SCHAUFENSTER
SICHERE DIGITALE IDENTITÄTEN
BEGLEITFORSCHUNG

OMNISECURE 22.-24. Mai 2023 in Berlin

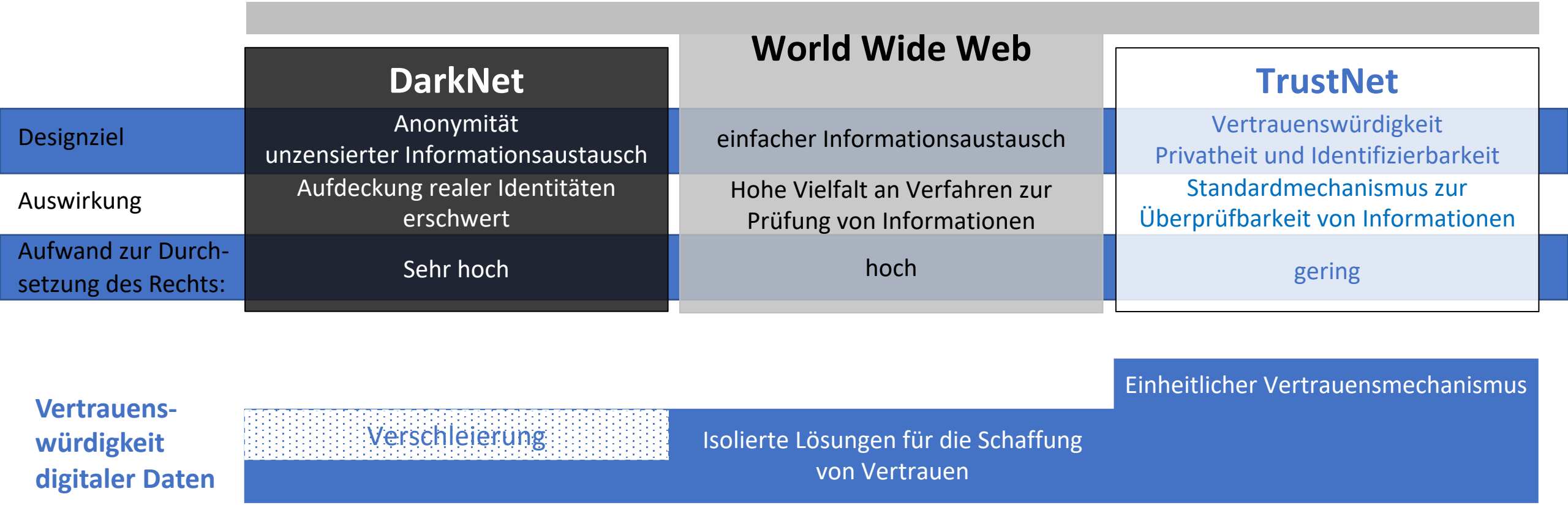
Schaufensterprogramm „Sichere Digitale Identitäten“

Moderation: Franziska Granc (Nimbus Technologieberatung/ Begleitforschung)

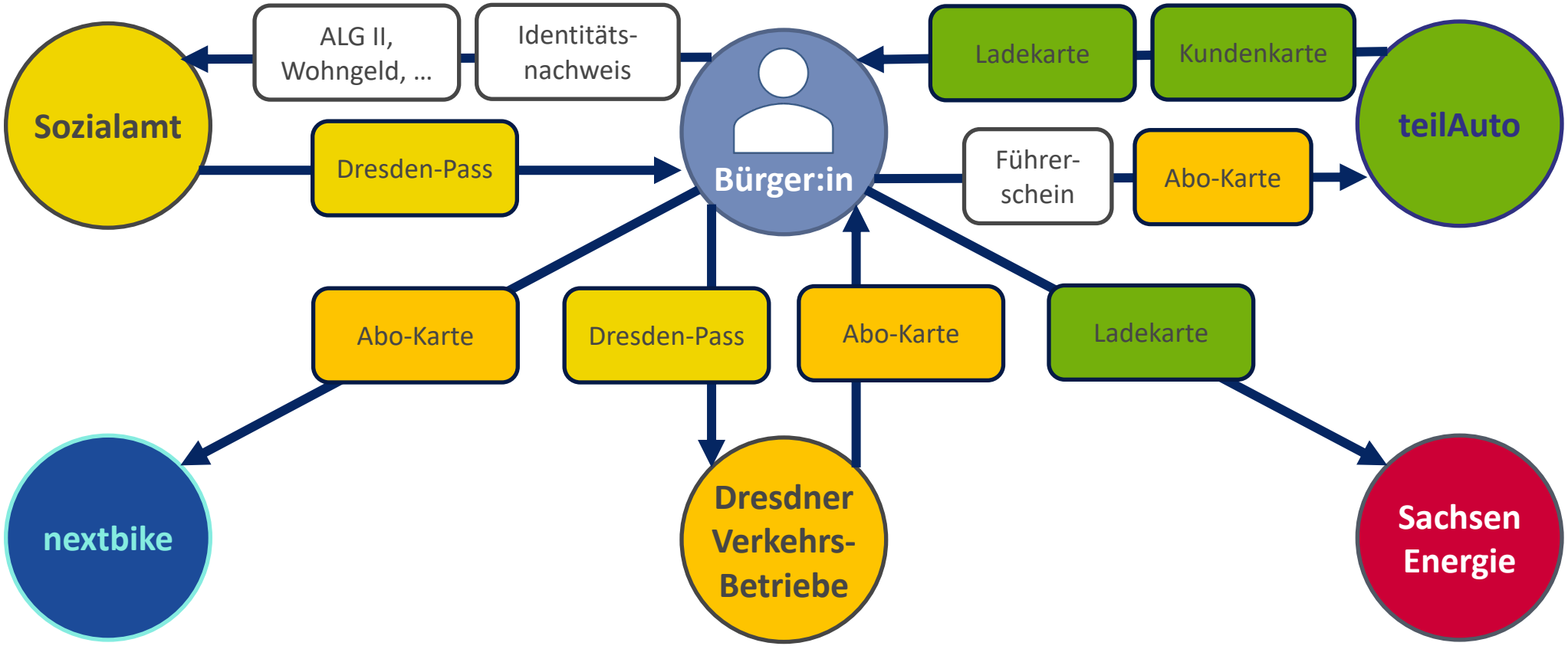
Keynote Axel Voss (Referatsleiter VIB3 BMWK)

Vortrag ID-Ideal – Prof. Dr. Jürgen Anke (HTW Dresden)

