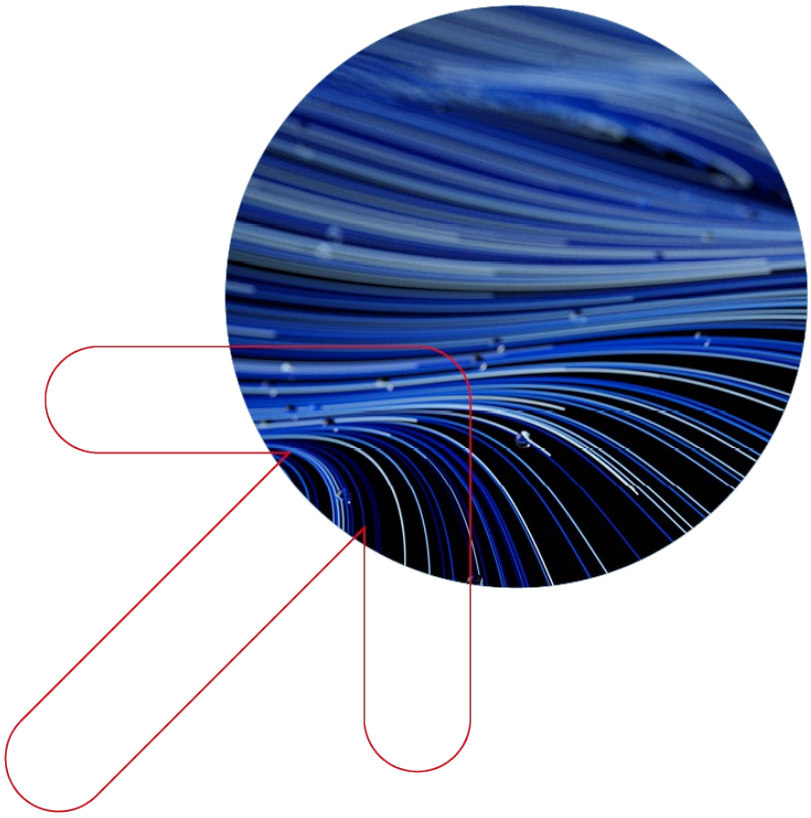
WIK • Diskussionsbeitrag

Nr. 503



# Digitale Identitäten als Fundament des Web 3.0

Autoren:
Pirmin Puhl
Malte Roloff
Christian Märkel
Martin Lundborg

Bad Honnef, Dezember 2023

WIK
Wissenschaftliches Institut
für Infrastruktur und
Kommunikationsdienste

# Impressum

WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Deutschland
Tel.: +49 2224 9225-0
Fax: +49 2224 9225-63
E-Mail: info@wik.org
www.wik.org

**Vertretungs- und zeichnungsberechtigte Personen**

| | |
|---|---|
| Geschäftsführerin und Direktorin | Dr. Cara Schwarz-Schilling |
| Direktor<br>Abteilungsleiter<br>Smart Cities/Smart Regions | Alex Kalevi Dieke |
| Direktor<br>Abteilungsleiter<br>Netze und Kosten | Dr. Thomas Plückebaum |
| Direktor<br>Abteilungsleiter<br>Regulierung und Wettbewerb | Dr. Bernd Sörries |
| Leiter der Verwaltung | Karl-Hubert Strüver |
| Vorsitzender des Aufsichtsrates | Dr. Thomas Solbach |
| Handelsregister | Amtsgericht Siegburg, HRB 7225 |
| Steuer-Nr. | 222/5751/0722 |
| Umsatzsteueridentifikations-Nr. | DE 123 383 795 |

Stand: Juli 2023

ISSN 1865-8997



Weitere Diskussionsbeiträge finden Sie hier:
https://www.wik.org/veroeffentlichungen/diskussionsbeitraege

In den vom WIK herausgegebenen Diskussionsbeiträgen erscheinen in loser Folge Aufsätze und Vorträge von Mitarbeitern des Instituts sowie ausgewählte Zwischen- und Abschlussberichte von durchgeführten Forschungsprojekten. Mit der Herausgabe dieser Reihe bezweckt das WIK, über seine Tätigkeit zu informieren, Diskussionsanstöße zu geben, aber auch Anregungen von außen zu empfangen. Kritik und Kommentare sind deshalb jederzeit willkommen. Die in den verschiedenen Beiträgen zum Ausdruck kommenden Ansichten geben ausschließlich die Meinung der jeweiligen Autoren wieder.

