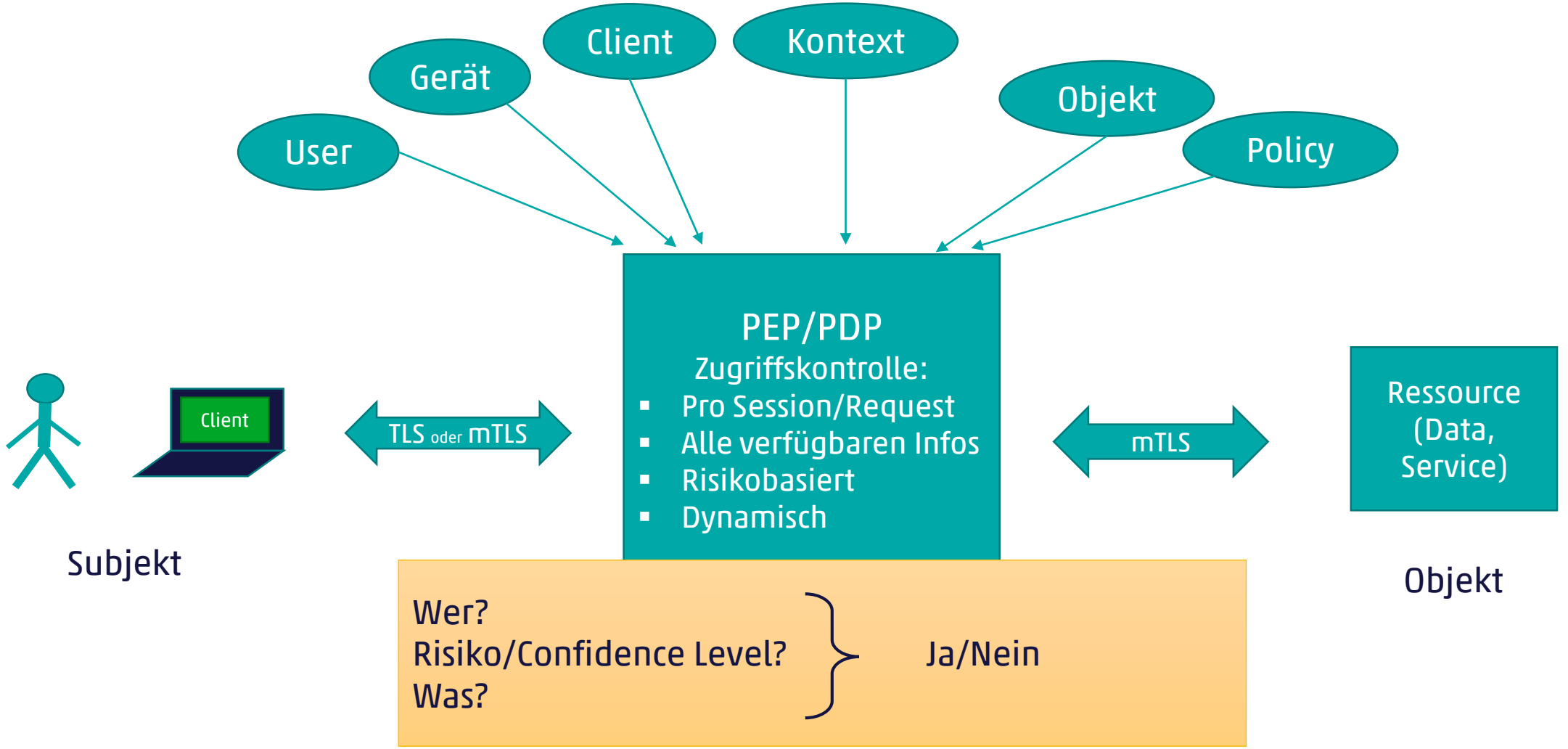
# Herbsttagung 2020
# Zero Trust: Zugriffskontrollen und Authentisierung

Zuzana Trubini
Zürich, 9. September 2020

cnlab

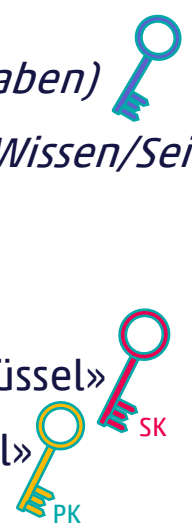
# Zugriffskontrollen und Prinzipien von Zero-Trust