Vision TrustNet

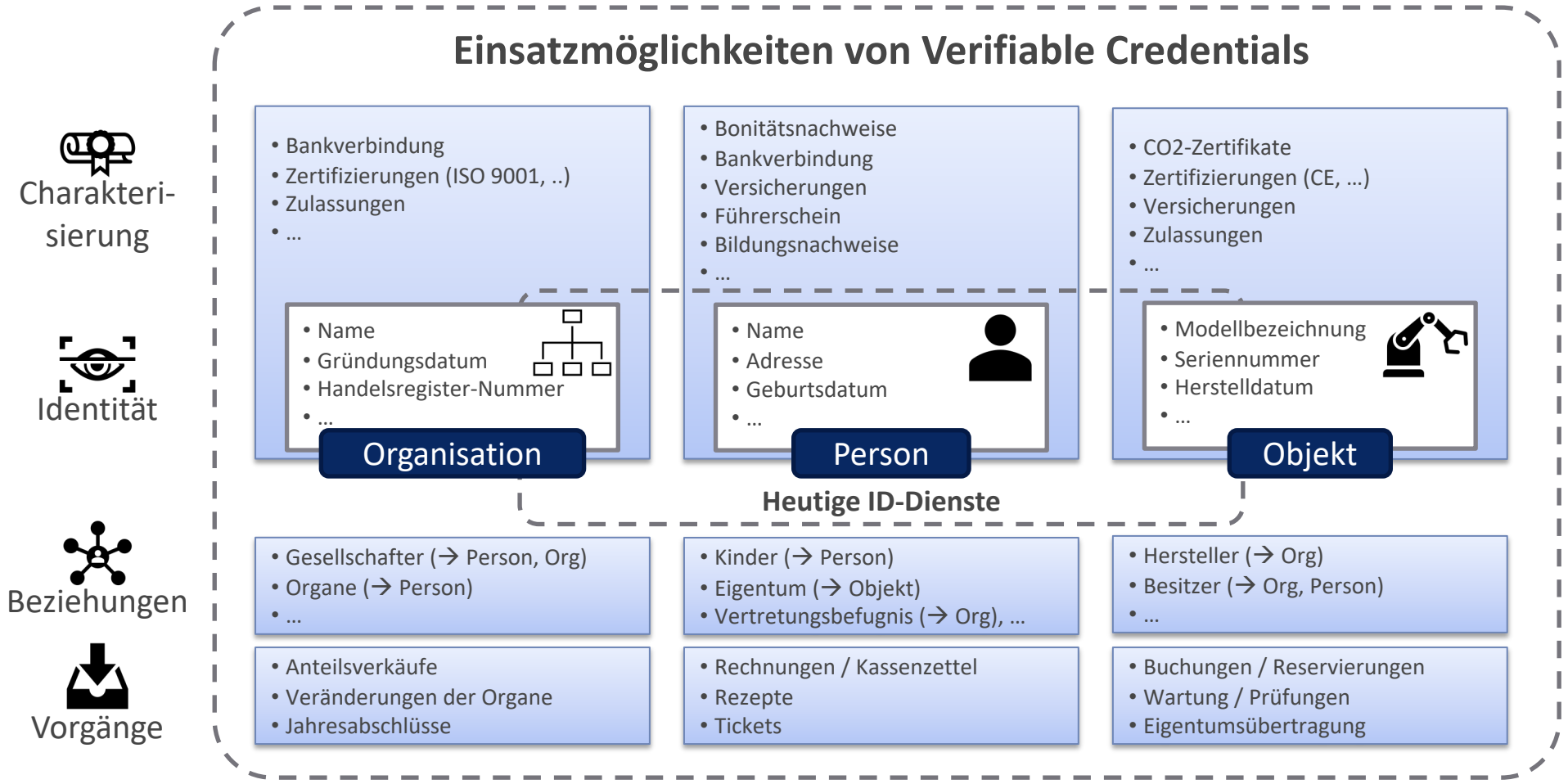


Zusammenspiel verschiedener digitaler Nachweise in einer Smart City



Für eine durchgängige Digitalisierung von Prozessen sind vertrauenswürdige Daten zum Nachweis von Eigenschaften der beteiligten Personen, Organisationen und Objekten erforderlich.

Digitale Nachweise als Basis der digitalen Transformation



Digitale Nachweise erlauben die Bestätigung und Überprüfung beliebiger Sachverhalte - Identifikation und Authentifizierung von Personen sind nur Spezialfälle.

Das TrustNet Trust Framework

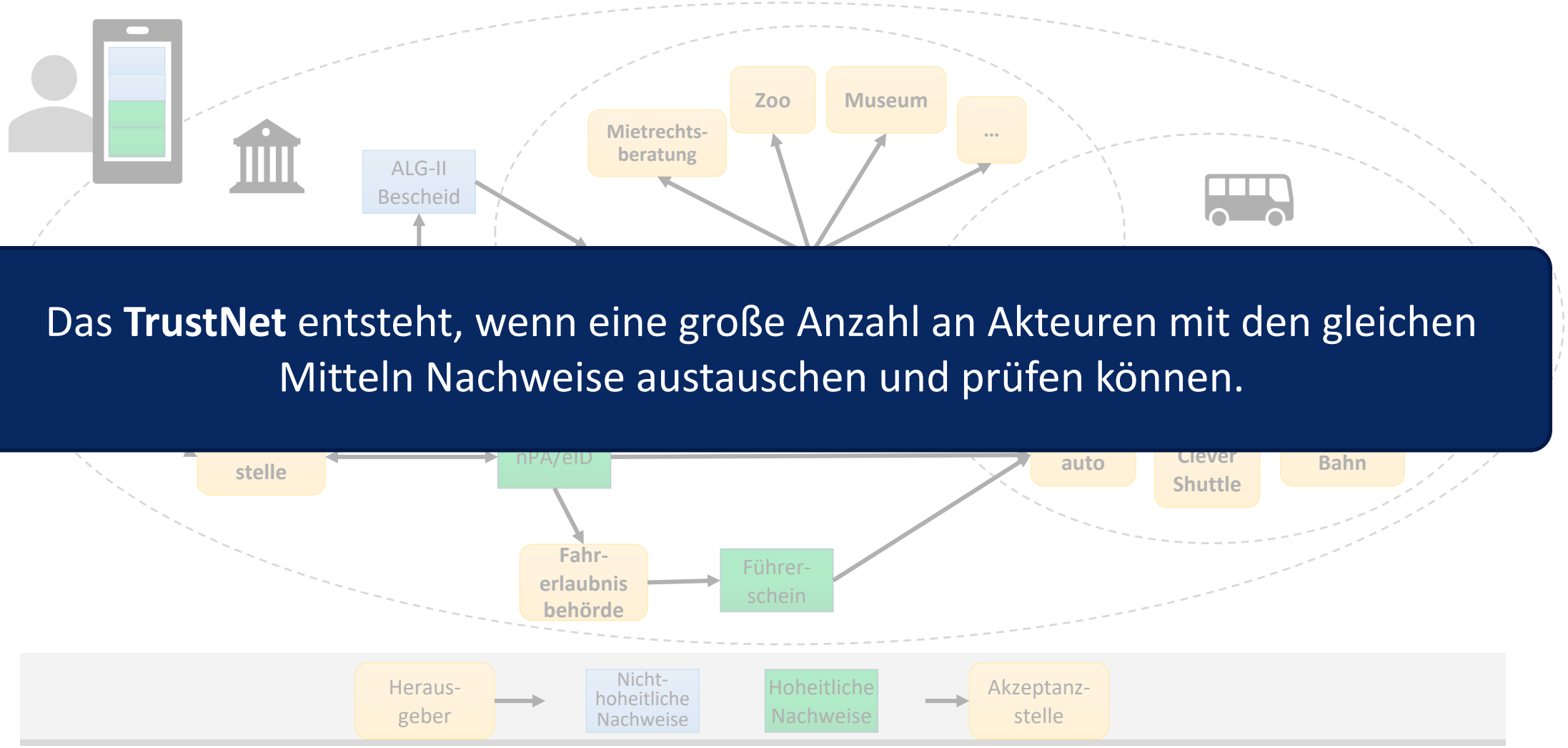
Das Trust Framework definiert standardisierte technische Mittel, um die digitale Koordination der Leistungserbringung durch mehrere Akteure in verschiedenen Domänen rechtskonform, ökonomisch und komfortabel zu ermöglichen.

