Öffentliche Verwaltung als Katalysator für selbstbestimmtes Datenteilen: Digitale Nachweise auf Basis von Registerdaten

Gunnar Hempel, Michael Kubach

Zusammenfassung

In einer Kooperation der beiden Schaufensterprojekte ID-Ideal und ONCE wird im Rahmen des Förderprogramms „Sichere Digitale Identitäten" des Bundesministeriums für Wirtschaft und Klimaschutz mit der „kommunalen Datenkarte" eine digitale Identitätslösung pilotiert und evaluiert, die Bürgern ein Werkzeug an die Hand gibt, digitale Nachweise zu generieren und die Weitergabe von Daten und Nachweisen selbst zu bestimmen. Die Lösung basiert auf einem Self-Sovereign Identity (SSI) Ansatz und einer Identity Wallet Applikation, die auf allen Android und Apple Smartphones mit aktuellen Betriebssystemversionen lauffähig ist. Ziel ist es, ein ausreichend hohes Sicherheits- und Datenschutzniveau mit einer niedrigen Schwelle für die Nutzerinnen und Nutzer zu kombinieren.

In beiden Schaufensterprojekten spielt die Vernetzung kommunaler Dienstleistungen eine wichtige Rolle. Dazu gehören neben Verwaltungsdienstleistungen im engeren Sinne auch Angebote wie der öffentliche Personennahverkehr, Stadtbibliotheken, Museen und Sporteinrichtungen. Die Digitalisierung dieser Dienstleistungen ist eine zentrale Aufgabe. Die Bereitstellung und Verwaltung geprüfter Nachweise mit möglichst geringem Zeit- und Arbeitsaufwand für alle Akteure ist in diesem Ökosystem von entscheidender Bedeutung. Mit der kommunalen Datenkarte kann der Bürger diese Nachweise nun selbst kontrollieren und für die Inanspruchnahme kommunaler Dienstleistungen nutzen. Die so erhaltenen Daten genießen ein hohes Maß an Vertrauen und Glaubwürdigkeit, da sie aus kommunal geführten Registern stammen.

1. Einleitung

Die Digitalisierung von Verwaltungsprozessen ist ein elementares Ziel, um öffentliche Dienstleistungen effizienter, zugänglicher und benutzerfreund-

licher zu gestalten. Dies gilt insbesondere auch für die kommunale Daseinsvorsorge. Im Rahmen der kommunalen Daseinsvorsorge stellen Gemeinden wirtschaftliche, soziale und kulturelle Dienstleistungen für ihre Bürger, z. B. durch öffentliche Einrichtungen oder Infrastruktur im öffentlichen Interesse, bereit. Für zahlreiche Anwendungsfälle werden Sondernutzungsmöglichkeiten und Tarifmodelle angeboten, die sich an Nutzereigenschaften orientieren. Bestimmte Personengruppen erhalten beispielsweise Ermäßigungen oder haben gesonderten Zugang. Um diese Leistungen in Anspruch zu nehmen, sind in der Regel Nachweise zu erbringen, beispielsweise durch einen Sozialpass, einen Schülerausweis oder auch durch den Nachweis, in einer Gemeinde gemeldet zu sein. Hierfür ist die Verarbeitung von personenbezogenen Daten der Bürger erforderlich. Die Erbringung der Nachweise erfolgt heute noch überwiegend auf analogem Wege, durch persönliche Vorlage bzw. Abholung entsprechender Dokumente, seltener auf dem Postweg. Dies belastet Verwaltungen angesichts einer angespannten Personaldecke und stellt eine Hürde für Bürger dar, ihnen zustehende Leistungen in Anspruch nehmen zu können. Auch der weitere Kontext der (stockenden) Digitalisierung der Verwaltung ist hier zu betrachten. Das Onlinezugangsgesetz (OZG) sollte eigentlich die Verfügbarkeit von digitalen Verwaltungsleistungen verbessern. In der Umsetzung konnte es jedoch trotz „Booster" die gesteckten Ziele nicht erreichen (Röhl 2023), so dass ein OZG 2.0 erarbeitet wurde.[1]

Eine zentrale Herausforderung bei der Digitalisierung von Verwaltungsdienstleistungen ist die Verfügbarkeit geeigneter digitaler Nachweise für die Bürger. Die Online-Ausweisfunktion des Personalausweises (eID), die als universelles und sicheres Identifizierungsmittel für verschiedene Online-Dienste fungieren könnte, findet bisher nur geringe Nutzung unter den Bürgern (und ist auch für viele Diensteanbieter aufwändig einzubinden). Obwohl technisch jeder Personalausweis dazu fähig ist (Stand Juni 2023 waren rund 62 Millionen gültige Personalausweise im Umlauf, rund 88 % mit aktivierter Online-Ausweisfunktion – ca. 55 Millionen) (Krempl 2023), haben laut eGovernment Monitor nur 14 % der in 2023 befragten Bürger die Funktion jemals genutzt. Dies liegt unter anderem an der mangelnden Bekanntheit seiner Funktionen, geringer Unterstützung durch Diensteanbieter, eines nicht wahrgenommenen Nutzens sowie einer

1 Dieses scheiterte jedoch im März 2024 im Bundesrat und bei Verfassung dieses Beitrages war die weitere Entwicklung unklar.

oft als umständlich wahrgenommenen Handhabung – auch wenn diese in der letzten Zeit immer weiter vereinfacht wurde. Mangelndes Vertrauen spielt nur eine untergeordnete Rolle (D21/TU München 2023). Das Vorhaben der Entwicklung einer etwas Nutzerfreundlicheren Smart-eID, welche die Übertragung der Online-Ausweisfunktion auf das Smartphone in ein zertifiziertes sicheres Hardwareelement (ausschließlich für die Online-Nutzung) ermöglichen hätte sollen, wurde Ende 2023 gestoppt (Steiner 2023). Derzeit läuft die Entwicklung einer European Digital Identity Wallet (EUDI Wallet), die auch der deutsche Staat seinen Bürgern anbieten und in seine Verwaltungsleistungen einbinden soll. Diese Entwicklung wird jedoch nach aktuellem Zeitplan frühestens 2026/2027 abgeschlossen sein (European Commission 2024). Die Folge ist, dass vielen Bürgern derzeit faktisch die Grundlage fehlt, um von digitalen Verwaltungsdienstleistungen vollumfänglich profitieren zu können.[2] Um diese Hürde zu überwinden, bedarf es einer gezielten Strategie: Einerseits muss die Benutzerfreundlichkeit des digitalen Personalausweises verbessert werden, um die Akzeptanz und Nutzungsbereitschaft zu erhöhen. Andererseits können jedoch auch alternative digitale Identitätsnachweise, wie die im Folgenden beschriebene „kommunale Datenkarte", gefördert und ihre Anwendung vereinfacht werden, um eine breitere Basis für digitalen Zugang zu Dienstleistungen zu schaffen, die nicht unbedingt das hohe Vertrauensniveau des Personalausweises mit Online-Ausweisfunktion benötigen. Eine Kombination aus technischer Optimierung und der Schaffung von diversen, benutzerorientierten Identifikationsmöglichkeiten könnte die Teilhabe aller Bürger an der digitalen Verwaltung verbessern.[3]

Vor diesem Hintergrund gewinnt außerdem die Wahrung des Datenschutzes eine zusätzliche Dimension. Personenbezogene Daten, deren Verarbeitung für den Erhalt kommunaler Leistungen oftmals erforderlich sind, müssen geschützt werden, um das Vertrauen der Bürger in digitale Verwaltungsprozesse zu stärken. Im Sinne des Grundrechts auf informationelle Selbstbestimmung soll es jeder betroffenen Person möglich sein, grundsätzlich selbst über die Verarbeitung ihrer personenbezogenen Daten zu bestimmen. Die Europäische Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG) und die für die Verwaltung der Länder

2 Diese steht aber auch einer mangelhaften verwaltungsinternen Digitalisierung gegenüber – letztlich handelt es sich um ein Art Henne-Ei-Problem.

