Secure Payment Confirmation (W3C Standard)

Stephan Verbücheln

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

cnlab

Motivation

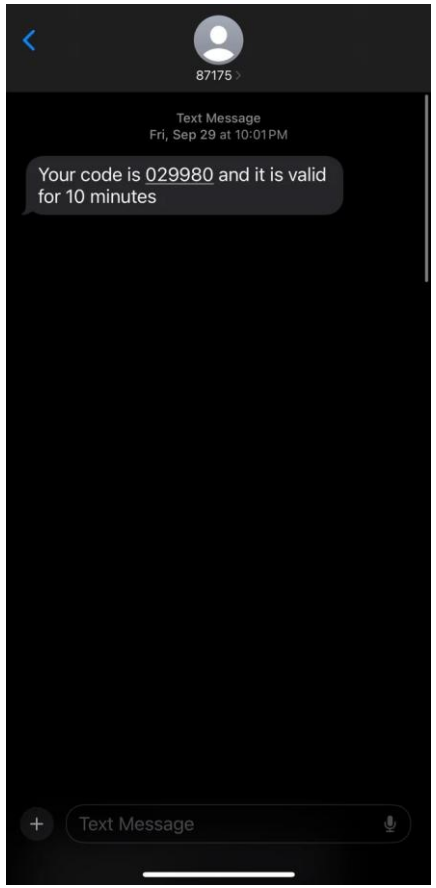
Transaktionsbestätigungen bisher

- Banking-Apps
- 3DS
- Frames mit Bezahlseiten

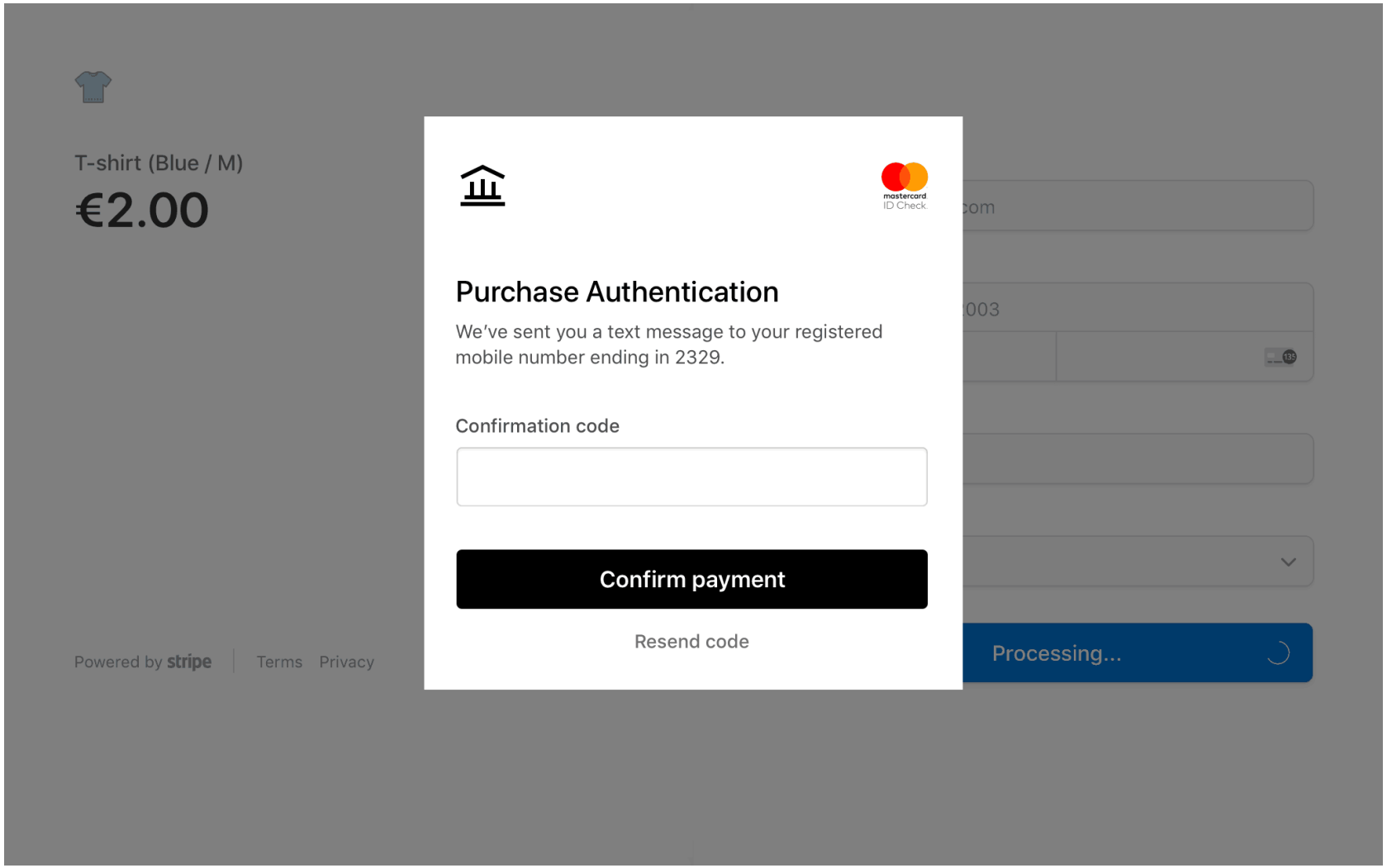
Probleme

- Schwierig von Phishing zu unterscheiden
- Hohe Abbrecherquote bei Einkäufen

UX 3DS



Telefon



Desktop

Bild: Stripe

Motivation

Grenzen von WebAuthn

- Man weiss nicht im Detail, was man bestätigt
- Kein einheitlicher Standard
  - Keine expliziten Datenfelder
  - Daten müssten in der Challenge übermittelt werden
  - Responses können nicht eindeutig zugeordnet werden
  - Zahlungsbestätigung für Login missbrauchen und umgekehrt

Secure Payment Confirmation (SPC)

W3C Candidate Recommendation **Draft** (14. August 2025)

Chrome 139	Firefox 142	Safari 18	Edge 139
58/72	7/70	10/72	61/72

Vorgänger

- WebAuthn
- FIDO Transaction Confirmation (Whitepaper)

SPC: Änderungen gegenüber WebAuthn

1. Neue explizite Felder
   - Zahlungsmittel
   - Währung
   - Betrag
   - Begünstigter (Payee)
2. Payee muss nicht Relying Party sein («Third-Party Enabled»)
3. Schlüssel können gerätegebunden sein («Browser Bound Keys»)