# Inhalt

# Abbildungsverzeichnis

## Abkürzungsverzeichnis

***A***

ARF ..... European Digital Identity Architecture and Reference Framework

***B***

BMI ..... Bundesministerium des Innern und für Heimat

BMWK ..... Bundesministerium für Wirtschaft und Klimaforschung

BSI ..... Bundesamt für Sicherheit in der Informationstechnik

***D***

DID ..... Decentralised Identifiers

DLT ..... Distributed-Ledger-Technologie

DMA ..... Digital Markets Act

DSGVO ..... Datenschutzgrundverordnung

***E***

EBSI ..... European Blockchain Services Infrastructure

ESG ..... Environmental, Social and Governance

ESSIF ..... European Self-Sovereign Identity Framework

ETSI ..... European-Telecommunications

EU ..... Europäische Union

EUDI ..... European Digital Identity Wallet

EUDIW ..... European Digital Identity Wallet Foundation

***I***

IAM ..... Identity and Access Management, Identitäts- und Zugriffsmanagement

***K***

KMU ..... Kleinere und mittlere Unternehmen

KOM ..... Europäische Kommission

KYC ..... Know-Your-Customer

***L***

LSP ..... Large Scale Pilots

***Q***

QWAC ..... Qualified Website Authentication Certificates

***S***

SSI ..... Self Sovereign Identities, Selbstbestimmte Identitäten

***V***

VC ..... Verifiable Credential

VDR ..... Vertrauenswürdiges Datenregister

VID ..... Vehicle Identity

VIN ..... Vehicle Identification Number, Fahrzeugidentifikationsnummer

VP ..... Verifiable Presentation

## Zusammenfassung

Die Evolution des World Wide Web führt zu einem verstärkten Wunsch nach und Bedarf an dezentralen, selbstverwalteten Digitalen Identitäten, auch als Self-Sovereign Identities (SSI) bekannt. Im Gegensatz zu gegenwärtig verbreiteten zentralisierten und föderierten Digitalen Identitäten ermöglichen SSI den Usern eine eigenständige und selbstbestimmte Kontrolle über ihre Digitalen Identitäten, wodurch Datenschutz und -sicherheit auf ein neues Niveau gehoben werden. Diese Studie zielt darauf ab, das Themenfeld "Digitale Identitäten" zu strukturieren und die Rolle von SSI als fundamentalen Baustein des Web 3.0 zu untersuchen.

Der Fokus liegt auf den theoretischen Anforderungen an Identitäts- und Zugriffsmanagementsystemen (IAMs), die dezentrale und selbstverwaltete Ansätze verfolgen. Das Trust Triangle Framework mit den Rollen des Ausstellers, des Identitätshalters und der Akzeptanzstelle wird als vielversprechende technische Umsetzungsmöglichkeit vorgestellt. Dabei werden aktuelle Diskussionen über die Struktur von Datenregistern und die Handhabung von Personenidentitätsdaten beleuchtet. Die Studie hebt in diesem Zusammenhang die Potenziale von SSI hervor. Durch dezentrale Datenspeicherung und fortschrittliche Verschlüsselungstechniken tragen SSI nicht nur zur Erschwerung von Cyberkriminalität bei, sondern fördern auch Vertrauen und Datenkontrolle in der digitalen Welt. Die Einführung neuer Identitätsformen eröffnet Chancen, innovative Geschäftsmodelle zu entwickeln und Effizienzgewinne durch Prozessoptimierung zu realisieren.

