

# Digitale Identitäten und Authentifizierung



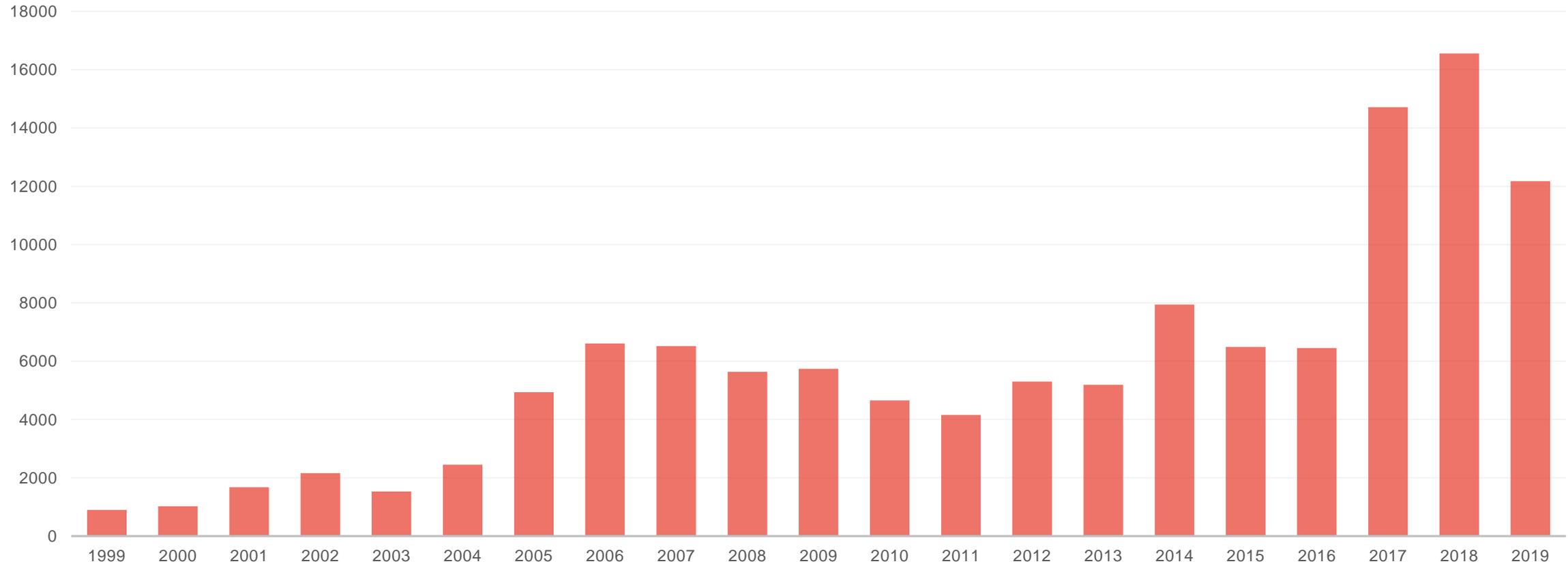
**WKOÖ Webinar “Vernetzt und Ausspioniert”, 2020-10-20 9:00-9:45 (UTC+2), virtuell**

