JOHANNES KEPLER UNIVERSITY LINZ

Aktuelle Entwicklungen zu Digitalen Identitäten

DIGiDOW

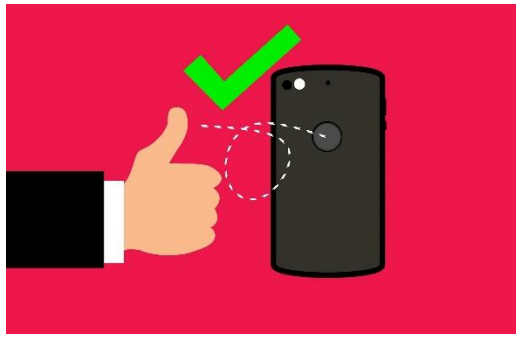
INSTITUTE OF NETWORKS AND SECURITY

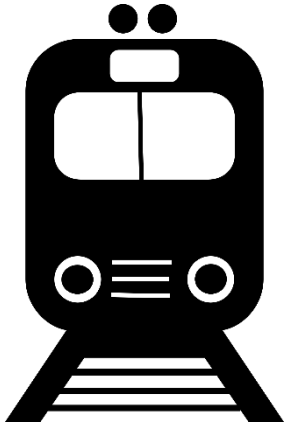
Keynote eEducation Praxistage, 2020-11-13 09:10-10:00 (UTC+1), virtuell

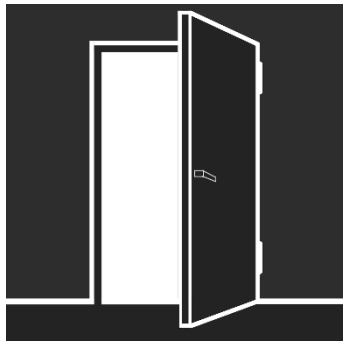
Univ.-Prof. Dr. **René Mayrhofer**
Institut für Netzwerke und Sicherheit und LIT Secure and Correct Systems Lab, JKU Linz

JOHANNES KEPLER UNIVERSITY LINZ
Altenberger Straße 69
4040 Linz, Austria
jku.at

Digitale Identitäten







Digitale Identitäten: Aktuelle Praxis

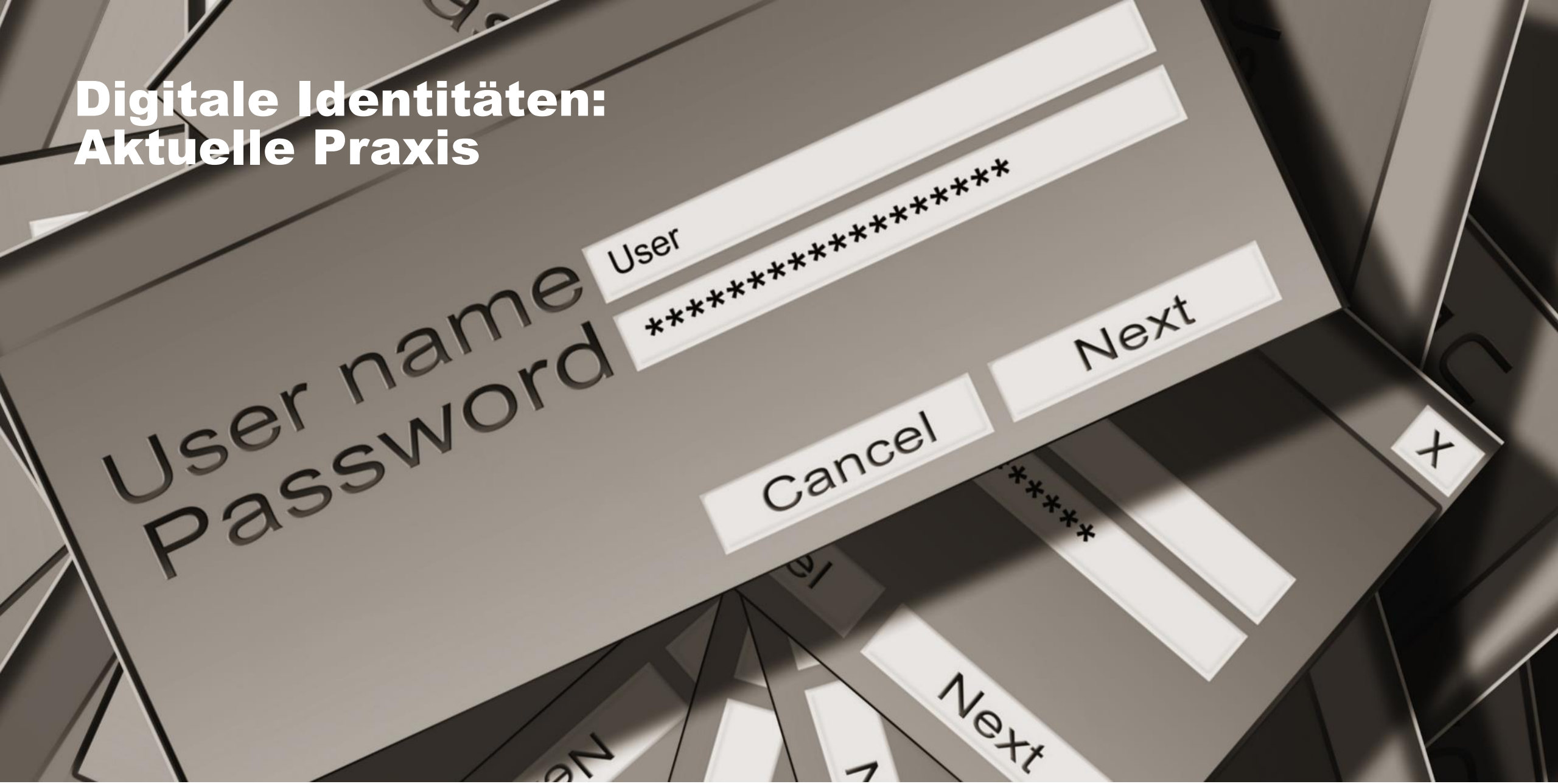


Image credit: https://pixabay.com/illustrations/password-keyword-codeword-solution-397652/

Digitale Identitäten: Authentifizierung im Wandel

Akademische Forschung

- Attribute/identity based cryptography (A/IBC), Attribute based access control (ABAC), Zero knowledge (ZK) proofs, etc.
- D. Chaum: “Security without Identification”, Comm. of the ACM, **October 1985**


Who
am
I?