3 Andere europäische Länder, etwa die Nachbarn Österreich und Dänemark, sind hier bedeutend weiter.

geltenden jeweiligen Datenschutzgesetze geben diesbezüglich zahlreiche Vorgaben für die Verarbeitung personenbezogener Daten vor. Dies betrifft insbesondere die Rechtsgrundlagen für die Verarbeitungen, Vorgaben für Informationsvermittlung und Auskunftserteilung zu den Verarbeitungen sowie Vorgaben zu technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten.

Das in diesem Beitrag vorgestellte Konzept einer „kommunalen Datenkarte" als digitales Äquivalent zu herkömmlichen Nachweisen verfolgt daher zwei wesentliche Ziele: die Vereinfachung des Zugangs zu kommunalen Leistungen und die strikte Einhaltung des Datenschutzes. Durch die Verwendung von Self-sovereign Identity Technologie können Bürger ihre Daten sicher in einer digitalen Wallet auf ihrem Smartphone verwalten und bei Bedarf vorlegen, ohne mehr Daten als notwendig preiszugeben.[4] Dies stellt einen wichtigen Schritt in Richtung einer modernen, serviceorientierten und datenschutzkonformen Verwaltung dar.

Das Ziel des Beitrags ist es, das Konzept der kommunalen Datenkarte zur Diskussion zu stellen. Zunächst erfolgt eine eingehendere Darstellung der Motivation für das gewählte Konzept angesichts vorhandener Alternativen sowie eine Skizzierung der technischen Realisierung. Anschließend wird auf die Pilotierung im Rahmen der Schaufensterprojekte „Sichere Digitale Identitäten" (SDI-Schaufenster) des Bundesministeriums für Wirtschaft und Klimaschutz (Bundesministerium für Wirtschaft und Klimaschutz 2024) eingegangen. Hiervon abgeleitet werden schlussendlich Thesen, die Potenziale und Herausforderungen der kommunalen Datenkarte zusammenfassen.

4 Als Folge des Digital Markets Acts der EU (DMA 2022) lassen sich Applikationen auf Smartphones auch ohne Nutzung eines App-Stores der Smartphone-(Betriebssystem-)Herstellern installieren. Die ID-Daten der Nutzenden werden beim Self-Sovereign Identity Ansatz (siehe Abschnitt 2.2) auf dem Smartphone verwaltet und nicht zu den Smartphone-(Betriebssystem-)Herstellern übertragen. Es existieren Android Smartphones, welche sich vollständig ohne Google Account nutzen lassen. Insofern besteht bei der ohnehin optionalen Nutzung digitaler Wallets auf aktuellen Smartphones weder ein Zwang zur Nutzung von App-Stores, noch ein Zwang zu Konten bei Apple und Google.

2. Die Kommunale Datenkarte: Konzept, Umsetzung und Pilotierung

In einer Kooperation der beiden Schaufensterprojekte ID-Ideal[5] und ONCE[6] wird im Rahmen des Förderprogramms „Sichere Digitale Identitäten" des Bundesministeriums für Wirtschaft und Klimaschutz mit dem Konzept der „kommunalen Datenkarte" seit 2021 eine digitale Identitätslösung entwickelt und evaluiert, die Bürgern ein Werkzeug an die Hand gibt, digitale Nachweise auf Basis kommunaler Registerdaten (z. B. aus dem Melderegister für Daten und dem Passregister für Lichtbild) zu erzeugen und die Weitergabe von Daten und Nachweisen selbst zu bestimmen. In beiden Schaufensterprojekten spielt die Erleichterung der digitalen Bereitstellung kommunaler Dienstleistungen eine große Rolle. Dazu gehören neben Verwaltungsleistungen im engeren Sinne auch Angebote wie öffentlicher Nahverkehr, städtische Bibliotheken, Museen und sportliche Einrichtungen. Die Nutzung dieser Dienstleistung ist in der Regel an den Nachweis bestimmter Merkmale gebunden. Dieser wird klassisch durch Vorlage und Sichtprüfung von Dokumenten, wie einer Meldebescheinigung, eines Bibliotheksausweises etc. erbracht. Die Digitalisierung der Dienstleistungen erfordert die Übertragung dieses Vorganges in digitale Prozesse, um keinen Medienbruch zu erzeugen und diese Leistungen werden teilweise online, aber auch vor Ort erbracht. Ein digitaler Nachweis auf dem Smartphone sollte sich also online, aber auch vor Ort nutzen lassen (Beispiel: Ausleihe eines digitalen Buches von Zuhause, aber auch Ausleihe eines physischen Buches in der Bibliothek). Die digitale Bereitstellung und Verwaltung geprüfter Nachweise mit möglichst geringem Zeit- und Arbeitsaufwand für alle Akteure ist damit in diesem Ökosystem von entscheidender Bedeutung. Das folgende Kapitel diskutiert zunächst knapp, ob für die Digitalisierung der deutschen Verwaltung tatsächlich noch eine weitere digitale Identitätslösung notwendig ist und stellt dann das Konzept der kommunalen Datenkarte vor.