Umsetzung durch Kombination bestehender Standards auf folgenden Interoperabilitäts-Ebenen:
- *Technisch:* InterOp-Profil auf Basis von W3C, DIF und eIDAS ARF
- *Semantisch:* Mechanismen zum Umgang mit Schemata auf Basis standardisierter Vokabulare
- *Organisatorisch:* Richtlinien über zulässige Herausgeber, Akzeptanzstellen, Prüfvorgaben, …

Nutzen für alle Beteiligten:
- *Anbieter:* Reduzierte Kosten, Komplexität und Integrationsaufwand, besserer Investitionsschutz
- *Nutzende:* Verbesserte Nutzererfahrung (UX) und Datenschutz
- *Technologieentwickler:* Höhere Reichweite der Produkte (→ zweiseitiger Markt)

Die Nutzung des Trust Frameworks führt zur Schaffung eines Markts für interoperable Produkte und Dienste sowie Leistungen für Beratung, Betrieb und Zertifizierung.

Digitale Ökosysteme erfordern interoperable Nachweise



Das **TrustNet** entsteht, wenn eine große Anzahl an Akteuren mit den gleichen Mitteln Nachweise austauschen und prüfen können.

Vortrag SDIKA – Richard Wacker (CAS Software AG)

Schaufenster Sichere Digitale Identitäten Karlsruhe

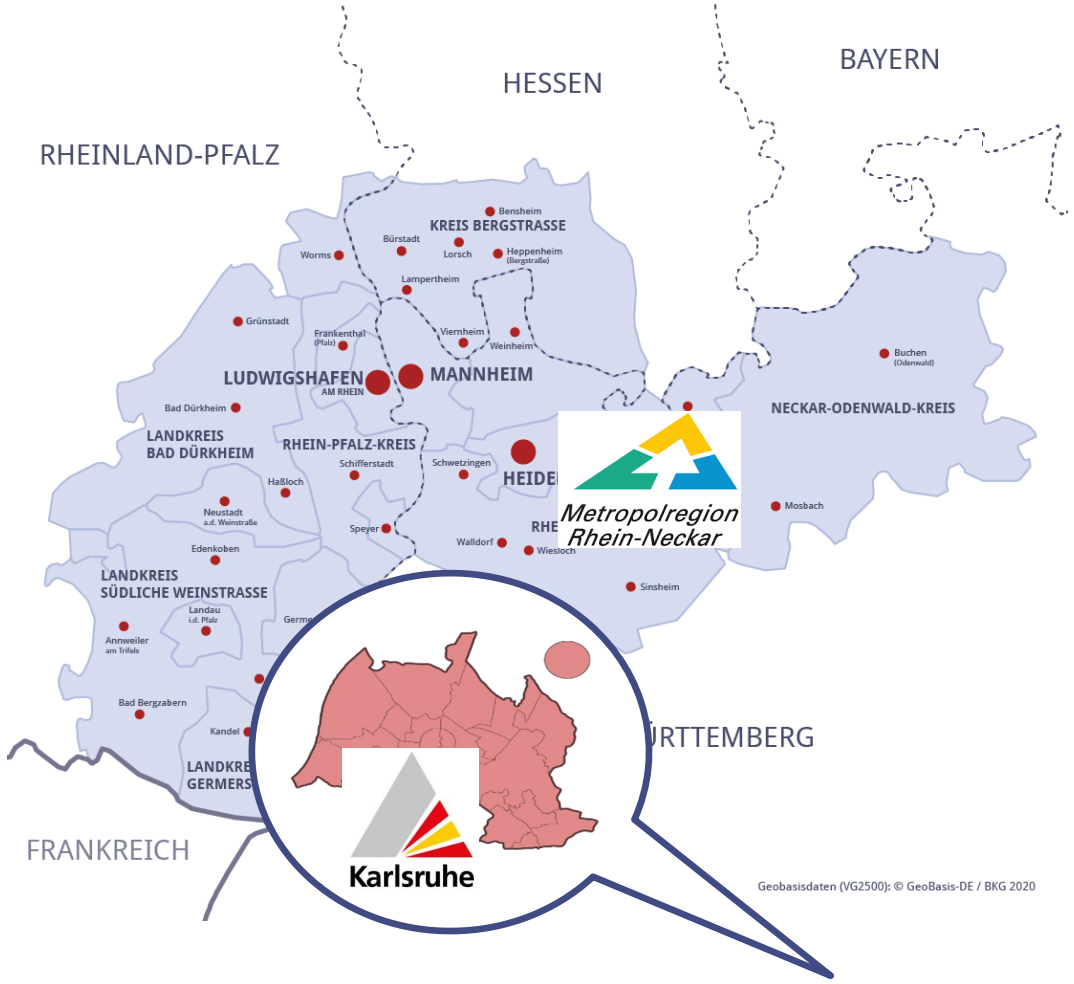
Wir verbinden Menschen, Organisationen und Prozesse.
digital souverän | fair und interoperabel | regionales Schaufenster