Digitale Identitäten: Authentifizierung im Wandel

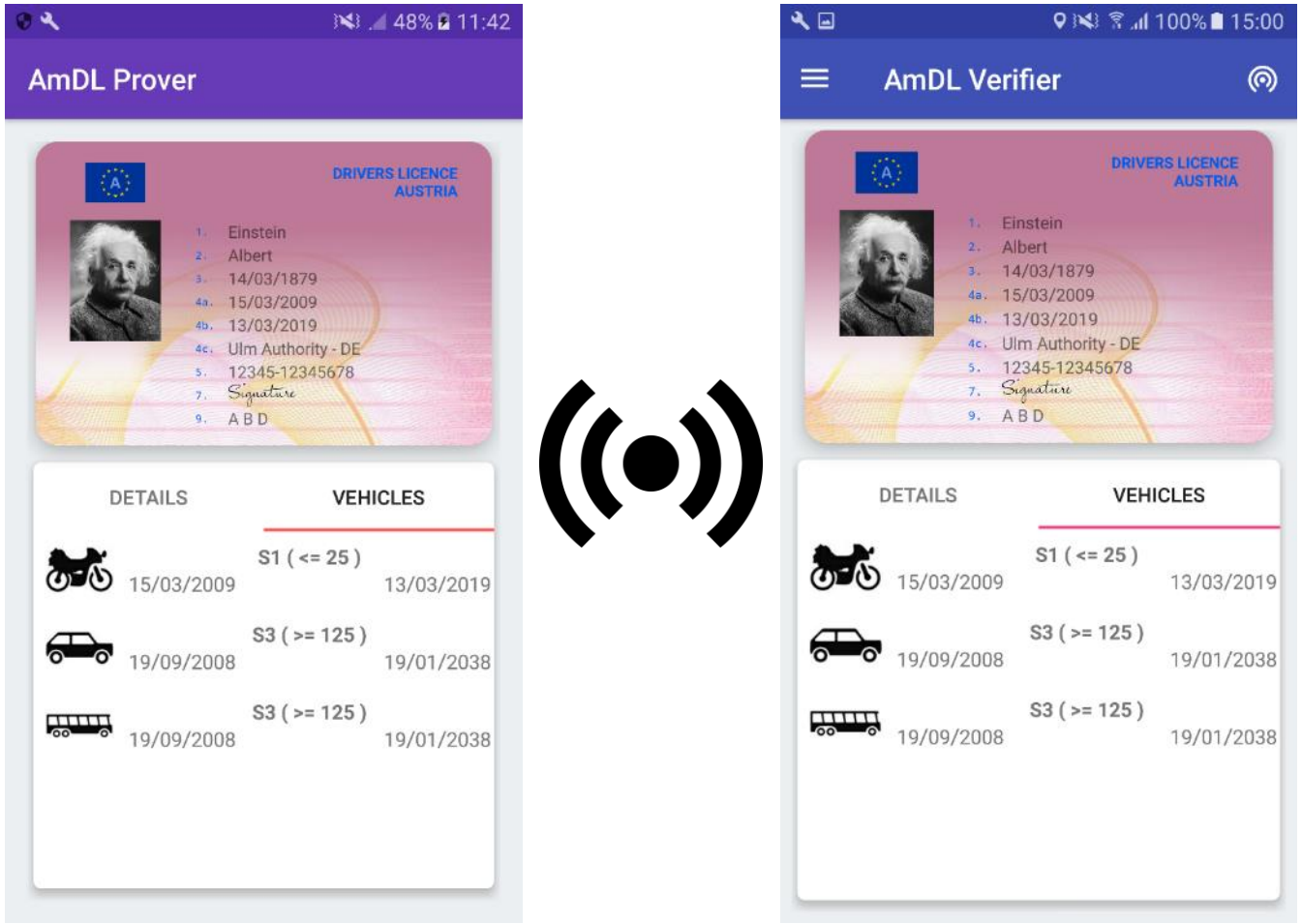
Akademische Forschung

- Attribute/identity based cryptography (A/IBC), Attribute based access control (ABAC), Zero knowledge (ZK) proofs, etc.
- D. Chaum: “Security without Identification”, Comm. of the ACM, **October 1985**

Öffentliche Standards

- ISO 18013-5 mobile driving license
- ISO 23220 digital identity
- EU: eIDAS
- Indien: Aadhaar
  China: Social Score