**Univ.-Prof. Dr. René Mayrhofer**

**Institut für Netzwerke und Sicherheit und LIT Secure and Correct Systems Lab, JKU Linz**

# IT-Sicherheit: Wahrnehmung vs. Realität

Published CVE numbers per year



Data source: <https://www.cvedetails.com/browse-by-date.php>

# IT-Sicherheit: Wahrnehmung vs. Realität



# No Silver Bullet – Keine Wundermittel!



Recommended decision helper: <http://doyouneedablockchain.com/>

# Digitale Identitäten



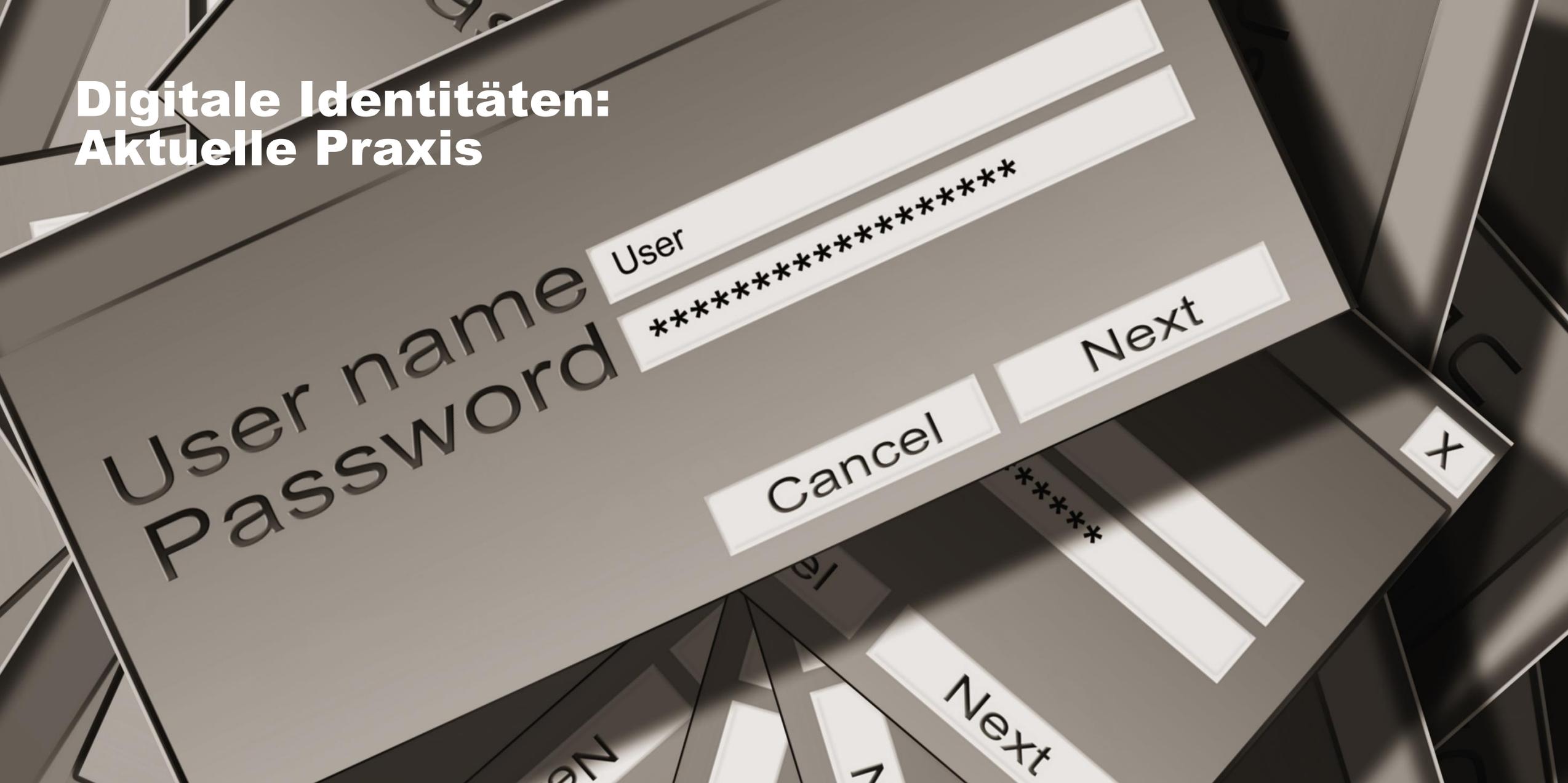
## ... dominieren zunehmend unser modernes Leben

- Kommunikation und soziale Netzwerke (Videokonferenzen, Instant Messaging, VoIP, Chatrooms, Email, etc.)
- Verschiedenste Internetdienste (Streaming)
- Bezahldienste

## ... einschließlich Interaktionen in der physischen Welt

- (Tür-) Zutrittskontrollen
- Reisefreiheit und öffentlicher Verkehr
- Versicherungsschutz, Bonität, etc.

