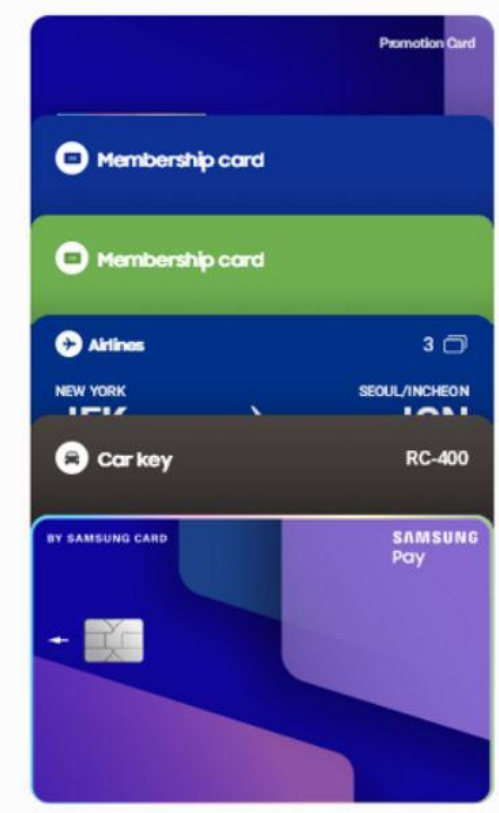
Deutsche Stiftung für Recht und Informatik

Die EU-ID-Wallet – eine datenschutzrechtliche Betrachtung

Prof. Dr. Katrin Blasek, LL.M.
Technische Hochschule Brandenburg a.d.H.

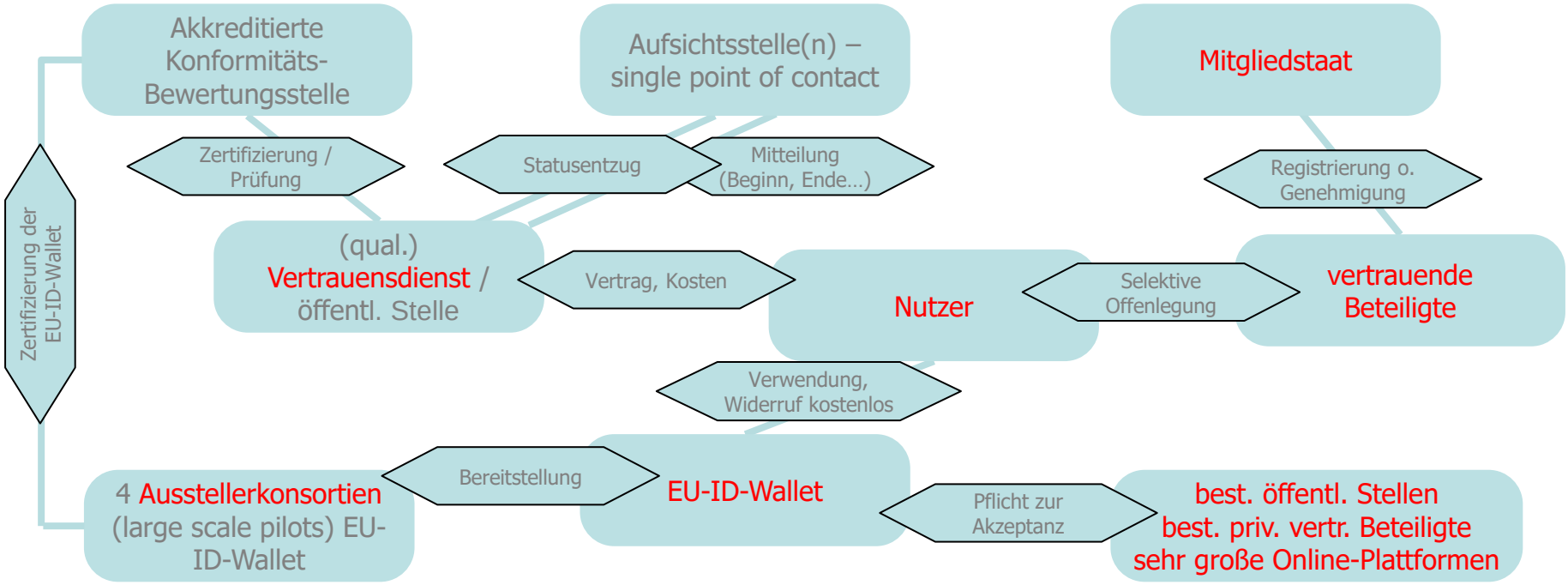
Herbstakademie 2023



EU-ID-Wallet

- (Studi-)Ausweis (eID)
- Führerschein
- Covid-Impfnachweis
- Grundbuch-Auszug?
- Steuer-ID
- Tickets
- Rezept
- BahnCard (…Cards)
- Zeugnisse/Abschlüsse
- Schufa-Auskunft
- Einkommensnachweis
- Schlüssel/Car key

