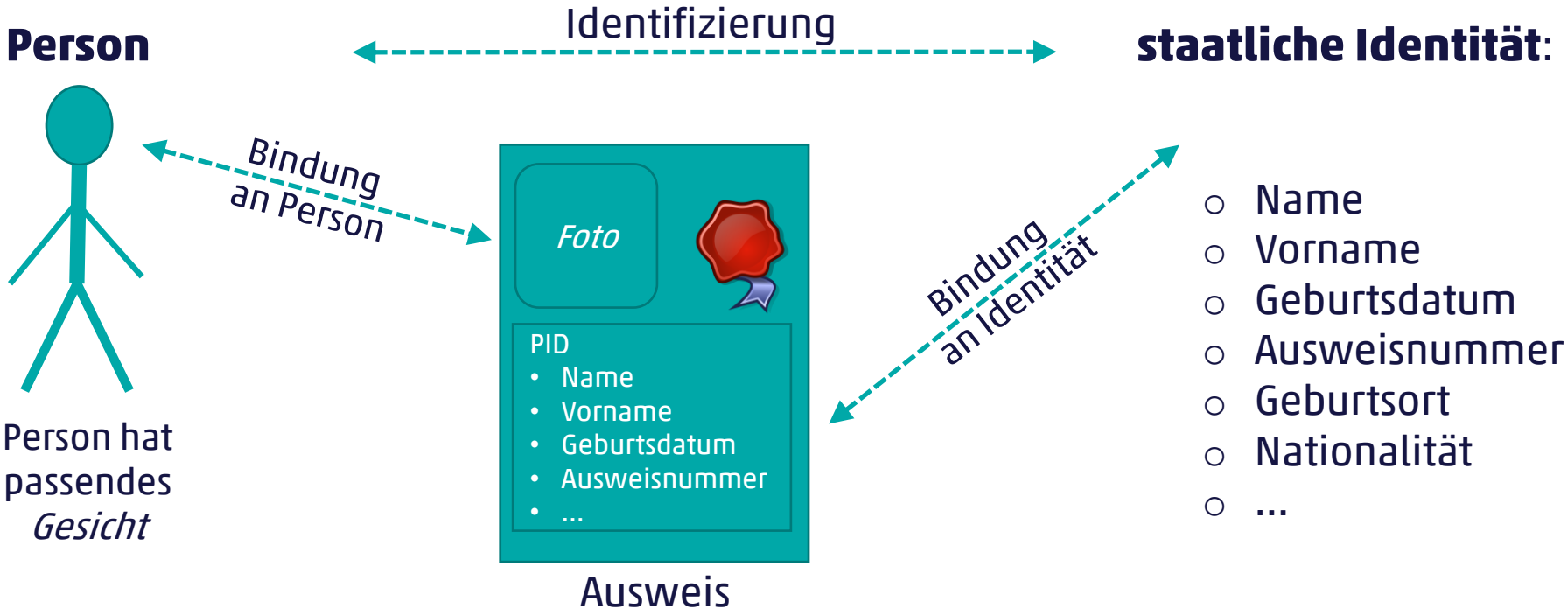
Herbsttagung 2021
Klassische Ausweise im Digitalen Raum

