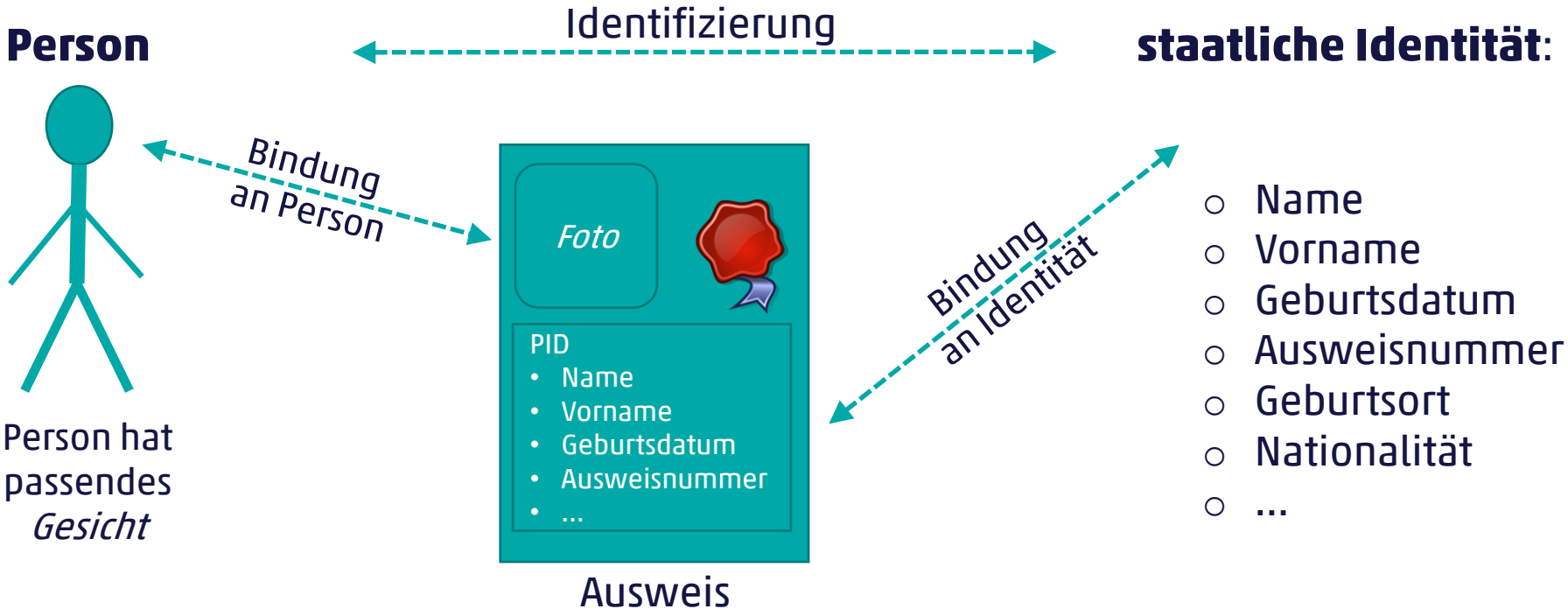
Klassische Ausweise im Digitalen Raum

Zuzana Trubini

29. November 2022
STAIR Talks HS2022, Hochschule Luzern

cnlab

