Anforderungen
aus Sicht
der SDI-Schaufenster ONCE und ID-Ideal
an die Entwicklung der EUDI-Wallet

Autoren:

aus dem Schaufensterprojekt ID-Ideal

- Dr. Matthias Fuhrland, Prof. Dr. Jürgen Anke - Hochschule für Technik und Wirtschaft Dresden
- Robert Schröder - Landeshauptstadt Dresden, Eigenbetrieb IT-Dienstleistungen
- André Röder – KAPRION Technologies GmbH
- Lukas Schroll – Stadt Leipzig, Referat Digitale Stadt

(https://id-ideal.de/)

aus dem Schaufensterprojekt ONCE

- Matthias Martin – ekom21
- Walter Landvogt – Bundesdruckerei

(https://once-identity.de/)

Dezember 2023

Inhalt

1. Zweck dieses Dokuments

Das BMI und das GovLab der Bundesministerien konsultieren Experten und potentielle Stakeholder bezüglich der Entwicklung einer sogenannten EUDI-Wallet. Es wird erwartet, dass die Novellierung der eIDAS-Verordnung auf EU-Ebene die Mitgliedsstaaten zur Bereitstellung einer solchen Wallet verpflichtet, um der Verordnung eIDAS 2.0 sowie der Nutzung der eID als digitalem Identifizierungsmittel zur breitenwirksamen Durchsetzung zu verhelfen. Die Schaufensterprojekte ID-Ideal, IDunion, ONCE und SDIKA bündeln das in Deutschland verfügbare Expertenwissen im Bereich sicherer digitaler Identitäten. Innerhalb der Projekte werden nicht nur verschiedene Arten von Wallets und zugehörigen Agents entwickelt, sondern insbesondere auch in verschiedenen Anwendungs-szenarien erprobt. Mit F&E-Aktivitäten zu sieben verschiedenen Edge-Wallets inkl. einer EUDI-Wallet, dazu drei Organisations-Wallets und einer Cloud-Wallet bilden die Schaufensterprojekte die weltweit breiteste Wissensbasis zur Entwicklung und Anwendung von Wallet-Apps für sichere digitale Identitäten.

Das BMWK als Initiator und Fördermittelgeber des Schaufensterprogramms „Sichere digitale Identitäten“ ist damit europaweit, vermutlich sogar weltweit der einzige politische Akteur, der wissenschaftlich fundierten Input in diesem Themenkomplex liefern kann. Die wissenschaftliche Expertise und das Anwendungswissen der beteiligten Akteure aus Forschung, Wirtschaft und öffentlicher Verwaltung insbesondere zu kommunalen Anwendungsszenarien soll in den Konsultationsprozess zur EUDI-Wallet einfließen. Ziel ist dabei nicht, die Forschungs- und Entwicklungsergebnisse und deren wirtschaftliche Verwertung an die bisher zu erwartenden technischen Vorgaben der eIDAS-Novellierung anzupassen, sondern den handelnden politischen Akteuren Empfehlungen zu geben, wie die Entwicklung der EUDI-Wallet und die weitere Novellierung der eIDAS-Verordnung von den Erkenntnissen der Schaufensterprojekte profitieren können.

2. Die grundlegende Idee und Philosophie der Schaufensterprojekte

1. Praxiserprobung vor Regulierung

Die Projekte ID-Ideal, ONCE, IDunion und SDIKA, gefördert im Schaufensterprogramm „Sichere digitale Identitäten“ des BMWK sind großformatige Verbundforschungsprojekte. Mit dem Bewusstsein, hier technologisches und gesellschaftliches Neuland zu betreten, wurden sie seitens des BMWK gezielt als Forschungsprojekte definiert. Der bewährte Grundsatz, erst Lösungsansätze zu erforschen, verschiedene Lösungen vergleichend zu entwickeln sowie Praxistests mit Evaluierung hinsichtlich Best Practice und rechtlichen Innovationsbarrieren durchzuführen, und erst danach auf Basis gesicherter Erkenntnisse die Fragen von Standardisierung und Regulierung anzugehen, war dabei der Leitgedanke. Die für Standardisierung und Regulierung erforderliche wissenschaftliche Expertise gilt es im Bereich der sicheren digitalen Identitäten durch praktische Erprobung und Feldforschung zu erarbeiten. Dabei wird die aktive Beteiligung von Kommunen an Entwicklung, praktischer Erprobung und Feldforschung als Schlüssel für das nachhaltige Identifizieren und Ausgestalten breitenwirksamer Anwendungen betrachtet.

2. Technologieoffenheit und Interoperabilität

Technische, semantische und organisatorische Interoperabilität sind maßgebliche Designziele bei der

Realisierung von Anwendungen im Rahmen der Schaufensterprojekte. Dabei geht nicht um die Einigung oder Festlegung auf einen einheitlichen Technologie-Stack, sondern um Technologieoffenheit und das Zusammenwirken verschiedener Lösungsansätze. Diese Interoperabilität wird als Schlüssel für eine breitenwirksame Etablierung in Wirtschaft, Verwaltung und Gesellschaft gesehen.

3. Überprüfbarkeit von Informationen als Designziel

Sichere digitale Identitäten haben dann einen wirklichen Nutzen, wenn man sie als Werkzeug zur Weiterentwicklung des Internets und der Digitalisierung begreift. Der grundlegend neue Ansatz zur Generierung von Vertrauen in der digitalen Welt ist dabei nicht in erster Linie Informationssicherheit, sondern die Überprüfbarkeit von Informationen. Der dafür erforderliche grundlegende Vertrauensmechanismus ist die Kombination überprüfbarer digitaler Nachweise (Verifiable Credentials) mit dem Prinzip der selbstbestimmten Identitäten (Self Sovereign Identities). Die Schaufensterprojekte entwickeln und erproben hierfür die erforderlichen Technologien und demonstrieren sie in verschiedenen Anwendungsszenarien.

4. Prozessdigitalisierung

Digitalisierung ist nicht länger als Digitalisierung von Dokumenten zu begreifen. Ziel muss es sein, die Digitalisierung und Automatisierung von Prozessen anzustreben. Erst durch die Automatisierung von Prozessen kann die Digitalisierung überhaupt ihr eigentliches ökonomisches, ökologisches und gesellschaftliches Potential entfalten.

3. Die übergeordnete Vision

Die über allem stehenden Fragen sind die nach dem Grund, der Motivation bzw. dem Fernziel für die hier thematisierten Entwicklungen. Die Schaufensterprojekte sind dabei, diese Fragen zu beantworten. Durch Mechanismen für digitales Vertrauen soll ein rechtssicherer digitaler Raum entstehen, in dem

- Akteure aus Wirtschaft, Verwaltung und Gesellschaft im Zuge der Abwicklung von Geschäfts- und Verwaltungsprozessen eindeutig identifizierbar sind,
- Informationen verifizierbar und damit vertrauenswürdig sind und einen Wert besitzen,
- Transaktionen sicher und rechtskonform stattfinden und
- die Nutzer Hoheit über ihre eigenen Daten haben.

Wir nennen es Trustnet. Das Schaufensterprojekt ID-Ideal entwickelt in Abstimmung mit den anderen Schaufensterprojekten die Vision und die Roadmap zur Realisierung des Trustnets – der nächsten Evolutionsstufe des Internets. Das Trustnet ist das universelle digitale Abbild von Beziehungen zwischen Personen, Organisationen und Objekten der Realwelt. Es ermöglicht vertrauenswürdige und rechtskonforme digitale Interaktionen und verhindert Fake und Betrug. Die Grundlage dafür ist ein einheitlicher, skalierbarer Vertrauensmechanismus für den Austausch und die Prüfung von digitalen Nachweisen zu beliebigen Sachverhalten. Damit wird die Organisation von und der Zugang zu offenen digitalen Ökosystemen radikal vereinfacht. Die Erweiterung des bestehenden Internets der Informationen um das Trustnet ist eine der größten digitalen Herausforderungen der kommenden Jahrzehnte und eine globale, gesamtgesellschaftliche Aufgabe.

Die Entwicklung des Trustnets erfordert das Wachstum eines ID-Ökosystems als Basis für eine Vielzahl von Anwendungsökosystemen. Kommunikationswerkzeuge im Trustnet werden nicht Browser und

Email sein, sondern Wallets und Agents, die weitestgehend automatisiert miteinander kommunizieren. Anstelle der bisherigen Digitalisierung von Dokumenten, die zwar zur Ressourcenschonung und Zeitersparnis beiträgt, jedoch ein Defizit an Vertrauenswürdigkeit hinterlässt, kann im Trustnet die Digitalisierung und **Automatisierung von Prozessen** erfolgen, wodurch die Digitalisierung überhaupt erst ihr eigentliches Potential entfaltet. Dafür benötigen jedoch alle Akteure sichere digitale Identitäten. Das betrifft nicht nur natürliche Personen, sondern auch hoheitliche Akteure (z.B. Fachabteilungen von Kommunen, Behörden) und juristische Personen.

Ein wesentlicher Pfeiler des künftigen Trustnets wird die Entwicklung eines einheitlichen Trust Frameworks sein. Es soll als Strukturhilfe und Regelwerk mit Standards zum sicheren Interaktions-management digitaler Identitäten und digitaler Nachweise die Entstehung eines ID-Ökosystems anregen, in dem verschiedene ID-Dienste koexistieren können. Das Trustnet wird die bestehende Welt der zentral verwalteten Basisidentitäten inkl. eID und die neue SSI-Welt miteinander verbinden. Der Gedanke dieses Brückenschlags ist zwar bereits in die eIDAS-Novellierung eingeflossen, das Trust Framework soll aber darüberhinausgehend die technische, semantische und organisatorische Interoperabilität sicherstellen, damit Credentials unabhängig von der Art der Wallet-App und von der jeweiligen in der Vertrauensdomäne verwendeten Basistechnologie oder Dateninfrastruktur überprüft werden können. Dieser Gedanke ist in bestehenden bzw. in Entwicklung befindlichen Trust Frameworks, wie dem kanadischen PCTF, dem US-amerikanischen NIST 800-63 oder bei den entsprechenden EU-Aktivitäten (eIDAS-Novellierung) noch zu gering ausgeprägt. Deswegen wird zur Entwicklung des Trustnets ein auf diesen Arbeiten aufbauender Neuentwurf erforderlich. Grundlegende Überlegungen dazu finden im Rahmen der Schaufensterprojekte statt.