Zuzana Trubini
Zürich, 8. September 2021

cnlab

Identitätsprüfung mit klassischen Ausweisen

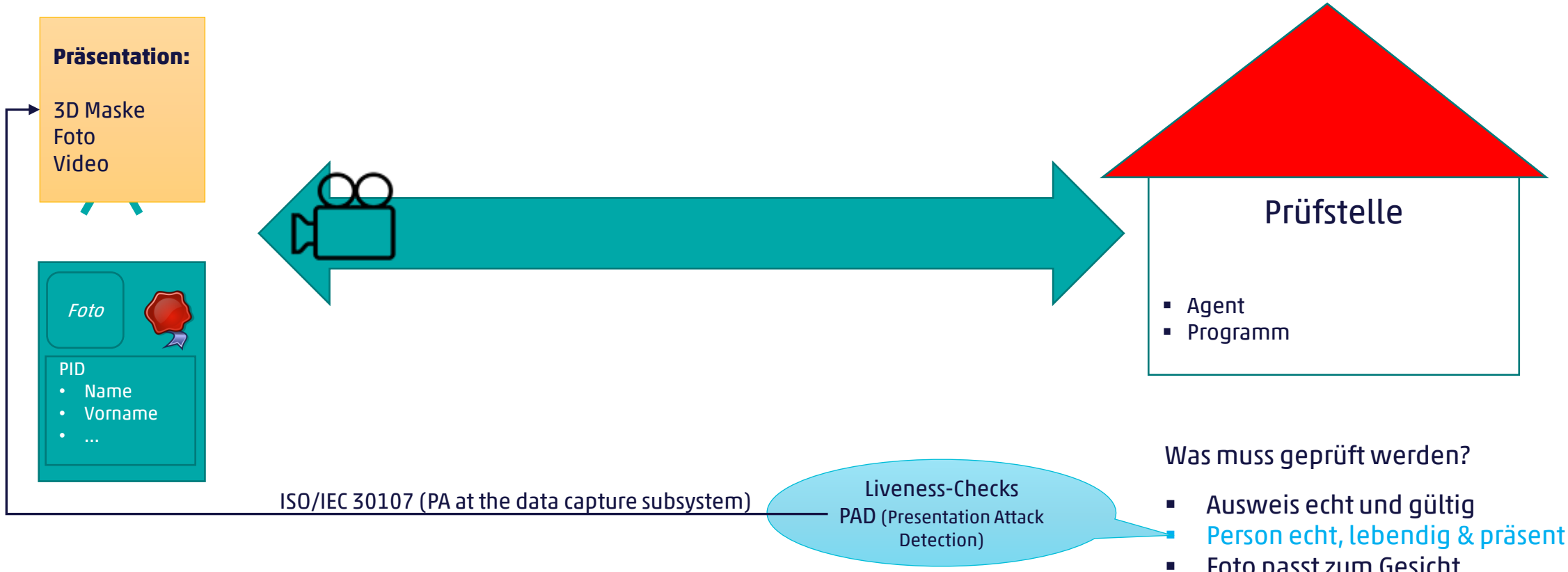


Angriffsvektoren
- Gefälschter, manipulierter Ausweis
- Impersonifizierung

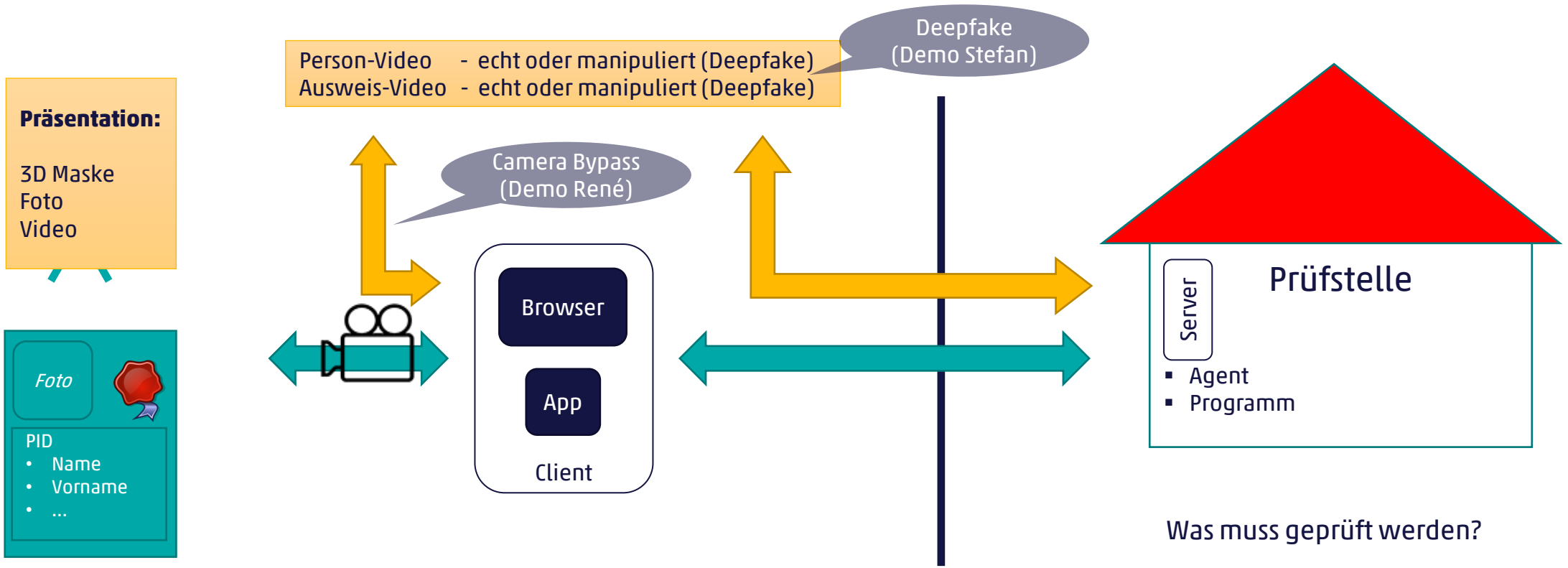
Was muss geprüft werden?
- Ausweis echt und gültig
- Foto passt zum Gesicht