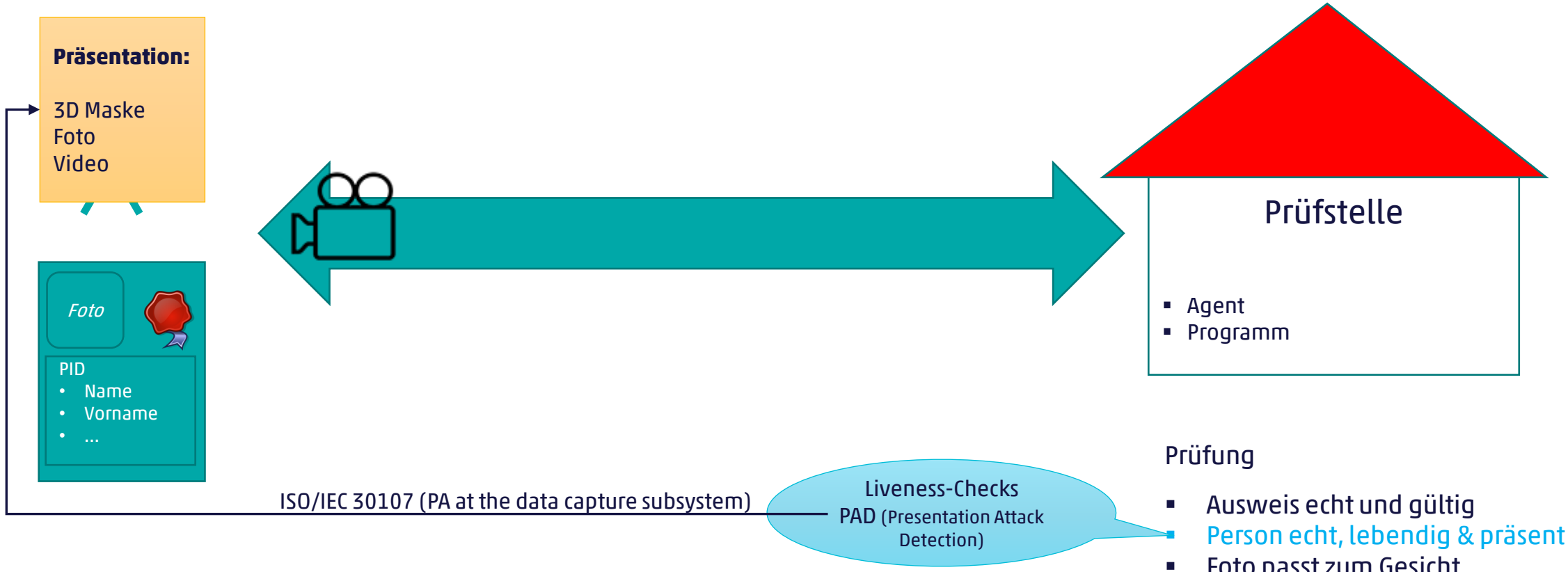
Identitätsprüfung mit klassischen Ausweisen



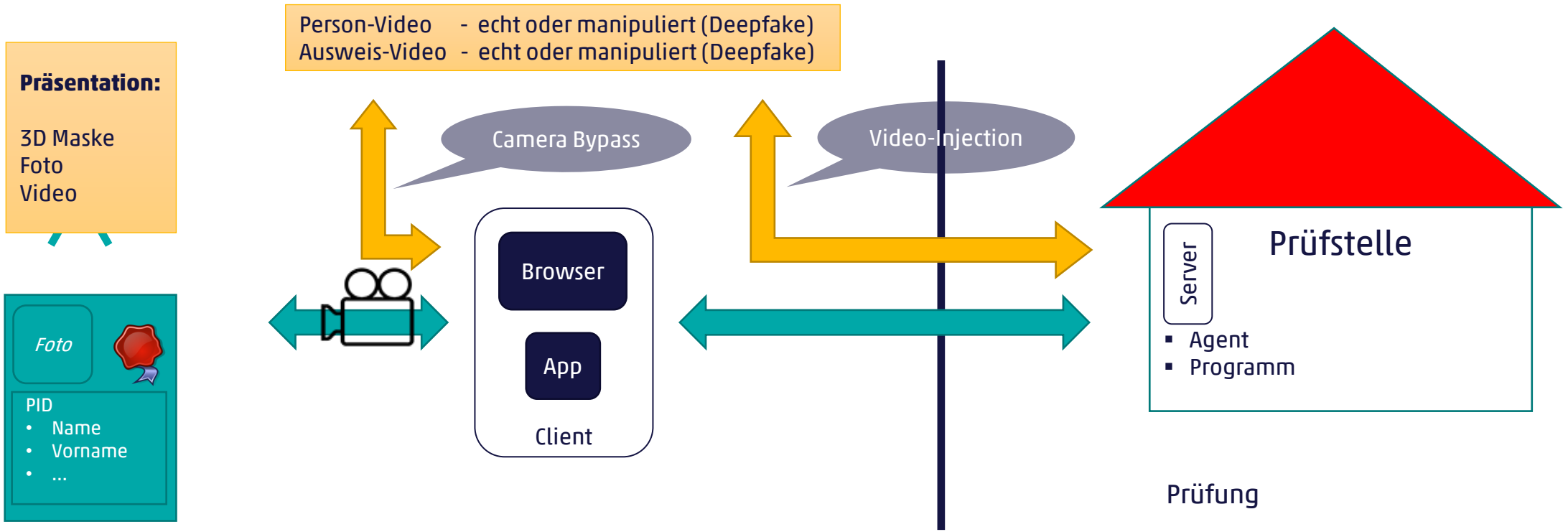
Prüfung
- Ausweis echt und gültig
- Foto passt zum Gesicht

