfache 2FA
- Keine „schwache“ Credentials
- Serverseitig müssen keine Secrets oder Passwort-Hashes gespeichert werden
- Private-Key ist in der Regel gut geschützt



Backup & Synchronisierung von Credentials

- Warum macht man das?
 - Sicherung der Credentials
 - Login auf mehreren Geräten mit demselben Credential (analog zu Passwort-Manager)
- Nicht Teil des Standards und abhängig vom Authenticator
- in der Attestation und Assertion steht jedoch
 - ob ein Backup von einem Credential erstellt werden darf (Backup Eligibility)
 - der Backup-Status des Credentials



Was sind Passkeys?

- Definiert in "Web Authentication Level 3" (W3C Working Draft) vom 27.01.2025:

Passkey = "discoverable" Public-Key-Credential

- WebAuthn unterscheidet "**discoverable**" und "**non-discoverable**" Public-Key-Credentials
- zur Verwendung von "discoverable" Public-Key-Credentials muss beim Aufruf des WebAuthn-API das zu verwendende Public-Key-Credential (Credential-ID) nicht spezifiziert werden
→ Benutzer muss den Benutzernamen nicht eingeben

Vielen Dank für Ihre Aufmerksamkeit_

Martin Kaufmann
martin.kaufmann@cnlab.ch
+41 55 214 33 45

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

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