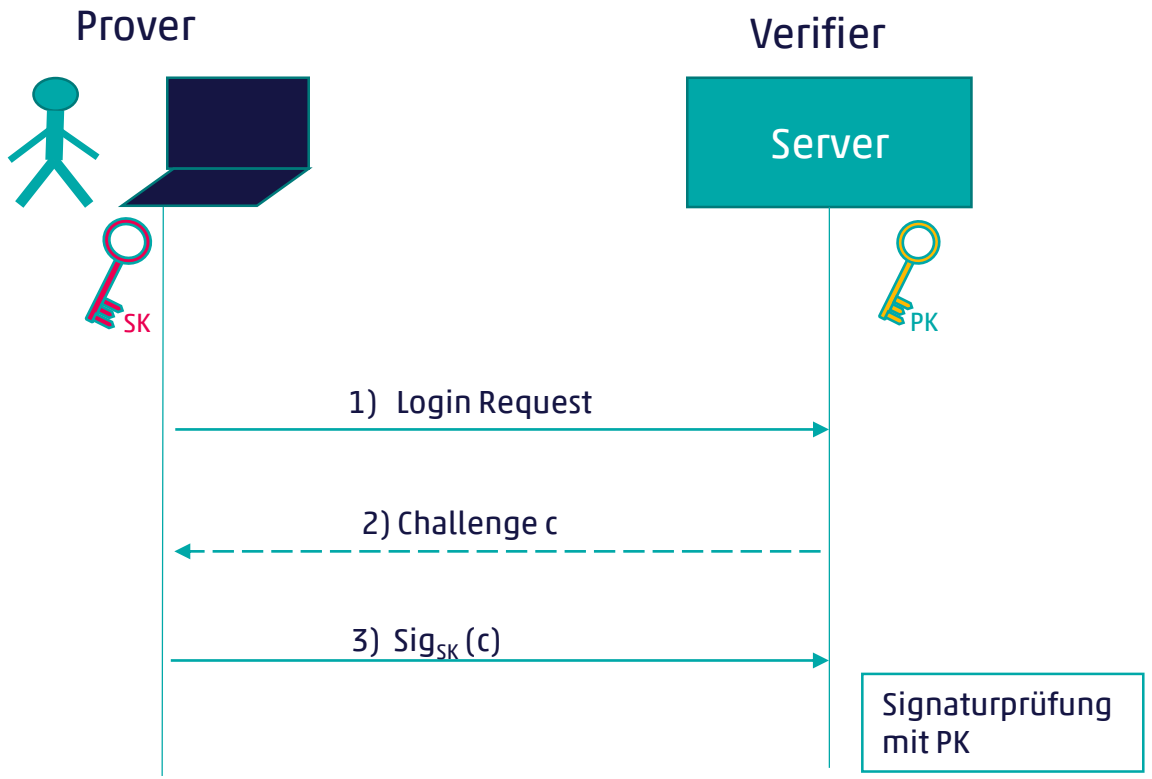


# Authentisierung

mit Hilfe eines Geheimnisses

- Kurz – z.B. Passwort *(Wissen)*
- Lang - Kryptographischer Schlüssel *(Haben)*
  - Ev. PIN oder Biometrie geschützt *(Wissen/Sein)*
  - Symmetrisch
  - Asymmetrisch – ein Schlüsselpaar
    - Secret Key - SK – «Signaturschlüssel»
    - Public Key - PK – «Prüfschlüssel»
    - Challenge/Response

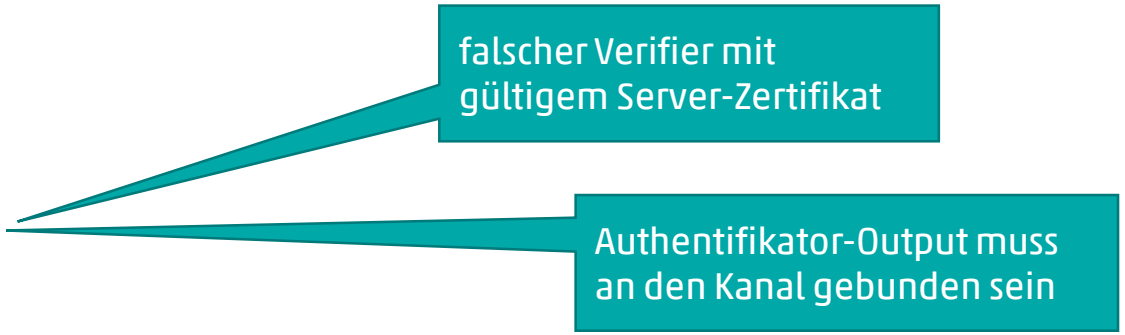


# Sicherheitskriterien für Authentisierungsverfahren

Resistenz gegen

- … Verifier Compromise
- … Replay Attacken
- … Phishing
- … Real-Time Phishing (MitM)
- … Verifier Impersonation (strong MitM)