Die bevorstehende Aktualisierung der Electronic Identification, Authentication and Trust Services (eIDAS)-Verordnung in der EU strebt die Schaffung einer dezentralen, selbstverwalteten Digitalen Identität für alle EU-Bürger an. Allerdings stehen rechtliche, regulatorische und Governance-Herausforderungen sowie offene Fragen zur Interoperabilität dem umfassenden Einsatz von SSI noch im Weg. Bedenken hinsichtlich Sicherheit und Benutzerfreundlichkeit könnten die Akzeptanz dieser Digitaler Identitäten beeinträchtigen.

Um den Herausforderungen gerecht zu werden und im Zusammenhang mit der Aktualisierung der eIDAS-Verordnung identifizierte Potenziale zu nutzen, eröffnen sich staatliche Handlungsoptionen und -bedarfe. Rechtliche Rahmenbedingungen müssen geschaffen, offene Fragen zu Standards und Technologien beantwortet und die Akzeptanz dezentraler Digitaler Identitäten gesteigert werden. Die Privatwirtschaft sollte durch Anreize ermutigt werden, innovative Geschäftsmodelle zu entwickeln und zur Entwicklung einer deutschen EU-Brieftasche (EUDI-Wallet-Lösung) beizutragen.

## Summary

The evolution of the World Wide Web is leading to an increased desire and need for decentralised, self-managed Digital Identities, also known as Self-Sovereign Identities (SSI). In contrast to current centralised and federated digital identities, SSIs allow users to have autonomous and self-determined control over their digital identities, taking privacy and security to a new level. This study aims to structure the topic of "Digital Identities" and to analyse the role of SSIs as a fundamental building block of Web 3.0.

The focus is on the theoretical requirements for identity and access management systems (IAMs) that pursue decentralised and self-managed approaches. The Trust Triangle Framework with the roles of the issuer, the identity holder and the acceptance centre is presented as a promising technical implementation option. Current discussions on the structure of data registers and the handling of personal identity data are highlighted. In this context, the study emphasises the potential of SSI. Through decentralised data storage and advanced encryption techniques, SSIs not only contribute to making cybercrime more difficult, but also promote trust and data control in the digital world. The introduction of new forms of identity opens up opportunities to develop innovative business models and realise efficiency gains through process optimisation.

The forthcoming update of the Electronic Identification, Authentication and Trust Services (eIDAS) Regulation in the EU aims to create a decentralised, self-managed digital identity for all EU citizens. However, legal, regulatory and governance challenges as well as open questions regarding interoperability still stand in the way of the widespread use of SSI. Concerns about security and user-friendliness could jeopardise the acceptance of these digital identities.

In order to meet the challenges and utilise the potential identified in connection with the updating of the eIDAS Regulation, government options and requirements for action are opening up. A legal framework must be created, open questions about standards and technologies must be answered and the acceptance of decentralised digital identities must be increased. The private sector should be incentivised to develop innovative business models and contribute to the development of a German EUDI-Wallet solution.

# 1 Einleitung

Spätestens mit der Idee mehrere User in einem Computersystem zusammenarbeiten zu lassen, stellte sich erstmals die Frage nach einem geeigneten Identitäts- und Zugriffsmanagement der User und damit deren sogenannter Digitalen Identität. Mit dem TCP/IP-Referenzmodell wurde die Möglichkeit eröffnet, eine sehr große Zahl von Endpunkten miteinander verbinden zu können. Die Grundlagen des Internets waren, sehr verkürzt dargestellt, geschaffen. In dieser Erfolgsgeschichte blieb allerdings ein zentraler Punkt offen: die zugrundeliegenden Netzwerkprotokolle lassen nur Rückschlüsse über die Adresse des verbundenen Rechners zu, nicht wer oder was ihn kontrolliert. Kim Cameron konstatierte Jahre später, dass das Internet ohne die Möglichkeit entwickelt wurde, zu wissen, mit wem und was man sich verbindet.[1] Cameron prognostizierte in diesem Zusammenhang, dass die Gesellschaft aufgrund dieses Mangels mit einer raschen Zunahme von Identitätsdiebstählen und Täuschungen konfrontiert sein werde, die das Vertrauen in das Internet zunehmend untergrabe.[2] Erschwerend kommt hinzu, dass die User bislang die Speicherung und Verwaltung ihrer Identitätsdaten aus der Hand geben müssen, um Onlineangebote und -dienstleistungen nutzen zu können. Ein Umdenken bei Digitalen Identitäten könnte dazu beitragen, diese Probleme zu überwinden, indem die Art und Weise, wie Identität und Vertrauen im Internet verwaltet werden, neu gestaltet werden.