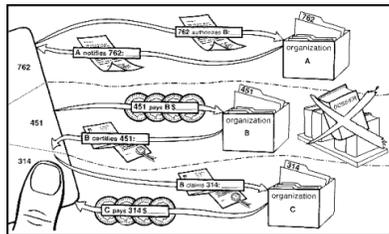
# Digitale Identitäten: Aktuelle Praxis



# 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**

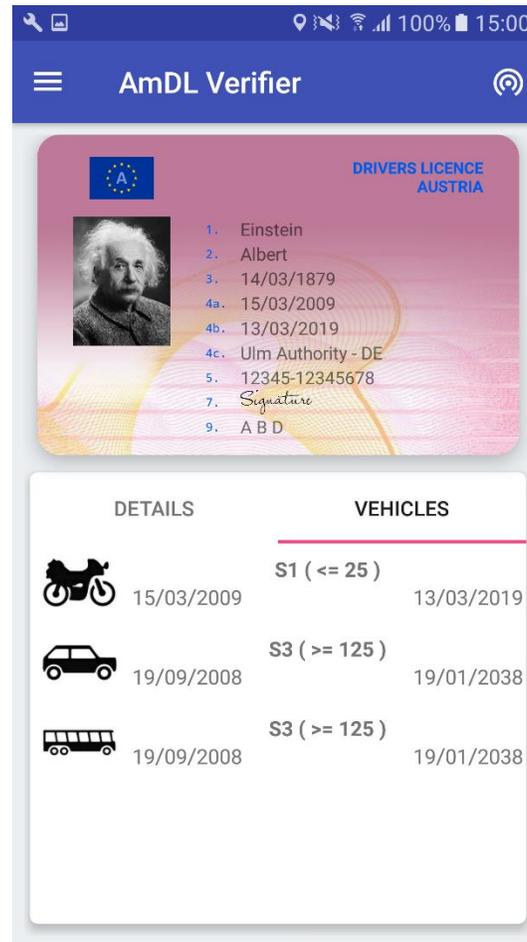
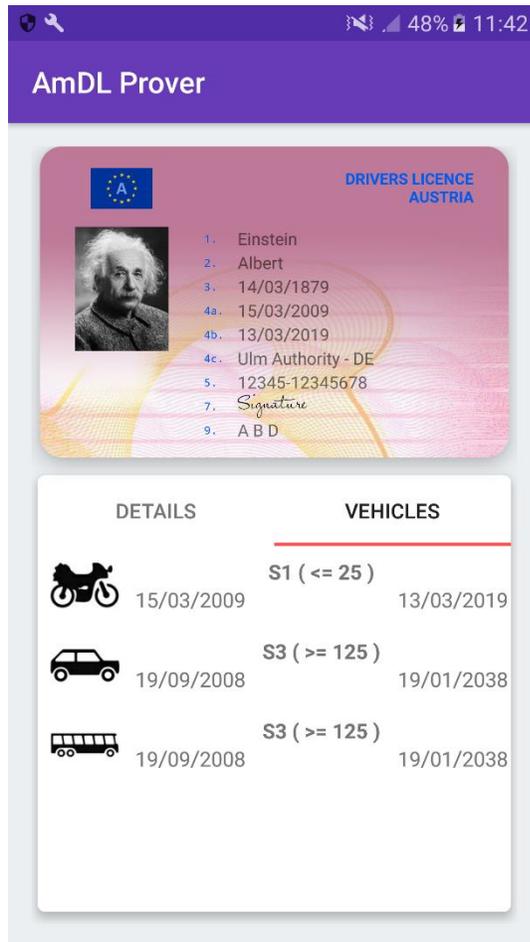
## Industriepraxis