Optische Prüfungen

Remote Identitätsprüfung mit klassischen Ausweisen



Remote Identitätsprüfung mit klassischen Ausweisen

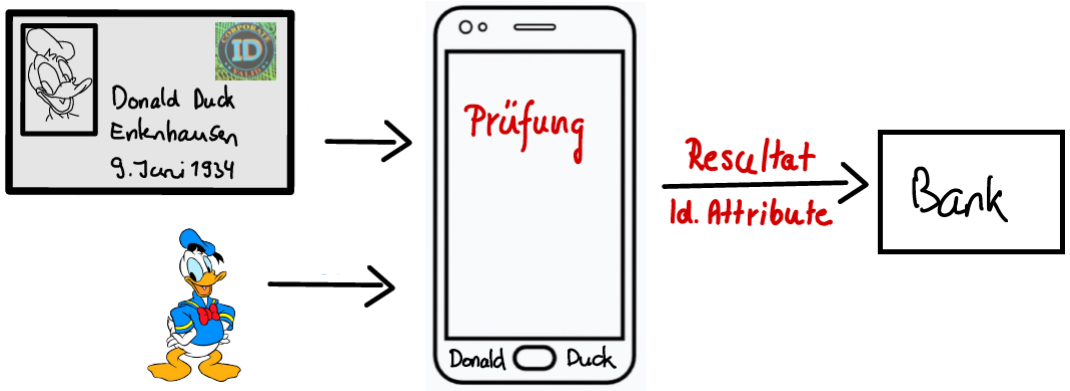


Was muss geprüft werden?

- Ausweis echt und gültig
- Person echt, lebendig & präsent
- Foto passt zum Gesicht

Remote Identitätsprüfung ohne Agent

Prüfungen Clientseitig



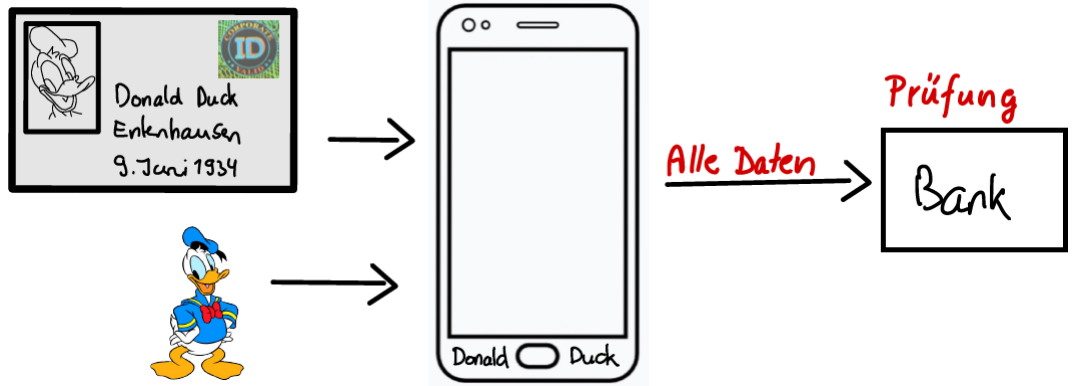
Angriff: Gegenüber der Bank die App vorspielen

Lösungsansatz: App-Authentisierung

Sicherste Lösung: Serverseitige Prüfung

App frisch aus dem App-Store
-> Schlüssel in der App versteckt
-> Sicherheit ungenügend