Das Trustnet entsteht durch Verschränkung und Interaktion vieler thematisch und/oder geographisch getrennter digitaler Vertrauensdomänen unter einem gemeinsamen Trust Framework.

4. Grundlegende Anforderungen an technische Lösungen und Anwendungsprozesse

Funktionale Mindestanforderungen an technische Lösungen der Akteure innerhalb des zukünftigen Trustnets sind:

1) Ausweisfunktion: Die sichere automatisierte Identifizierung eines Akteurs muss bei Bedarf möglich sein. Hierfür sollten Identifizierungsmittel auf allen Vertrauensniveaus für jede Art von Akteur verfügbar sein.
2) Nachweisfunktion: Die Herausgabe und automatisierte Prüfung von Nachweisen und einzelnen gesicherten Attributen muss möglich sein, auch ohne dass eine eindeutige Identifizierung erforderlich ist.
3) Technische, semantische und organisatorische/rechtliche Interoperabilität
4) Vertretungsfähigkeit: Neben Wallets für Bereitstellung einfacher Aus- und Nachweise werden auch Wallets und Verifiable Credentials für die Abbildung von persönlichen und juristischen Beziehungen gebraucht.

5) Privacy- und Vertragswerkzeuge zur Filterung und Binärisierung des Informationsgehaltes von Attributen bzw. zum Festlegen der Bedingungen für die Freigabe und Nutzung verifizierbarer Informationen.

Derzeit (Ende 2023) bildet die Technologiereife der in Entwicklung befindlichen Wallet-Apps und der anderen Technologiekomponenten diese Mindestanforderungen noch nicht in Gänze ab. Es ist jedoch nur eine Frage von Zeit und verfügbaren Entwicklungsressourcen, bis diese Ziele erreicht werden.

Anforderung A1: Angesichts der geplanten Wirkungsdimension der EUDI-Wallet und der damit zu erwartenden Kosten sollten o.g. Mindestanforderungen an technische Lösungen einer nachhaltigen Produktentwicklung zugrunde gelegt werden.

Funktionale Mindestanforderungen an Anwendungsprozesse innerhalb des künftigen Trustnets sind:

6) sichere und eindeutige Identifizierbarkeit aller am Prozess beteiligten Akteure (inkl. Herausgeber und Akzeptanzstelle)
7) umfassende Überprüfung aller innerhalb des Prozesses ausgetauschten Informationen
8) eindeutige Definition der Prozessabläufe, Rollen, Rechte, Kontrollorgane und Regularien inkl. der Sanktionierungsmechanismen innerhalb des Anwendungsökosystems
9) DSGVO-konforme Datenverarbeitung
10) optionale Redundanz, d.h. die Möglichkeit, bei Bedarf den Wahrheitsgehalt bzw. die Aktualität von Informationen zu prüfen

Anforderung A2: Soll die EUDI-Wallet im Rahmen von digitalen Verwaltungs- und Geschäftsprozessen zum Einsatz kommen, dann muss sie den o.g. Mindestanforderungen an Anwendungsprozesse mit ihrer Funktionalität Rechnung tragen.

Die bisherige Diskussion in Fachwelt und Politik fokussierte stark auf die technischen Aspekte der Ausstellung hoheitlicher digitaler Identifizierungsmittel und anderer Credentials in eine Wallet. Es ist aber evident, dass die o.g. funktionalen und prozessseitigen Anforderungen weder allein durch die Verfügbarkeit der eID in einer Wallet, noch allein durch das Ausstellen anderer Verifiable Credentials erfüllt werden können. Der Entwurf eines nachhaltigen ID-Ökosystems erfordert einerseits eine *strukturierte ganzheitliche Betrachtung* und andererseits eine *detaillierte Betrachtung der digitalen Anwendungsprozesse* über den gesamten Lebenszyklus der dafür erforderlichen Credentials.

5. Das Erklärmodell

Die Basis für die o.g. ganzheitliche Betrachtung bildet der in Abb. 1 dargestellte Trustnet-Stack, der maßgeblich auf dem von der Trust Over IP Foundation entwickelten Trust over IP-Stack[1] beruht, welcher u.a. auch bei den eID-Konsultationen in der Schweiz Diskussionsgrundlage ist.[2] Der Stack soll angesichts der Komplexität der Thematik als Orientierungshilfe zur Strukturierung der Diskussion

[1] https://trustoverip.org/wp-content/toip-model/
[2] https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/staatliche-e-id/partizipationsmoeglichkeiten.html

dienen. Der technische Teil des ID-Ökosystems sind Ebene 1 und 2 und der organisatorische Teil des ID-Ökosystems sind die ID-Lösungen für sämtliche Akteure auf Ebene 3. Damit bildet das ID-Ökosystem die Basis für die Anwendungsökosysteme in Ebene 4.

Die Entwicklung von Anwendungen ist – unabhängig vom zu digitalisierenden Prozess - ein komplexer Vorgang. Der Trustnet-Stack verdeutlicht, dass bei jeder geplanten Anwendung nicht nur die einzusetzenden *technischen Komponenten* auf allen vier dargestellten Ebenen festgelegt werden müssen. Es muss auch die *Governance* auf allen vier Ebenen des Trustnet-Stacks geregelt und organisiert werden. Hinzu kommen die Definition, Umsetzung und Pflege erforderlicher Dateninfrastrukturen (Vertrauensregister) auf allen vier Ebenen, die für die Überprüfbarkeit von Informationen eine entscheidende Rolle spielen.

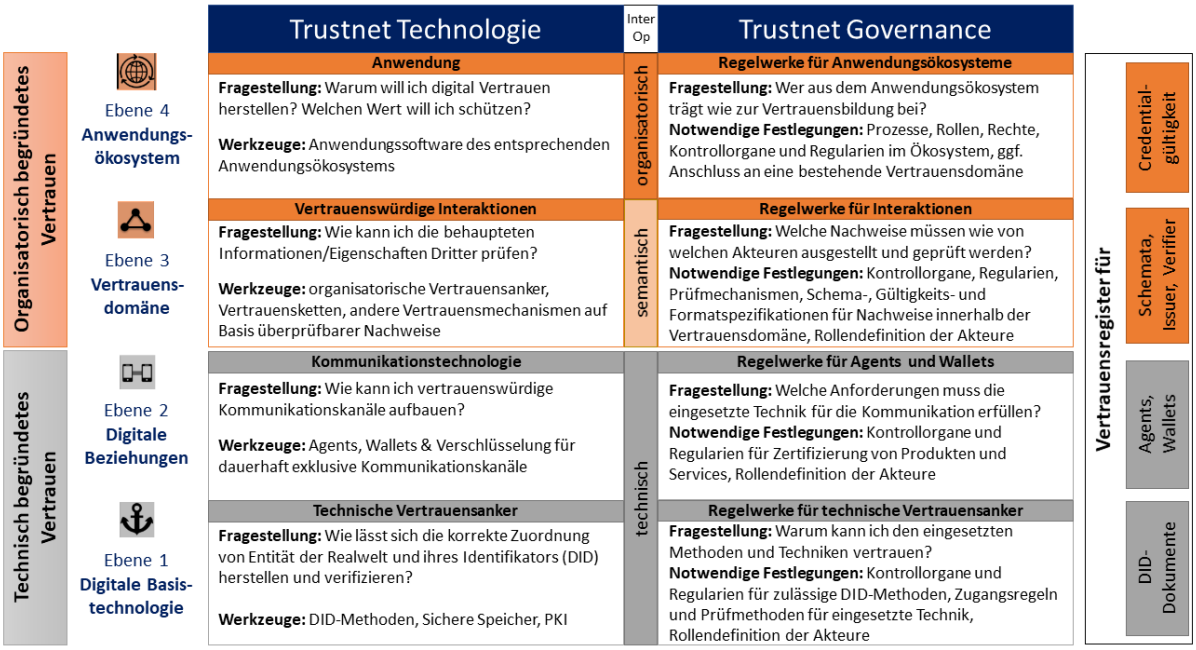

Abb. 1: Trustnet-Stack

<u>Anforderung A3:</u> Die technische Ausgestaltung von Vertrauensregistern ist vom jeweiligen Anwendungsfall und vom IT-Umfeld der jeweiligen Vertrauensdomänen bzw. Anwendungsökosysteme abhängig und muss daher generell technologieoffen angegangen werden.

6. Kommunale Anwendungsszenarien

Die kommunalen Anwendungsszenarien dienen im Rahmen der Schaufensterprojekte der detaillierten Untersuchung digitaler Anwendungsprozesse über den gesamten Lebenszyklus der dafür erforderlichen Credentials. Bleiben sie technologieoffen und unbehelligt von staatlicher Regulierung, bieten sie die Möglichkeit zu lernen, wie ID-Ökosysteme und Anwendungsökosysteme zusammenwirken müssen, um nachhaltig Vertrauen in die digitale Welt zu übertragen.

6.1. Vertrauen durch Überprüfbarkeit

Die öffentliche Verwaltung muss organisatorische Vertrauensanker in die digitale Welt setzen. Voraussetzung sind dafür Autorität und sichere Prozesse seitens der beteiligten hoheitlichen Akteure, die als Herausgeber, Akzeptanzstellen und auch als Halter digitaler Nachweise fungieren können. Perspektivisch sind solche organisatorischen Vertrauensanker alle überprüfbaren digitalen Nachweise, die hoheitliche Akteure an natürliche und juristische Personen ausstellen. Die Ausstellung jedes Nachweises, egal ob Ausweis-Credential, Registerauszug, Bild-Credential oder amtlicher Bescheid, in eine wie auch immer geartete Wallet muss in Form von Verifiable Credentials (idealerweise nach W3C-Standard) erfolgen, anhand deren jede für die Anwendung relevante Akzeptanzstelle prüfen kann,

- wer Herausgeber des Nachweises war (Signatur des Herausgebers),
- an wen der Nachweis herausgegeben wurde (Identifikator des Inhabers),
- ob der Inhalt des Nachweises noch authentisch ist (Hash),
- ob der Nachweis noch gültig ist (Gültigkeitsregister),
- ob der Herausgeber berechtigt war, diesen Nachweis herauszugeben (Register der Issuer)
- ob das Schema des vorgezeigten Nachweises korrekt ist (Register der VC-Schemata)

Optional kann perspektivisch geprüft werden

- ob die Kommunikationsmittel (Wallet, Agent) des Inhabers den Prozessanforderungen der Kommune genügen (Register der Wallets und Agents)
- ob der Identifikator des Inhabers der Kommune bekannt ist (DID-Register)

Hat der Eigentümer der Wallet in einem Anwendungsprozessschritt die Rolle des Inhabers (Holders), so muss bei Anfrage einer Akzeptanzstelle die Identität derselben und ihre Berechtigung zum Stellen der Anfrage geprüft werden können (Register der Verifier).