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Geographie und Konsortium



Karlsruhe

cantamen

FZI

[ui!] the urban institute

brain-SCC IT- und Mediendienstleister

CAS SOFTWARE

DPS IT FOR FINANCE AND RETAIL

init

Signicat

Leibniz Universität Hannover

YellowMap

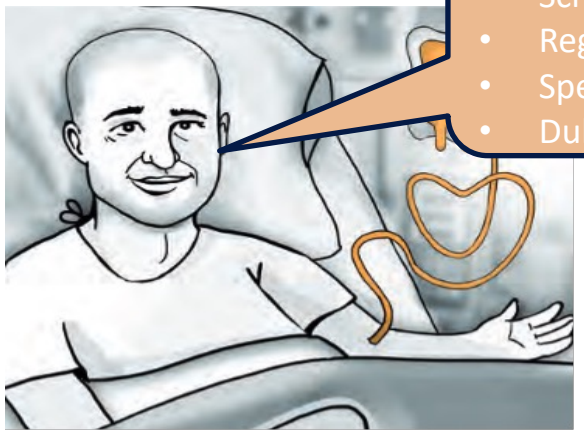
raumobil

ZKRD Zentrales Knochenmarkspender-Register Deutschland

Metropolregion Rhein-Neckar

Anwendungsfelder

Gesundheit



Herausforderungen
- Schnell ein passender Spender!
- Registerdaten aktuell halten.
- Spenderdaten richtig erfassen.
- Dubletten verhindern.

E-Government

Herausforderungen
- Zugänge vereinfachen.
- Teilnahme erleichtern.
- Prozesse verschlanken.
- Bequemer (diskreter) Nachweis.

Digitaler Stadtschlüssel

Einkaufs- und Erlebnisstadt Karlsruher Mobilitätsbonussystem

Herausforderungen
- Rabattsysteme verbinden
- Anreize individualisieren
- Attraktivität steigern

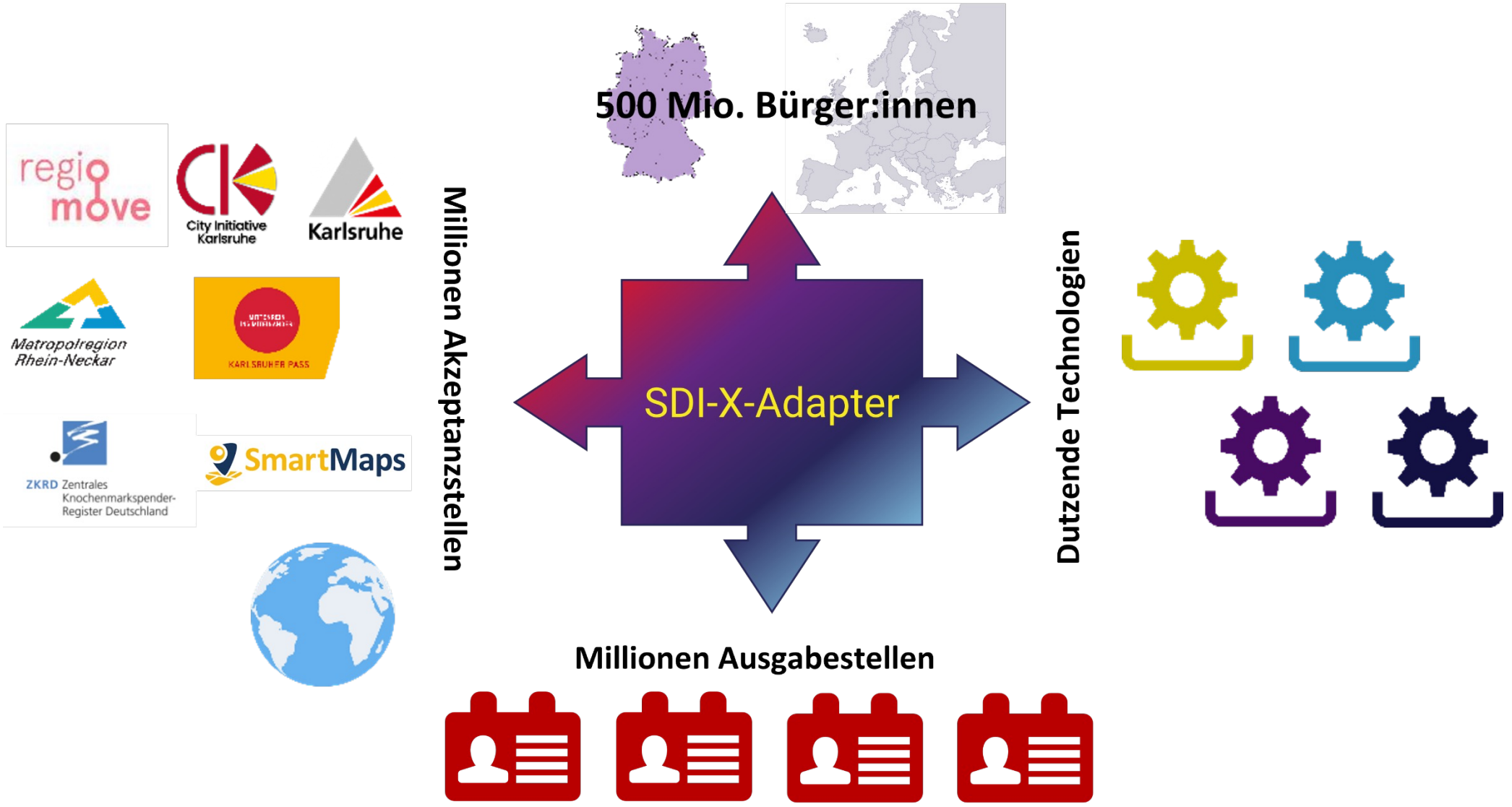
Mobilität

Herausforderungen
- Alle Angebote aus einer Hand!
- Nachweis der Berechtigung.
- Nachweis spezieller Merkmale.
- Individuelle Auskunft.

Planen und Bauen

Herausforderungen
- Bauherr, Architekt, Behörde, Gutachter,…
- Etliche Nachweise / Dokumente nötig.
- Transparenz steigern.
- Papierkrieg vermeiden.