UX SPC

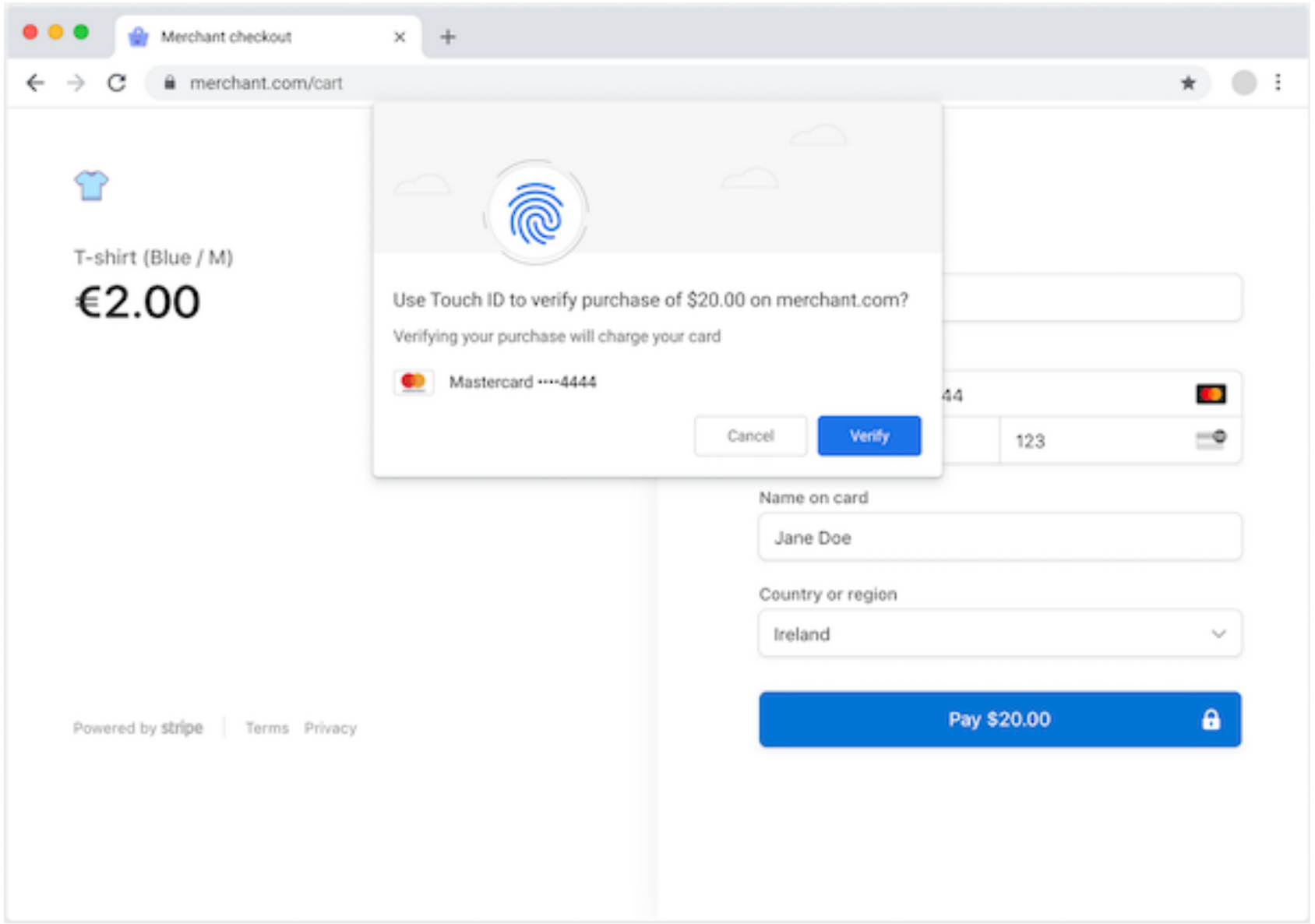