Digitale Identitäten: Beispiel Mobile Driving License – Verkehrskontrolle

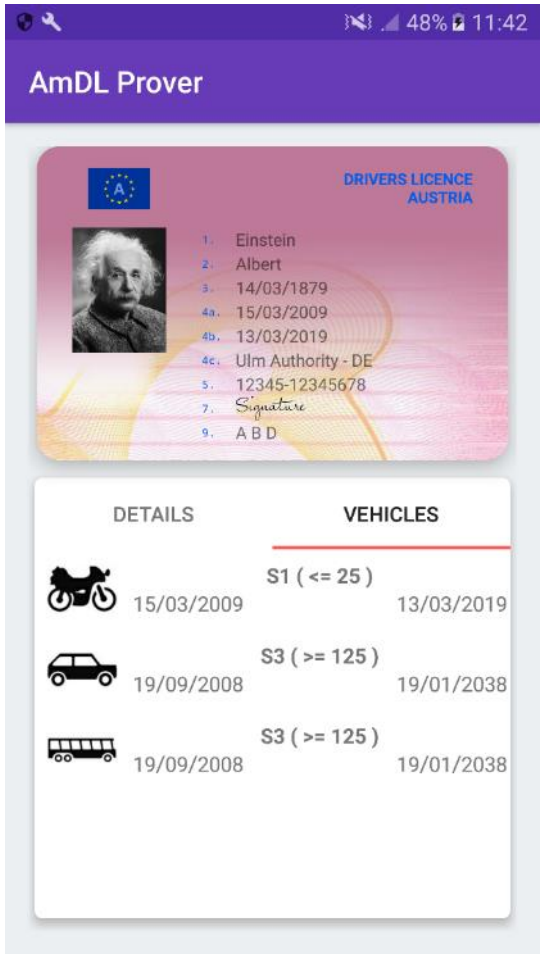


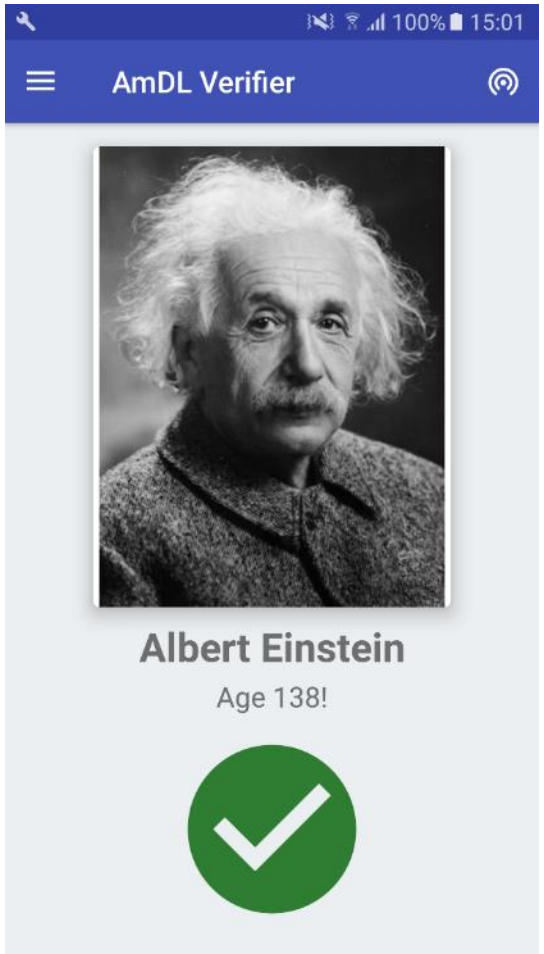
Alle Attribute übertragen

- Name
- Geburtsdatum
- Gesichtsbild in voller Auflösung
- (optional) Wohnort
- (optional) biometrische Merkmale
- Fahrzeugklassen, Einschränkungen

Soll auch offline funktionieren!

Digitale Identitäten:
Beispiel Mobile Driving License – Altersnachweis

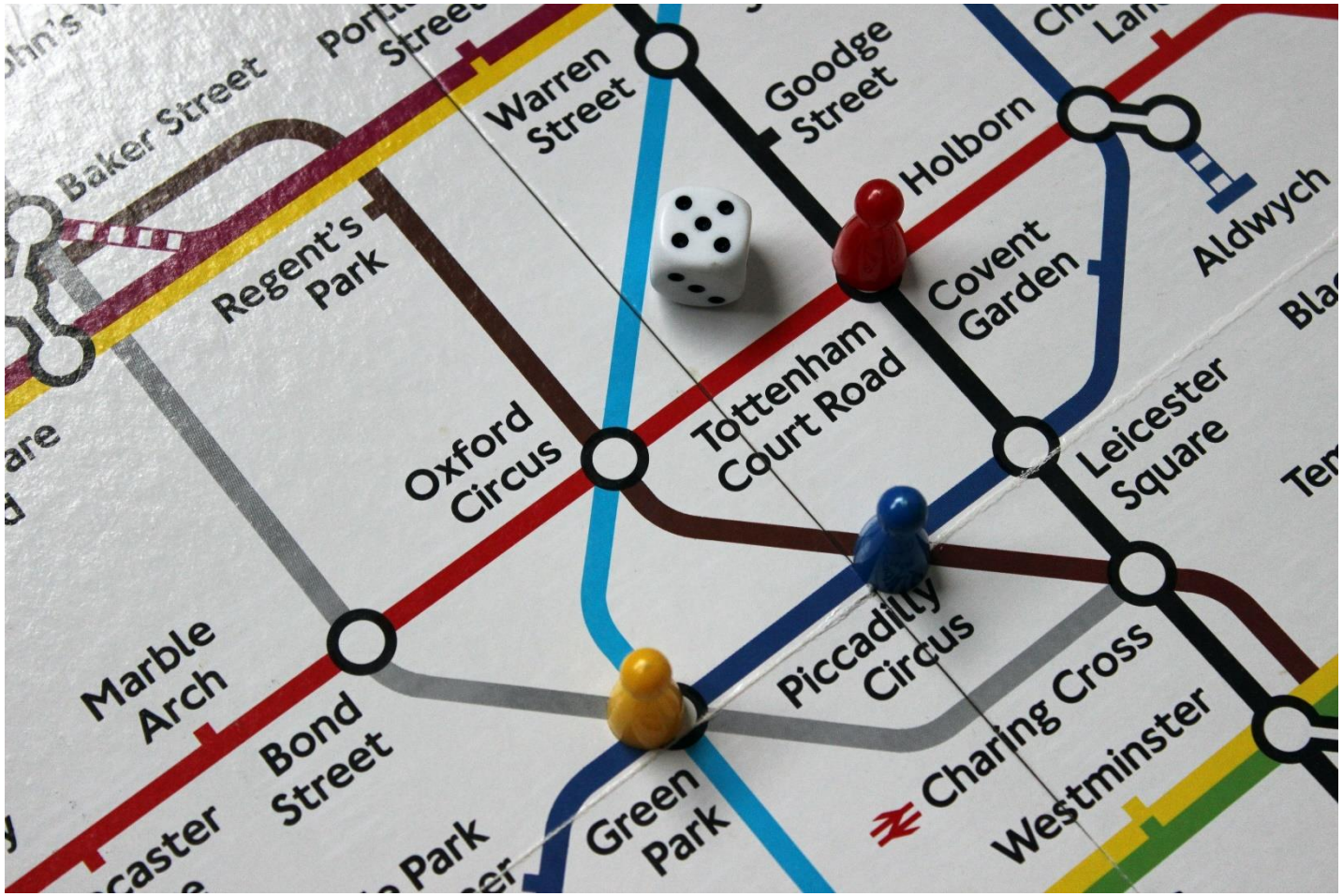




Nur notwendige Attribute

- Gesichtsbild
- Alter

Digitale Identitäten: Beispiel Contact Tracing



Bewegungsprofile sind hochsensible Daten

- Wohnort, Arbeitsort
- Religionszugehörigkeit
- Krankheiten
- Hobbies, besondere Vorlieben