2.1 Noch eine weitere Identitätslösung?

Sinn und Zweck der kommunalen Datenkarte ist es, mit der Lösung einen in mehrfacher Hinsicht niederschwelligen digitalen Nachweis zu ent-

5 https://id-ideal.de
6 https://once-identity.org

wickeln. Niederschwellig, um Hürden der Digitalisierung für den Nutzer (aber auch hinsichtlich der Einbindung in die Prozesse der Diensteanbieter, siehe unten) abzubauen. Hier kann die Verwendung einer Smartphone-App (kommunale Datenkarte) mit einer angebundenen Wallet einen nutzerfreundlichen Einstieg schaffen, der aus der Verwendung von existierenden Smartphone Wallets beispielsweise für Kino- und Flugtickets bekannt ist. Die Nutzung der Corona-Warn-App mit Impfnachweis während der Covid-19 Lockdowns hat die Bürger zudem an den Umgang mit Nachweisen auf dem Smartphone und die Interaktion mit QR-Codes gewöhnt, so dass es sich hier für sie um ein vertrautes Interaktionsparadigma handelt. Smartphone Wallets nach dem Self-Sovereign-Identity Prinzip stellen zudem die Kontrolle des Nutzers über seine Daten und deren Verwendung ins Zentrum. Der Nutzer sieht und bestimmt, welche Daten er für welche Dienstleistung er an welche Organisation freigibt und erhält eine Historie seiner Nutzungen. Der Wallet-Ansatz kann potenziell für ein breites bzw. wachsendes Spektrum von Dienstleistungen eingesetzt werden. Die Bedienungsoberfläche einer Wallet kann fortlaufend an die Bedürfnisse von Nutzern und mögliche Erweiterungen des Funktionsumfangs angepasst werden, ohne dass sich der Nutzer grundlegend umgewöhnen muss. Die in der Wallet gespeicherten Nachweise können ohne den Umgang mit einer Smartcard und NFC-Schnittstelle genutzt werden, was in der Praxis der Nutzung des Personalausweises mit Online-Ausweisunktion derzeit zu bedeutenden Abbruchraten führt.

An dieser Stelle ist gleichfalls die Frage zu stellen, inwieweit die eID, welche beispielsweise über den Personalausweis eingesetzt werden kann, diese Funktionen nicht bereits erfüllt. Die Einbindung der eID in die hier diskutierten Anwendungen ist für viele Diensteanbieter aufgrund der hohen technischen Anforderungen und Kosten der eID-Nutzung derzeit nicht sinnvoll darstellbar. Insofern sind auch die Schwellen zum Einsatz bzw. zur Prozessintegration auf dieser Seite zu senken. Auch die weniger aufwendige Integration von Benutzerkonten (z. B. BundID) ist dennoch mit signifikanten Hürden verbunden. In diesem Fall wird dann auch wieder der Nutzer mit mindestens drei Technologien (Fachverfahren, Nutzerkonto und AusweisApp bzw. zukünftig vermutlich EUDI Wallet) und unterschiedlichen User Interfaces konfrontiert. Einfache, medienbruchfreie, schnelle und integrative Prozesse, insbesondere auch vor Ort, sind so nicht ohne weiteres umsetzbar. BundID und die (zwischenzeitlich eingestellte) Smart-eID (welche die Nutzung der Online-Ausweisfunktion ohne das Halten des Personalausweises an das Smartphone für die Nutzung der NFC-Schnitt-

stelle ermöglichen sollte) sind nur für die Nutzung von Onlinediensten ausgelegt. Sie liefern auch kein verifiziertes Lichtbild des Bürgers mit sich, welches eine einfach Sichtprüfung ermöglicht. Auch wenn ein Bürger also meint, seine sichere digitale Identität auf dem Smartphone dabei zu haben, so kann er sie doch nicht für „vor Ort"-Anwendungen nutzen. Hierzu müsste er wieder auf den physischen Personalausweis zurückgreifen. Dies ist den Bürgern sicherlich kaum zu vermitteln. Bislang schwer absehbar ist, inwieweit die EUDI Wallet über den digitalen Führerschein (mDL – mobile Drivers' License) hinaus solche vor Ort Anwendungen unterstützen wird.

Weiter ist auch der Umfang der Attribute maßgebend dafür, welche kommunalen Anwendungen mit einer digitalen Identität unterstützt werden. Der Datensatz aus dem Melderegister kann umfangreicher sein als der eID-Datensatz. Er kann beispielsweise Informationen zum Zuzugsdatum oder zur Adresse des Nebenwohnsitzes aus einem kommunalen Melderegister enthalten, die für bestimmte kommunale Szenarien benötigt werden. Außerdem lässt sich eben ein verifiziertes Lichtbild aus dem Passregister mit ableiten. Den konkreten Attributumfang bestimmt schließlich die Kommune nach den Erfordernissen der in ihrem Hoheitsbereich zu unterstützenden Anwendungsprozesse. Eine Interoperabilität der kommunalen Datenkarte zwischen Kommunen erfordert aber sicherlich die Definition eines Sets an Basisattributen sowie eines standardisierten Regelwerks. Dies ist erst mittelfristig erreichbar – kurzfristig liegt der Fokus darum auf der lokalen Anwendung. Die konkrete Umsetzung sowie technische Basis der kommunalen Datenkarte wird im folgenden Abschnitt dargestellt.

2.2 Praktische Realisierung

Die technische Grundlage der kommunalen Datenkarte basiert auf der Self-Sovereign Identity (SSI)-Technologie. SSI repräsentiert ein Paradigma, das jedem Individuum ermöglicht, Besitz und Kontrolle über seine digitale Identität und die damit verbundenen Daten auszuüben, ohne auf Intermediäre oder zentrale Autoritäten angewiesen zu sein (Allen 2016). Diese Autonomie in der digitalen Identitätsverwaltung wurzelt in der Idee, dass ebenso wie in der realen Welt jedes Individuum selbstverantwortlich für seine Identitätsnachweise ist. Die konzeptionelle Herkunft der SSI kann auf die Fortschritte in verteilten Register-Technologien (DLT - Distributed Ledger Technology), insbesondere der Blockchain, zurückgeführt werden,

welche Mechanismen für dezentrales Vertrauen und Sicherheit ohne eine zentrale Überwachungsinstanz bietet.

Für SSI-Ansätze spielen Verifiable Credentials (VCs) eine entscheidende Rolle. VCs sind digitale Zertifikate, die von einer vertrauenswürdigen Entität ausgestellt werden und bestimmte Ansprüche über eine Person oder Entität bestätigen. Diese Zertifikate sind so gestaltet, dass sie von Dritten privatsphärenfreundlich verifiziert werden können, ohne dass die ursprünglich herausgebende Entität kontaktiert werden muss (W3C 2022). Grundsätzlich sind auch sogenannte Zero Knowledge Proofs realisierbar, welche beispielsweise einen Volljährigkeitsnachweis ohne Offenlegung des zugrunde liegenden Geburtsdatums ermöglichen. VCs beruhen also auf kryptographischen Methoden, die es ermöglichen, die Echtheit, Integrität und Nichtabstreitbarkeit der Credentials zu gewährleisten. Somit bilden sie die Grundlage für eine vertrauensvolle und gleichzeitig datenschutzfreundliche digitale Interaktion.

Die kommunale Datenkarte nutzt eine Identity Wallet Applikation, welche als eine sichere Speicher- und Präsentationsumgebung für VCs auf Smartphones mit gängigen Betriebssystemen wie Android und iOS dient. Es wird sichergestellt, dass Nutzende ohne die Notwendigkeit spezieller Hardware (wie high-end Smartphones mit zertifizierten Hardwaresicherheitselementen wie bei der Smart-eID) oder aufwendiger Prozesse, wie etwa dem fehleranfälligen Auslesen von NFC-Chips (wie bei der Online-Ausweisfunktion des Personalausweises), Zugang zu ihren digitalen Identitätsnachweisen erhalten.