Prüfungen Serverseitig



Angriff: Camera-Bypass

Lösungsansatz: App-Härtung/App-Authentisierung

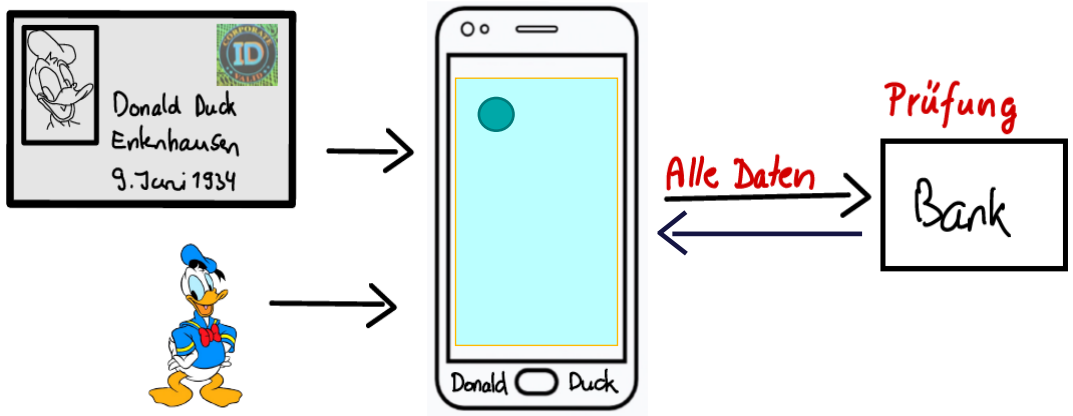
Sicherste Lösung: reaktive Liveness-Checks (Challenge/Response)

- Kopf- oder Gesichtsbewegungen
- Augenbewegungen (Pkt. verfolgen)
- Farb-Blitze (Reflektionen)

Sichere Remote Identitätsprüfung

Serverseitige Prüfung mit reaktiven Liveness-Checks (oder Agent)

Gleich sicher wie vor Ort?



Probleme:
- Deepfakes (Ausweis oder Person)
- Keine kontextspezifische Aktion
  - Fehlende User-Awareness
  - Fehlende Willensäusserung

Angriff:
- Deepfake (Ausweis oder Person)
- MitM – Physisch oder Virtuell

Sicherste Lösung:
- kontextspezifische Aktion & Willensäusserung
- Ausweis digital auslesen (& serverseitig prüfen)
- App-Authentisierung & -Härtung, Deepfake Erkennung

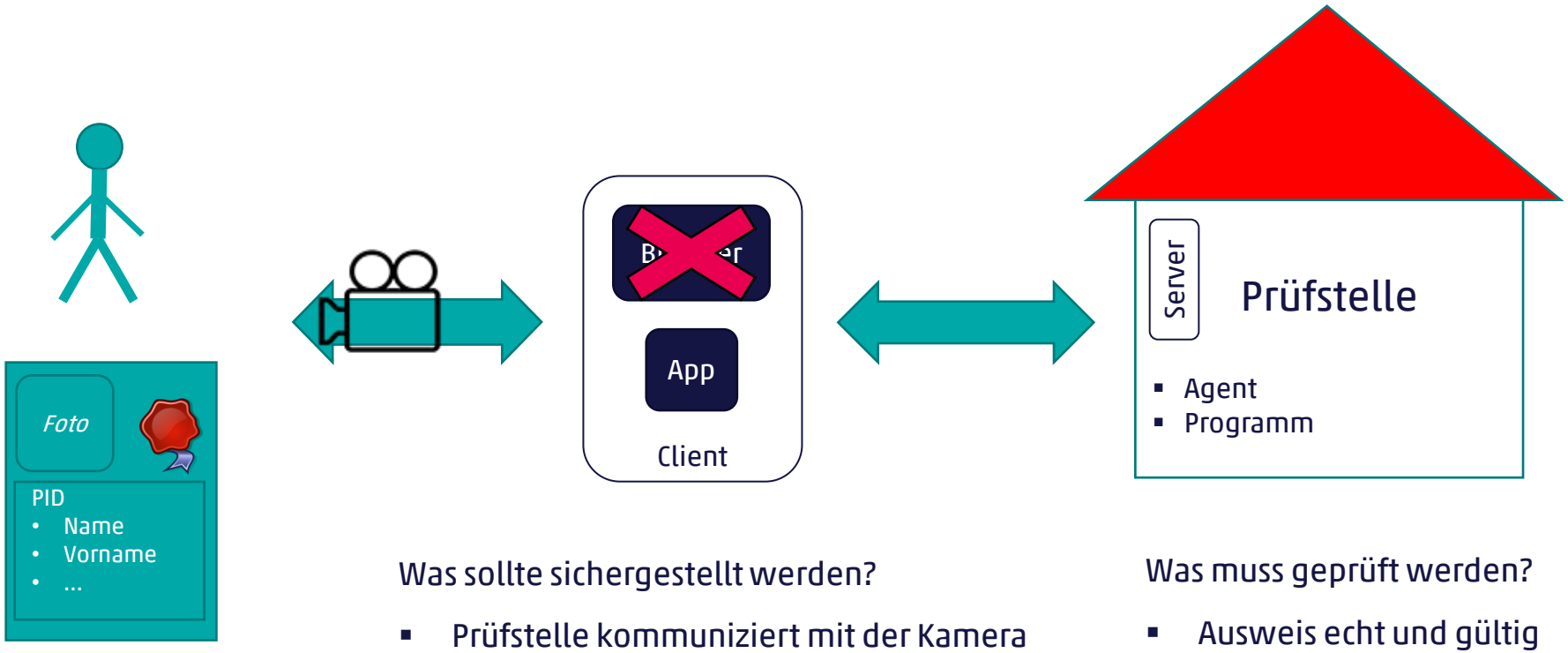
z.B. Prüfung der User-Awareness durch einen Agent