EU-ID-Wallet – Beteiligte im Überblick (Auswahl)



Für einen Überblick: Blasek, ZdiW 2023, 125 ff. (Heft 4)

EU-ID-Wallet

(Studi-)Ausweis (eID)
Führerschein
Covid-Impfnachweis
Grundbuch-Auszug?
Steuer-ID
Tickets
Rezept
BahnCard (…Cards)
Zeugnisse/Abschlüsse
Einkommensnachweis
Schlüssel/Car key
…

Inhalt?
- PIDs und Attribute

Warum?
- Fehlen digitaler Nachweise (Binnenmarkt, Wachstum)
- Lock-In-und Netzwerk-Effekte
- Große Datenmengen/Marktmacht/Missbrauch
- Demokratie, Souveränität

Lösung:
- Kompatible digitale Nachweise
- Selektive Offenlegung (Datenhoheit, Datenminimierung)

Einleitung – Regulierungsstand neue eIDAS-VO

- eIDAS-VO 2014

- Digital Decade 2030: Proposal EU-KOM (03.06.2021)

- RatsE Dez. (25.11.2022)
- EP-E März (16.03.2023)
- Triolog beendet (29.06.2023), finaler Text noch in Arbeit

- Zahlreiche (28) weitere (technische) Implementierungen nach Erlass oder Inkrafttreten durch KOM oder MS

- ***EU-ID-Wallet*** *verfügbar* ***24 bzw. 18 Monate*** *nach Erlass eIDAS-VO*

Datenschutz – Verhältnis zur DSGVO?

- EP-E:
  - Art. 5 Abs. 1: „The processing of personal data shall be carried out in accordance with Regulations (EU) 2016/679 …, by implementing the principles of data minimisation, purpose limitation, and data protection by design and by default, in particular with respect to the technical measures for the implementation of this Regulation and the interoperability framework…"
  - Weitere explizite Verweise auf DSGVO
  - Mehr als DSGVO (IT-Sicherheit, Clouds)

Datenschutz – Datenminimierung (over-identification)

- DSGVO: Datenminimierung (DV auf für den Zweck „notwendiges Maß beschränkt“)
- Ziel EU-ID-Wallet: selektive Offenlegung/Datenminimierung