Unsere Vision – Ein Adapter verbindet alle…



Zwischenergebnisse und Herausforderungen

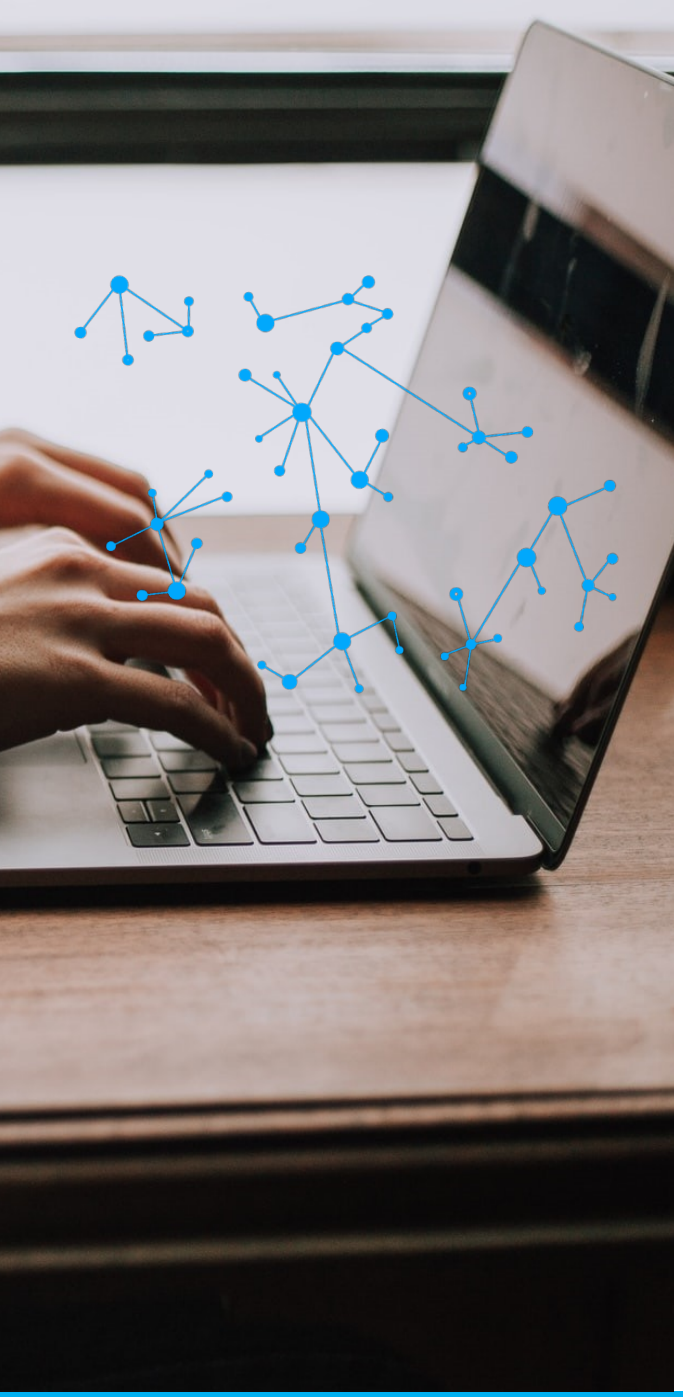
Bald können erste Bürger:innen frei testen

Erste Piloten und Demonstratoren aller Schaufenster stehen

Erste Version des SDI-X-Adapters läuft.

- **Umfeld derzeit unsicher.**
- **Bundeswallet geplant.**
- **EU-Wallet geplant.**
- **Details noch unklar…**

Erste Akzeptanzstellen an Bord



Wichtige Erkenntnisse

„Stakeholder brauchen Investitionssicherheit!“

- Stakeholder investieren Zeit und Geld
  - Ausgabe-, Akzeptanzstellen investieren in IT, Prozesse.
  - Bürger:innen schenken Vertrauen / investieren Zeit.
- Änderungen und Verzögerungen bedeuten Schaden!
- Wegfall von Anbietern / Produkten muss verkraftbar sein.

Adapteransatz mindert Risiko erheblich. (Er kann es aber nicht eliminieren.)

Wichtige Erkenntnisse

„Wirtschaftliche Stakeholder fordern konkrete Vorteile!“

- Kosten des Umstiegs für ihr Geschäft
  - Einmal-Investitionen in Technik und Prozesse,
  - Laufende Kosten.
- Erreichbare Nutzenpotenziale für ihr Geschäft
  - kurzfristig,
  - mittel- und langfristig.

Adapteransatz kann Kosten senken, transparent machen und Nutzen steigern.

Wichtige Erkenntnisse

„Stakeholder brauchen Rechtssicherheit!“

- Technik wendet rechtsrelevante Regeln automatisch an.
- Ersetzt / verschiebt vorgeschriebene (Prüf-)Prozesse:
  - (Sonder-)Berechtigungen,
  - Vertragsvoraussetzungen (bspw. Geschäftsfähigkeit),
  - Jugendschutzvorschriften
  - Tangiert Sorgfaltspflichten (bspw. Qualifikationen)

Adapter-Semantik kapselt Regeln! (die jedoch aktuelles Recht korrekt abbilden müssen).

Wichtige Erkenntnisse

„Staat und Organisationen müssen eingebunden sein!“

- Sie definieren, vergeben und widerrufen Credentials,
- Sie definieren akzeptierte Credentials,
- (neu) Definieren / ändern zulässige Ableitungen z.B.
  - Bauhandwerker + X => bauvorlageberechtigt GK 1/2
  - ALG2-Empfänger + Karlsruher => Sozialpassinhaber
  - Führungskraft + verantwortlich => weisungsbefugt

Unser Ansatz könnte abstrakte Regelungshoheit und unmittelbare Kontrolle kombinieren!

und

Standardisieren ~~oder~~ Adaptieren? ~~?~~ !

„Das beste aus beiden Welten – und noch mehr!“

- Niedrige Einstiegsbarrieren durch Adapter
- Vereinfachte Integration komplementärer Lösungsansätze
- Vergleichbarkeit verschiedener Lösungen
- Günstigere Entwicklung des Adapters
- Einfacher Einstieg ins Ökosystem für neue ID-/Wallet-Services

Standardisierung und Adaption sind gemeinsam Grundsteine für offene und faire Ökosysteme sicherer digitaler Identitäten.