Reduziert MitM Angriffe

Verhindert Ausweisfälschung

Erhöht die Angriffskomplexität (Camera-Bypass & Deepfake)

Remote Identitätsprüfung mit klassischen Ausweisen



Was sollte sichergestellt werden?

- Prüfstelle kommuniziert mit der Kamera
  - i. Prüfstelle kommuniziert mit der richtigen App — App-Authentisierung
  - ii. App kommuniziert mit der Kamera — App-Härtung

Was muss geprüft werden?

- Ausweis echt und gültig
- Person echt, lebendig & präsent — Reaktive Liveness-Checks, PAD, Deepfake-Erkennung
- Foto passt zum Gesicht
- Person mit Aktion einverstanden — Kontext-Spezifische Aktion

Biometrischer Pass (ePass, MRTD, eMRTD)

Biometrischer Pass
(Demo Dominic)

Komponenten

«Papier-Pass» («Infokarte») – Optische Daten und Sicherheitselemente

- Identitätsdaten – Name, Geburtsdatum, Foto, Ausweisnummer, Unterschrift, …
- Sicherheitselemente – Hologramme, Wasserzeichen, UV-Elemente, …
- Machine Readable Zone - MRZ – Einige Identitätsdaten & Prüfziffer

Chip mit digitalen Daten - Auslesbar mit NFC – berührungslos und ohne Sichtkontakt

- Basis Daten – Identitätsdaten die auch optisch (auf Papier) vorliegen
- Sensible Daten – Fingerabdrücke
- Sicherheitsdaten – Schlüssel, Zertifikate, Signaturen, …

Biometrischer Pass – NFC Chip

Was will man erreichen?

- Sichere Kommunikation zw. Pass und Lesegerät
- Prüfstelle: Pass ist echt

Was heisst das?
- Daten unverändert – Datenauthentizität
- Kein Klon – Chipauthentizität

- Passinhaber: Nur berechtigte können Daten aus dem Chip auslesen

Wer ist berechtigt?
- Name, Geburtsdatum, Foto – Alle denen ich den Pass zeige/gebe
- Fingerabdrücke – Nur befugte Stellen (Zollbeamte, Polizei, …)

Biometrischer Pass – NFC Chip

Sicherheitsmechanismen (nach ICAO 9303)