Grundsätzlich ist auch eine Interoperabilität der SSI-basierten kommunalen Datenkarte mit europäischen Initiativen angestrebt. Die Vorgaben und Standards, die durch die eIDAS-Verordnung (eIDAS 2.0) und das Architecture Reference Framework (ARF) (eIDAS Expert Group 2024) für die EU Digital Identity Wallet (EUDI Wallet) definieren und derzeit in den EU Large Scale Pilot Projekten (LSP) (EU Commission 2024) erprobt werden, dienen als Leitlinien. Da die Arbeiten an der Architektur und der EUDI Wallet derzeit jedoch noch nicht abgeschlossen sind, muss sich zeigen, inwieweit eine Interoperabilität möglich ist oder die kommunale Datenkarte vielmehr eine Ergänzung oder Brückentechnologie bis zur Verfügbarkeit der EUDI Wallet darstellt.

Die kommunale Datenkarte dient somit als ein verifizierbarer digitaler Nachweis (Verifiable Credential), der durch die Nutzung von SSI-kompatiblen Systemen innerhalb der kommunalen IT-Infrastruktur (kommunalen IT-Fachverfahren) generiert und verwaltet werden kann. Der Ausstellungs-

prozess dieses Nachweises bedient sich vertrauenswürdiger Datenquellen der öffentlichen Verwaltung, wie beispielsweise Melderegister (Register auf Landes- oder kommunaler Ebene), um die Authentizität und Zuverlässigkeit der digitalen Identität des Bürgers zu gewährleisten. Vom Bürger wird er über die App und die Wallet auf handelsüblichen Smartphones verwaltet und mittels dieser für den Zugang zu Anwendungen online und vor Ort genutzt.

Personenbezogene Daten werden gemäß den rechtlichen Rahmenbedingungen durch kommunale Behörden im Zuge administrativer Verfahren erfasst – beispielsweise bei der An- und Ummeldung des Wohnsitzes oder der Beantragung von Ausweisdokumenten – und von den jeweiligen kommunalen Einrichtungen verwaltet sowie aktualisiert. So werden sie im Melderegister gespeichert und gepflegt.

Der Nutzer der App, in der Rolle der betroffenen Person, kann nach Art. 15 Abs. 1 S. 1 DSGVO gegenüber der registerführenden Behörde (Verantwortlicher) generell Auskunft darüber verlangen, ob personenbezogene Daten verarbeitet werden und – sofern eine solche Verarbeitung vorliegt – auch über diese Daten selbst Auskunft zu erhalten. Wird das Auskunftsersuchen elektronisch eingereicht, so ist der Verantwortliche nach Maßgabe des Art. 15 Abs. 3 S. 1 und 3 DSGVO und unter Berücksichtigung des § 10 BMG angehalten, eine Kopie der verarbeiteten personenbezogenen Daten im Sinne einer elektronischen Bereitstellung in gängigem Format zu übermitteln. Der Auskunftsanspruch kann praktisch vom Nutzer direkt aus der App elektronisch eingereicht, die Kopie der verarbeiteten personenbezogenen Daten in einem elektronischen Format empfangen werden.

Die Daten aus dieser Auskunftserteilung (z. B. XML, PDF) werden hieraufhin aus der Datei entnommen und als das Verifiable Credentials der kommunalen Datenkarte in die Wallet übertragen. Im Rahmen der Projekte ID-Ideal und ONCE wurde dies technisch bereits prototypisch realisiert. Hierzu kooperierten Anbieter kommunaler Fachverfahren, öffentliche IT-Dienstleister, Entwickler von SSI-Backend und Wallet-Lösungen und Kommunen für den Zugang zu den Registern und kommunale Angebote.

Für die kommunale Datenkarte ist ein Basisdatenset von Angaben wie Name, Geburtsdatum, Wohnadresse, Familienstatus sowie Daten bezüglich der Anmeldung oder des Zuzugs in die betreffende Kommune angedacht, das im Zuge der Pilotierung noch weiter zu spezifizieren ist. Die kommunale Verwaltung bestätigt durch ein qualifiziertes digitales Siegel ausschließlich, dass die Daten zum Zeitpunkt der Ausgabe im Melderegister so vorhanden waren. Die rechtliche Zulässigkeit einer Ergänzung um das

digitale Lichtbild aus dem Pass- oder Personalausweisregister ist derzeit Gegenstand juristischer Abklärungen. Dem Bürger ist es nun möglich, die erhaltenen Nachweise eigenständig zu verwalten und für die Nutzung kommunaler (oder darüber hinaus gehender) Angebote heranzuziehen. Die Annahme ist, dass die aus den kommunalen Registern bezogenen Daten von den Akzeptanzstellen, zu denen ja insbesondere Angebote der jeweiligen Kommune zählen, als vertrauenswürdig erachtet werden.

2.3 Pilotierung der kommunalen Datenkarte im Rahmen der Forschungsprojekte

Das Konzept der kommunalen Datenkarte wird im Rahmen der SDI-Schaufenster ONCE und ID-Ideal in mehrere Stufen praktisch getestet. Es wurden etwa User Interface Mockups sowie Test Credentials für die kommunale Datenkarte in der Wallet erstellt und die Usability mit Bürgern erprobt. Eine kommunale Pilotimplementierung erfolgt schließlich in Zusammenarbeit mit der Landeshauptstadt Dresden.

In einem ersten Schritt werden verifizierbare Daten zu einer Person aus dem kommunalen Melderegister in ein Basis-Credential überführt, welches in einer Wallet gespeichert werden kann. Es kann fortan als Nachweis im kommunalen Umfeld für die Inanspruchnahme ausgewählter kommunaler Dienstleistungen verwendet werden. Das Credential ermöglicht es prinzipiell, einzelne Attribute des Datensatzes zu einer Person aus der Wallet heraus automatisiert in ausgewählten Anwendungsszenarien für kommunale Dienstleistungen zu präsentieren, auszulesen oder in Formulare einzufügen.

In einem zweiten Schritt ist die Infrastruktur der Verwaltung anzupassen. Ziel ist es, die Fachabteilungen, welche Verifiable Credentials ausstellen, prüfen und akzeptieren müssen, mit Softwarekomponenten zur Realisierung der gesamten Prozesskette auszustatten.

Diese Aufgaben obliegen prinzipiell der Kommune, was zumindest dahingehend sinnvoll ist, dass sie bedarfsgerecht und entsprechend der jeweils vorhandenen kommunalen IT-Landschaft gelöst werden müssen. Idealerweise erfolgt die Bereitstellung der technischen Komponenten zukünftig auch in Form von Software Development Kits (SDK) zur Integration in kommunale Anwendungen und kommunale Hintergrundsysteme (ID-Ideal/ONCE 2023).