Vortrag ONCE – Walter Landvogt (Bundesdruckerei)

Schaufenster-Projekte: ONCE

Der aktuelle Stand

Kommunale Identitätsattribute

- Kommunaler Personendatensatz aus **Melde- und Personalausweisregister**
- **Bestätigtes Bild aus kommunalem Register (**in Ausbaustufe 2)
- Technologiewechsel

Smartphone-Führerschein - mDL

- Smartphone-Führerschein gemäß ISO 18013 Teil 5
- **Technologie- und Ressourcentransfer** in den EU LSP **POTENTIAL**

Hotelcheck-in und Kur- und Gästekarte

- Hotel-Registrierungsdaten als Schlüssel zu Vergünstigungen für touristische Angebote
- Integriertes ÖPNV Ticket für Zieldestination

Schaufenster-Projekte: ONCE

Schwerpunkt Kommunale Nachweise

Digitalisierungs-baustein „Nachweise“

Eine Digitalisierung von Ausweisen und Nachweisen ist für eine bürgerorientierte Weiterentwicklung der öffentlichen Verwaltung notwendig.

Industrie, Gewerbe, kommunale Betriebe und Behörden selbst benötigen valide Verwaltungsdaten, um ihre Leistungen schnell und effektiv für Bürger bereitzustellen.

Smartphone als Digitalcockpit

Bei Digitalisierungskonzepten mit hoher Akzeptanz nimmt das Smartphone eine Schlüsselrolle ein.

Im Alltag von Bürgern wird es zum zentralen Medium für das Aus- und Nachweisen. Entwicklung.

Nachweise-Ausstellen „as a Service“

Geprüfte Daten aus Verwaltungsregistern brauchen eine sichere Ausstellungsinfrastruktur.

Nachweise-Ausstellen ist ein komplexer technischer und organisatorischer Prozess.

Nachweise-Ausstellen „as-a-Service“ muss die Verwaltung technisch und organisatorisch entlasten.

Schaufenster-Projekte als Ausgangspunkt

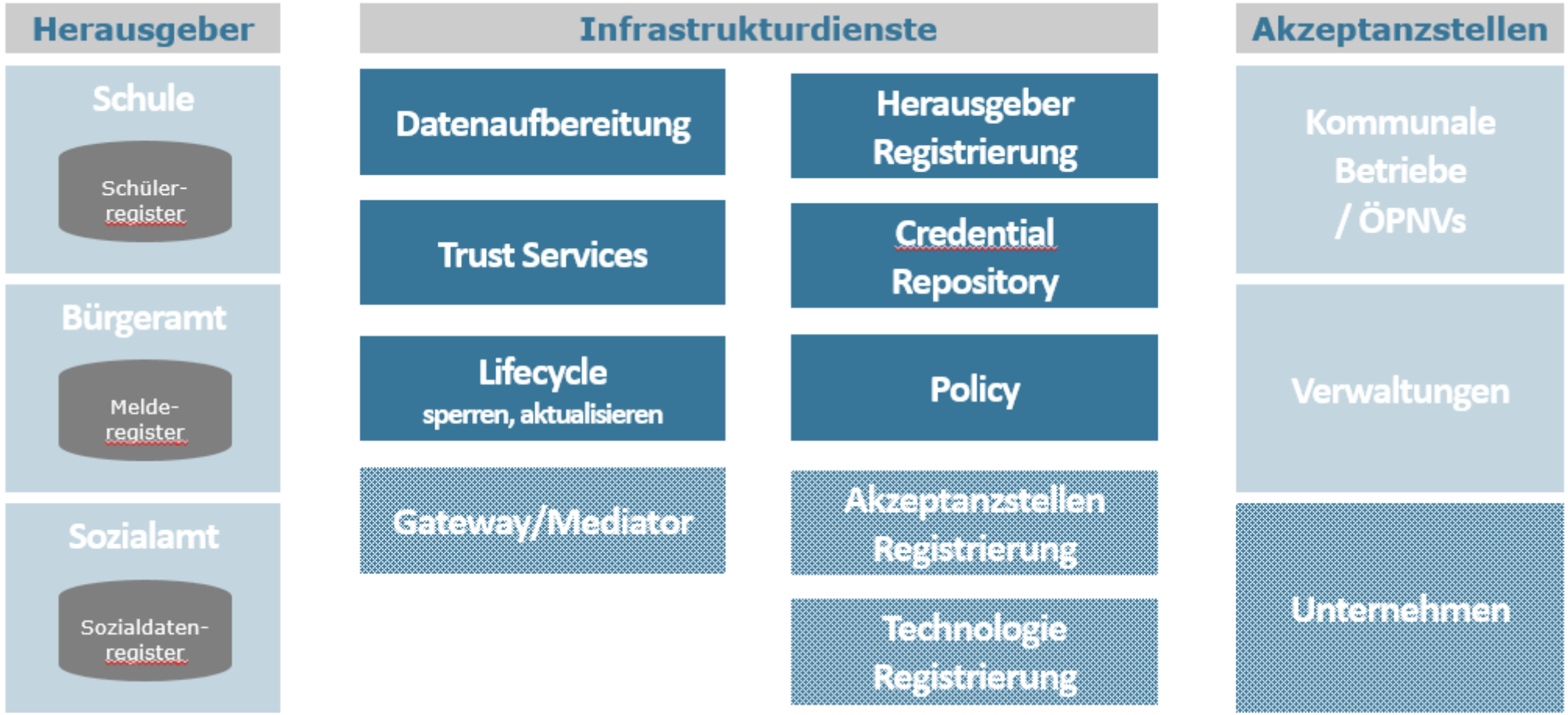
Die Schaufenster-Projekte haben Konzepte und Bausteine entwickelt, die für den Aufbau und Betrieb einer auf Verwaltungen ausgerichteten Ausstellungs-nfrastruktur nutzbar sind.

Fazit

„Nachweise-Ausstellen as a Service“
Ein einfach nutzbares Angebot zur Ausstellung von Nachweisen und Ausweisen als Grundlage für eine weitere Digitalisierung muss entwickelt werden.