- **Zugriffsschutz (Access Control)**
  - Schutz der «Basis Daten» - BAC - Basic Access Control (wird langsam abgelöst durch PACE)
  - Schutz der sensiblen Daten - EAC – Extended Access Control
- **Authentizität/Integrität**
  - Datenauthentizität – Daten unverändert
    - PA – Passive Authentication (Data Authentication)
  - Chipauthentizität - Schutz gegen Klonen
    - AA – Active Authentication (nicht in Schweizer Pässen)
    - CA – Chip Authentication
- **Sichere Kommunikation** – Schlüsselaustausch - BAC/PACE, CA

BAC & PACE

Auslesen der Daten

Abhören

Schutz vor Skimming und Eavesdropping

1. MRZ Lesen - Optisch
2. Chip-Auslesen - NFC
   i. Authentisierung & Schlüsselaustausch
   ii. ...
   iii. Secure Messaging

Idee – Wer die MRZ kennt, darf & kann die Basis-Daten auslesen

Verfahren – authentisierter Schlüssel-Austausch – basierend auf der MRZ

Wer die MRZ kennt (oder raten kann), kann den SessionKey berechnen (auch offline)

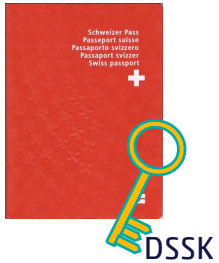
- BAC – Basic Access Control
  - MRZ -> Schlüssel -> Verschlüsselte(SessionKey-Komponenten, Challenge) -> SessionKey
  - symmetrische Kryptographie, veraltet, unsicher gegen offline Attacken
- PACE – Password Authenticated Connection Establishment
  - MRZ -> Passwort -> Generator für DH Key Exchange -> DH Key-Exchange
  - PW-Authentisierter DH Key-Exchange, keine offline Angriffe möglich

Sicher selbst wenn der Generator öffentlich bekannt

Passive Authentication (Data Authentication)

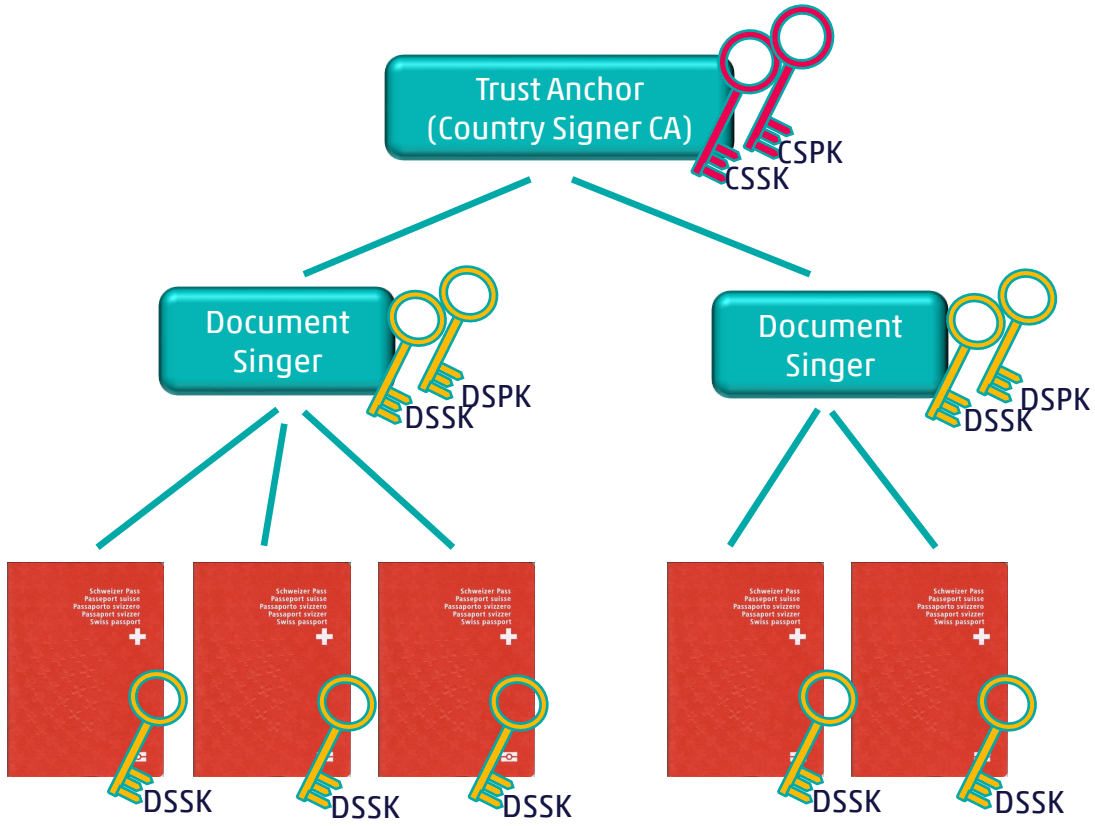
Authentizität/Integrität der Daten

- Alle Daten sind digital unterschrieben mit dem «Document-Signer-SK» der Ausstellungsbehörde