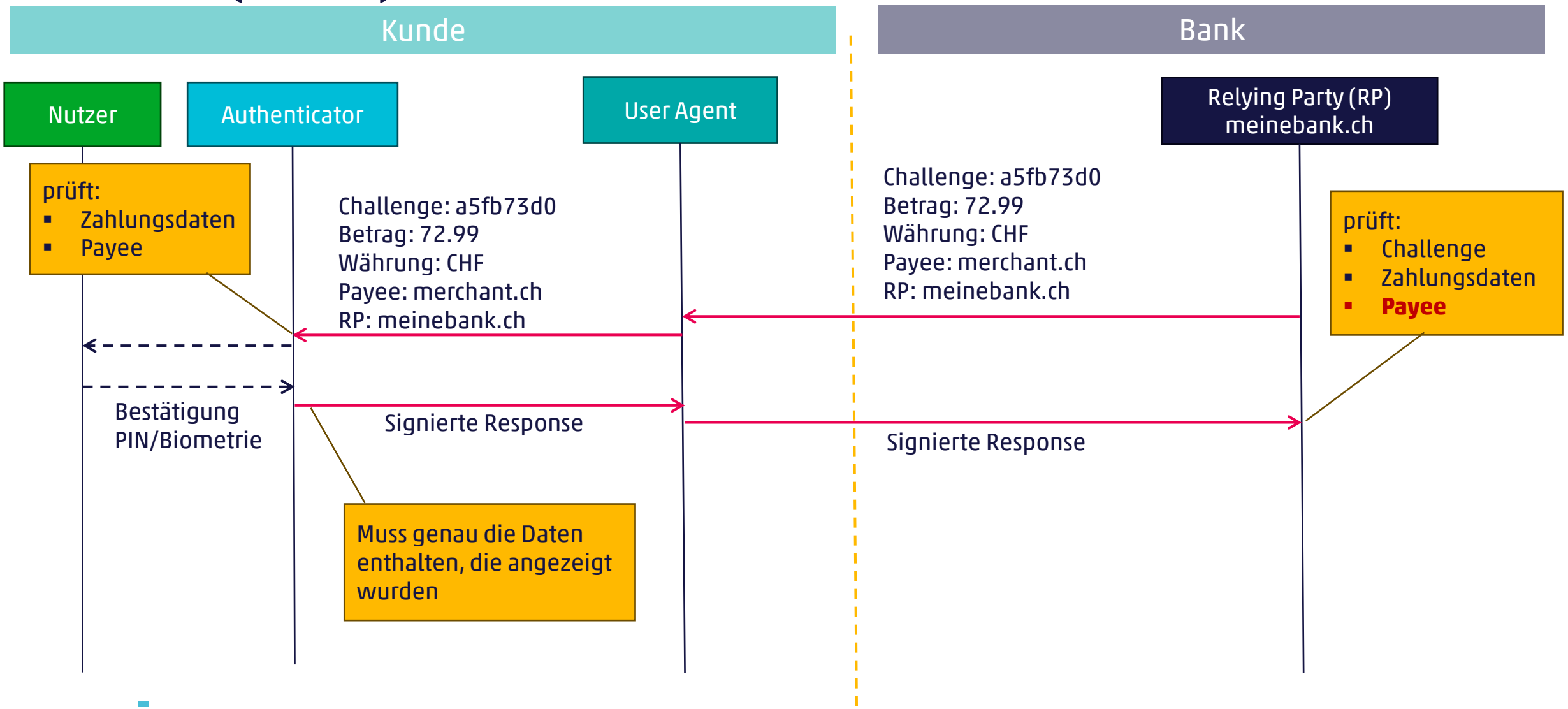