# Sicherheitsanalyse

| Resistenz gegen: | Passwort | Challenge/Response |
|---|---|---|
| **Verifier Compromise** | Nein | Ja / Nein |
| **Replay Attacken** | Nein | Ja |
| **Phishing** | Nein | Ja |
| **Real-Time Phishing (MitM)** | Nein | Nein |
| **Verifier Impersonation** | Nein | Nein |

Schwäche auch bei 2FA
- PW + mTAN
- PW + PhotoTAN
- PW + PushTAN

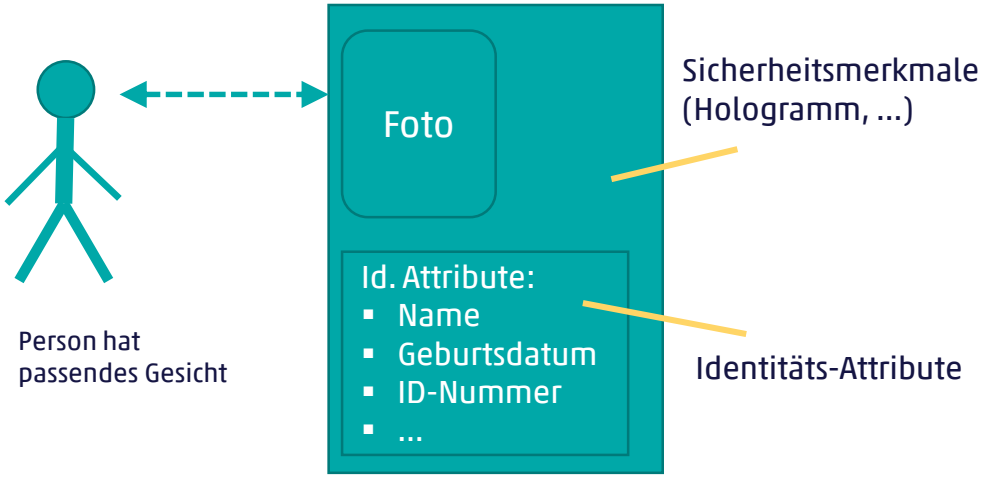
Laut MELANI 2019: Immer mehr Angriffe dieser Art

Wie kann man sich schützen?

mTLS (Zertifikatsbasiert)
FIDO2

# Zertifikatsbasierte Authentisierung

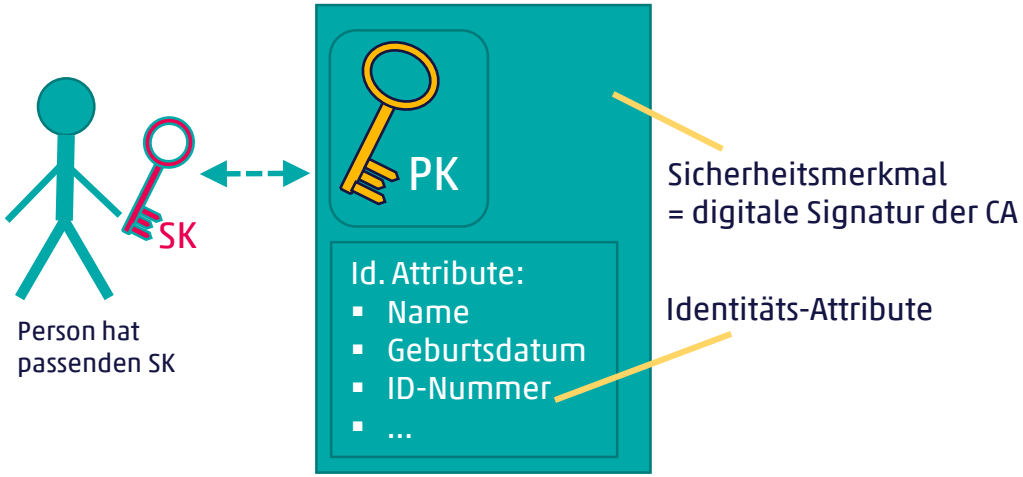
- Reale Welt - Ausweis




Bedeutung: Die Person deren Gesicht zu diesem Foto passt ist Inhaberin dieses Ausweises und folglich Trägerin dieser Attribute