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



**FIDO2/WebAuthn**

# Digitale Identitäten: Beispiel Mobile Driving License – Verkehrskontrolle

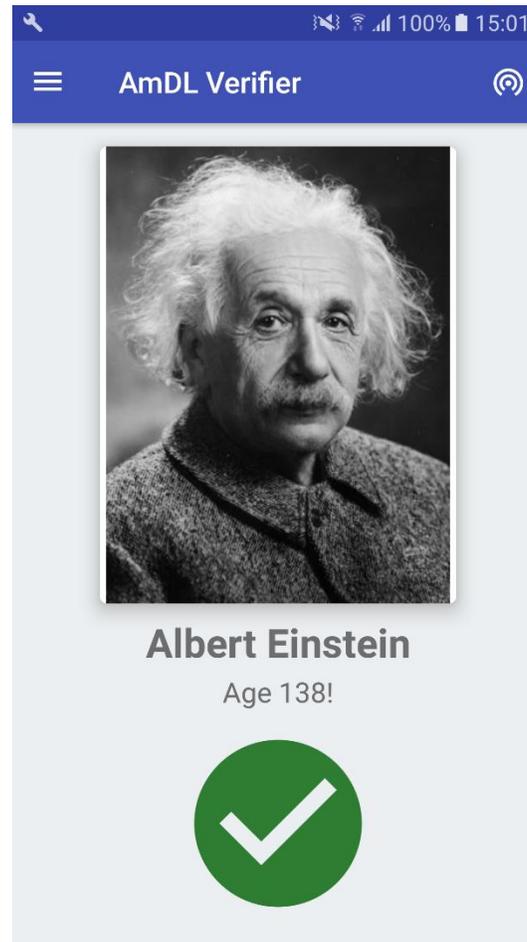
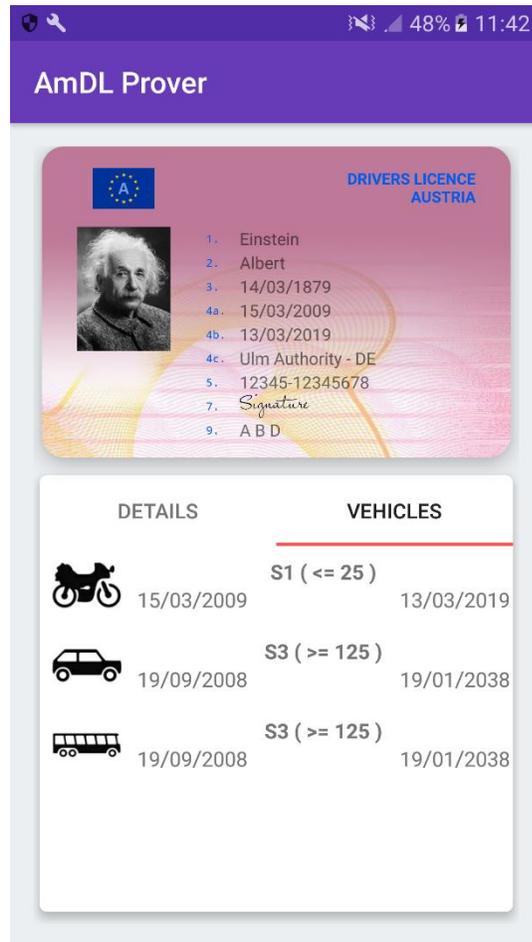