Für die Anwendung der kommunalen Datenkarte in kommunalen Test-Szenarien werden gegenwärtig zwei Ansätze verfolgt:

a) Beantragung eines kommunalen Berechtigungsnachweises – Dresden-Pass

Der Dresden-Pass berechtigt zum kostengünstigeren Besuch kultureller Einrichtungen der Landeshauptstadt Dresden und des Freistaates Sachsen in der Stadt Dresden, zur kostenlosen Mietrechtsberatung sowie zur Inanspruchnahme von Ermäßigungen bei der Dresdner Verkehrsbetriebe AG (DVB AG). Anspruch auf den Dresden Pass haben Einwohner mit Hauptwohnsitz in Dresden, die ausgewählte Sozialleistungen beziehen (Landeshauptstadt Dresden 2022). Ausstellende Behörde des Dresden Passes ist das Sozialamt der Landeshauptstadt.

Für die Beantragung verifiziert sich der Antragsteller mit seinem Basis-Credential aus seiner Wallet gegenüber der ausstellenden Behörde und erhält von dieser den Dresden Pass als Verifiable Credential (Dresden Pass Credential) in seine Wallet übertragen. Das Dresden Pass Credential ist ab diesem Zeitpunkt gültig bis zum Widerruf (in der Regel 1 Jahr, angelehnt an die Dauer des Bezugs der Sozialleistungen) und berechtigt den Inhaber dazu, Vergünstigungen in den zahlreichen Einrichtungen der Stadt zu beanspruchen.

Der Inhaber muss für die Ermäßigungen lediglich, vor Ort (z. B. via QR-Scan) oder online seine Wallet mit dem Serviceanbieter verbinden und das Dresden Pass Credential präsentieren.

b) Nachweis der Berechtigung zur Teilnahme an einem Bürgerbegehren

Ein Bürgerbegehren nach § 25 Abs. 1 SächsGemO eröffnet Bürgern in Sachsen die Möglichkeit zur politischen Mitbestimmung. Das Bürgerbegehren ist als ein Antrag der Bürger einer Gemeinde auf einen Bürgerentscheid zu verstehen, bei dem die Bürgerschaft (anstelle des Stadtrates) direkt über Angelegenheiten der Gemeinde entscheiden kann. Die Themen und Inhalte für einen Bürgerentscheid sind kommunalpolitische Sachfragen, für die der Stadtrat zuständig ist (Stadt Leipzig 2024).

Antragsberechtigter Bürger ist nach § 15 Abs. 1 i. V. m. § 16 Abs. 1 S. 2 SächsGemO, wer am Tag der Unterzeichnung des Bürgerbegehrens Deutscher im Sinne von Artikel 116 Abs. 1 GG ist oder die Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union besitzt, das 18. Lebensjahr vollendet hat und seit mindestens drei Monaten in der Gemeinde wohnt.

Die Besonderheit dieses Szenarios liegt darin, dass die Berechtigung zur Teilnahme davon abhängt, wie lange die Person bereits in der Gemeinde wohnt. Dieser Nachweis kann nicht anhand eines Passes oder Personalausweises geführt werden, da diese Information nicht aus dem Dokument bzw. dem zugehörigen Datensatz aus der eID ersichtlich sind. Für die Nachweisführung sind vielmehr Informationen aus dem kommunalen Melderegister (Einwohnermeldeamt) erforderlich.

Mit der kommunalen Datenkarte wäre der Nachweis generell möglich. Jedoch kommt im Fall des Bürgerbegehrens noch eine weitere Besonderheit hinzu. Die Beantragung hat nach § 25 Abs. 1 S. 1 SächsGemO schriftlich zu erfolgen, die elektronische Form ist explizit ausgeschlossen.

Der Ausschluss der elektronischen Form führt dazu, dass Mitarbeiter der Stadt Dresden die Gültigkeit der Unterschriften zum Bürgerbegehren, immerhin mind. 5 % der Wahlberechtigten Dresdener[7], händisch prüfen müssen, was in der jüngeren Vergangenheit personelle Aufwendungen von bis zu 6 Vollzeitäquivalenten über mehrere Wochen hinweg verursacht hat. Für die Testung des Szenarios wird deshalb eine Ausnahmeregelung im Rahmen einer Experimentierklausel nach § 20 Sächsisches E-Government-Gesetz für eine Reallabor sondiert, um die Auswirkungen und Potentiale der elektronischen Form in diesem Szenario zu untersuchen.

3. Zwischenfazit aus der Entwicklung und Pilotierung

Die Realisierung des SSI-Ansatzes erfordert eine gewisse Transformation herkömmlicher Prozessabläufe und Strukturen. In technischer Hinsicht müssen Prozesse re-moduliert, Systeme angepasst oder neu errichtet werden. Das Personal muss entsprechend qualifiziert und es müssen notwenige Kompetenzen aufgebaut werden, um die Serviceangebote zu bewirtschaften und auch dem Nutzer die Anwendung zu erklären und bei Bedarf zu unterstützen.

In organisatorischer Hinsicht sind auf kommunaler Ebene die notwenigen Strukturen und Verantwortlichkeiten (Governancestrukturen) zu schaffen. Konkret ist hierfür ein gültiger Rechtsrahmen zu schaffen, federführende und beteiligte Stellen zu legitimieren und entsprechende personelle und finanzielle Mittel bereitzustellen.

7 Ab ca. 20.000 Unterschriften.

3.1 Rechtlich-organisatorische Einordnung der Akteure, Rollen und Prozessabläufe

Für den Einsatz der kommunalen Datenkarte in der Praxis, sind die rechtlichen Voraussetzungen zu schaffen. Die rechtlich zuständige Stelle, die als Kontrollorgan (und juristische Person) die hierfür geltenden Regeln formuliert, für verbindlich erklärt und auch ihre Einhaltung überwacht, muss nach den geltenden deutschen Staatsstrukturprinzipien nach Art. 20 Abs. 1 GG als ein rechtssetzendes staatliches Organ demokratisch legitimiert sein. Auf kommunaler Ebene ist die Gemeinde, bzw. der Stadt- oder Gemeinderat als Hauptorgan der Gemeinde, ermächtigt, für ihren Wirkungsbereich Rechtsvorschriften zu schaffen. Sachliche und räumliche Grenzen sind hierbei zu beachten, ein hinreichender Bezug zum eigenen Gebiet, entweder weil ein Vorgang dort stattfindet oder eine Leistung dort angeboten und erbracht wird oder weil die zugehörigen Einwohner allein oder hauptsächlich dort betroffen oder begünstigt sind. Eine Begünstigung und Erstreckung der Nutzungsbedingungen im Hinblick auf öffentliche Einrichtungen der Gemeinde (§ 10 Abs. 2, 5 SächsGemO) kommt generell auch im Hinblick auf Gäste oder Nicht-Gemeindeansässige in Betracht. Dies gilt gleichfalls für rechtlich selbstständige Anstalten wie Verbände und privatrechtsförmige kommunale Unternehmen, die auch gebietsfremden Kunden frei zugängliche Leistungen anbieten und die die Reichweite Ihrer Tätigkeiten nicht auf das Gebiet der Kern-Gemeinde begrenzen (z. B. Personenbeförderung, Sparkassen, etc.). Die Gemeinde (Stadt- oder Gemeinderat sowie bei entsprechender Zuständigkeit Bürgermeister und Oberbürgermeister) ist damit befugt, Regeln in rechtsverbindlicher Form als Satzung oder innerhalb der Gemeindeverwaltung (z. B. Sozialamt) durch „Richtlinien" aufzustellen und zu ändern. Die konkret zuständige Stelle ergibt sich aus dem Organisationsplan beziehungsweise aus der erlassenen Hauptsatzung der Gemeinde (§ 4 Abs. 2 SächsGemO), im Hinblick auf den Einsatz von finanziellen und personellen Ressourcen arbeiteten eine federführende Stelle und andere Stellen zusammen.