1. Person zeigt Ausweis
2. Verifier prüft, ob die Person ein Gesicht hat, das zum Foto passt

- Digitale Welt - Zertifikat




Bedeutung: Die Person die den SK hat, der zu diesem PK passt, ist Inhaberin dieses Zertifikats und folglich Trägerin dieser Attribute

1. User schickt Zertifikat
2. Verifier prüft, ob die Person einen SK hat, der zum PK passt

# TLS und mTLS

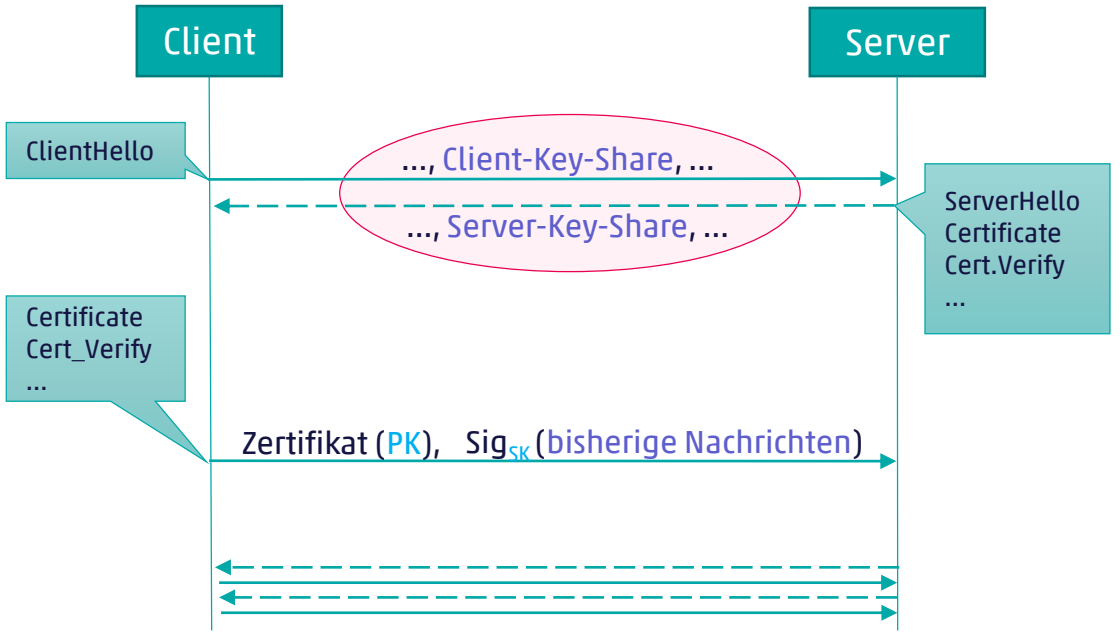
Geheim & Authentisch

- Sichere Kommunikation über unsichere Leitung
- TLS-Handshake
  1. Schlüsselaustausch
     - Unsicherer Kanal -> geheimer Kanal
  2. Authentisierung
     - Server-Authentisierung

     oder
     - Beidseitige Authentisierung - mutual TLS = mTLS
     - Zertifikatsbasiert
     - Signatur von zuvor ausgetauschten Nachrichten

       Damit wird
       a) Besitz des zugehörigen SK bewiesen
       b) Authentisierung an den Kanal gebunden