Nur notwendige Attribute

- Kontakt mit Person X für mehr als Y Minuten pro Tag Z

Image credit: https://pixabay.com/photos/underground-tube-map-stations-2725336/

Digitale Identitäten: Authentifizierung im Wandel

Akademische Forschung

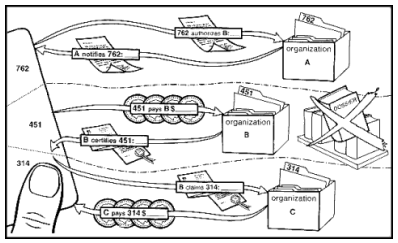
- Attribute/identity based cryptography (A/IBC), Attribute based access control (ABAC), Zero knowledge (ZK) proofs, etc.
- D. Chaum: “Security without Identification”, Comm. of the ACM, **October 1985**

Öffentliche Standards

- ISO 18013-5 mobile driving license
- ISO 23220 digital identity
- EU: eIDAS
- Indien: Aadhaar
  China: Social Score

Industriepraxis

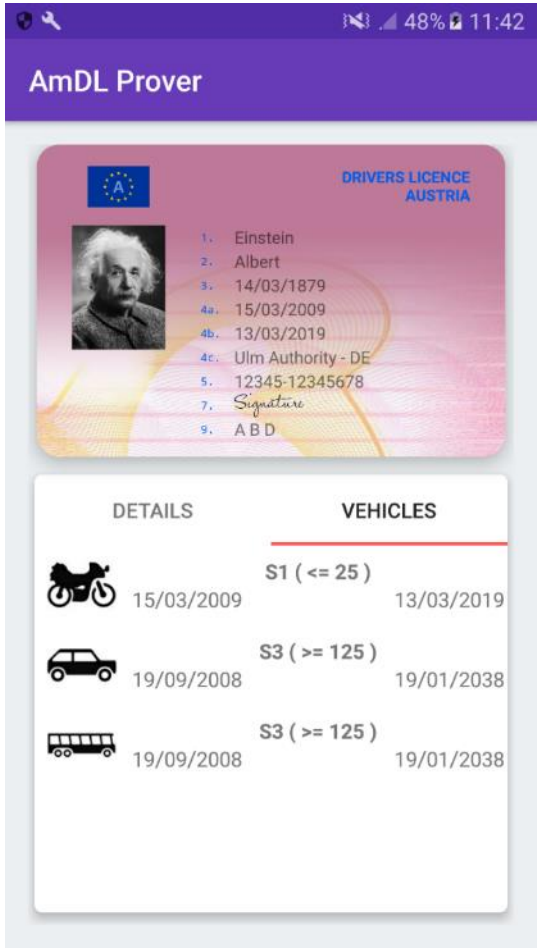
- Passwortrichtlinien
- Facebook/Google/etc. Login
- SMS Verifikation
- OAuth(2), OATH (TOTP/HOTP), OpenID, uvam.