<u>Anforderung A4:</u> Eine Wallet-App, die im Kontext kommunaler Anwendungsszenarien auf Seiten natürlicher oder juristischer Personen eingesetzt werden können soll, muss mit den zentralen und/oder dezentralen Vertrauensregistern der jeweiligen Kommune kommunizieren und die o.g. Prüfungen eines Verifiable Credentials zur Beantwortung der entsprechenden Vertrauensfragen vornehmen können.

Die am Markt verfügbaren Wallets von Apple/Google/Samsung etc. erfüllen diese Anforderung derzeit nicht. Somit ist unklar, worauf sich bei dieser Art Wallets das Vertrauen gründen soll. Die im Rahmen der Schaufensterprojekte stattfindenden Wallet-Entwicklungen zielen hingegen explizit darauf ab, diese Anforderungen zu erfüllen.

6.2. Rollenverteilung in realen Geschäftsprozessen

Ein Akteur kann bei unterschiedlichen digitalen Interaktionen unterschiedliche Rollen einnehmen:

Der *Herausgeber (Issuer)* ist ein Akteur, der einen digitalen Nachweis ausstellt und dem Nachweis-Inhaber übergibt. Im Ausstellungsprozess wird durch eine digitale Signatur sichergestellt, dass der Nachweis vom Herausgeber selbst stammt und dass er auf den korrespondierenden kryptografischen Schlüssel des Inhabers ausgestellt ist. Gleichzeitig kümmert sich der Herausgeber darum, dass die ausgestellten Nachweise ungültig gemacht werden, falls notwendig. Im Hinblick auf die hohe Vertrauenswürdigkeit hoheitlicher Register wurde für diese der Begriff *Trusted Issuer* geprägt.

Der *Inhaber (Holder)* ist ein Akteur, welcher digitale Nachweise vom Herausgeber entgegennimmt und sie sicher in seiner Wallet speichert. Die digitalen Nachweise des Inhabers können unabhängig vom Herausgeber gegenüber anderen Parteien präsentiert werden.

Die *Akzeptanzstelle (Verifier)* ist ein Akteur, welcher den Nachweis vom Inhaber anfordert bzw. entgegennimmt und ihn auf Richtigkeit überprüft. Anhand des Ausstellungsprozesses vertraut die Akzeptanzstelle dem Herausgeber und gewährt dem Nachweis-Inhaber nach erfolgreichem Prüfprozess die angefragten Rechte.

Der *Modifizierer (Modifier)* ist ein Akteur, der in enger Beziehung zum Herausgeber steht und die Möglichkeit hat, den Nachweisstatus zu ändern. Oft ist der Herausgeber gleichzeitig auch der Modifizierer, jedoch gibt es einige Fälle, bei denen der Modifizierer eine separate Partei ist, z.B. die Polizei, die den digitalen Führerschein nach einem Verkehrsdelikt entzieht oder ein Ticket-Entwerter, der beim Vorzeigen eines Tickets dieses entwertet.

Die für diese Interaktionen erforderliche Wallet-App auf dem digitalen Endgerät des Inhabers besteht aus der Wallet, in der die Nachweise gespeichert werden, und einem digitalen Agent. Der Agent übernimmt dabei die digitale Kommunikation inkl. der Herausgabe und Prüfung von Nachweisen.

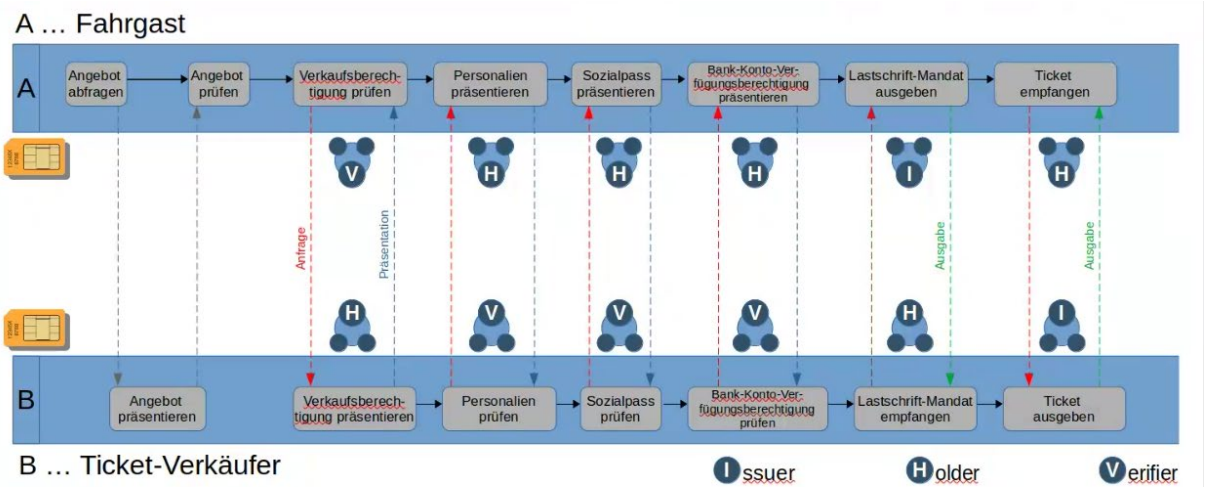

Abb. 2: Wechselnde Rollen in einem digitalen Geschäftsprozess

Bei Erklärungen zum SSI-Prinzip wird die Rollenverteilung üblicherweise als einfache Dreiecksbeziehung zwischen Herausgeber, ID-Inhaber und Akzeptanzstelle dargestellt. Die Dreiecksbeziehung entsteht, indem die Akzeptanzstelle die Herausgeberschaft eines vom Inhaber präsentierten Nachweises prüft. Betrachtet man allerdings den gesamten Geschäftsprozess einer realen Anwendung, wird schnell klar, dass diese Rollenverteilung sich nur auf einen einzelnen Prozessschritt bezieht. Selbst innerhalb eines einfach erscheinenden Anwendungsprozesses, wie dem Kauf eines ÖPNV-Tickets, nehmen Käufer und Verkäufer nacheinander unterschiedliche Rollen ein. Das in Abb. 2 dargestellte Prozessbeispiel des Online-Kaufs einer ermäßigten ÖPNV-Monatskarte zeigt, dass innerhalb des rein digitalen Geschäftsprozesses sowohl Käufer als auch Verkäufer jeweils drei verschiedene Rollen einnehmen und dabei auch verschiedene Nachweise austauschen müssen. Gleiches gilt auch bei Interaktion des Bürgers mit der Verwaltung im Rahmen anderer Anwendungsszenarien. Entsprechend muss für diese Variabilität auf beiden Seiten die dafür erforderliche Funktionalität und Interoperabilität bei Wallet und Agent gegeben sein.

<u>Anforderung A5:</u> Eine Wallet-App, die im Kontext kommunaler Anwendungsszenarien eingesetzt werden können soll, muss in der Lage sein, sowohl die Rolle des Inhabers, als auch die des Herausgebers und der Akzeptanzstelle einzunehmen.

Idealerweise erhalten die Wallets der Interaktionspartner während eines Geschäftsprozesses bzw. eines kommunalen Anwendungsprozesses ihre Verbindung anhand ihrer Identifikatoren aufrecht (wie z.B. bei Verwendung des DIDCommV2-Protokolls), so dass nicht für jeden einzelnen Interaktionsschritt innerhalb des Anwendungsprozesses eine neue gegenseitige Identifizierung/Authentifizierung erforderlich ist. Letzteres scheint jedoch bei der auf den OpenID-Protokollen basierenden Entwürfen zur EUDI-Infrastruktur der Fall zu sein. D.h. die im aktuellen Entwurf von eIDAS, ARF und EUDI-Infrastruktur festgelegten Protokolle erlauben nur die sichere Digitalisierung einzelner Prozessschritte, keiner vollständigen Anwendungsprozesse. Der theoretisch denkbare Ausweg einer Bündelung einzelner Interaktionen/Prozessschritte in einer gemeinsamen Authenfizierungssession bietet bekanntermaßen Angriffsfläche für Cyberkriminalität. Damit scheint der aktuelle Infrastruktur-Entwurf aus Usability-Aspekten heraus für kommunale Anwendungsszenarien und auch andere Geschäftsprozesse ungeeignet zu sein.

<u>Anforderung A6:</u> Eine EUDI-Infrastruktur die im Kontext kommunaler Anwendungsszenarien eingesetzt werden können soll, muss nachweislich in der Lage sein, vollständige Geschäfts- und Anwendungsprozesse abzubilden, ohne für jeden einzelnen Prozessschritt eine neue gegenseitige Identifizierung/Authentifizierung der Interaktionspartner zu erfordern.

6.3. Kommunale Anwendungsszenarien in den Schaufensterprojekten

Folgende kommunale Anwendungsszenarien werden in den SDI-Schaufensterprojekten ONCE und ID-Ideal entwickelt:

- Kommunale Datenkarte (kDK)
- Sozialpass (kDK-Verfügbarkeit kann als Voraussetzung dienen)
- Digitales Bürgerbegehren (kDK-Verfügbarkeit kann als Voraussetzung dienen)
- Kur- und Gästekarte / -taxe (kDK-Verfügbarkeit kann keine Voraussetzung sein)
- Bibliothekswesen (kDK-Verfügbarkeit kann als Voraussetzung dienen)
- ÖPNV-Tickets (kDK-Verfügbarkeit kann keine Voraussetzung sein)
- …

Die kommunale Datenkarte, die Kur- und Gästekarte und der Sozialpass werden in verschiedenen Varianten entwickelt, so dass Inhalt, Prozess und technologische Basis nicht einheitlich beschrieben werden können. Eine Beurteilung, welche Variante in der praktischen Erprobung die besten Ergebnisse erzielt und die höchste Chance auf Transfer in andere Kommunen hat, ist beim derzeitigen Stand der Entwicklungen noch nicht möglich.