Optische Prüfungen

Remote Identitätsprüfung mit klassischen Ausweisen



Remote Identitätsprüfung mit klassischen Ausweisen

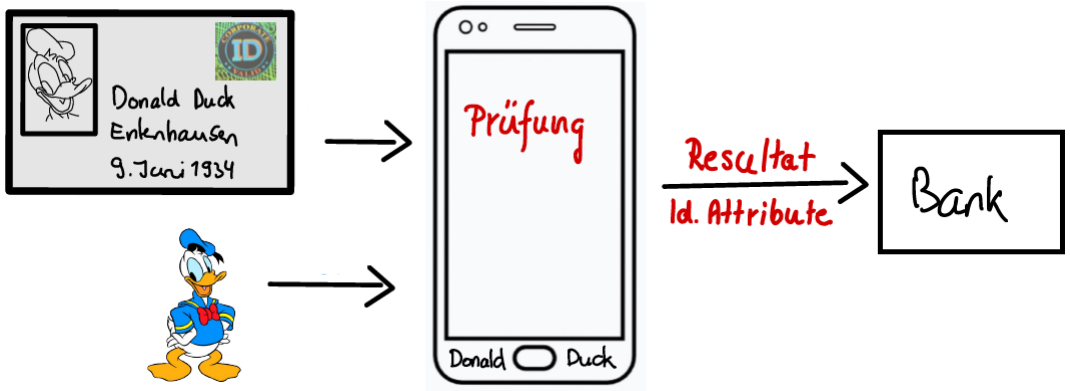


Prüfung

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

Remote Identitätsprüfung ohne Agent

Prüfungen Clientseitig



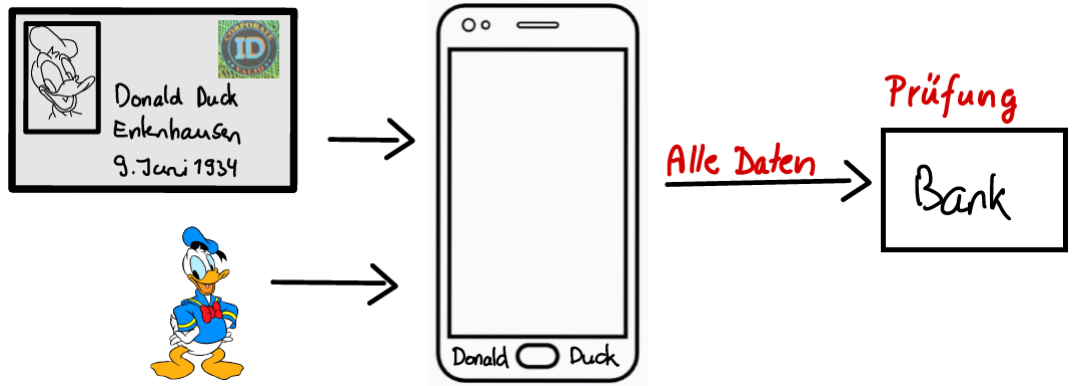
Angriff: Gegenüber der Bank die App vorspielen