2019

FIDO2/WebAuthn

Digitale Identitäten: Mobile Driving License



2020

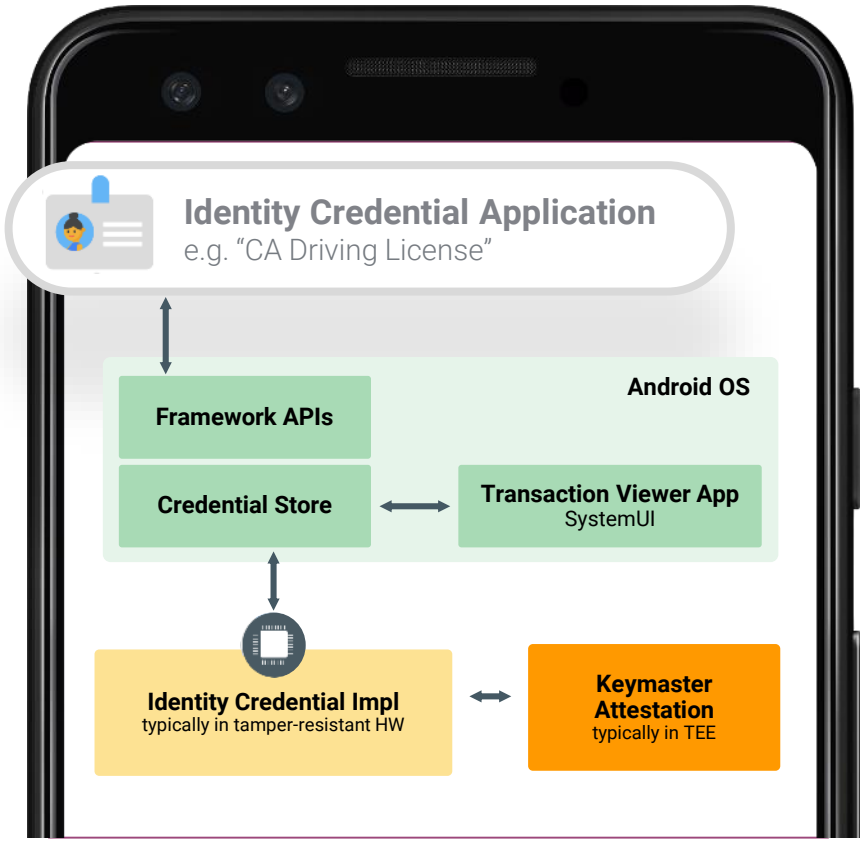
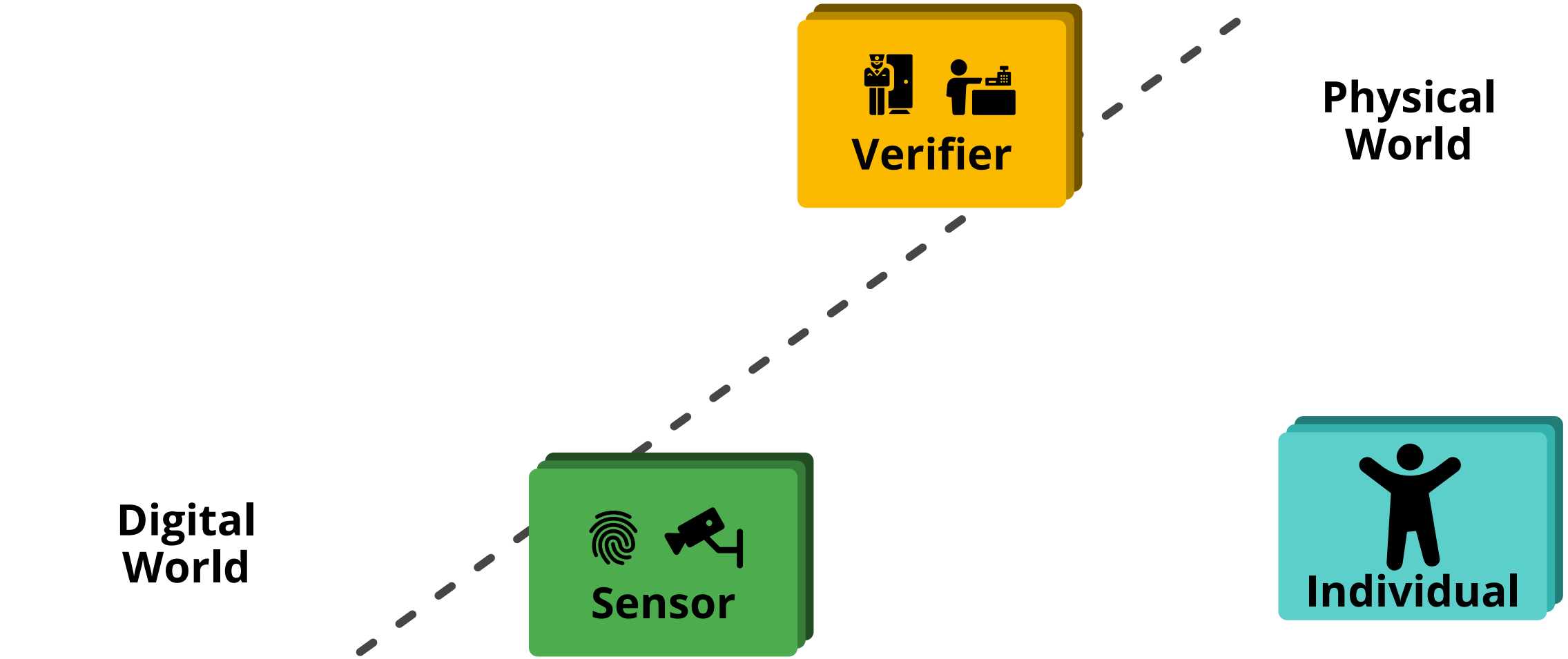
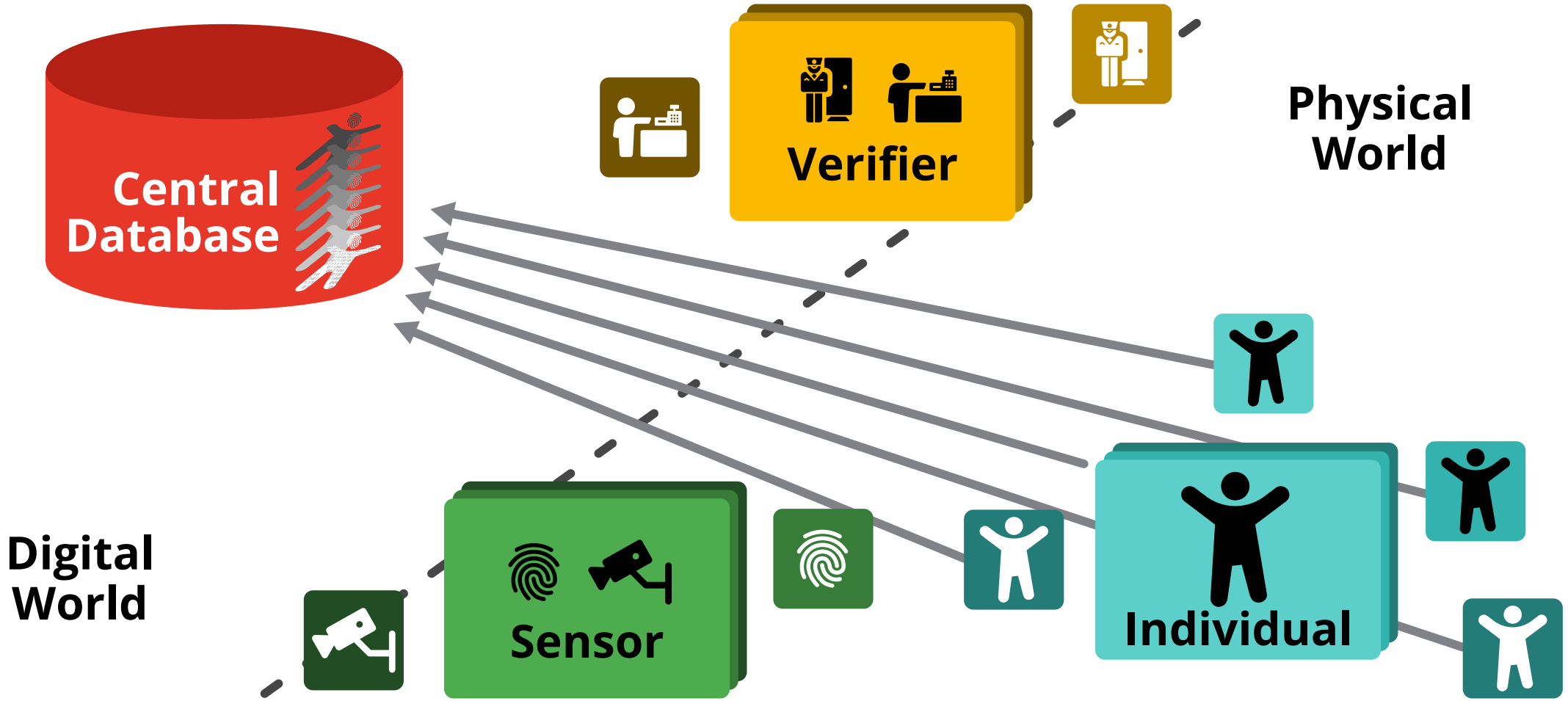