Der Herausgeber (herausgebende Stelle) der kommunalen Datenkarte wird diesen Bestimmungen unterstellt. Er verantwortet die Prozessschritte zur Integration der Daten in das Basis-Credential und dessen Ablage in der Wallet, und damit sowohl den Vorgang der Übernahme der Daten aus der elektronisch bereitgestellten Auskunft (z. B. PDF) in die Wallet, der Übermittlung oder zur Verfügung Stellung von Daten innerhalb des kommunale Datenkarte-Ökosystems als auch die maßgebliche Steuerung und Kontrolle

der vorausliegenden Vorgänge. Hier ist auch an die Schaffung und/oder Bereitstellung der Wallet oder deren Vergabe an Dritte und dabei auch die Weitergabe der erforderlichen Informationen an die für den Herausgeber tätig werdenden (juristischen) Personen (Dritte) zu denken. Die herausgebende Stelle ist dann, neben der erstmaligen Ausgabe der kommunalen Datenkarte auch für das Überwachen der Regeln des Umlaufs, auch für das Aus-dem-Verkehr-ziehen bei Wegfall der Gültigkeit zuständig.

Inhaber kann allgemein jede zu identifizierende Person sein, die im Fall der kommunalen Datenkarte zu einer für bestimmte Funktionen oder Maßnahmen berechtigten Personengruppe (hier natürliche Personen) gehört (z. B. Berechtigte für Sozialleistungen). Abhängig vom Berechtigungszweck kann dabei z. B. das Alter ein wesentliches Differenzierungsmerkmal sein (generell Geschäftsfähigkeit nach § 104 BGB, Vergünstigungen für Minderjährige oder Senioren). Im Fall der Nationalität als Differenzierungsmerkmal ist der allgemeine Gleichheitssatz (Art. 3 Abs. 1 GG) zu beachten. Sofern der Inhaber den Nachweis aufgrund der Zugehörigkeit zu einer Organisation (juristischen Person) erhält, ist die Organisationszugehörigkeit die differenzierende Eigenschaft (z. B. Mitgliedsausweis).

Die Rolle als Inhaber setzt voraus, dass die jeweilige Person unmittelbarer Besitzer (i.S.v. § 854 BGB) der einzusetzenden Hardware (als Speicher der elektronischen Informationen) für die kommunale Datenkarte ist. Bei Software oder elektronischen Informationen für Nachweise, ist ein „Besitz" nur an dem physischen Trägermedium möglich, da Software insoweit keine Sach-Qualität zukommt. Entsprechend ergeben sich statt Besitz- oder Eigentumsrechten vielmehr Verfügungsrechte aus den Vorschriften des Immaterialgüterrechtes.

Die kommunale Datenkarte wird zum Nachweis der Identität und/oder einer Berechtigung gegenüber Akzeptanzstellen (Verifier) eingesetzt. Je nach rechtlichem Rahmen erfolgt hier neben der Identifizierung des Inhabers auch eine Verifizierung der Akzeptanzstelle als des „richtigen" Vertragspartners. Nur dann, wenn die betreffende Stelle im Rahmen der gesetzlich oder vertraglich gestalteten Kommunikation auch berechtigt ist, die Echtheit und Richtigkeit der Daten des Inhabers zu prüfen, handelt diese Stelle als Verifier. Soweit der Verifier eine andere öffentliche Stelle des herausgebenden Trägers ist, aber auch bei („eigenen") öffentlichen Unternehmen, kann sich die Pflicht zur Anerkennung der mit der kommunalen Datenkarte nachgewiesenen Eigenschaften direkt auf verbindliche Regelungen der Gemeinde stützen. Im Fall von privaten Unternehmen

als Akzeptanzstelle muss eine Anerkennungspflicht vertraglich begründet werden. Im Hinblick auf den Inhaber liegt hier ein Vertrag zugunsten Dritter vor. Bei der Ausgestaltung und beim Abschluss dieser vertraglichen Vereinbarungen ist die kommunale Seite an die haushaltsrechtlichen und kommunalwirtschaftlichen Grundsätze gebunden.[8]

Im Sinne der verfassungsrechtlich garantierten kommunalen Selbstverwaltung obliegt es hier dem Aufgabenbereich der Gemeinde, den Service für die kommunale Datenkarte zu errichten und zu betreiben. Hierfür kann sie sich eigener hinreichend kontrollierter öffentlicher Unternehmen in öffentlicher oder privater Rechtsform bedienen. Da Gemeinden generell kostendeckend arbeiten müssen, können kommunale Dienstleistungen (bei entsprechender Satzung) auch gegen Entgelt (Gebühr oder privatrechtlicher Preis) angeboten werden.

Im Rahmen der Servicebereitstellung sind natürlich die technischen, organisatorischen und tatsächlichen Anforderungen an Hard- und Software sowie Schnittstellen zu beachten, welche gesetzlich reguliert sind. So ist an eine entsprechende Offline-Nutzbarkeit und Barrierefreiheit zu denken, sowie gleichermaßen auch an (technische) Anforderungen (Smartphone) an den Nutzer und dessen Fähigkeiten. Die Verantwortlichkeit des Herausgebers bzw. Betreibers unterschiedet sich im Hinblick auf Datenschutz, Datensicherheit und Datensicherung nicht grundsätzlich von herkömmlichen Anforderungen an Betreiber „herkömmlicher" Identifizierungs- und Authentifizierungsbetreiber (physische Karten). Die Akzeptanz der Nachweise in dem kommunalen Datenkarten-Ökosystem sollte von der Gemeinde in ein Regelwerk überführt werden.