Lösungsansatz: App-Authentisierung

Sicherste Lösung: Serverseitige Prüfung

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

Prüfungen Serverseitig



Angriff: Vorbereitetes Video & Camera-Bypass

Lösungsansatz: App-Härtung/App-Authentisierung

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

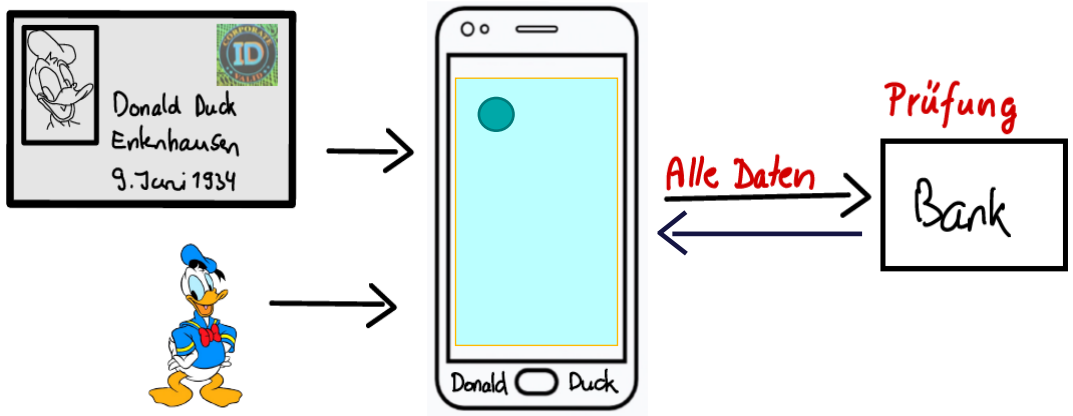
- Kopf- oder Gesichtsbewegungen
- Augenbewegungen (Pkt. verfolgen)

Sichere Remote Identitätsprüfung

Serverseitige Prüfung mit reaktiven Liveness-Checks (oder Agent)

Gleich sicher wie vor Ort?

Probleme:
- Deepfakes (Ausweis oder Person)
- Keine kontextspezifische Aktion



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

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

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

Reduziert MitM Angriffe

Erhöht die Angriffskomplexität (Video-Injection, Camera-Bypass & Deepfake)

Verhindert Ausweisfälschung

Biometrischer Pass (ePass, MRTD, eMRTD)

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
- Keine Kopie – 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 – Echter Chip im Einsatz
    - 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

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

Verfahren – authentisierter Schlüssel-Austausch – basierend auf der MRZ

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

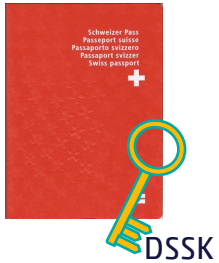
- BAC – Basic Access Control
  - MRZ -> Schlüssel -> Verschlüsselte(SessionKey-Komponenten) -> SessionKey
  - symmetrische Kryptographie, veraltet, unsicher gegen offline Attacken
- PACE – Password Authenticated Connection Establishment
  - MRZ -> Passwort -> Generator für DH Key Exchange -> DH Key-Exchange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

Sicher selbst wenn der Generator öffentlich bekannt

Passive Authentication (Data Authentication)