Die Einbindung der eID in diese Anwendungen, z.B. zum Identifizieren / Authentifizieren gegenüber dem Herausgeber des anwendungsspezifischen Verifiable Credentials, ist derzeit aufgrund der hohen technischen Anforderungen und Kosten der eID-Nutzung nicht sinnvoll darstellbar. Auch die weniger aufwändige Integration von Nutzerkonten (z.B. BundID) bringt Hürden mit sich. In diesem Falle wird der Nutzer mit mindestens drei Technologien (Fachprozess, Nutzerkonto und AusweisApp oder EUDI-

Wallet) konfrontiert, was hinsichtlich der Usability zu Problemen führt. Einfache, schnelle und integrative Prozesse, insbesondere auch on-site, sind hiermit nicht vorstellbar. Deswegen und als Basis für unterschiedliche kommunale Use Cases wurde hierfür die kommunale Datenkarte (kDk) entwickelt.

7. Die kommunale Datenkarte

7.1. Definition

Die kommunale Datenkarte (Arbeitstitel) ist ein kommunales Basis-Credential, das in verschiedenen kommunalen Anwendungen zum Einsatz kommen kann. Sie entspricht im Kern einem verifizierbaren Auszug aus dem Melderegister, der mehr Attribute enthält als die eID. Der Umfang der Attribute ist maßgebend dafür, welche kommunalen Anwendungen damit unterstützt werden. Mit der kDK bzw. den Attributen wird die eindeutige Identifikation eines Einwohners einer Kommune im Rahmen kommunaler Angelegenheiten ermöglicht. Die Daten einer kDK entstammen aus einem kommunalen Register. Sie wurden im Rahmen eines Verwaltungsverfahrens - z.B. der Anmeldung am Wohnort, der Beantragung eines Personalausweises oder eines Aufenthaltstitels - von einer Kommunalbehörde auf Basis einer Rechtsgrundlage (z.B. dem Melderecht oder dem Personalausweisrecht) erhoben und werden gemäß den rechtlichen Vorgaben von der Kommune vorgehalten und gepflegt.

Der kDK-Datensatz wird von einem Einwohner auf der Basis des Selbstauskunftsrechts der DSGVO (§15 Abs. 3) von der datenführenden Kommunalbehörde angefordert. Damit initiiert der Einwohner die Ausstellung des Identifikationsmittels kDK. Der Inhaber (Holder) einer kDK ist der Einwohner, der Herausgeber (Issuer) einer kDK ist die datenführende kommunale Behörde (Stadt oder Gemeinde).

Mit Hilfe der kommunalen Datenkarte können personenbezogene Attribute automatisiert in kommunalen Anwendungsprozessen präsentiert, ausgelesen und in Formulare eingefügt werden. **Der Vorteil einer kommunalen Datenkarte ist, dass sie explizit nicht der Regulierung auf Landes-, Bundes- oder EU-Ebene unterliegt, sondern unter der Hoheit der jeweiligen Kommune deren jeweiligen Bedürfnissen in technischer und organisatorischer Sicht entsprechend ausgestaltet werden kann.** D.h. die Kommune entscheidet, ob und in welcher Ausprägung sie eine kommunale Datenkarte ausgibt und welche eigenen Anwendungsprozesse damit unterstützt werden sollen.

Anforderung A7: Die kommunale Datenkarte darf nicht unter die Regulierung und Governance der eIDAS 2.0-Infrastruktur fallen.

Anforderung A8: Eine Wallet-App, die mit jeder Ausprägung der kommunalen Datenkarte interoperabel sein soll, muss hinsichtlich Austauschprotokollen, Schnittstellen, Formaten und Schemata der Verifiable Credentials technologieoffen sein.

Die Bandbreite der in Entwicklung befindlichen Ausprägungen lässt zwar prinzipiell die Zuordnung von verschiedenen eIDAS-Vertrauensniveaus als möglich erscheinen. Da die verschiedenen Prozesse für Ausstellung, Anwendung und Sperrung der kommunalen Datenkarte in sämtlichen Ausprägungen noch Gegenstand der laufenden F&E-Aktivitäten sind, kann jedoch noch keine wie auch immer geartete Aussage zu künftigen/intendierten Sicherheits- oder Vertrauensniveaus getroffen werden.

<u>Anforderung A9:</u> Da die kommunale Datenkarte ausschließlich kommunale Anwendungen unterstützen soll, obliegt die Einstufung der Vertrauenswürdigkeit bei Bedarf der jeweils implementierenden Kommune.

Der Mindestumfang eines kDK-Datensatzes besteht aus den folgenden Daten:

Daten aus einem kommunalen Register

- Familienname (1)
- Vorname (2)
- Geburtsdatum (3)
- Geburtsort (4)
- PLZ (5)
- Wohnort (6)
- Straße (7)
- Hausnummer (8)
- Lichtbild (9)

Ausstellungsdaten

- Datum der Ausstellung (A)
- Datenquelle (Register) (Q)
- letzter Tag der Gültigkeit der kDK (G)
- datenführende Behörde (B)
- Datensatztyp kDK (T)

Darüber hinaus können weitere Daten, z.B. das Zuzugsdatum oder die Adresse des Nebenwohnsitzes, aus einem kommunalen Register ergänzt werden. Den Attributsumfang bestimmt die Kommune anhand des Bedarfs der in ihrem Hoheitsbereich zu unterstützenden Anwendungsprozesse.

7.2. Basiseigenschaften

Das Konzept und die Demonstratoren zur kDK haben zurzeit einen experimentellen Status. Belastbare Aussagen zu Basiseigenschaften und daraus ableitbare konkrete Anforderungen an eine im Kontext der kDK zu verwendende Wallet-App lassen sich erst nach einer praktischer Erprobung in einer kommunalen Anwendung ableiten. Dies gilt insbesondere für technische und organisatorische Eigenschafteneiner kDK. Die hier aufgeführten Anforderungen haben daher konzeptionellen Charakter und spiegeln den aktuellen Stand der Diskussion in den Konsortien ONCE und ID-Ideal.

Rechtliche Eigenschaften

- Selbstauskunftsrecht nach DSGVO als Rechtsgrundlage für die Ausstellung einer kDK
- rechtssichere Nachvollziehbarkeit der Authentizität des Ausstellers des vollständigen Datensatzes und einzelner Daten (z.B. über digitales Siegel)
- Haftungsausschluss des Ausstellers für Aktualität/Korrektheit der Daten

Funktionale Eigenschaften

- Selektive Verifikation des Alters
- Selektive Verifikation der Kombination Familienname und Vorname
- Selektive Verifikation der Adresse
- Selektive Verifikation der Einwohnerschaft
- Selektive Verifikation des Lichtbilds

Selektiv meint in diesem Kontext die Abfrage und Übermittlung ausschließlich der Attribute, die zur Klärung des Sachverhalts erforderlich sind (selective disclosure).

Technische Eigenschaften

- Zugangs- und Nutzungssicherung der kDk über biometrische Authentifizierung oder PIN in der mobilen App / Wallet-App
- Verwaltung der kDk in geeigneter Smartphone-Anwendung. Dieses kann auch eine kommunale App (z.B. Städte-App) sein.
- App-Neutralität, d.h. keine Prüfung der Beschaffenheit einer App durch einen Aussteller, die über notwendige technische Belange hinausgeht
- Verwendung Prozess-unterstützender Protokolle, die mehrere Transaktionen (Present Proof, Issue Credential) innerhalb eines Authentifizierungszyklus ermöglichen
- Geräte-Neutralität, d.h. keine Prüfung der Beschaffenheit eines mobilen Endgeräts durch einen Aussteller, die über notwendige technische Belange hinausgeht
- keine Bindung an ein konkretes einzelnes Kommunikationsgerät (z.B. Smartphone)
- Technikneutralität, d.h. keine Bindung an ein Datenformat für Credentials oder ein Übertragungsformat für den Austausch von Credentials
- exemplarische Datengruppen, die digital gesiegelt an Akzeptanzstellen übermittelt werden können (das Beispiel nutzt die Datennummerierung unter 7.1)

.	digitale Personenidentifikation	(1)+(2)+(3)+(4)	+(G)+(T)
.	Personenidentifikation	(1)+(2)+(3)+(4)+(9)	+(G)+(T)
.	Adressidentifikation	(5)+(6)+(7)+(8)	+(G)+(T)
.	Wohnortidentifikation	(5)+(6)	+(G)+(T)
.	Altersverifikation	(3)	+(G)+(T)
.	Sichtausweisfunktion	(1)+(2)+(3)+(9)	+(G)+(T)

Ökonomische Eigenschaften

- kostenfreie Erstausstellung, Verlängerung und Aktualisierung einer kDk (gemäß DSGV §15, Abs, 3)

Organisatorische Eigenschaften

- kurze Gültigkeitsdauer (vergleichbar Meldebescheinigung, z.B. 6 oder 12 Monate)
- Verlängerung der Gültigkeit über einfachen digitalen Prozess mit Authentisierung mittels kDK
- keine verpflichtende Dokumentations-, Nachweis- oder Auskunftspflicht des Ausstellers
- keine Sperrpflicht bei Verlust des mobilen Endgeräts durch Einwohner oder Aussteller
- keine Änderung oder Aktualisierung von kDK-Daten auf dem Endgerät

- prinzipielle Überprüfbarkeit der Authentizität von kDK-Daten ohne technische Verbindung zum Aussteller (ggf. durch Verifikation eines digitalen Siegels mittels eines Prüfsiegels)
- optional: Bindung an eine verifizierte E-Mail-Adresse des Einwohners

weitere Eigenschaften

- n.n.

Anforderung A10: Wenn eine EUDI-Wallet sowie ggf. weitere Komponenten einer EUDI-Infrastruktur und deren organisatorischer Rahmen im Kontext kommunaler Anwendungen eine Rolle spielen sollen, müssen sie die sich aus den Basiseigenschaften der kommunalen Datenkarte logisch ableitbaren Mindest-Spezifikationen erfüllen.