3.2 (Europa-) rechtliche Entwicklungen

Mit der Verordnung 910/2014 der EU über Electronic Identification, Authentication and Trust Services (eIDAS 2014) wurde 2014 ein Rahmen geschaffen, um die gegenseitige Anerkennung der verwendeten Identifizierungsmittel und Vertrauensdienste sowie deren Interoperabilität zu fördern. Die Verordnung dient der Stärkung des Vertrauens in elektronische Transaktionen im Binnenmarkt, indem eine gemeinsame Grundlage für eine sichere elektronische Interaktion zwischen Bürgern, Unternehmen und

8 Dies geht aus einer für das Projekt ID-Ideal erstellten Stellungnahme aus 2024 hervor.

öffentlichen Verwaltungen geschaffen wird, wodurch die Effektivität öffentlicher und privater Online-Dienstleistungen, des elektronischen Geschäftsverkehrs und des elektronischen Handels in der Union erhöht wird.[9]

Mit der der Novellierung vom 11. April 2024 (EU Parliament 2024) werden mit Artikel 6a digitale Brieftaschen/Wallets als zentrales Element und weitgehend einheitliches Mittel zur Identifizierung in der EU eingeführt. Jeder Mitgliedstaat ist nach Artikel 6a Abs. 2 verpflichtet, eine notifizierte European Digital Identity Wallet (EUDI Wallet) herauszugeben. Jede natürliche und juristische Person muss einen nahtlosen Zugang bekommen (Artikel 6a Abs. 1). Die EUDI Wallet muss sowohl gesetzliche Daten zur Identifizierung einer Person enthalten und auch elektronische Attribute online und offline managen können (Artikel 6a Abs. 3 lit. a). Sie muss Schnittstellen für Vertrauensdiensteanbieter bieten, welche Attributsbescheinigungen herausgeben können. Vorgesehen ist, dass die EUDI Wallet neben (direkten) hoheitlichen Attributen (High Level of Assurance, Type 1, communication protocol: OpenID4VC (OpenID for verifiable credentials)) wie solche aus dem Personalausweis auch solche Nachweise unterstützen soll, die nicht dem High Level of Assurance und/oder dem OpenID4VC Protokoll entsprechen (Type 2). Mit der vorgesehenen Konfiguration wird das Imitieren und Verwalten von Diensten wie der kommunalen Datenkarte über die EUDI Wallet generell möglich.

4. Potenziale und Herausforderungen der kommunalen Datenkarte für selbstbestimmtes Datenteilen

Die Erfahrungen aus der Pilotierung der kommunalen Datenkarte sowie die Betrachtung der Entwicklungen im Umfeld der Schaufensterprojekte ermöglicht die Formulierung einer Reihe von Thesen, die im Folgenden erläutert werden. Sie leiten die weiteren Forschungs- und Entwicklungsarbeiten rund um das Konzept und werden hiermit zur breiteren Diskussion gestellt.

Die Implementierung der kommunalen Datenkarte, die auf der Technologie der Self-Sovereign Identity (SSI) fußt, bietet neue Perspektiven im Umgang mit personenbezogenen Daten und weist das Potenzial auf, die Datenhoheit der Bürger signifikant zu stärken. SSI ermöglicht es Nutzern, ihre Identitätsdaten eigenständig zu verwalten und zu kontrollieren,

9 Erwägungsgrund 2 der eIDAS-VO.

was eine wesentliche Abkehr von zentralisierten Identitätsmanagementsystemen darstellt. Dies trägt zu einem verbesserten Datenschutz bei, da die Datenverarbeitung und -speicherung dezentralisiert wird und Bürger genau bestimmen können, welche Daten sie für welche Zwecke freigeben. Indem die kommunale Datenkarte verifizierbare digitale Nachweise, die aus zuverlässigen Quellen wie dem Melderegister der öffentlichen Verwaltung stammen, in einer mobilen Wallet zugänglich macht, werden nicht nur Verwaltungsprozesse effizienter gestaltet, sondern es wird auch die Selbstbestimmung des Einzelnen über seine persönlichen Daten gefördert. Faktisch werden zahlreiche digitale Verwaltungsprozesse so erst möglich.

Die Verfügbarkeit von Werkzeugen, wie der kommunalen Datenkarte, die selektive Datenbereitstellung ermöglichen, könnte das Verhalten der Bürger im Umgang mit ihren personenbezogenen Daten entscheidend verändern. Die Hypothese, dass Bürger solche Spielräume aktiv nutzen werden, fußt auf dem zunehmenden Bewusstsein für Datenschutz und dem Wunsch nach mehr Kontrolle über die eigenen Daten. Mit einer SSI-basierten Lösung haben sie die bedienungsfreundliche Möglichkeit, selbst zu entscheiden, welche Informationen sie für welche Dienste freigeben, und können diese Datenfreigabe jederzeit widerrufen. Dies stärkt nicht nur das Vertrauen in digitale Dienstleistungen, sondern erhöht auch die Bereitschaft, digitale Verwaltungsdienste in Anspruch zu nehmen. Voraussetzung hierfür ist jedoch, dass die Bürger sowohl über das nötige Wissen verfügen, um die Technologien adäquat zu nutzen, als auch dass die Dienste selbst benutzerfreundlich und leicht zugänglich gestaltet sind. Damit diese Potenziale voll ausgeschöpft werden können, müssen die öffentlichen Verwaltungen und Dienstleister sicherstellen, dass die Schnittstellen und Prozesse für die Datenbereitstellung an die Bedürfnisse der Bürger angepasst sind und eine ausreichende Aufklärung über die Funktionsweise und Vorteile der selektiven Datenbereitstellung erfolgt.

Die Annahme, dass sowohl private als auch öffentliche Anbieter digitaler Dienstleistungen Konzepte zur Datenminimierung und zur Datensparsamkeit aufgreifen, solange dies ihre Wertschöpfung und Kostenstruktur unberührt lässt, spiegelt eine pragmatische Herangehensweise an das Datenschutzprinzip der Datenminimierung wider. Unter der Voraussetzung, dass durch die Beschränkung auf das Notwendigste keine finanziellen Einbußen oder Einbußen in der Servicequalität entstehen, könnten Anbieter geneigt sein, weniger Daten zu sammeln und zu verarbeiten. Dieses Vorgehen wäre nicht nur konform mit datenschutzrechtlichen Anforderungen, wie sie etwa die DSGVO vorschreibt, sondern könnte auch das Vertrauen

der Nutzer stärken und somit langfristig zur Kundenbindung beitragen. Darüber hinaus senkt es das Risiko aus potenziellen Datenabflüssen. Um dieses Potenzial zu realisieren, ist es jedoch erforderlich, dass die Anbieter den Mehrwert der Datenminimierung erkennen und ihnen der Umstieg auf diese so leicht wie möglich gemacht wird.

Es wurden jedoch auch noch einige Herausforderungen deutlich. Mit der kommunalen Datenkarte, wie generell mit SSI Credentials, erhalten Bürger die Möglichkeit, signierte Nachweise aus vertrauenswürdigen Quellen einfach weiterzugeben. Diese Nachweise könnten auch für potenzielle Angreifer äußerst wertvoll sein und es sind Situationen denkbar, in denen von einem selbstbestimmten Datenteilen nicht mehr die Rede sein kann. Illustriert werden kann dies mit dem Bild des 800-Pfund Gorillas: *„"What do you give an 800-pound gorilla?", answer: "Anything that it asks for". Examples of such 800-pound gorillas are some big-tech websites, immigration offices and uniformed individuals alleging to represent law-enforcement. Also, the typical client-server nature of web transactions reinforces this power imbalance, where the human party behind its client agent feels coerced into surrendering personal data as otherwise they are denied access to a product, service or location.*" (van Deventer 2020). Die Daten der kommunale Datenkarte müssen entsprechend gegen solche 800-Pfund Gorillas abgesichert werden. Hierzu können etwa Maßnahmen getroffen werden, die lediglich zertifizierten Stellen erlauben, auf diese Daten zuzugreifen – wie es im Falle des Berechtigungszertifikates des Personalausweises bereits praktiziert wird und wofür bereits verschiedene technische Ansätze für Wallets existieren. Diese zusätzliche Governance-Anforderung ist jedoch nicht ohne wesentliche Nachteile, erschwert sie doch wiederum die Adoption der Technologie durch Serviceanbieter.