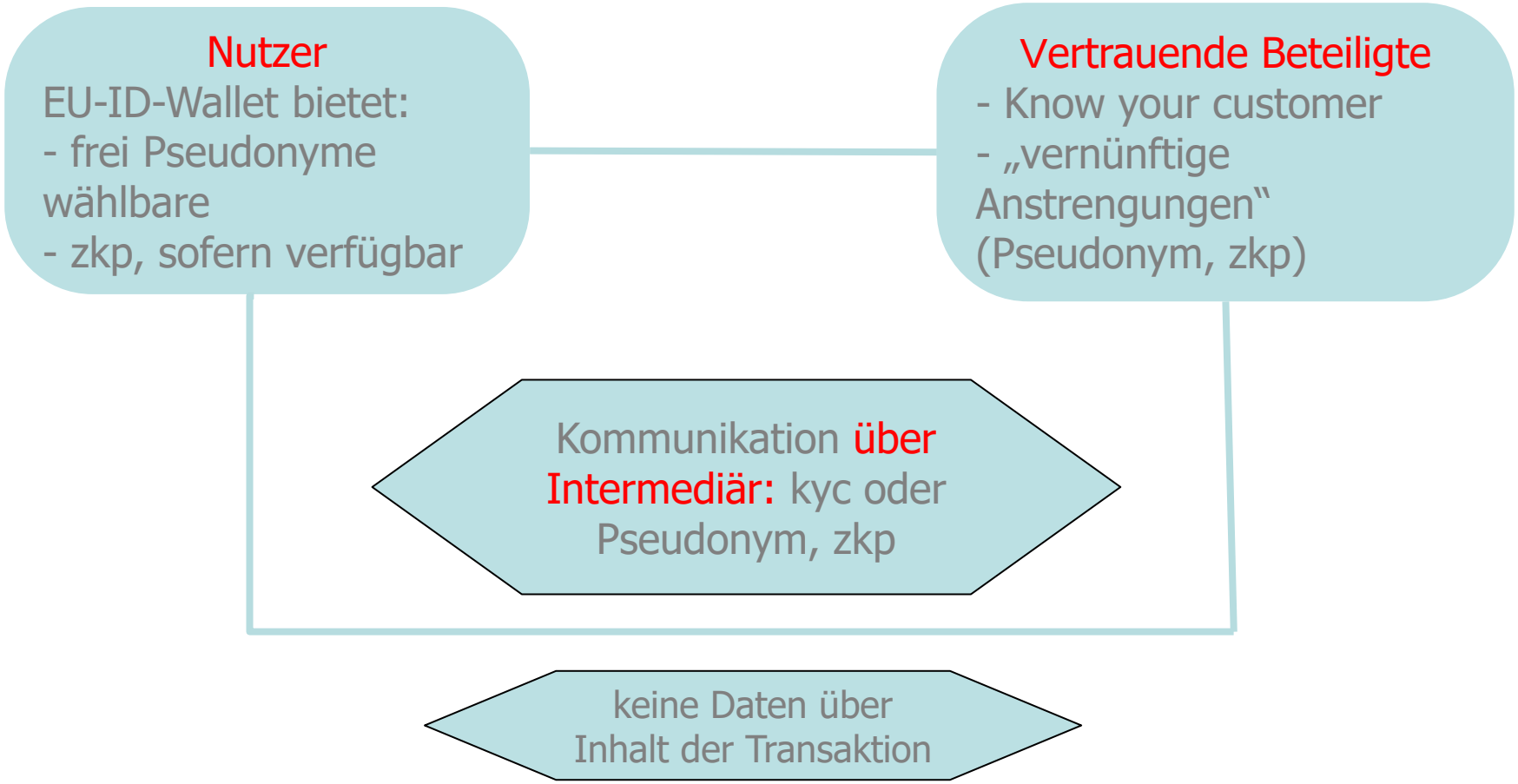
- KOM-E und RatsE:
  - Wallet enthält Mechanismus zur Authentifizierung der Nutzer durch vertrauende Beteiligte (KOM-E)
  - Authentifizierung? elektronische Identifizierung (PIDs, die eine Person eindeutig repräsentieren) (RatsE)

- Kritik: over-identification statt selektiver Offenlegung (Beispiel: Altersverifikation)

Datenschutz – Datenminimierung (Overidentification)

- EP-E:
  - Mechanismus gestrichen
  - Identifizierung nur, wenn gesetzlich vorgeschrieben, ansonsten:
    - Vernünftige Anstrengungen der vB, Dienste ohne Identifizierung oder Authentifizierung anzubieten
    - Pseudnonyme möglich; nicht abdingbar durch Vertrag oder AGB
    - Zero knowledge proof („sofern verfügbar“)
- Altersverifikation: „zulässiges Alter liegt vor“ o.ä. Formulierungen statt Altersangabe und weitere PID
- Umsetzung/Herausforderungen Praxis?

EU-ID-Wallet – Pseudonyme



Datenschutz – unique persistent identifier

- Nicht EU-weit kompatible nat. eID-Systeme; einige MS nutzen bereits dauerhafte allgemeine Kennzeichen
  - KOM-E: Aufnahme eindeutige dauerhafte Kennung in Mindestsatz der PID für Identifizierung falls gesetzlich vorgeschrieben
  - RatsE: hohes Schutzniveau und Verhinderung von Profiling durch TOMs (MS)

- Kritik:
  - Offener Brief: Super-Cookie für BigTechs (Profiling)
  - BVerfG-Volkszählungsurteil: kein einheitliches PKZ für alle Register