Ein viel diskutierter Ansatz sind die Self-Sovereign Identities (SSI), die es Personen, Organisationen und Maschinen ermöglichen, universell gültige und interoperable Digitale Identitäten zu schaffen. Sie können vom User unabhängig von Ausstellern oder Online-Diensten für jeden Zweck und bei jedem beliebigen Online-Dienst genutzt werden. Die Kontrolle über den Datenzugriff und die Datenverwendung verbleiben dabei bei dem User. Statt in einem zentral verwalteten Datensilo (wie bisher üblich) liegen die Daten und Identitätsnachweise nun in einer digitalen Wallet, aus der die jeweils benötigten Datenpunkte zielgenau für eine Transaktion herangezogen werden können. Aus der dezentralen Lösung der SSI resultiert eine Stärkung der digitalen Souveränität der User. Dieses Prinzip bietet Potenzial für neue Dienste und Geschäftsmodelle, die weniger von den zentralen Anbietern der Plattformökonomie abhängig sind. Die bestehenden Strukturen der (Internet-)Wirtschaft könnten maßgeblich verändert werden.

Ziel dieser Studie ist es, das Themenfeld „Digitale Identitäten“ in einem ersten Schritt zu systematisieren, indem die verschiedenen Ansätze analysiert und kategorisiert werden. Dabei wird festgehalten, welche Anforderungen Digitale Identitäten erfüllen müssen, damit sie das Fundament des Web 3.0[3] bilden können (Kapitel 2). Im folgenden Schritt soll erarbeitet werden, welche Chancen diese Web 3.0-konformen Digitalen Identitäten

1 Vgl. Cameron, K. (2005).
2 Vgl. ebd.
3 Mit dem Begriff Web 3.0 wird in der Literatur mitunter auch Bezug auf das „Semantic Web“ im Sinne eines maschinenlesbaren World Wide Web genommen. Im vorliegenden Forschungsprojekt wird der Begriff Web 3.0 hingegen als synonym für den Begriff Web3 verwendet.

bieten, aber auch welche Herausforderungen damit einhergehen (Kapitel 3). Daraus leiten wir notwendige (staatliche) Handlungsbedarfe und -optionen ab und geben eine Schlussbemerkung, inwiefern Digitale Identitäten das Web 3.0 prägen können (Kapitel 4).

Folgende Forschungsfragen wurden der Studie zu Grunde gelegt:

1. Welche Ansätze zu Digitalen Identitäten gibt es und wodurch zeichnen sich diese aus?
2. Welche Anforderungen müssen Digitale Identitäten erfüllen, damit sie als Fundament des Web 3.0 dienen können? Welche Bedeutung kommt SSI zu?
3. Welche Chancen bieten Web 3.0-konforme Digitale Identitäten für die Wirtschaft, z. B. unter den Aspekten Informationssicherheit, Datensouveränität, Vertrauen und User-Akzeptanz, und welche Herausforderungen gehen hiermit einher?
4. Welcher (staatliche) Handlungsbedarf besteht bezüglich der Realisierung dezentraler, selbstverwalteter Digitaler Identitäten?

## 2 Web 3.0 und Digitale Identitäten: Definition und Ansätze

Im folgenden Kapitel werden die Notwendigkeiten und Anforderungen dargestellt, die auf Digitale Identitäten im Web 3.0 zukommen. Dazu wird ausgeführt, welche Rolle das Web 3.0 sowie seine Vorgänger im Zusammenhang mit der Datensouveränität spielen. Zudem werden die existierenden Ansätze Digitaler Identitäten sowie deren Charakteristika eingeführt. Dabei wird das Konzept der SSI näher betrachtet und skizziert, welche Bedeutung ihm zukommen könnte.