Die fortlaufende Dynamik regulatorischer Entwicklungen sowie der technologischen Basis stellt darüber hinaus eine wesentliche Herausforderung für Projekte wie die Implementierung der kommunalen Datenkarte dar. Sowohl auf deutscher (Onlinezugangsgesetz, gestoppte Einführung der Smart-eID, etc.) wie auf europäischer Ebene mit eIDAS 2.0 und der EUDI Wallet ist der Wandel die einzige Konstante. Dies führt jedoch dazu, dass es aus Sicht vieler Beteiligter noch keinen Sinn ergibt, sich bereits jetzt auf eine bestimmte Lösung festzulegen. Beispielsweise wird dann argumentiert, dass die europäische Lösung in mehr oder weniger naher Zukunft ohnehin bald alle anderen Lösungen ersetzen wird. Entsprechend mache die Integration einer Lösung derzeit wenig Sinn. Gleichzeitig entwickeln sich auch Standards und Protokolle der SSI-Technologie kontinuierlich

weiter, Inkompatibilitäten bestehen und teilweise ist der technologische Reifegrad noch nicht begrenzt. Auch dies verstärkt die nachvollziehbare Tendenz zahlreicher Entscheider, erst einmal abzuwarten, bis sich eine stabile technische Basis herausgebildet hat. Schließlich will man nicht aufs falsche Pferd setzen und in einer technologischen Sackgasse enden. Das Resultat dieser Entscheidungen ist dann jedoch ein faktischer Stillstand.

5. Fazit

Self-Sovereign Identity und Wallets sind Werkzeuge, um digitale Identität von Personen und Organisationen zu verwalten, Identitäts- und Berechtigungsnachweise zu erbringen und zu kontrollieren, aber auch um Daten auszutauschen und die Verarbeitung zu legitimieren. Für die Nutzer dieser Werkzeuge bieten sie neue Möglichkeiten im Hinblick auf Selbstbestimmtheit und Transparenz. Im Hinblick auf die Digitalisierungsbestrebungen eröffnen sich neue Gestaltungsräume, um die Aufwände für die Datenhaltung zu minimieren, die Qualität von Daten zu verbessern und Daten interessengerechter verarbeiten zu können. Es ist erkennbar, dass SSI und Wallets, durch neuartige Mechanismen für Identitäts- und Berechtigungsnachweise sowie für Datenbereitstellungen, einen Paradigmenwechsel herbeiführen können, hin zu einer verbesserten Selbstbestimmtheit und zu interessengerechterer Data Governance. Positive Nutzererlebnisse und Akzeptanz sind neben den technischen Weiterentwicklungen, der Schlüssel zu diesen Verbesserungen. Diese Potentiale zu heben, ist deshalb Gegenstand weiterer interdisziplinärer Forschung.

Literatur

Allen, Christopher (2016): The Path to Self-Sovereign Identity. GitHub. URL: https://github.com/ChristopherA/self-sovereign-identity (besucht am 5.2.2024).

Bundesministerium für Wirtschaft und Klimaschutz (2024): Schaufenster Sichere Digitale Identitäten. URL: https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html (besucht am 8.2.2024).

D21 und TU München (2023): eGovernment MONITOR 2023. URL: https://initiatived21.de/uploads/03_Studien-Publikationen/eGovernment-MONITOR/2023/egovernment_monitor_23.pdf (besucht am: 6.2.2024).

van Deventer, Oskar (2020): Verify the verifier: anti-coercion by design | TNO. tno.nl/en. URL: https://www.tno.nl/en/newsroom/insights/2020/10/verify-verifier-anti-coercion-design/ (besucht am: 25.3.2024).

DGA (2022): Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868&from=EN (besucht am: 25.3.2024).

DMA (2022): Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). URL: https://eur-lex.europa.eu/eli/reg/2022/1925/oj (besucht am: 25.3.2024).

eIDAS (2014): Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32014R0910 (besucht am: 25.3.2024).

eIDAS 2.0 (2024): Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1183&qid=1716387048511 (besucht am 20.5.2024)).

eIDAS Expert Group (2024): EUDI Wallet - Architecture and Reference Framework 1.3.0. URL: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.3.0/ (besucht am: 25.3.2024).

EU Commission (2024): What are the Large Scale Pilot Projects - EU Digital Identity Wallet. URL: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+are+the+Large+Scale+Pilot+Projects (besucht am: 25.3.2024).

European Commission (2024): EU Digital Identity Wallet Home - EU Digital Identity Wallet. URL: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/ (besucht am: 25.3.2024).

ID-Ideal und ONCE (2023): Anforderungen aus Sicht der SDI-Schaufenster ONCE und ID-Ideal an die Entwicklung der EUDI Wallet. URL: https://id-ideal.de/wp-content/uploads/2024/01/Anforderungen-an-EUDIW-aus-Sicht-von-ONCE-ID-Ideal.pdf (besucht am: 25.3.2024).

Krempl, Stefan (2023): Smart-eID: Online-Ausweisen mit dem Handy soll von Ende 2023 an machbar sein. heise online. URL: https://www.heise.de/news/Smart-eID-Online-Ausweisen-mit-dem-Handy-soll-von-Ende-2023-an-machbar-sein-9304284.html (besucht am: 25.3.2024).

Landeshauptstadt Dresden (2022): Faltblatt Dresden Pass. URL: https://www.dresden.de/media/pdf/infoblaetter/faltblatt-dresden-pass.pdf (besucht am: 25.3.2024).

Röhl, Klaus-Heiner (2023): Verwaltungsdigitalisierung in Deutschland: Der Stand zum Zielzeitpunkt des Onlinezugangsgesetzes Anfang 2023. IW-Report 20/23.

Stadt Leipzig (2024): Bürgerbegehren und Bürgerentscheid - Stadt Leipzig. URL: https://www.leipzig.de/buergerservice-und-verwaltung/buergerbeteiligung-und-einflussnahme/buergerbegehren-und-buergerentscheid (besucht am: 25.3.2024).

Steiner, Falk (2023): *Smarte eID: Online-Ausweis wegen Haushaltslage vorerst gestoppt*. heise online. URL: https://www.heise.de/news/Smarte-eID-Online-Ausweis-wegen-Haushaltslage-vorerst-gestoppt-9576180.html (besucht am: 25.3.2024).

W3C (2022): Verifiable Credentials Data Model v1.1. W3C Recommendation. URL: https://www.w3.org/TR/vc-data-model/ (besucht am: 16.3.2022).