## Alle Attribute übertragen

- 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: Mobile Driving License

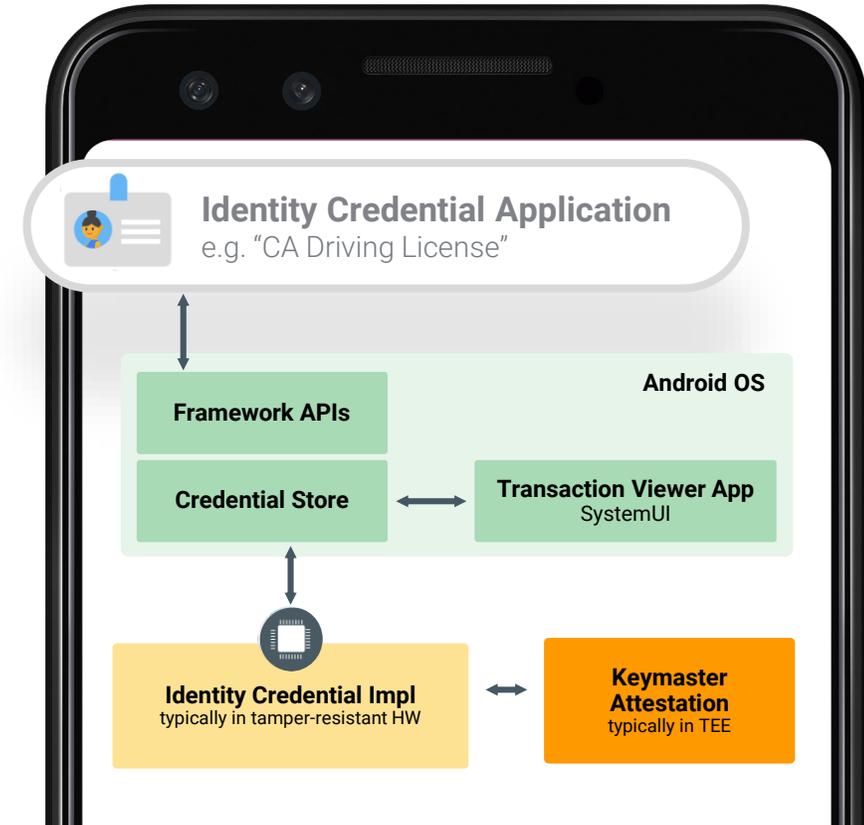
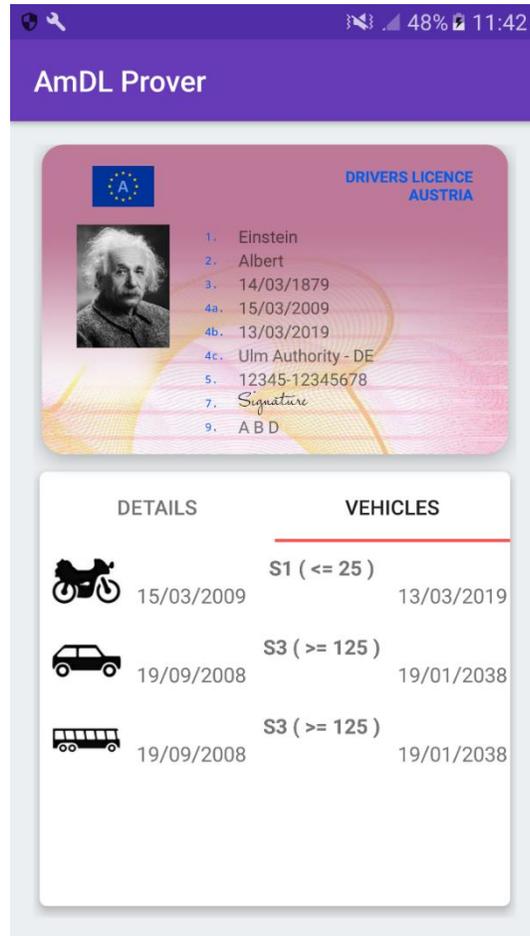


Image credit: Google

# Konkrete Herausforderungen: Chat / Audio / Video / ... am Smartphone



Wichtige Fragen für eine Auswahl von Lösungen:

- 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?
- Welche technische, organisatorische und rechtliche Zugriffsmöglichkeit gibt es beim Provider?
- Was ist die **Benutzeridentität**? **Telefonnummer**, Email, eigene Accounts? Integriert diese ins Unternehmen? Kann ein beruflicher Account von dem privaten getrennt werden?

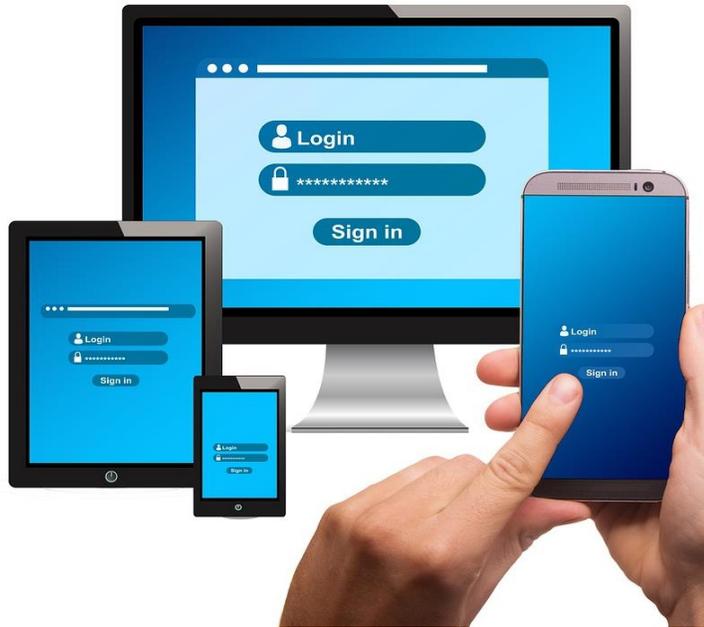
# Konkrete Herausforderungen: Videokonferenzen