### 2.1 Das Web 3.0 als Grundlage der Datensouveränität

Der Begriff Web 3.0 bezeichnet eine Weiterentwicklung des World Wide Webs, welche sich von den Entwicklungsstufen des Web 1.0 und des Web 2.0 insbesondere durch eine dezentral organisierte souveräne Selbstverwaltung des Datenzugriffs unterscheidet. Während sich das Web 1.0 durch den monodirektionalen und statischen Zugang zu Daten bzw. Informationen ausgezeichnet hat („Read-only Web“[4]) und für das Web 2.0 das bidirektionale Generieren und Teilen von Daten bzw. Informationen in zentral organisierten Netzwerken bzw. Plattformen prägend ist („Participative Social Web“[5]), steht beim dezentral geprägten Web 3.0 die individualbezogene souveräne Kontrolle über den Zugang zu Daten bzw. Informationen sowie die Ermöglichung des eindeutigen digitalen Nachweises von Identitätsmerkmalen und des Besitzes von digitalen Assets im Vordergrund („Web of Values“[6]). Hierdurch ermöglicht das Web 3.0 die Tokenisierung, also die digitale Abbildung von Vermögenswerten, und wird damit zur Grundlage der Tokenökonomie, von der neue Geschäftsmodelle und -felder für die Volkswirtschaft ausgehen können. Grundgerüst für ein Funktionieren des Web 3.0 sind eindeutige Digitale Identitäten, die sich durch Datensouveränität und Datensicherheit auszeichnen.

Abbildung 1: Entwicklung und Unterschiede des Web 1.0, 2.0 und 3.0


Quelle: WIK, eigene Darstellung.

4 Vgl. Nath, K. et al. (2014).
5 Vgl. Zavratnik, J. (2022).
6 Vgl. Winfield, A. (2017).

## 2.2 Definition „Digitale Identität“

Eine **Digitale Identität** hat den Zweck, die Akteure im digitalen Raum auszuweisen: „*Mit Hilfe einer digitalen Identität kann sich jeder, der im Netz kommuniziert, eindeutig zu erkennen geben – sei es eine natürliche oder eine juristische Person, eine Maschine oder ein Prozess.*“[7] Sie dient also der virtuellen Repräsentation einer realen Identität (auch Entität genannt) bei Interaktionen in digitalen Systemen.[8]

Eine Digitale Identität setzt sich aus einer (Teil-)Menge von **Attributen** zusammen, die eine **Entität** (natürliche oder juristische Person, aber auch Objekte) eindeutig von anderen unterscheidet.[9] Dies können entweder:

- Einzigartige Merkmale sein, die offensichtlich mit einer Entität in Verbindung gebracht werden und auf sie hinweisen, wie etwa Vor- und Nachname sowie die Adresse einer natürlichen Person, Firmenname und Umsatzsteuer-Identifikationsnummer sowie die Adresse einer juristischen Person oder auch Serien- und Gerätenummern von Maschinen und Geräten (also Objekten).
- Oder aber Merkmale sein, die mehrere Entitäten aufweisen wie etwa Zeugnisse, Qualifikationen und Befugnisse von natürlichen Personen, Produkteigenschaften von Objekten oder sogar das Verhalten von Entitäten wie etwa Zugriffgewohnheiten im Internet.