Datenschutz – unique persistent identifier

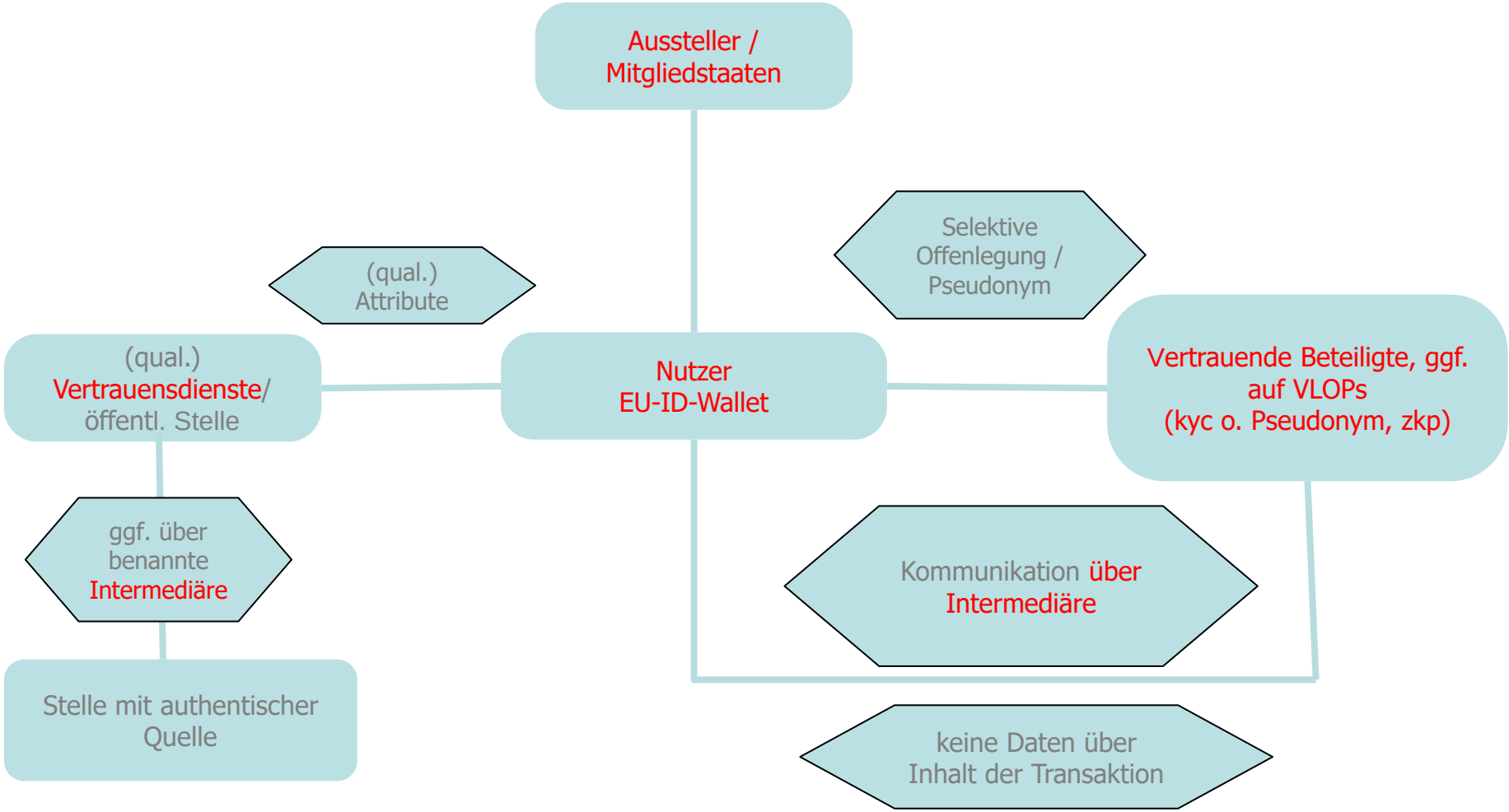
- Einordnung: „im Einklang mit Unions und nat. Recht“
  - Art. 87 DSGVO Kennziffern von allgemeiner Bedeutung, „geeignete Garantien“ (Vermeidung umfassender Profile)
  - Deutsche eID-Nummer: nicht sprechend, keine Übermittlung

- EP-E:
  - MS: ID-Abgleich für cross-border Zugang zu öffentlichen Dienstleistungen sicherstellen (Mindestsatz-PID)
  - MS mit unique identifiers: stellen nur auf Antrag des Nutzers, nur cross-border identifier aus (nur für best. Sektoren oder vB möglich)
  - MS: TOMs zum Schutz vor Profiling
  - KOM: binnen 6 Monaten nach Inkrafttreten DVO („privacy enhancing“, „secure … cross-border identification“ via EU-ID-Wallet)

EUid-Wallet

(Studi-)Ausweis (eID)
Führerschein
Covid-Impfnachweis
Grundbuch-Auszug?
Steuer-ID
Tickets
Rezept
BahnCard (…Cards)
Zeugnisse/Abschlüsse
Einkommensnachweis
Schlüssel/Car key
…

EU-ID-Wallet – Profiling?