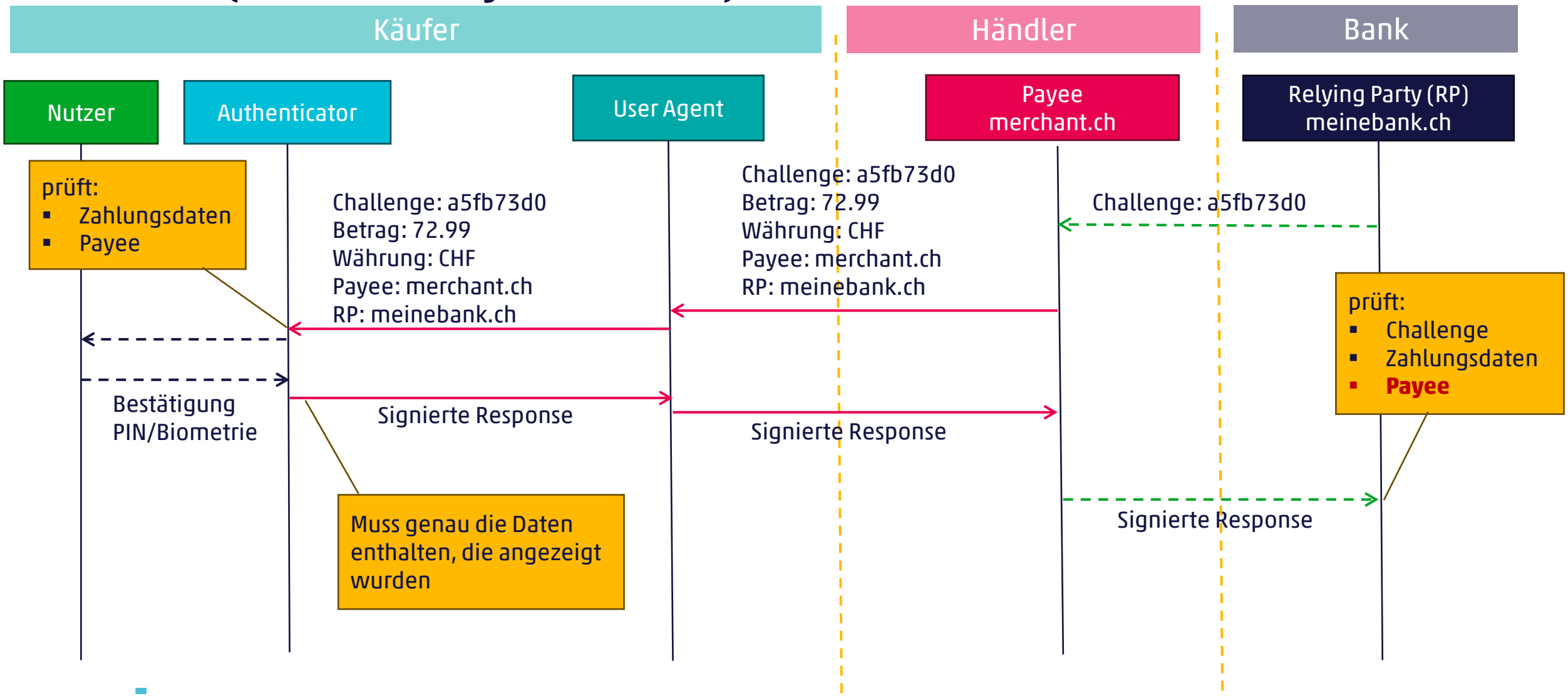