8. Anforderungen aus Kostensicht der Kommunen

Klamme Kassen der Kommunen setzen künftigen Kostenmodellen für ID-Ökosysteme klare Grenzen. Der derzeitige eIDAS-Entwurf billigt Vertrauensdiensten eine systemrelevante Rolle zu, was es einerseits (analog zur Bankenkrise) schwierig macht, einen möglichen Vertrauensverlust gegenüber einem solchen Vertrauensdienstleister konsequent zu ahnden, und was andererseits enorme Kosten auf Seiten der Kommunen produziert, wenn sie verpflichtet werden, diese Vertrauensdienste zu nutzen. Das betrifft einerseits die Investitionskosten aber vor allem die operativen Kosten für die Einbindung einer eventuellen eIDAS-Infrastruktur inkl. Vertrauensdienstleistungen in kommunale Fachanwendungen. ID-Lösungen für hoheitliche Akteure mindestens auf Ebene der kommunalen Fachabteilungen sind erforderlich, um Dokumente in Form von Verifiable Credentials signieren zu können. Nach Einschätzung von D-Trust sind ID-Lösungen für kommunale Akteure mit einer solchen Granularität und die damit verbundenen Kosten eines Vertrauensdienstes (Siegelung der Credentials anstelle der Kommune) durch eine deutsche Kommune finanziell nicht leistbar.

Ähnliches gilt für die EUDI-Wallet. Es steht nach aktuellem Diskussionsstand zu befürchten, dass es in Europa pro Staat eine andere EUDI-Wallet geben wird und dass die Kommunen ab 2025 verpflichtet werden, mit jeder in Europa existierenden staatlichen Einzellösung interagieren zu können. Unabhängig davon, dass fachlicher und finanzieller Aufwand der Entwicklung und Implementierung bei dieser geringen Technologie- und Anwendungsreife in keinem Verhältnis zum erwarteten Nutzen stehen, wird diese Pflicht eine unverhältnismäßig hohe finanzielle Belastung der Kommunen darstellen.

Anforderung A11: Die EUDI-Wallet und weitere ggf. erforderliche technische Komponenten/ Infrastruktur sollten den Kommunen kostenlos bereitgestellt werden.

Die EU-weite Verpflichtung zur Herausgabe einer eID und die im Hoheitsbereich einer Kommune zu digitalisierenden Prozesse haben regulatorisch nichts miteinander zu tun. Künftige eID-/EUDI-Infrastrukturen können und sollten daher den **Charakter eines Angebots an die Kommunen** im Sinne einer Unterstützung für ihre eigenen Prozesse haben.

Anforderung A12: Keinesfalls kann eine Verpflichtung zur Nutzung einer eID-/EUDI-Infrastruktur im Kontext kommunaler Aufgaben definiert werden. Dies würde die Kosten kommunaler Prozesse explodieren lassen und der Verwaltungsdigitalisierung massiv entgegenwirken.

Um den regulatorischen Anforderungen der eIDAS gerecht zu werden, müssten Kommunen entsprechende Verfahren und spezialisierte Dienstleistungen von Trust Service Providern (TSP) nutzen oder sogar selbst als TSP fungieren. Sollte eine Kommune selbst als TSP agieren, würden damit Anforderungen für die Einhaltung strenger Sicherheitsstandards und entsprechende Forderungen aus Zertifizierungs- und Auditverfahren einhergehen. Derzeit ergibt sich diese Notwendigkeit noch nicht, sollte man aber insbesondere als Aussteller im Kontext der eID-/EUDI-Infrastruktur agieren (z.B. bei Änderung von Personalausweis und eID wegen Umzug des Inhabers), müsste man dies betrachten. Nach jetzigem Kenntnisstand ergeben sich damit Anforderungen aus Kostensicht an Kommunen in den Kostenpositionen:

- **Initialkosten:** Kosten für die Einrichtung der erforderlichen Infrastruktur, Software, Hardware und Sicherheitssysteme.
- **Betriebskosten:** Laufende Kosten für Wartung, Personal, Sicherheitsupdates und Audits.
- **Zertifizierungskosten und Audit-Kosten:** Gebühren für die Zertifizierung und regelmäßige Überprüfungen in Form von Audits durch akkreditierte Stellen.
- **Schulungskosten:** Kosten für die Schulung des Personals in Bezug auf Sicherheit, Datenschutz und technische Verfahren.
- **Risikomanagement und Versicherung:** Kosten für Risikomanagementmaßnahmen und möglicherweise für Versicherungen gegen Sicherheitsverletzungen oder Ausfallzeiten.

Anforderung A13: Sollte der Bund die Kommunen verpflichten wollen, die unter seine Regulierungskompetenz fallenden Anwendungen bzw. Prozessschritte in seinem Auftrag nach Vorgaben der eIDAS-Verordnung umzusetzen, sind konkrete Pflichten, Risiken und damit einhergehende Kosten den Kommunen öffentlich zu machen und zur Diskussion zu stellen. Der Bund als Auftraggeber muss vor der Durchsetzung die Kostendeckung für die Kommunen sicherstellen.

9. Anforderungen aus technischer und organisatorischer Sicht der Kommunen

Die vertrauenswürdige Digitalisierung von Anwendungsprozessen der Kommunen erfordert deutlich mehr als nur die Ausstattung des Bürgers mit einer EUDI-Wallet. Jede Fachabteilung, die Verifiable Credentials herausgeben, prüfen und akzeptieren soll, braucht Software-Komponenten für die Realisierung der gesamten Prozesskette.

Identitätslösungen für hoheitliche Akteure und juristische Personen des Privatrechts sowie des öffentlichen Rechts sind im Rahmen der EUDI-Infrastruktur bislang nicht geplant, im Rahmen kommunaler Anwendungen aber zwingend erforderlich. Diese Notwendigkeit wurde auch im Rahmen der bisherigen eIDAS-Regulierung komplett ignoriert. Diese Aufgaben obliegen somit den Kommunen,

was zumindest dahingehend sinnvoll ist, dass sie bedarfsgerecht und entsprechend der jeweils vorhandenen kommunalen IT-Landschaft gelöst werden müssen.

Neben den im EUDIW-Spezifikationsentwurf beschriebenen Wallet-Apps werden Server-basierte Wallet-Services für den Einsatz innerhalb von Organisationen benötigt (Organisationswallets). Die rechtlich verankerte Souveränität der Organisationen darf nicht durch übertriebene Zertifizierungszwänge und erzwungene Integration von am eigentlichen Prozess unbeteiligten Dritten eingeschränkt werden. Vielmehr muss es Organisationen unter Verwendung eigener Wallet-Services ermöglicht werden, Credentials im eigenen Namen oder in legitimierter Vertretung Dritter auszustellen, Credentials zu halten und Credentials zu verifizieren.

Auch Softwarelösungen für Registerabfragen zum Erzeugen von überprüfbaren Nachweisen sind im Rahmen der EUDI-Infrastruktur nicht geplant. Auch diese Aufgabe obliegt den Kommunen und muss entsprechend der jeweiligen Registersoftware gelöst werden. Gleiches gilt für Softwarelösungen zur automatisierten Abfrage von Attributen und Integration abgefragter Attribute in Dokumente und Prozesse der Akzeptanzstellen. Komponenten einer EUDI-Infrastruktur, die mit den Komponenten der Kommunen interagieren können sollen, müssen leicht in die kommunale IT-Umgebung integrierbar sowie technisch und semantisch interoperabel sein.

Idealerweise erfolgt die Bereitstellung technischer Komponenten auch in Form von Software Development Kits (SDK) zur Einbindung in Städte-Apps und städtische Hintergrundsysteme. Insbesondere für eine Übergangszeit bis zur Etablierung zentraler Wallet-Apps, aber auch aus Gründen der Usability und Integration in kommunale Anwendungen, wäre die Nutzung von ID-SDK's äußerst attraktiv. Im Falle einer Städte- oder Tourismus-App für Gäste, welche nicht in Deutschland leben und somit keine bundeseinheitliche Wallet benutzen, ist die Integration kommunaler Credentials in einer mobilen, fachorientierten App ebenfalls sinnvoll.

Die Bereitstellung von SDK's hätte mehrere Vorteile:

- **Anpassbarkeit:** SDKs ermöglichen es Kommunen, maßgeschneiderte Lösungen zu entwickeln, die speziell auf ihre Bedürfnisse und die ihrer Bürger zugeschnitten sind.
- **Integration von Drittanbieter-Diensten:** Durch SDKs können Kommunen leichter Dienste von Drittanbietern, wie Zahlungssysteme oder interaktive Karten, in ihre Apps integrieren.
- **Datensicherheit und Datenschutz:** Mit eigenen Apps können Kommunen bessere Kontrolle über Datensicherheit und Datenschutz gewährleisten, was bei der Nutzung von Diensten externer TSPs möglicherweise schwieriger ist.
- **Skalierbarkeit:** Die App kann bei wachsenden Anforderungen oder zur Einführung neuer Dienste leicht aktualisiert und erweitert werden.
- **Nachnutzung mit einheitlichen Standards:** Die Basistechnologien können durch individuelle Lösungen (z.B. ein kommunales Credential in einer Städte-App oder eine Gästekarte in einer Tourismus-App) nachgenutzt werden. Hierdurch müssen keine proprietären Technologien entwickelt und gehärtet werden.

Um die Interoperabilität zu gewährleisten, müssten diese SDK's auf gemeinsamen Standards und Protokollen basieren, welche im Vorfeld festgelegt werden müssten.

- **Standardisierte Schnittstellen:** SDKs können standardisierte Schnittstellen und APIs (Application Programming Interfaces) bereitstellen, die es verschiedenen Kommunen ermöglichen, ihre Systeme und Apps miteinander zu verbinden.

- **Gemeinsame Datenformate:** Durch die Verwendung gemeinsamer Datenformate und Protokolle können SDKs den Austausch und die Verarbeitung von Daten zwischen unterschiedlichen kommunalen Systemen erleichtern.
- **Modulare Architektur:** SDKs können eine modulare Architektur unterstützen, die es Kommunen ermöglicht, bestimmte Funktionen oder Dienste zu integrieren, die von anderen Kommunen entwickelt wurden, ohne die gesamte App neu entwickeln zu müssen.
- **Kompatibilität mit verschiedenen Plattformen:** SDKs können so gestaltet sein, dass sie mit verschiedenen Betriebssystemen und Plattformen kompatibel sind, was die Entwicklung von plattformübergreifenden Lösungen erleichtert.