- Document-Signer-PK
  - im Chip gespeichert
  - mit «Country-Signer-SK» unterschrieben

- Country-Signer-PK kann und muss von vertraulichen Quellen bezogen werden



Active Authentication & Chip Authentication

Authentizität des Chips (Schutz gegen Klonen)

Idee – Beweis der Kenntnis des eigenen Secret-Keys

Verfahren (ICAO)

- Active Authentication
- Chip Authentication
  - DH mit einem statischem Schlüssel-Paar
    - Lesegerät wählt sein Schlüssel-Paar zufällig
    - Pass-Chip verwendet immer das gleiche Schlüssel-Paar
  - Ausgehandelter Schlüssel wird auch für Secure Messaging verwendet
    - bessere Sicherheit (falls vorher BAC und kein PACE)

- Challenge/Response Verfahren - Anfällig auf «Challenge Semantics»
- Im Schweizer Pass nicht implementiert

Chip-PK auslesbar & mit Document-Signer-SK unterschrieben

Chip-SK verlässt nie den Chip

Remote Identitätsprüfung mit biometrischen Ausweisen

Optisch

Optisch & NFC

App

Client

Server

Prüfstelle

- Agent
- Programm

Was muss geprüft werden?

- Ausweis echt und gültig
- Person echt, lebendig & präsent
- Foto passt zum Gesicht
- Person mit Aktion einverstanden

Hohe (kryptographische) Sicherheit – falls Prüfung serverseitig

unverändert

Bessere Sicherheit dank Foto in hoher Auflösung

unverändert

Klassische Ausweise im digitalen Raum gemäss ETSI TS 119 461 (2021-07)

Ziel – Basic Level of Assurance (für digitale Zertifikate, ...)

Anforderungen

- Alle Prüfungen – serverseitig
- Datenübertragung – authentisch, integer und vertraulich
- Echtheit des Ausweises – digital oder optisch anhand vom Video

Foto vom Ausweis nicht ausreichend

- Echtheit der Person – Liveness-Checks, PAD (ISO 30107-3); DeepFake-Erkennung (empfohlen)
- Bindung Ausweis <-> Person
  - falls ohne Agent und mit vollautomatischer Prüfung – nur mit digital auslesbarem Ausweis

Remote Identitätsprüfung mit Schweizer ID-Karte

1. mit Agent
   a) rein manuelle Prüfung möglich
   b) hybride Prüfung stark empfohlen
2. ohne Agent
   a) vollautomatische Prüfung nicht erlaubt
   b) hybride Prüfung nötig
      a) Echtheit vom Ausweis – automatisch
      b) Bindung an Person – manuell

Remote Identitätsprüfung mit Schweizer Pass

1. mit Agent
   a) rein manuelle Prüfung möglich
   b) hybride Prüfung stark empfohlen
2. ohne Agent
   a) vollautomatische Prüfung erlaubt falls digital ausgelesen
   b) sonst hybride Prüfung nötig

Fazit

- Remote Identification - viel Potenzial
- Mit Agent deutlich sicherer als ohne – falls Kontext-Awareness vom Agenten geprüft
- Stand Heute – Daten-Lesen meistens rein optisch
  - Liveness-Checks schlechte Usability/Sicherheit
  - Sicherheit gegen Kamera-Bypass oder MitM Angriffe – oft kein Thema

  - **ausreichend** – für Onboarding oder zur Erhöhung der Sicherheit von anderen Verfahren
  - **ungeeignet** – als alleiniges Sicherheitselement - z.B. fürs Login oder Credential Recovery (da kein kontext-spezifisches Geheimnis/Aktion verlangt)

Vielen Dank für Ihre Aufmerksamkeit_

Zuzana Trubini
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