Bild: W3

Ablauf (direkt)



Ablauf («Third-Party Enabled»)



Beispiel

```
5     rpId: "fancybank.example",
```

```
12    payeeName: "Merchant Shop",
13    payeeOrigin: "https://merchant.example",
```

```
37    total: {
38      label: "Total",
39      amount: {
40        currency: "USD",
41        value: "5.00",
42      },
43    },
```

```
const request = new PaymentRequest([{
  supportedMethods: "secure-payment-confirmation",
  data: {
    credentialIds,
    rpId: "fancybank.example",
    challenge: new Uint8Array([21,31,105 /* 29 more random bytes generated by the bank */]),
    instrument: {
      displayName: "FancyBank Platinum Card",
      details: "****1234 | 01/29",
      icon: "https://fancybank.example/card-art.png",
    },
    payeeName: "Merchant Shop",
    payeeOrigin: "https://merchant.example",
    paymentEntitiesLogos: [
      {
        url: "https://fancybank.example/logo.png",
        label: "Fancy Bank",
      },
      {
        url: "https://securenetwork.example/logo.png",
        label: "Secure Network",
      },
    ],
    locale: ["en"],
    timeout: 360000,  // 6 minutes
    browserBoundPubKeyCredParams: [
      {
        type: "public-key",
        alg: -7 // "ES256"
      },
      {
        type: "public-key",
        alg: -257 // "RS256"
      }
    ]
  }], {
    total: {
      label: "Total",
      amount: {
        currency: "USD",
        value: "5.00",
      },
    },
  });

```

Browser Bound Keys

«A public-private key pair that signs over the transaction details in addition to the WebAuthn credential and is **tied to a single device** by the user agent.»

- Irreführender Name
- Gerätebindung durch Schlüssel in Hardware empfohlen
- Hardwarebindung mit PIN bzw. Biometrie erreicht 2FA
- Unterstützte Algorithmen noch unbekannt (Chrome)

Mehrere Geräte

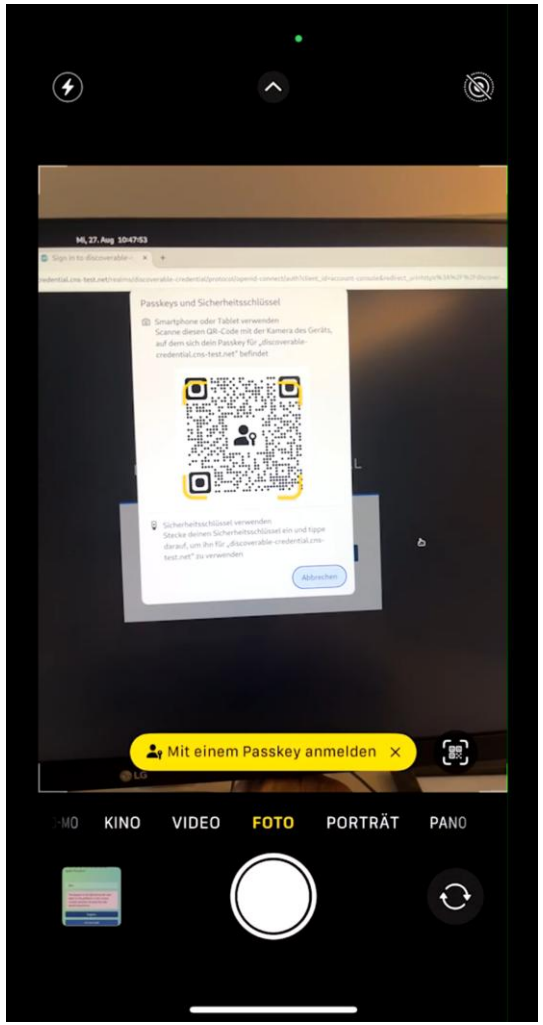
Schutz auf kompromittiertem Gerät schwach