Anforderung A14: Wenn nicht nur die EUDI-Wallet sondern ggf. auch weitere Komponenten einer EUDI-Infrastruktur und deren organisatorischer Rahmen im Kontext kommunaler Anwendungen eine Rolle spielen sollen, müssen sie hinsichtlich Austauschprotokollen, Schnittstellen, Formaten und Schemata der auszutauschenden bzw. zu prüfenden Informationen technologieoffen und flexibel anpassbar sein. Idealerweise erfolgt Bereitstellung technischer Komponenten in Form von Software Development Kits (SDK) zur Einbindung in Städte-Apps und städtische Hintergrundsysteme.

Derzeit ist der Ausstellungsprozess der PID in die EUDI-Wallet vollkommen unklar. Die Kommunen sind mit Bürgerämtern und deren Verfahren derzeit Teil der Infrastruktur und Prozesse für die Ausstellung und Verteilung des Personalausweises, dem Chipkarten-basierten Pendant der PID. Wenn die Kommunen auch im Rahmen der EUDI-Infrastruktur verantwortlich sein sollen für den initialen Ausgabeprozess bzw. für Änderungsprozesse (z.B. Bürger zieht innerhalb der Kommune um oder in eine andere Kommune), stehen o.g. Kostenargumente und technischer Aufwand als Innovationsbarrieren.

Wenn eine Kommune selbst als TSP nach eIDAS fungiert, könnte sie mit den entsprechenden Diensten in den Bereich der kritischen Infrastrukturen (KRITIS) fallen, insbesondere wenn ihre Dienste für die Aufrechterhaltung wichtiger gesellschaftlicher und wirtschaftlicher Funktionen unerlässlich sind. KRITIS bezieht sich auf Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe, Gefährdung der öffentlichen Sicherheit oder andere dramatische Folgen hätte. Die Einstufung als KRITIS hätte verschiedene Implikationen für eine Kommune, welche sowohl finanziellen Aufwand als auch notwendige organisatorische Prozesse fordern:

- **Erhöhte Sicherheitsanforderungen:** Es müssen strengere Sicherheitsmaßnahmen eingehalten werden, um die Zuverlässigkeit und Verfügbarkeit der kritischen Dienste zu gewährleisten. Dies umfasst sowohl physische als auch IT-Sicherheit.
- **Regelmäßige Risikoanalysen:** Die Kommune müsste regelmäßig Risikoanalysen durchführen, um potenzielle Schwachstellen zu identifizieren und entsprechende Gegenmaßnahmen zu ergreifen.
- **Meldepflicht bei Sicherheitsvorfällen:** Im Falle von Sicherheitsvorfällen besteht eine Meldepflicht gegenüber den zuständigen Behörden. Diese Meldungen müssen in der Regel schnell und detailliert erfolgen.
- **Notfall- und Krisenmanagement:** Es müssen Pläne für das Notfall- und Krisenmanagement vorhanden sein, um auf Vorfälle reagieren zu können, die die kritischen Dienste beeinträchtigen könnten.

- **Regelmäßige Überprüfungen und Audits:** Die Einrichtungen müssen sich regelmäßigen Überprüfungen und Audits unterziehen, um die Einhaltung der KRITIS-Vorgaben zu gewährleisten.
- **Investitionen in Infrastruktur und Personal:** Möglicherweise sind zusätzliche Investitionen in die IT-Infrastruktur und qualifiziertes Personal erforderlich, um die erhöhten Anforderungen zu erfüllen.
- **Zusammenarbeit mit Sicherheitsbehörden:** Es kann eine engere Zusammenarbeit mit nationalen Sicherheitsbehörden und anderen KRITIS-Betreibern erforderlich sein, um Informationen auszutauschen und auf Bedrohungen zu reagieren.

Im Zusammenhang mit der Verwendung der digitalen Identität ist auch die Ausstellung von Dokumenten durch den Bürger zu berücksichtigen. Insbesondere bei der Errichtung von Gesellschaften und Vereinen, aber auch beim Betrieb von Dienstleistungen durch kleine und mittelständische Unternehmen ist sicherzustellen, dass von diesen ebenfalls Berechtigungen ausgestellt werden können (z.B. KITA-Abholberechtigungen, Vollmachten etc.). Die obligatorische Beauftragung zentralisierter Vertrauensdiensteanbieter ist wirtschaftlich hinderlich und diskriminiert die benannten Teilnehmer.

Anforderung A15: Wenn die Kommunen auch im Rahmen der EUDI-Infrastruktur verantwortlich sein sollen für Ausgabe-/Veränderungsprozesse oder Teile davon, so sind die Entwürfe für die entsprechenden Prozesse zunächst durch das Architekturteam öffentlich zur Diskussion zu stellen, um technisch-organisatorischen Aufwand und Kostenmodell nicht nur für die Kommunen, sondern auch für an den Anwendungsprozessen beteiligte Stakeholder, Bürger und Unternehmen transparent und bewertbar zu machen.

Alle SDI-Schaufensterprojekte sind an konstruktiver Zusammenarbeit in Sachen Interoperabilität interessiert. Es wurden Aktivitäten gestartet, die Interoperabilität zwischen der OpenID-basierten Protokollen, die in der EUDI-Wallet verwendet werden sollen und anderen Austauschprotokollen, z.B. DIDCommV2, zum Ziel haben. Auch auf EU-Ebene im Kontext des Achitecture Reference Frameworks (ARF) von eIDAS 2.0 gibt es bereits eine Diskussion alternativer Austauschprotokolle. Das für Anwendungsprozesse unter Usability- und Sicherheitsaspekten dringend erforderliche, aber mit einer auf den OpenID-Standards basierenden Technologie unmögliche Aufrechterhalten exklusiver Kommunikationskanäle zwischen den Akteuren macht eine Erweiterung des deutschen EUDI-Architekturentwurfs notwendig.

Zudem ist vor der Regulierung zu prüfen, inwiefern der jeweils aktuelle Entwurf der EUDI-Wallet eine alltagstaugliche Nutzung erlaubt. Dazu ist zum einen sicherzustellen, dass verschiedene Nachweise (hoheitliche Identität / PID, Führerschein / mDL, qualifizierte und nicht-qualifizierte elektronische Attributsnachweise) gleichermaßen unterstützt werden. Der Umgang mit diesen muss auch die Überprüfung verschiedener Teilaspekte (siehe Abschnitt 6.1) ermöglichen und dabei auch die Verwendung nicht-hoheitlicher Vertrauensregister für diese unterstützen. Weiterhin erfordern die meisten kommunalen Anwendungen nicht das im eIDAS-Kontext definierte Vertrauensniveau (Level of Assurance) „Hoch“, die von der EUDI Wallet verpflichtend unterstützt werden muss. Für eine verbesserte Alltagstauglichkeit sowie zur Vereinfachung von Prozessen und Reduktion von Kosten muss die EUDI-Wallet auch Identifizierung und Authentifizierung auf niedrigeren Vertrauensniveaus erlauben.

Eine maßgebliche Frage ist daher die nach dem Anspruch, dem die Entwicklung der EUDI-Wallet gerecht werden soll, und den sich daraus ergebenden Konsequenzen. Hier zeichnen sich zwei Optionen ab:

Option 1: Der Anspruch besteht darin, dass die EUDI-Wallet nur die Bereitstellung hoheitlicher Nachweise auf dem Vertrauensniveau „hoch“ unterstützen soll. Diese Option ließe sich schneller realisieren, reduziert aber die Einsatzmöglichkeiten der deutschen EUDI-Wallet sehr stark.

Die Folgen wären:

- Mit der EUDI-Wallet wird nur die Digitalisierung von Dokumenten und keine automatisierten Anwendungsprozesse unterstützt, d.h. es gibt keinen wirklichen Nutzen für die Kommunen.
- Die EUDI-Wallet erschließt keine Anwendungen mit Alltagsrelevanz und/oder Breitenwirkung.
- Jeder Nutzer braucht künftig mindestens zwei Wallets
- Kommunen haben doppelten technischen Aufwand und Kosten: eine Lösung für hoheitliche Nachweise bei hohem Vertrauensniveau, zu der sie per Gesetz verpflichtet werden, und eine zweite Lösung, die alltagsrelevante Anwendungsprozesse der Bürger unterstützt und die auch den Kommunen multidimensionalen Nutzen bringt

Option 2: Der Anspruch besteht darin, dass die EUDI-Wallet Anwendungen mit allen Vertrauensniveaus sowie hoheitliche und nicht-hoheitliche Nachweise unterstützen soll. In diesem Fall wäre eine Überarbeitung der Architektur erforderlich, was den Umsetzungsaufwand vergrößert.

Die Folgen wären:

- Die praktische Erprobung geht vor Standardisierung und Regulierung.
- Automatisierte Anwendungsprozesse werden möglich, wodurch ein breiter Nutzen für Bürger und Kommunen erschließbar wird.
- Der Nutzer braucht künftig nur die EUDI-Wallet.
- Kommunen brauchen nur eine Architektur technisch umzusetzen, aber die zu entwickeln, braucht Zeit.

Anforderung A16: Die politische Klärung und Spezifizierung des Anspruchs der EUDI-Entwicklung in Deutschland hinsichtlich der Breitenwirkung inkl. der Konsequenzen für die Kommunen ist dringend erforderlich.

10. Zusammenfassung der Anforderungen an die EUDI-Wallet

A1.) Angesichts der geplanten Wirkungsdimension der EUDI-Wallet und der damit zu erwartenden Kosten sollten o.g. Mindestanforderungen an technische Lösungen einer nachhaltigen Produktentwicklung zugrunde gelegt werden.

A2.) Soll die EUDI-Wallet im Rahmen von digitalen Verwaltungs- und Geschäftsprozessen zum Einsatz kommen, dann muss sie den o.g. Mindestanforderungen an Anwendungsprozesse mit ihrer Funktionalität Rechnung tragen.

A3.) Die technische Ausgestaltung von Vertrauensregistern ist vom jeweiligen Anwendungsfall und vom IT-Umfeld der jeweiligen Vertrauensdomänen bzw. Anwendungsökosysteme abhängig und muss daher generell technologieoffen angegangen werden.