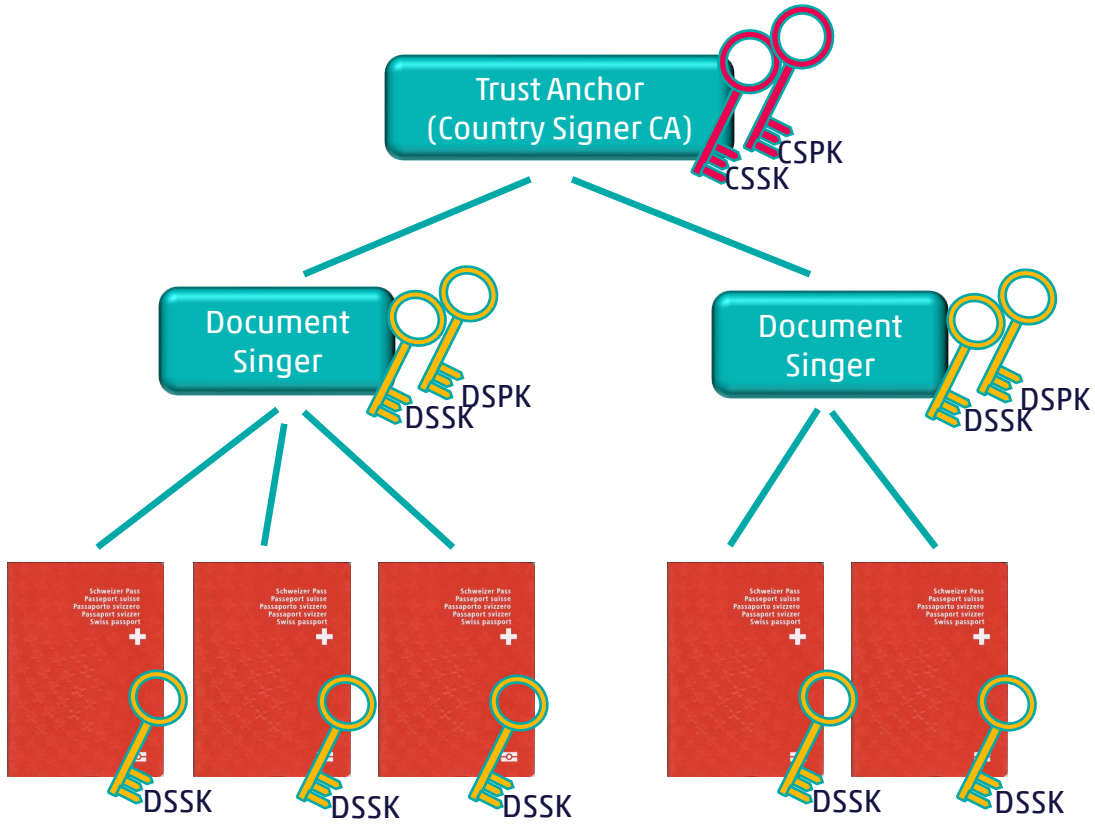
Authentizität/Integrität der Daten

- 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 Replay & 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

Browser

App

Client

Server

Prüfstelle

- Agent
- Programm

Prüfung

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

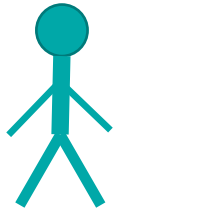
Hohe (kryptographische) Sicherheit

unverändert

Bessere Sicherheit dank Foto in hoher Auflösung

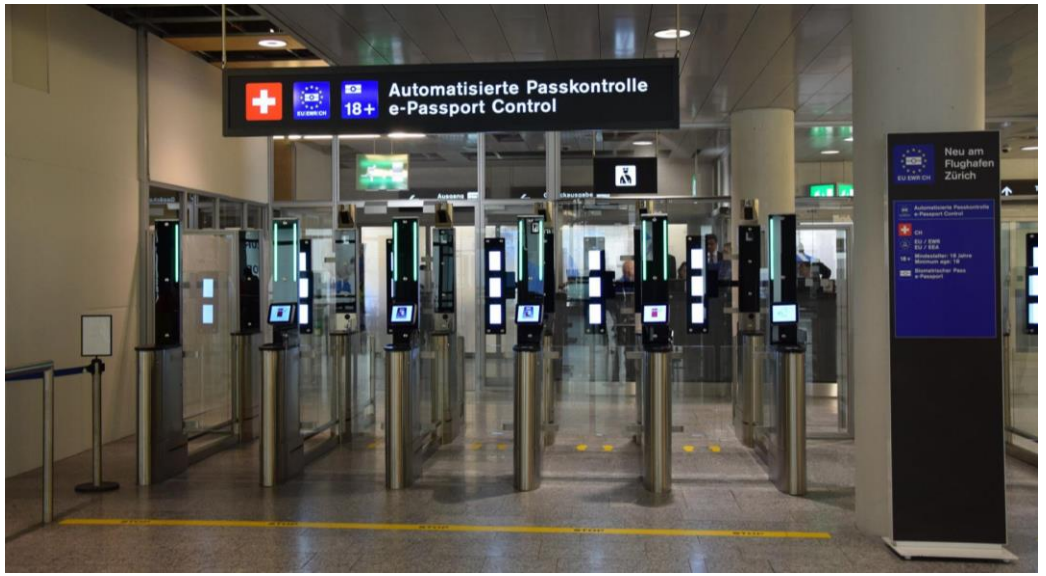
unverändert

Identitätsprüfung mit Biometrischen Ausweisen



Optisch

Optisch & NFC



- Konzipiert für **automatisierte Identitätsprüfung vor Ort** und nicht für den digitalen Raum
- Kein Elektronischer Ausweis -> es braucht eine eID

Hohe (kryptographische) Sicherheit

Prüfung

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

Bessere Sicherheit dank Foto in hoher Auflösung

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