Datenschutz – Profiling I

- Technische Architektur der Wallet:
  - verhindert Erhalt oder Sammlung von PIDs oder Attributen der Wallet durch Aussteller, MS oder andere Parteien (vB) gegen Willen des Nutzers (Antrag)
  - verhindert, dass VD Kenntnis über Nutzerverhalten erlangen
  - keine Weitergabe von Attributen an nicht registrierte vB
  - ist sicher auch gegenüber „skilled attackers“
- VD: Trennungsvorgaben, Kombinationsverbote
- Intermediäre der VD? („benannte IM“ noch zu regeln)
- VB:
  - VLOPs: Kombinationsverbot (aber ausdrückliche Nutzer-EW)
  - übrige vB: keine Regelung zu Profiling, aber DSGVO
  - Intermediäre der vB? (Profiling-Risiko?, DSGVO)

Datenschutz – Profiling II

- Grds. Speicherung der Daten in der Wallet („securely and controlled by user“)
- Aber Speicherung der Daten der Wallet möglich bei Dritten oder in cloud möglich
  - „unless user freely consents“ (Art. 6a Abs. 7c EPE, EWG 11: „explicit consent“, kein Verweis auf DSGVO)
  - KOM muss Klarheit durch DVO schaffen (6 Monaten nach Inkrafttreten eIDAS-VO) (Art. 6a Abs. 11 EPE)

- Kritik des BfDI: direkte Kommunikation für user immer besser als indirekte; erhöhtes Profiling-Risiko, insb. bei zentral ausgestalteter Cloud

Datenschutz – verfügbare Endgeräte (Secure Element)

- P: Identitätsdiebstahl; L: sog. secure elements (hardware oder software?)

- EP-E:
  - Wallet „shall ensure security-by-design“…“shall offer resistance to skilled attackers, ensure confidentially of their content…
  - “cryptographic material [of Wallet] should be, ***when technologically possible***, stored in the ***secure elements*** of the wallet“ (EWG 11)
  - Weitere Implementierung durch KOM binnen 6 Monaten nach Inkrafttreten

- DVO eIDAS 2014: keine explizite hardware-Vorgabe bei Sicherheitsniveau „hoch“

Datenschutz – verfügbare Endgeräte (Secure Element)

- Hintergrund:
  - Wenige verfügbare Endgeräte (teuer)
  - Apples Weigerung hardware secure element zu öffnen
- Kritik:
  - hardware! softwaregestützte Lösungen (Sicherheitstoken) nicht ausreichend (BfDI)
  - Sicherheit nur für Wohlhabende (epicenter.works)
- Sturm im Wasserglas?
  - DMA-Interoperabilitätspflichten (Apple Torwächter! Ausnahme?)
  - Technische Entwicklung? (Wallet soll 2015/2016 kommen)
  - Wallet dennoch teilweise nutzbar (Attribute)
  - D: externes secure element (chip auf Ausweiskarte)

Vielen Dank für Ihre Aufmerksamkeit und Fragen?

Blasek, EU-ID-Wallet – eine elektronische Brieftasche für die Europäische Union, ZdiW (Heft 4) 2023, 125 ff.

Blasek, Die EU-ID-Wallet – eine datenschutzrechtliche Betrachtung, Tagungsband Herbstakademie 2023.

Large scale pilots – Bsp. Konsortium Potential

- Pilotprojekte am Bsp. von POTENTIAL:
  - Freischaltung SIM-Karten
  - Zugang zu eGov-Dienstleistungen
  - Bankkonto eröffnen
  - Digitaler Führerschein
  - E-Rezept
  - QES
- Juli 2023 Feldversuch Freischaltung SIM-Karten per Wallet gestartet (Vodafone, Telekom, O2 Telefonica)
- Funding der Pilots endet 2025

Datenschutz – unique persistent identifier

- Aber:
  - BFH 2012: Steuer-ID nicht zu beanstanden
  - Parl. Dienst: RegModG: Steuer-ID bis 2026 in 51 Registern als zusätzl. Ordnungsmerkmal (bereichsübergreifende Kennziffer)
  - Literatur
  - Art. 87 DSGVO „geeignete Garantien“