A4.) Eine Wallet-App, die im Kontext kommunaler Anwendungsszenarien auf Seiten natürlicher oder juristischer Personen eingesetzt werden können soll, muss mit den zentralen und/oder dezentralen Vertrauensregistern der jeweiligen Kommune kommunizieren und die o.g. Prüfungen eines Verifiable Credentials zur Beantwortung der entsprechenden Vertrauensfragen vornehmen können.

A5.) Eine Wallet-App, die im Kontext kommunaler Anwendungsszenarien eingesetzt werden können soll, muss in der Lage sein, sowohl die Rolle des Inhabers, als auch die des Herausgebers und der Akzeptanzstelle einzunehmen.

A6.) Anforderung: Eine EUDI-Infrastruktur die im Kontext kommunaler Anwendungsszenarien eingesetzt werden können soll, muss nachweislich in der Lage sein, vollständige Geschäfts- und Anwendungsprozesse abzubilden, ohne für jeden einzelnen Prozessschritt eine neue gegenseitige Identifizierung/Authentifizierung der Interaktionspartner zu erfordern.

A7.) Die kommunale Datenkarte darf nicht unter die Regulierung und Governance der eIDAS 2.0-Infrastruktur fallen.

A8.) Eine Wallet-App, die mit jeder Ausprägung der kommunalen Datenkarte interoperabel sein soll, muss hinsichtlich Austauschprotokollen, Schnittstellen, Formaten und Schemata der Verifiable Credentials technologieoffen sein.

A9.) Da die kommunale Datenkarte ausschließlich kommunale Anwendungen unterstützen soll, obliegt die Einstufung der Vertrauenswürdigkeit bei Bedarf der jeweils implementierenden Kommune.

A10.) Wenn eine EUDI-Wallet sowie ggf. weitere Komponenten einer EUDI-Infrastruktur und deren organisatorischer Rahmen im Kontext kommunaler Anwendungen eine Rolle spielen sollen, müssen sie die sich aus den Basiseigenschaften der kommunalen Datenkarte logisch ableitbaren Mindest-Spezifikationen erfüllen.

A11.) Die EUDI-Wallet und weitere ggf. erforderliche technische Komponenten/Infrastruktur sollten den Kommunen kostenlos bereitgestellt werden.

A12.) Keinesfalls kann eine Verpflichtung zur Nutzung einer eID-/EUDI-Infrastruktur im Kontext kommunaler Aufgaben definiert werden. Dies würde die Kosten kommunaler Prozesse explodieren lassen und der Verwaltungsdigitalisierung massiv entgegenwirken.

A13.) Sollte der Bund die Kommunen verpflichten wollen, die unter seine Regulierungskompetenz fallenden Anwendungen bzw. Prozessschritte in seinem Auftrag nach Vorgaben der eIDAS-Verordnung umzusetzen, sind konkrete Pflichten, Risiken und damit einhergehende Kosten den Kommunen öffentlich zu machen und zur Diskussion zu stellen. Der Bund als Auftraggeber muss vor der Durchsetzung die Kostendeckung für die Kommunen sicherstellen.

A14.) Wenn nicht nur die EUDI-Wallet sondern ggf. auch weitere Komponenten einer EUDI-Infrastruktur und deren organisatorischer Rahmen im Kontext kommunaler Anwendungen eine Rolle spielen sollen, müssen sie hinsichtlich Austauschprotokollen, Schnittstellen, Formaten und Schemata der auszutauschenden bzw. zu prüfenden Informationen technologieoffen und flexibel anpassbar sein.

Idealerweise erfolgt Bereitstellung technischer Komponenten in Form von Software Development Kits (SDK) zur Einbindung in Städte-Apps und städtische Hintergrundsysteme.

A15.) Wenn die Kommunen auch im Rahmen der EUDI-Infrastruktur verantwortlich sein sollen für Ausgabe-/Veränderungsprozesse oder Teile davon, so sind die Entwürfe für die entsprechenden Prozesse zunächst durch das Architekturteam öffentlich zur Diskussion zu stellen, um technisch-organisatorischen Aufwand und Kostenmodell nicht nur für die Kommunen, sondern auch für an den Anwendungsprozessen beteiligte Stakeholder, Bürger und Unternehmen transparent und bewertbar zu machen.

A16.) Die politische Klärung und Spezifizierung des Anspruchs der EUDI-Entwicklung in Deutschland hinsichtlich der Breitenwirkung inkl. der Konsequenzen für die Kommunen ist dringend erforderlich.

Glossar

Die Identität einer natürlichen Person wird durch eine Vielzahl von Identitätsmerkmalen beschrieben. Dies gilt prinzipiell auch im Digitalen, allerdings sind die technisch, philosophisch und politisch geprägten Darstellungen dazu in der Literatur teilweise sehr widersprüchlich. Für das bessere Verständnis ist eine klare begriffliche Unterscheidung wichtig. Daher versuchen wir nachfolgend eine konsistente Begriffserklärung, die auch Anwendungen außerhalb regulierter Anwendungsbereiche integriert.

Digitale Identitäten repräsentieren Personen, Organisationen und auch Objekte der Realwelt im digitalen Raum. Eine reale Person kann mehrere digitale Identitäten haben. Dies kann ein Avatar sein, ein vorgegebener Benutzername oder ein selbstgewähltes Pseudonym, wie im Darknet oder im WWW üblich. Es kann aber auch eine sogenannte ***sichere digitale Identität*** sein. Die digitale Identität ist in jedem Fall die Summe aller in einem IT-System einer Entität zuzuordnenden digitalen Identitätsmerkmale (Attribute). Bei einer sicheren digitalen Identität stimmen diese Merkmale nachweislich mit der Realität überein. Die selbst verwaltete digitale Identität ist nicht zu verwechseln mit dem üblicherweise von anderen Akteuren ausgewerteten digitalen Fußabdruck einer Person, der die Spuren beinhaltet, die diese Person im Internet hinterlässt. Solche fremdverwalteten Profile (z.B. Suchverhalten auf Amazon) repräsentieren aber nicht die Person, sondern bilden nur deren Verhalten im Internet ab.

Identitätsmerkmale (**Attribute)** sind Merkmale, die die Identität von Personen, Organisationen bzw. Objekten beschreiben und anhand derer sie identifiziert werden können. Bei natürlichen Personen gehören dazu die im amtlichen Melderegister geführten Meldedaten (Basisidentität), biometrische Daten, Angaben in Nachweisen und Urkunden, aber auch Rechte/Berechtigungen und die Beziehungen gegenüber anderen natürlichen Personen, Organisationen sowie Objekten. Solche Identitätsmerkmale der realen Person können durch autorisierte Akteure in Form überprüfbarer digitaler Nachweise (***Verifiable Credentials***) ausgegeben und bei Bedarf von einem Dritten überprüft werden. Ein Attribut, das eine digitale Identität eindeutig identifiziert bezeichnet man als ***Identifikator***. Dies kann z.B. eine Email-Adresse, die Steuer-ID, eine Kundennummer oder auch die Wirtschaftsidentifikationsnummer eines Unternehmens sein.

Identifizierungsmittel sind Dokumente/Nachweise, die die Zuordnung i.d.R. mehrerer Identitätsmerkmale zu einer Person eindeutig belegen. In der Realwelt sind dies Ausweisdokumente mit Foto, wie Personalausweis, Betriebsausweis oder Krankenkassenkarte. Der Chip auf der Krankenkassenkarte dient der digitalen Identifikation, dem Nachweis der Echtheit und der Übermittlung der darauf gespeicherten Identitätsmerkmale bei physischem Kontakt, die Authentifizierung erfolgt anhand des Fotos auf der Karte. In der digitalen Welt sind hingegen rein elektronische Identifizierungsmittel gefragt, wie die hoheitliche eID, die kommunale Datenkarte oder der digitale Betriebsausweis auf dem Smartphone.

Zur besseren Unterscheidbarkeit soll folgendes **Beispiel** dienen: Alle Daten, die ein Nutzer einem Internet-Versandhandel bei Einrichtung seines Accounts mitteilt, bilden für diesen Versandhandel in Summe seine *digitale Identität*. Dazu gehört ein vom Nutzer selbstgewählter Benutzername (z.B. Rotkäppchen23), der auf der Versandhandelsplattform als *Identifikator* dient. Bei der Account-Erstellung übergibt der Nutzer zudem eine Reihe weiterer *Identitätsmerkmale*, wie Name, Geburtsdatum, Anschrift, Lieferadresse oder ggf. auch eine Kreditkartennummer. Solange diese Identitätsmerkmale nicht überprüft wurden, kann der Versandhandel dem Nutzer nicht ohne Risiko vertrauen und muss je nach Schadenspotential ggf. viel Rechercheaufwand zu seiner Person betreiben, um sein Risiko zu minimieren. Zeigt der Nutzer bei der Account-Erstellung aber ein *Identifizierungsmittel* vor, das der Versandhandel als vertrauenswürdig einstuft, z.B. weil es von einem vertrauenswürdigen Dritten bestätigt wurde, der wiederum anhand seiner eigenen digitalen Signatur oder seines digitalen Siegels eindeutig identifizierbar ist, so bildet die darin enthaltene Auswahl an Identitätsmerkmalen für den Versandhandel eine *sichere digitale Identität*. Alle zusätzlichen Daten, die der Versandhandel über die Aktivitäten des Nutzers sammelt (Käuferprofil), sind sein *digitaler Fußabdruck* in diesem IT-System.