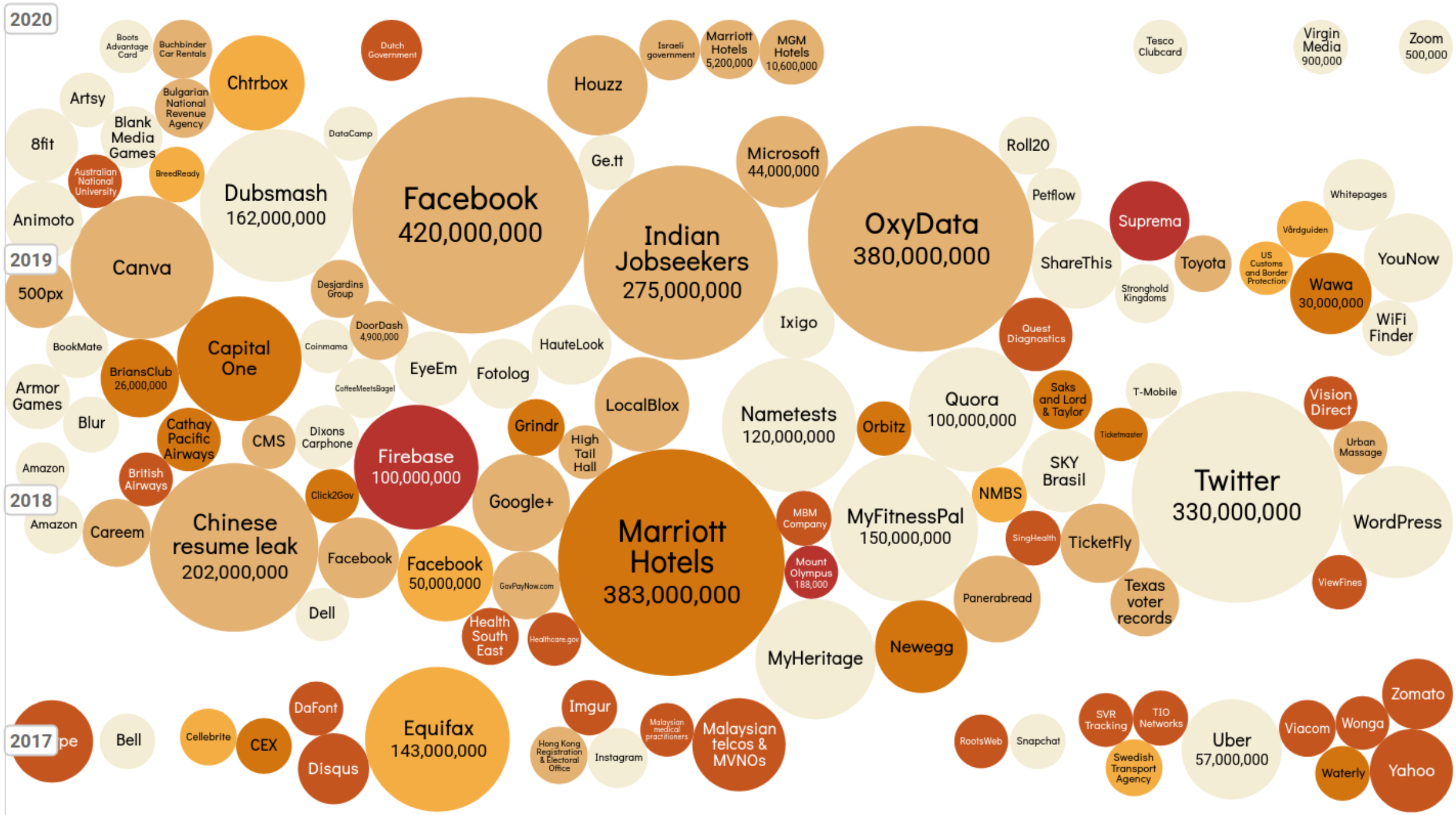
Image credit: Google

Digitale Authentifizierung – Vision

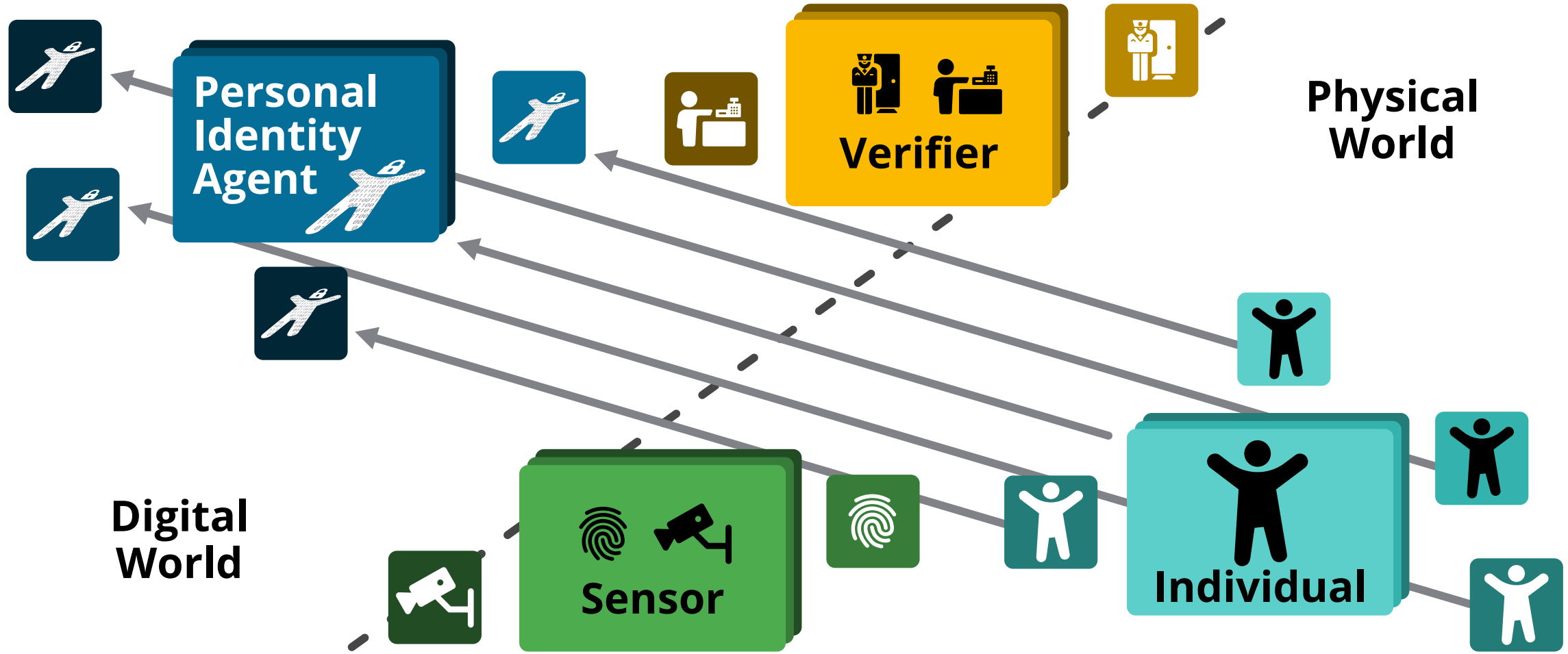


Digitale Identitäten – zentralisierter Ansatz




2020
2019
2018
2017
Boots Advantage Card
Buchbinder Car Rentals
Chtrbox
Dutch Government
Houzz
Israeli government
Marriott Hotels 5,200,000
MGM Hotels 10,600,000
Tesco Clubcard
Virgin Media 900,000
Zoom 500,000
Artsy
Bulgarian National Revenue Agency
Blank Media Games
8fit
DataCamp
Australian National University
BreedReady
Dubsmash 162,000,000
Facebook 420,000,000
Ge.tt
Microsoft 44,000,000
Indian Jobseekers 275,000,000
OxyData 380,000,000
Roll20
Petflow
Animoto
Canva
Desjardins Group
DoorDash 4,900,000
Coinmama
Ixigo
Suprema
ShareThis
Toyota
Stronghold Kingdoms
Whitepages
Vårdguiden
US Customs and Border Protection
Wawa 30,000,000
YouNow
WiFi Finder
500px
BookMate
Capital One
HauteLook
Quest Diagnostics
BriansClub 26,000,000
CoffeeMeetsBagel
EyeEm
Fotolog
LocalBlox
Armor Games
Blur
Cathay Pacific Airways
CMS
Dixons Carphone
Grindr
High Tail Hall
Nametests 120,000,000
Orbitz
Quora 100,000,000
Saks and Lord & Taylor