Schaufenster-Projekte: ONCE

Zentrale Dienste entlasten Herausgeber und Akzeptanzstellen



Vortrag IDunion – Peter Eisenhofer (yes)

IDunion SCE – Die europäische Genossenschaft

Eine Marke, zwei Organisationen:
Die Gründung einer europäischen Genossenschaft war ein Meilenstein des geförderten Forschungsprojekts

IDunion

Öffentlich gefördertes Projekt

Zweck

Aufbau eines dezentralen Identitätsökosystems für natürliche Personen, Maschinen und Unternehmen

15 Konsortialmitglieder

- Neosfer GmbH
- TU Berlin
- Bundesdruckerei GmbH
- esatus AG
- Robert Bosch GmbH
- Bank-Verlag GmbH
- GS1 Germany GmbH
- Deutsche Bahn AG
- Institut für Internetsicherheit
- Stadt Köln
- ING Deutschland
- Deutsche Telekom AG, T-Labs
- Siemens AG
- Spherity GmbH
- Verimi GmbH (yes IDP GmbH)

+ Assoziierte Partner & Contributoren

IDunion

Europäische Genossenschaft

Zweck

Betrieb einer Infrastruktur für digitale Organisationsidentitäten

10 Mitglieder der Genossenschaft

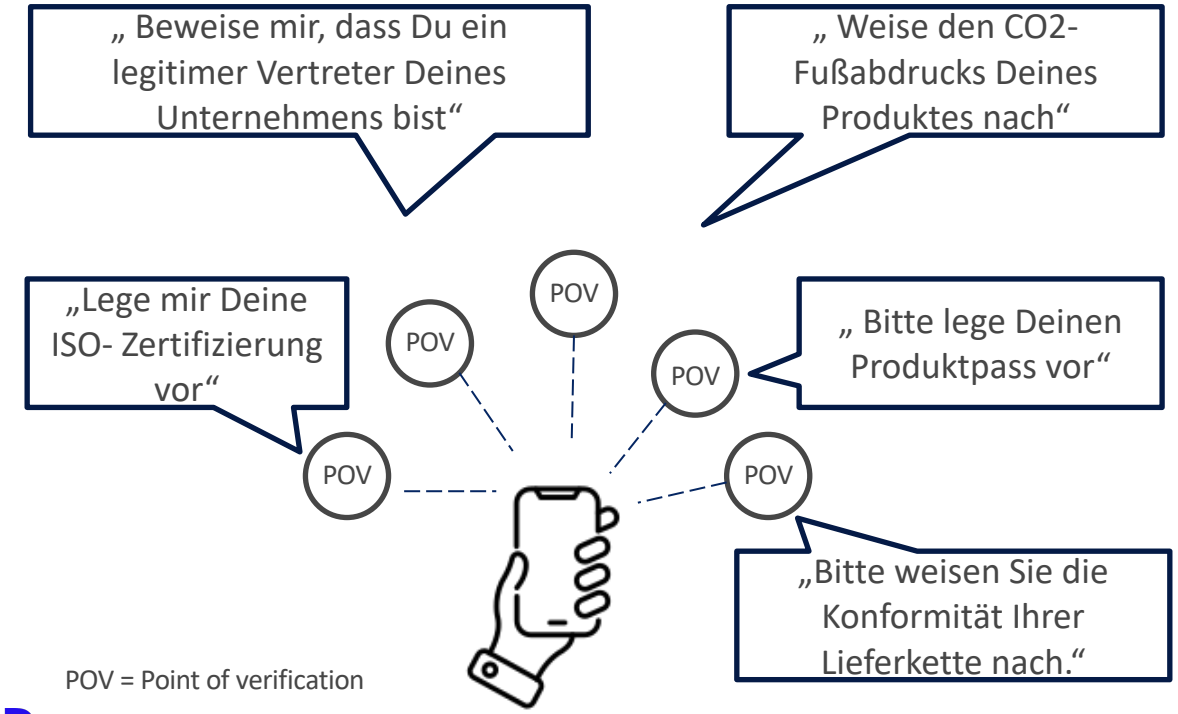
- Danube Tech GmbH
- Spherity GmbH
- TrustCerts GmbH
- Deutsche Telekom AG, T-Labs
- esatus AG
- Datev eG
- Governikus GmbH & Co. KG
- Siemens AG
- estainium e.V.
- Robert Bosch GmbH

IDunion SCE – Die europäische Genossenschaft

Damit ein Vertrauens-Ökosystem gedeihen kann, ist initial eine Digitale Organisationsidentität erforderlich.

Hypothese

Die Vertreter der Unternehmen müssen künftig häufig digitale Nachweise vorlegen.

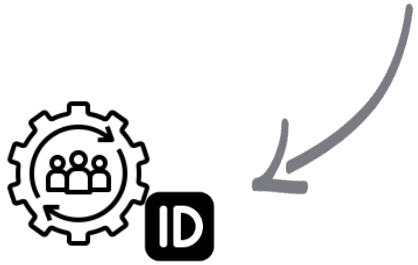


POV = Point of verification

Vision

Nachweise

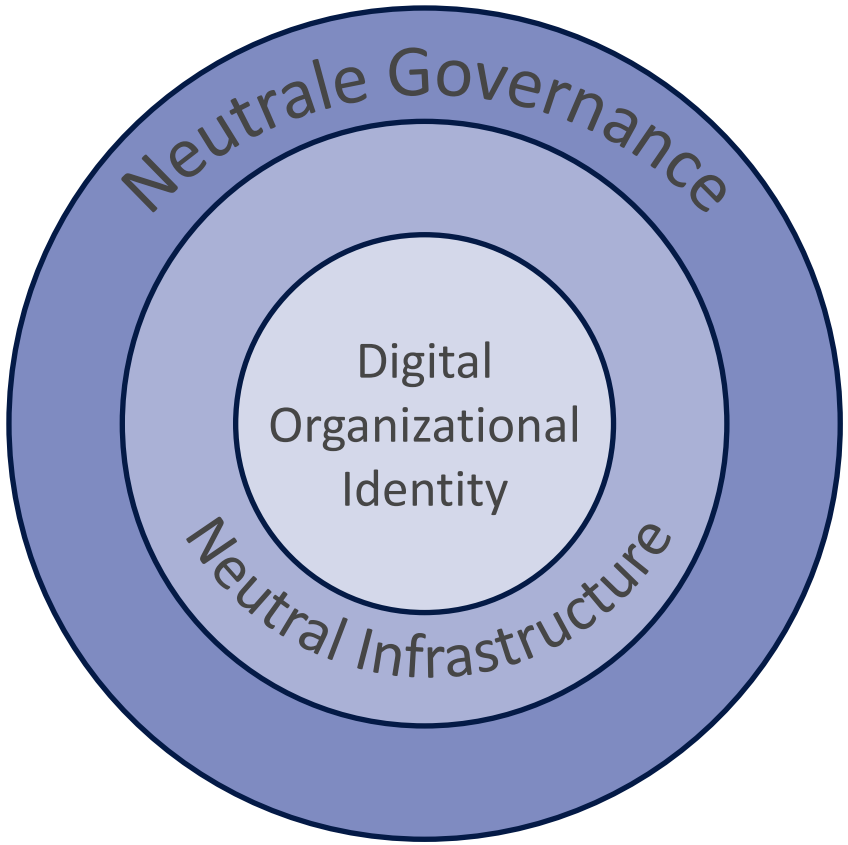
- Werden in Form von **verifizierten Daten** durch
- Vorlage von **überprüfbaren Bescheinigungen** die
- von **vertrauenswürdigen juristischen Personen** ausgestellt wurden erbracht.