Überprüfbare digitale Nachweise (Verifiable Credentials): Ein digitaler verifizierbarer Nachweis (Verifiable Credential) wird von einer Entität (Person, Organisation, Objekt) ausgestellt. Er besteht im Kern aus einem oder mehreren gesicherten Attributen (Inhalt) und einer kryptografischen Signatur. Die Signatur, obwohl eine Abfolge von Zeichenketten, ist nicht zu vergleichen mit einer händischen Unterschrift. Sie ist fälschungssicher, unnachahmlich, unveränderlich und sowohl dem Aussteller als auch dem Dokumenteninhalt sowie optional auch dem Empfänger eindeutig zuzuordnen. Dafür bindet der Herausgeber mit Hilfe des entsprechenden digitalen Schlüsselmaterials seinen eigenen Identifikator sowie optional den Identifikator des Empfängers und einen Hash des Inhalts kryptographisch in die Signatur ein. Der Kernaspekt verifizierbarer Nachweise ist, dass anhand der Signatur die Authentizität von Herausgeberschaft sowie optional von Empfänger und Inhalt der Nachweise orts- und zeitunabhängig in Echtzeit überprüft und belegt werden kann. Verifiable Credentials sind bereits ein internationaler W3C-Standard. Angesichts der Tatsache, dass mit signierten PDF-Dokumenten und der eID bereits technische Lösungen für digitale Nachweise und Ausweise natürlicher Personen existieren, stellt sich die berechtigte Frage, worin konkret der Mehrwert von Verifiable Credentials liegt. Tabelle 1 stellt hierzu die im Kontext des Trustnets relevanten Eigenschaften vergleichend gegenüber.

Eigenschaft	Signiertes PDF	eID	VC nach W3C
Herausgeberschaft prüfbar	X	X	X
Inhaber prüfbar	-	X	X
Authentizität des Inhalts prüfbar	X	X	X

Portables Datenformat	X	-	X
Austauschprotokoll	-	X	X
Maschinenlesbarer Inhalt	-	X	X
Auslesbarkeit einzelner Attribute (Selective Disclosure)	-	X	X
Skalierbarkeit im Internet	-	-	X
Flexible Abbildung von Sachverhalten	X	-	X
Kompatibilität mit bestehenden Systemen	X	-	In Zukunft
Einfache Zugänglichkeit für Dienstanbieter	X	-	In Zukunft
Identifizierbarkeit von Objekten	-	-	X
Identifizierbarkeit hoheitlicher Entitäten	-	-	X
Identifizierbarkeit juristischer Personen	-	X	X

Tabelle 1: Unterschiede zwischen signiertem PDF, eID und Verifiable Credential nach W3C-Standard

Es ist offenkundig, dass mit Verifiable Credentials als einheitlichem Vertrauensmechanismus die nächste Evolutionsstufe des Internets erreicht werden kann, unabhängig davon, welche zusätzlichen Vertrauensmechanismen für das Trustnet künftig noch entwickelt/genutzt werden.

Selbstsouveräne Identitäten (SSI): Selbstsouveräne oder selbstbestimmte digitale Identitäten sind ein Konzept, bei dem die Verwaltung der eigenen Identitätsdaten in die Hände der Nutzer gelegt wird. Der Nutzer gewinnt damit prinzipiell die Hoheit über seine eigenen Daten, die nur für ihn zugreifbar in seiner digitalen Wallet gespeichert sind. Die Wallet ist eine digitale Brieftasche. Vergleichbar mit dem physischen Portemonnaie werden darin Ausweisdokumente (eID, digitaler Führerschein, Bankkarte etc.) und Nachweisdokumente (amtl. Bescheinigungen, Registerauszüge, Berechtigungsnachweise, Urkunden u. ä.) sowie werthaltige und weitere Arten von Credentials abgelegt. Mit SSI geht der Begriff der digitalen Identität deutlich über das hinaus, was bislang im Kontext hoheitlicher Identitätslösungen (eID) diskutiert wurde. Das SSI-Prinzip ist ein Gegenentwurf zu den aktuell genutzten Konzepten, bei denen ein Nutzer verschiedene Identitäten bei verschiedenen Identitätsanbietern besitzt, die in der Regel die Kontrolle über die Daten haben. Mit SSI hat der Nutzer alleinigen Zugriff auf seine ID-Daten und kann entscheiden, welche Teile er davon wem zur Verfügung stellt. ID-Dienste liefern dafür die für den Nutzer primäre Infrastruktur, z.B. in Form von sicheren Cloudspeichern oder Wallet-Apps für Smartphones. Mit SSI lassen sich nicht nur digitale Identitäten natürlicher Personen abbilden, sondern auch digitale Identitäten von juristischen Personen, hoheitlichen Entitäten und (smarten) Objekten. Es lassen sich auch Beziehungen einer natürlichen Person zu anderen natürlichen Personen, zu juristischen Personen und zu Objekten digital abbilden und gesichert nachweisen. Mit dem SSI-Prinzip lässt sich jede Art von überprüfbaren Nachweisen digital herausgeben, vorzeigen und verifizieren. Damit wird das SSI-Prinzip zum Gamechanger im Kontext des Trustnets.

Trustnet: Das Trustnet ist das universelle digitale Abbild von Beziehungen zwischen Personen, Organisationen und Objekten der Realwelt. Es ermöglicht vertrauenswürdige und rechtskonforme digitale Interaktionen und verhindert Fake und Betrug. Die Grundlage dafür ist ein einheitlicher, skalierbarer Vertrauensmechanismus für den Austausch und die Prüfung von digitalen Nachweisen zu beliebigen Sachverhalten. Damit wird die Organisation von und der Zugang zu offenen digitalen Ökosystemen radikal vereinfacht.

Trust Framework: Ein wesentlicher Pfeiler des künftigen Trustnets wird die Entwicklung eines einheitlichen Trust Frameworks sein. Es soll als Strukturhilfe und Regelwerk mit Standards zum

sicheren Interaktionsmanagement digitaler Identitäten und digitaler Nachweise die Entstehung eines ID-Ökosystems anregen, in dem verschiedene ID-Dienste koexistieren können. Das Trustnet wird die bestehende Welt der zentral verwalteten Basisidentitäten inkl. eID und die neue SSI-Welt miteinander verbinden. Der Gedanke dieses Brückenschlags ist zwar bereits in die eIDAS-Novellierung eingeflossen, das Trust Framework soll aber darüberhinausgehend die technische, semantische und organisatorische Interoperabilität sicherstellen, damit Credentials unabhängig von der Art der Wallet-App und von der jeweiligen in der Vertrauensdomäne verwendeten Basistechnologie oder Dateninfrastruktur überprüft werden können. Dieser Gedanke ist in bestehenden bzw. in Entwicklung befindlichen Trust Frameworks, wie dem kanadischen PCTF, dem USamerikanischen NIST 800-63 oder bei den entsprechenden EU-Aktivitäten (eIDAS-Novellierung) noch zu gering ausgeprägt. Deswegen wird zur Entwicklung des Trustnets ein auf diesen Arbeiten aufbauender Neuentwurf erforderlich. Grundlegende Überlegungen dazu finden im Rahmen der Schaufensterprojekte statt.

Vertrauensdomäne: Eine Vertrauensdomäne ist eine in der realen und digitalen Welt identische Gruppe von Akteuren (Interessensgemeinschaft), die in einer definierten Auswahl von Prozessen klare Regeln (Trust Policies) für Interaktionen und Datenaustausch etabliert hat und Autoritäten für Überwachung und Durchsetzen der Einhaltung dieser Regeln etabliert hat. Auf der Kenntnis der Regeln und Autoritäten sowie der Identifizierbarkeit des jeweiligen Interaktionspartners basiert das Vertrauen innerhalb einer solchen Domäne. Zum Beispiel sind alle Aussteller, Inhaber und Akzeptanzstellen des Sozialpasses in einer Großstadt Teil einer Vertrauensdomäne, in der es klare Regeln für die Ausstellung, die Inhaberschaft und den Entzug des Sozialpasses gibt (z.B. Richtlinie zur Gewährung des Dresden-Passes). Die Übertragung der Prozesse in die digitale Welt erfordert die Definition digitaler Schemata und Protokolle für Inhalte und Transfer überprüfbarer Ausweise und Nachweise. Im Beispiel betrifft dies Nachweise zu Personalien und Anspruchsgrundlagen sowie den auszustellenden Sozialpass. Der Akteur, der Inhaber eines Credentials wird, wird erst in dem Moment Mitglied der Vertrauensdomäne, wenn er das Credential erwirbt und bleibt es auch nur, solange das Credential gültig ist. Das Trustnet entsteht durch Verschränkung und Interaktion vieler thematisch und/oder geographisch getrennter Vertrauensdomänen unter einem gemeinsamen Trust Framework.

Anwendungsökosystem: Ein Anwendungsökosystem ermöglicht einen thematisch und geographisch eingegrenzten Prozess zur gemeinsamen Wertschöpfung durch verschiedene Akteure (= Anwendung / Use case), bei dem Credentials aus mindestens einer, oft aus mehreren Vertrauensdomänen genutzt werden. Es beinhaltet die Akteure sowie deren Strukturen und Infrastrukturen, die Bestandteil der realen und digitalen Interaktionen im Rahmen der Anwendung sind. In einer definierten Auswahl von anwendungsbezogenen Prozessen werden auch hier klare Regeln (Trust Policies) für Interaktionen und Datenaustausch etabliert hat und Autoritäten für Überwachung und Durchsetzen der Einhaltung dieser Regeln etabliert hat. Auf der Kenntnis der Regeln und Autoritäten sowie der Identifizierbarkeit des jeweiligen Interaktionspartners basiert das Vertrauen innerhalb eines Anwendungsökosystems. Zum Beispiel sind alle Betreiber und Nutzer des ÖPNV in Dresden Teil eines Anwendungsökosystems, in dem es klare Regeln für die Benutzung der öffentlichen Verkehrsmittel gibt (Nutzungs- und Gebührenordnung) und Autoritäten (Fahrdienstpersonal, Kontrolleure), die die Einhaltung der Regeln überwachen. Das Credential Sozialpass wird in diesem Anwendungsökosystem zum Nachweis der Ermäßigungsberechtigung verwendet, d.h. die betreffenden Inhaber und Akzeptanzstellen (Ticket-Shops) sind Teil der Vertrauensdomäne Sozialpass. Oft ist also das Anwendungsökosystem kleiner als die Vertrauensdomäne. Die Akteure des Anwendungsökosystems sind hier aber gleichzeitig Teil einer

weiteren Vertrauensdomäne, die durch Herausgabe, Nutzung und Akzeptanz der ÖPNV-Tickets definiert wird. Der Akteur, der in einer Vertrauensdomäne die Rolle des Herausgebers inne hat, ist nicht zwingend Bestandteil des Anwendungsökosystems. Das Sozialamt als Herausgeber des Sozialpasses hat z.B. mit dem Anwendungsökosystem ÖPNV nichts zu tun.