T-Mobile
Ticketmaster
Vision Direct
Urban Massage
Amazon
British Airways
Firebase 100,000,000
Click2Gov
Google+
SKY Brasil
NMBS
Twitter 330,000,000
WordPress
Amazon
Careem
Chinese resume leak 202,000,000
Facebook
Facebook 50,000,000
GovPayNow.com
Marriott Hotels 383,000,000
MBM Company
Mount Olympus 188,000
MyFitnessPal 150,000,000
SingHealth
TicketFly
Dell
Health South East
Healthcare.gov
Panerabread
Texas voter records
ViewFines
MyHeritage
Newegg
Bell
Cellebrite
CEX
DaFont
Disqus
Equifax 143,000,000
Imgur
Hong Kong Registration & Electoral Office
Instagram
Malaysian medical practitioners
Malaysian telcos & MVNOs
RootsWeb
Snapchat
SVR Tracking
TIO Networks
Swedish Transport Agency
Uber 57,000,000
Viacom
Wonga
Zomato
Waterly
Yahoo

Digitale Identitäten – dezentraler Ansatz



Konkrete Herausforderungen: Authentifizierung entfernter Benutzer*innen

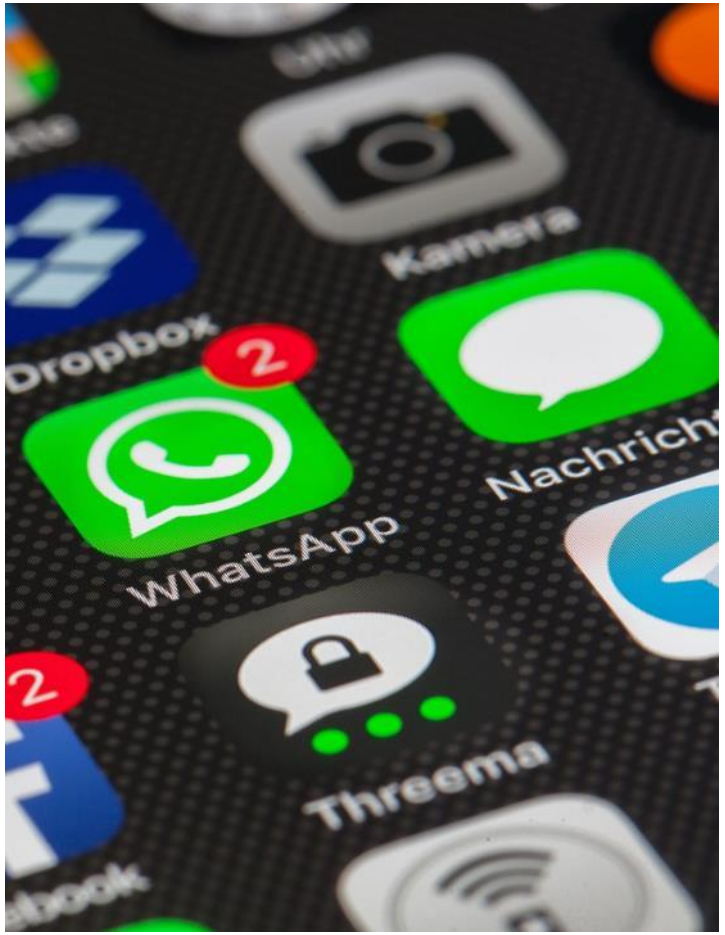
Wichtige **Fragen für eine Auswahl** von Lösungen:

- Wie viele verschiedene Services werden verwendet?
- Von welchen Endgeräten wird angemeldet?
- Gibt es gemeinsame Schnittstellen (USB, NFC, Kamera)?