Initiales Vertrauen = Digitale Organisationsidentität

IDunion – Die europäische Genossenschaft

Die IDunion SCE bietet eine neutrale Verwaltung und betreibt eine neutrale Infrastruktur als Vertrauensanker für digitale Organisationsidentitäten.



Neutrale Governance

- Kartellrechts-konforme Zusammenarbeit in einer europäischen öffentlichen Genossenschaft
- 1 Mitglied = 1 Stimme
- Kein Wertsteigerung der Genossenschaftsanteile oder Übernahmen durch Dritte möglich
- Einflussnahme erfolgt durch das Generieren von Mehrheiten

Neutrale Infrastruktur

- Technologieunabhängig und sicher
- Vertrauensregister mit dezentralen und zentralen Komponenten
- Parallelbetrieb von mehreren Technologiestacks

Digitale Organisationsidentität

- Digitale Identität für jede Organisation als verifizierbarer Identitätsnachweis in einer digitalen Unternehmens-Wallet
- Ausstellung und Prüfung von digitalen Produktpässen für hohe Datenqualität und eine transparente Lieferkette

IDunion – Tech Stack 2.0

Erfahrungen mit Hyperledger Indy, Aries und AnonCreds führten zum Wunsch nach einem neuen Ansatz

- AnonCreds:
  - Hoher Grad an Datenschutz (Privacy) aber Herausforderungen in Bezug auf die Sicherheit
    - Zu kurze Schlüssellänge (RSA mit 2048 Bits)
    - Keine Hardware-gebundenen Schlüssel mit breit verfügbarer Hardware (Impersonation, Replay möglich)
    - Keine Freigabe durch BSI oder vergleichbare Regierungsorganisation
  - Schlechte Performanz (und damit User Experience)
- Aries
  - Schlechte Skalierbarkeit
  - Hohe Komplexität in Entwicklung und Betrieb
- Indy
  - Schlechte Skalierbarkeit der Revocation (max bis zu 60k)
- Generell
  - Keine Standardisierung durch anerkannte Standardisierungsorganisationen

IDunion – Tech Stack 2.0

Bewertung

	Anoncreds	W3C JSON-LD /BBS+	W3C JSON-LD /EdDSA	W3C JWT-VC	W3C SD-JWT-VC	ISO mdoc
Selective Disclosure	yes	yes	no	no	yes	yes
Unlinkability	yes	yes[1]	no	no	no	no
Hardware security support	no	no	yes	yes	yes	yes
PQC & cryptographic agility	no	no	yes	yes	yes	yes
Standardisation	Community Specification	W3C Recommendations / IETF	W3C Recommendations / IETF	W3C Recommendations / IETF	W3C Recommendations / IETF	ISO 18013-5 / ISO23220-2
Technology Readiness Level	6-8	6-7	7-8	7-8	4-5[3]	8-9 (on-site) 5-6 (remote)
Predicates	yes	no	no	no	no	no
Semantic support	no	yes	yes	no[2]	no[2]	no

[1] : BoundBBS+ offers unlinkability, BBS+ with did:key holder binding not
[2] : JSON-LD as pure data payload is possible
[3] : fast maturity increase expected

IDunion Tech Stack 2.0: SD-JWT wurde ausgewählt wegen der aktuellen besten Balance zwischen Privacy (Selective Disclosure), Sicherheit (erlaubt Hardware-gebundene Schlüssel) und Entwickler-Freundlichkeit.

IDunion – Tech Stack 2.0

Status / erste Erfahrungen

- OpenID 4 VC wurden wegen der Einfachheit und Sicherheit ausgewählt.
- Erprobung in Hackathon war außerordentlich erfolgreich (Ausstellung, Verwaltung im Wallet und Präsentation beim Login zur Nextcloud in 1,5 Tagen unter Nutzung von SD-JWT-Bibliotheken, ansonsten alles neu).
- Evaluation und Erprobung von Methoden für die Verwaltung von Schlüsselmaterial und Vertrauen. Hier sind wir mit der internationalen Community in Abstimmung, gleiches gilt mit der eIDAS Expert Group.
- Das Ergebnis wird in einem High Assurance Profile für OpenID for Verifiable Credentials (mit SD-JWT) festgehalten und publiziert werden.
- Innerhalb und außerhalb von IDunion stehen Implementierer in den Startlöchern, die damit konkrete Projekte implementieren und ausrollen möchten.

IDunion – ARF 1.0

Inhalt

- Das ARF definiert zwei Arten von Credentials, Type 1 und Type 2. Für beide gelten unterschiedlich starke Sicherheitsanforderungen.
  Link: https://ec.europa.eu/newsroom/dae/redirection/document/83643

- Es definiert welche technischen Standards eingesetzt werden sollen
  - Protokolle:
    - **OpenID for Verifiable Credentials** (Online-Präsentation, Issuance, Pseudonyme Authentifizierung)
      Link: https://openid.net/openid4vc/
    - ISO 18013-5 (mDL) (Offline-Präsentation)
  - Credential-Formate:
    - **Selective Disclosure JWTs** (SD-JWT)
      Link: https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/
    - **ISO mdoc** (definition in ISO 18013-5)
      Link: https://www.iso.org/standard/69084.html

  - PIDs müssen **in beiden Formaten ausgestellt werden**

IDunion – ARF 1.0

Status

- Es bleibt eine Menge zu tun: Insbesondere die Vertrauens-Verwaltung für die verschiedenen Parteien.
- Erfahrungen mit den Protokollen und den Credential Formaten werden im Rahmen von IDunion und verschiedenen LSPs gesammelt und in die Weiterentwicklung sowohl des ARF als auch der Standards eingebracht.
- Sowohl **OpenID for Verifiable Credentials** als auch **Selective Disclosure JWTs** wurden mit Mitteln des Projekts entwickelt
- Noch unklar ist, wie die Standardisierung nach Abschluss der Förderung der Schaufenster-Projekte gesponsort wird.

Vielen Dank!