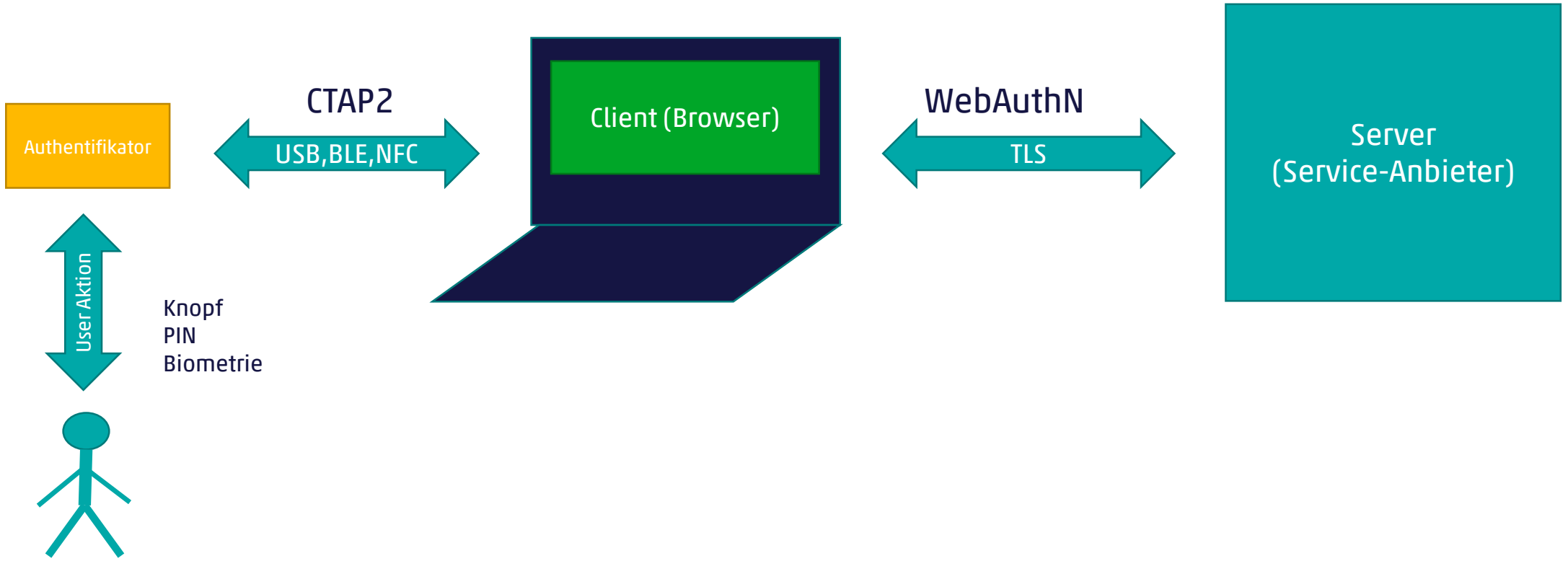
Verifier-Impersonation Resistenz



# Sicherheitsanalyse mTLS

| Resistenz gegen: | Passwort | ChallengeResponse | mTLS |
|---|---|---|---|
| **Verifier Compromise** | Nein | Ja / Nein | Ja |
| **Replay Attacken** | Nein | Ja | Ja |
| **Phishing** | Nein | Ja | Ja |
| **Real-Time Phishing (MitM)** | Nein | Nein | Ja |
| **Verifier Impersonation** | Nein | Nein | Ja |

# FIDO 2 – Passwortfreie Authentisierung



# FIDO 2

1. Registrierung beim Service-Anbieter
   - neues SK/PK Paar
   - PK -> Service-Anbieter
   - SK im Authentifikator gespeichert (*Haben*)
     - ev. PIN/Biometrie geschützt (*Wissen/Sein*)
     - gebunden an den Service-Anbieter

2. Login - Authentisierung
   - Challenge/Response Protokoll
   - Signatur von
     - Challenge
     - User Verification bit
     - Origin (URL)
     - Optional: TokenBindingID

Real-Time Phishing Resistenz

Verifier-Impersonation Resistenz

# Sicherheitsanalyse FIDO2

| Resistenz gegen: | Passwort | ChallengeResponse | FIDO2 | mTLS |
|---|---|---|---|---|
| **Verifier Compromise** | Nein | Ja / Nein | Ja | Ja |
| **Replay** | Nein | Ja | Ja | Ja |
| **Phishing** | Nein | Ja | Ja | Ja |
| **Real-Time Phishing (MitM)** | Nein | Nein | Ja | Ja |
| **Verifier Impersonation** | Nein | Nein | Nein / Ja | Ja |

Demo: Renè Vogt

# Authentisierung und Malware

- Authentisierung bietet keinen Schutz bei Malware
- Lösung
  - Transaktionsbestätigungen
  - Risikobasierte AuthN/AuthZ

    z.B. Gerät ohne Malwareschutz -> hohes Risiko -> eingeschränkter Zugriff/Funktionalität
- Registrierung von neuen Authentisierungs- und Autorisierungsmitteln
  - sicherheitsrelevante Operation
  - erfordert
    - Transaktionsbestätigung

    oder
    - Tiefen Risiko-Level

z.B. Conditional Access
- Trusted Location
- Joint/Compliant Device

Demo: Thomas Lüthi

# Sichere Authentisierung - Fazit

- Ausschlaggebend für sichere Zugriffskontrollen
- Sicherheitskriterien
  - Anzahl der Authentisierungsfaktoren
  - Resistenz gegen Angriffe
- Komplex
  - Gesamtkontext - Registrierung, Authentisierung, Recovery, ...
- Idealerweise zentralisiert
  - Identity Federation - SAML, OpenID Connect, Kerberos

# Vielen Dank für Ihre Aufmerksamkeit_

zuzana.trubini@cnlab.ch
+41 55 214 33 34

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

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

cnlab