- Malware kann alle Anzeigen und Eingaben verändern

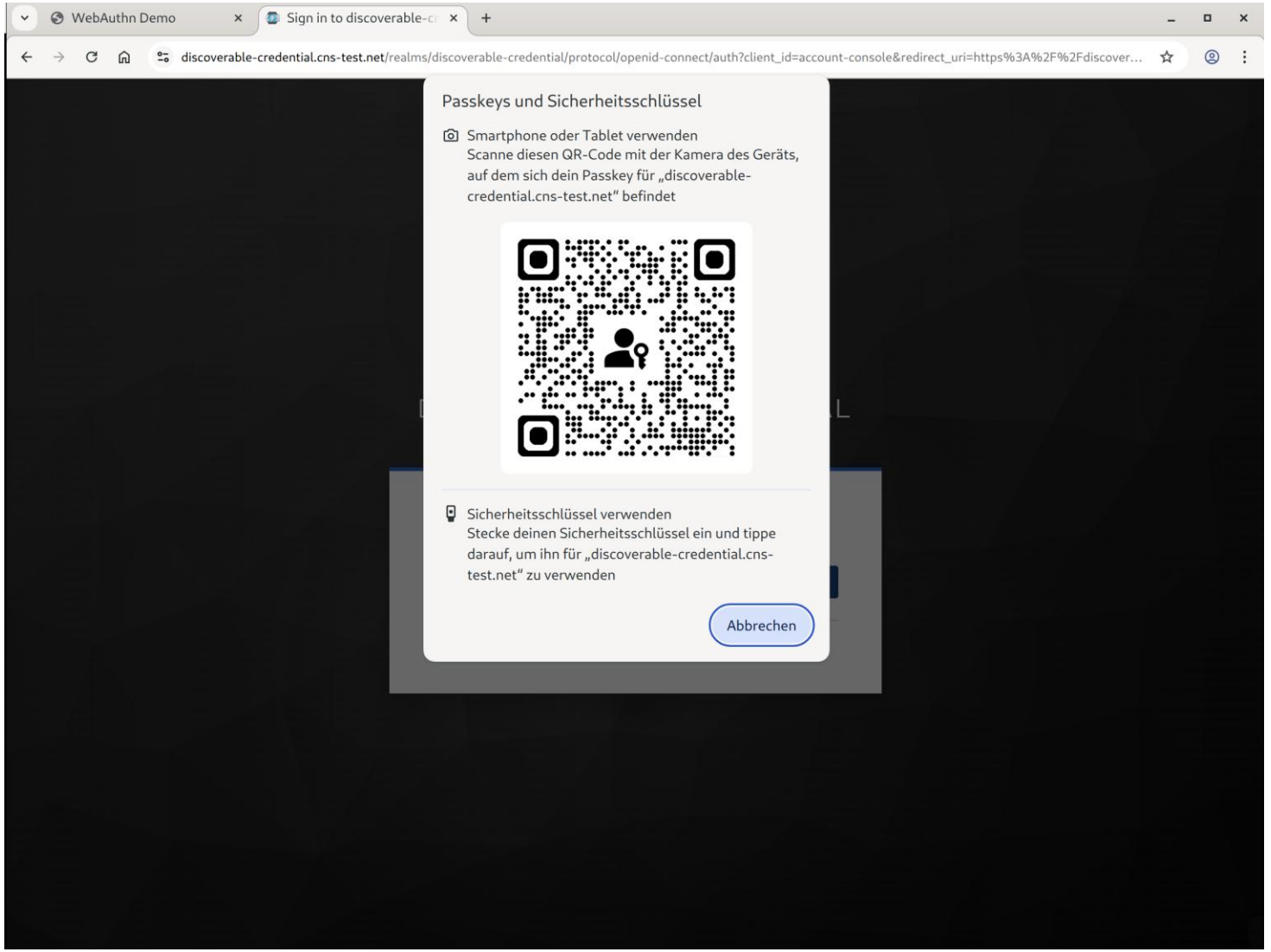
Transaktionen können auf zweitem Gerät bestätigt werden (via BLE)