Wichtige Fragen für eine Auswahl von Lösungen:

- Verfügbarkeit
  - Inkl. Bandbreitenbedarf für Mitarbeiter\*innen mit schlechter Anbindung
  - Inkl. Unterstützung aller Plattformen (browserbasiert?)
- 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: 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: Vertrauliche Übermittlung von Daten



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

- Eingeschränkter oder offener Empfängerkreis (z.B. Datenaustausch mit engen Kooperationspartnern oder Rechnungen/Kontoauszüge an beliebige Kunden)?
- 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 langfristig archiviert und prüfbar bleiben?

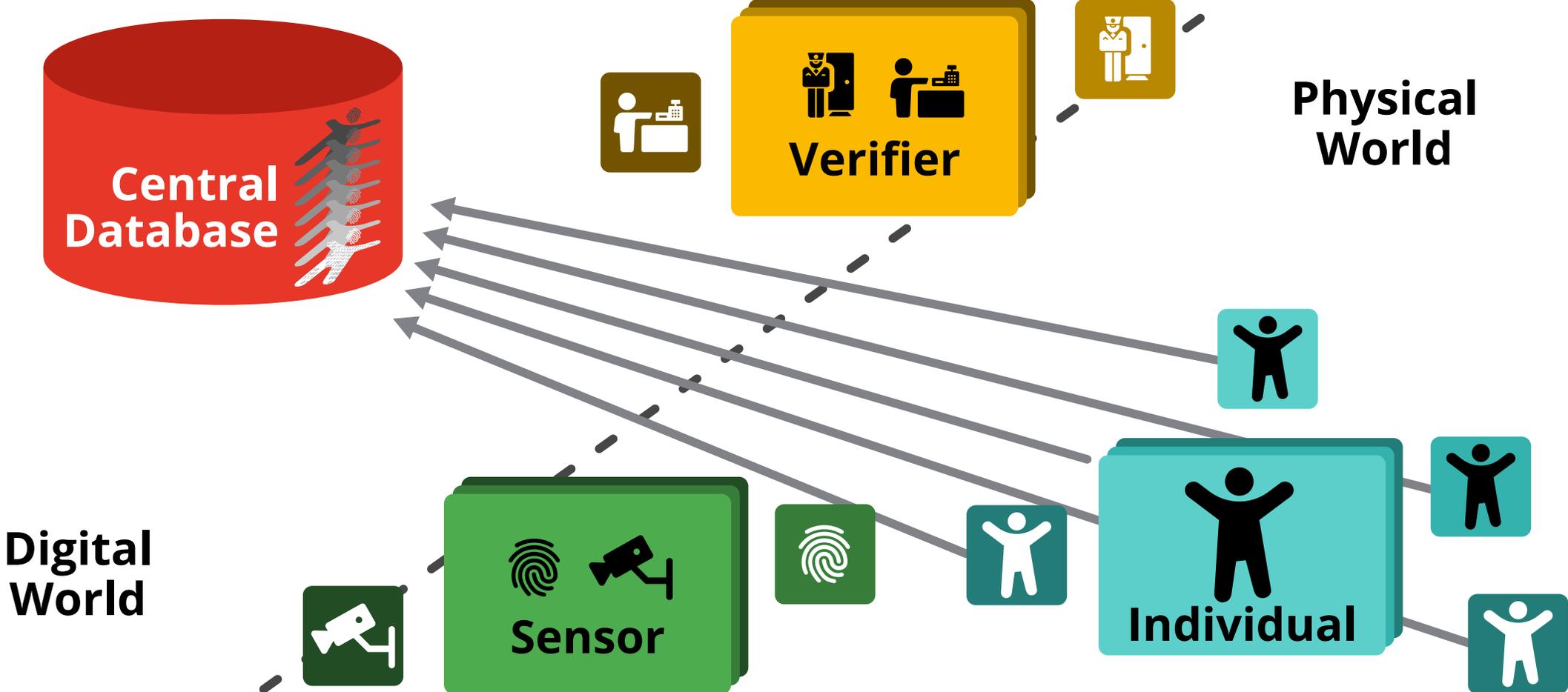
**Empfehlungen** aus der Praxis:

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

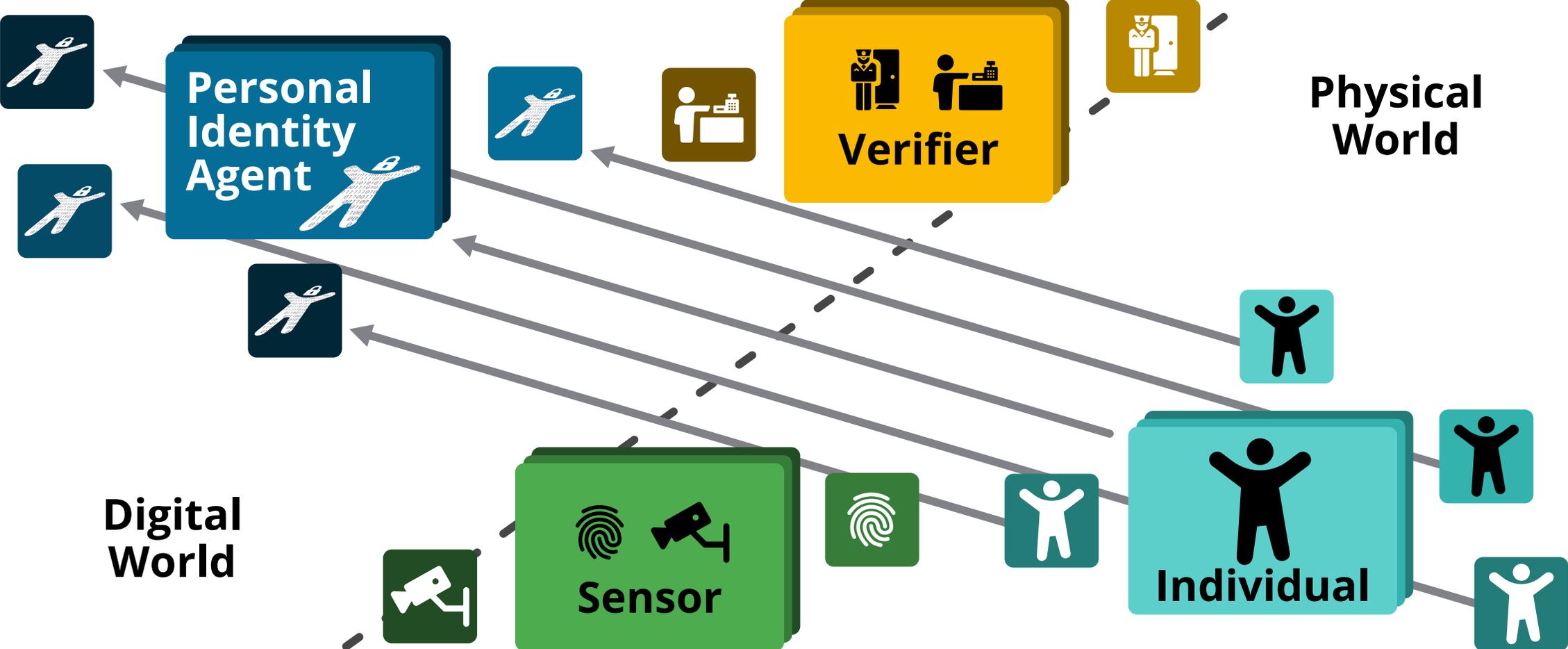
# Konkrete Herausforderungen: Vendor Lock-In



# Digitale Identitäten – zentralisierter Ansatz



# Digitale Identitäten – dezentraler Ansatz



# Fragen?



Web: <https://jku.at/ins>  
Email: [rm@ins.jku.at](mailto: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](http://jku.at)