Empfehlungen aus der Praxis:

- **Passwortmanager mit Client-Integration verwenden!**
- Passwörter alleine sind zu wenig (unabhängig von Komplexität ist Phishing das Hauptproblem) → **2FA**
  - ideal: **FIDO2** / U2F (per USB, NFC oder eingebettet)
  - gut: TOTP
  - in Ordnung: HOTP
  - nur wenn nicht anders möglich: SMS
- Wenn möglich, biometrische Authentifizierung (Fingerprint)

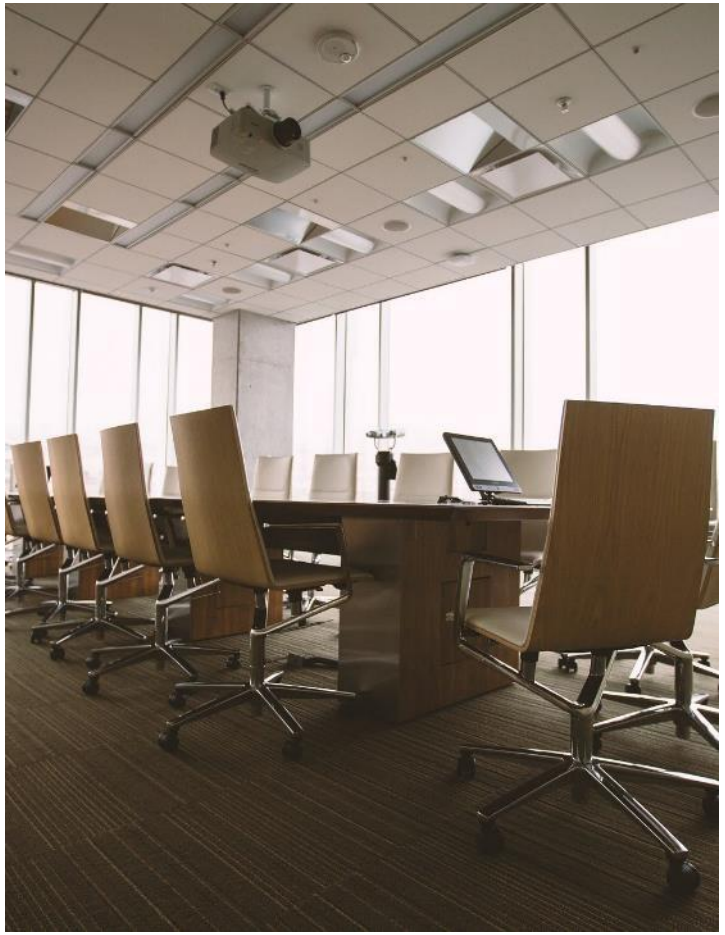
Konkrete Herausforderungen: Chat / Audio / Video / … am Smartphone



Wichtige **Fragen für eine Auswahl** von Lösungen:

- Was ist die **Benutzeridentität**? ~~Telefonnummer~~, Email, eigene Accounts? Integriert diese in den Betrieb? Kann ein beruflicher Account von dem privaten getrennt werden?
- Echte **Ende-zu-Ende Verschlüsselung**? Auch von Gruppen-Kommunikation (inkl. live Audio/Video)?
  - Möglichkeit zu automatischem Ablauf von Nachrichten?
- Wo fallen **Meta-Daten** an? Wie werden diese technisch gesichert?
  - Besonders problematisch: Übermittlung von Daten aus Telefonbuch an Server mit unklarer Rechtssituation
- Welche technische, organisatorische und rechtliche Zugriffsmöglichkeit gibt es beim Provider (unverschlüsselte Inhalte sowie Meta-Daten)?

Konkrete Herausforderungen: Videokonferenzen



Wichtige **Fragen für eine Auswahl** von Lösungen:

- Verfügbarkeit
  - Inkl. Bandbreitenbedarf für Teilnehmer*innen mit schlechter Internet-Anbindung
  - Inkl. Unterstützung aller Plattformen (nicht nur Windows)
    → browserbasierte Zugänge in der Praxis einfacher
- Sicherheit
  - **Lokale Client-Software als mögliche Sicherheitslücke**
  - **Verschlüsselung der Inhalte** (Transport vs. E2E)
  - **Meta-Daten** (besonders wichtig: werden u.U. persönliche, geschützte Lebensumstände mit erfasst?)
- Benutzbarkeit
  - Alle notwendigen Features (z.B. Moderation, Screenshare, gemeinsames Whiteboard etc.)?

Konkrete Herausforderungen: Vertrauliche Übermittlung von Daten

Wichtige **Fragen für eine Auswahl** von Lösungen:

- Eingeschränkter oder offener Empfängerkreis (z.B. Datenaustausch mit immer selben Personen mit Account oder Information an beliebige Adressen)?
- Endgeräte zur Entschlüsselung (oder muss es z.B. allgemein im Browser oder mit allen Email-Clients funktionieren)?

Bekannte **Schwierigkeiten** aus der Praxis:

- (Open)PGP funktioniert nur in geschlossenen Gruppen
- ZIP / PDF - “Verschlüsselung“ hängt stark am Passwort (wie komplex, wie oft geändert, wie übermittelt?)
- Download per HTTPS hängt an guter Authentifizierung…

Kein gutes Standard-Verfahren, das alle Anforderungen löst

Konkrete Herausforderungen: Digitale Unterschriften

Wichtige **Fragen für eine Auswahl** von Lösungen:

- Rechtsgültige (qualifizierte) Signatur notwendig? → **eIDAS**
- Von welchen Endgeräten wird signiert?
- Von welchen Endgeräten wird die Signatur geprüft?
- Muss die Signatur nur einmal beim Empfänger geprüft werden oder langzeitig archiviert und prüfbar bleiben?

Empfehlungen aus der Praxis:

- Digitale PDF-Signatur mit qualifiziertem Key (per 2FA)
- Web-Services zur Signaturerstellung nicht unbedingt interoperabel

Konkrete Herausforderungen: Vendor Lock-In

JOHANNES KEPLER
UNIVERSITY LINZ

Fragen?

DIGiDOW

INSTITUTE
OF NETWORKS
AND SECURITY

Web: https://jku.at/ins
Email: rm@ins.jku.at
Wire: @rm

Twitter: @rene_mobile
Signal: (phone number by request only)

JOHANNES KEPLER
UNIVERSITY LINZ
Altenberger Straße 69
4040 Linz, Austria
jku.at