- Unklar, ob dies mit Browser Bound Keys möglich ist

UX

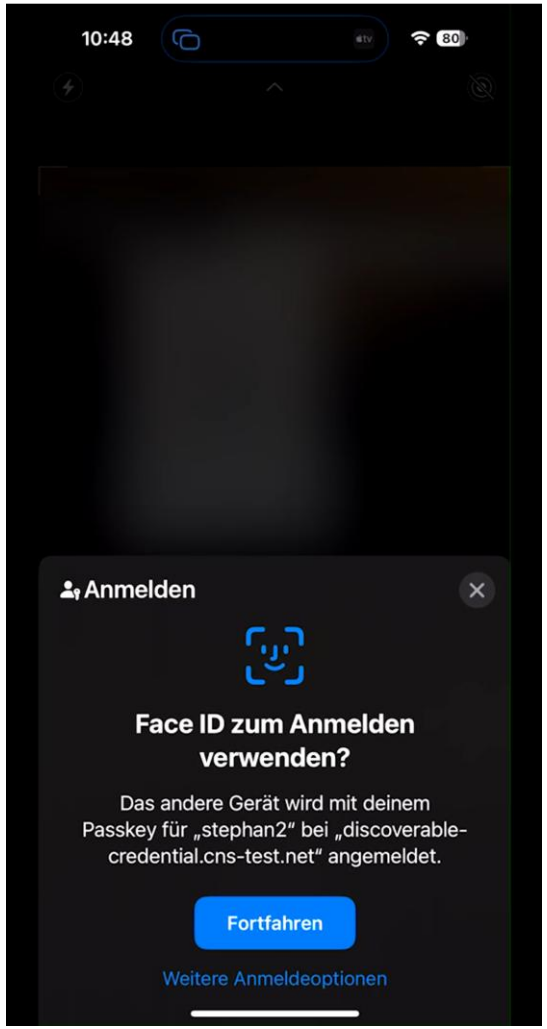


Smartphone

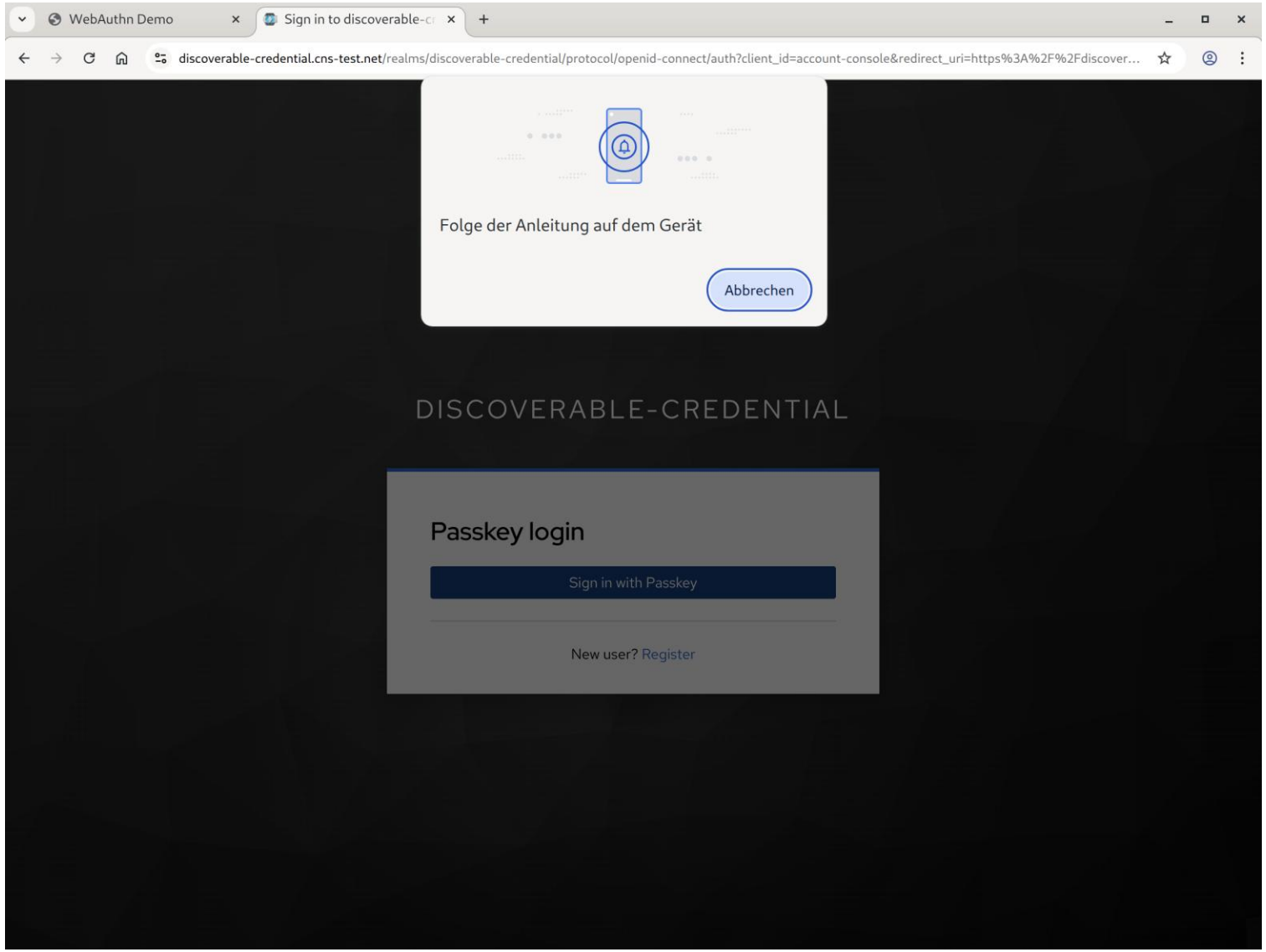


Desktop

UX



Smartphone



Desktop

Fettnäpfchen

Third-Party Enabled Passkeys bieten neue Angriffsmöglichkeiten

- Merchants können versuchen, mit SPC-Passkeys Login durchzuführen
  - Relying Party entscheidet, wofür derselbe Passkey verwendet werden kann
  - Passkey und Daten müssen genau geprüft werden

Vorteile zu bestehenden Lösungen

- Etablierter Standard
- Breite Unterstützung auf verschiedenen Plattformen
  - Webbrowser (Firefox, Safari, Chrome, Edge)
  - Betriebssysteme (Windows, iOS, macOS, Android, Linux)
  - Geräte (Smartphones, TPMs, Yubikeys usw.)
- Keine eigene App notwendig

Nachteile zu bestehenden Lösungen

- Noch nicht implementiert
- Andere Sicherheitsgarantien als bestehende Lösungen
- Mehr-Geräte-Paradigma kann ggf. nicht erzwungen werden

Fazit

Viele neue Ideen

- Public-Key-Kryptographie statt Passwörter und OTPs

Macht viele Szenarien sicherer

- Insbesondere vor Phishing

Eignung für spezielle Szenarien muss evaluiert werden

- Erzwingung spezieller Anforderungen

Links

WebAuthn

- https://www.w3.org/TR/webauthn/

Secure Payment Confirmation

- https://www.w3.org/TR/secure-payment-confirmation/

Vielen Dank für Ihre Aufmerksamkeit_

Stephan Verbücheln
stephan.verbuecheln@cnlab.ch
+41 55 214 33 36

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

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