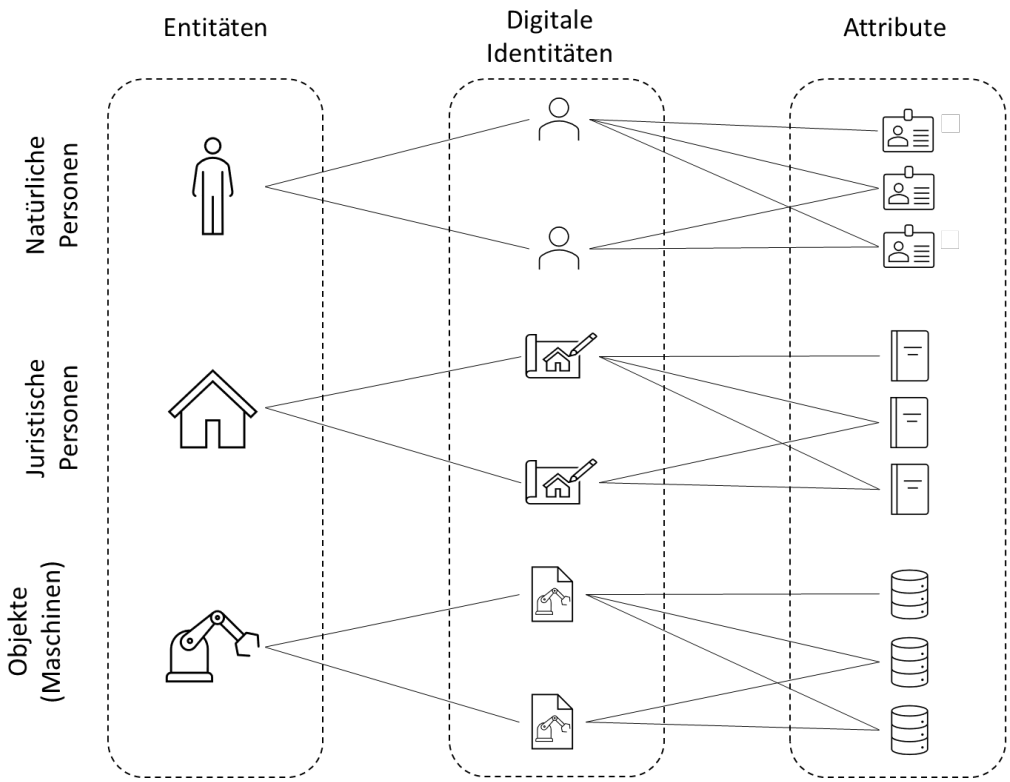
Einer Entität können Attribute entweder von anderen Entitäten zugesprochen werden oder eine Entität kann sich Attribute selbst zusprechen. Dabei können alle oder auch nur eine Teilmenge der Attribute digital festgehalten sein (siehe Abbildung 2).

Eine Entität kann mehrere Digitale Identitäten haben (s. Abbildung 2), die jeweils mit einem eindeutigen **Identifikator** (Identifier) wie z. B. einem Usernamen, einer E-Mail-Adresse oder einer Kennnummer verknüpft sind.[10] Der Zugriff auf einen digitalen Dienst muss jedoch nicht unbedingt bedeuten, dass die Identität der Entität im wirklichen Leben bekannt ist.[11] Eine Entität kann bei unterschiedlichen Diensten z. B. unterschiedliche Usernamen wählen, die auch in keiner Weise Rückschlüsse auf die Entität zulassen.

---

**7** Vgl. VSDI (2020), S. 2.
**8** Vgl. Camp, J. L. (2004).
**9** Vgl. Pohlmann, N. (2023); ISO/IEC (2019): 3.1.2 partial identity.
**10** Vgl. ISO/IEC 24760-1:2019: 3.1.4 identifier.
**11** Vgl. Grassi, P. et al. (2017).

Abbildung 2: Zusammenhang zwischen Entitäten, Digitalen Identitäten und Attributen




Quelle: WIK, eigene Darstellung in Anlehnung an Jøsang, A., Pope, S. (2005).

Im Zusammenhang mit Digitalen Identitäten sind sogenannte **Credentials** (Berechtigungsnachweise) von entscheidender Bedeutung. Credentials sind Informationen, die zum Nachweis der Identität bei der Authentifizierung verwendet werden. In physischer Form handelt es sich dabei z. B. um einen Ausweis. In digitaler Form handelt es sich um Informationen, über die nur die Entität verfügt (z. B. Zugangsdaten wie ein Passwort). Auch die Kombination aus beidem ist möglich. Credentials können auch eigene Attribute besitzen, wie z. B. Ausgabedatum, Gültigkeitsdauer.[12]

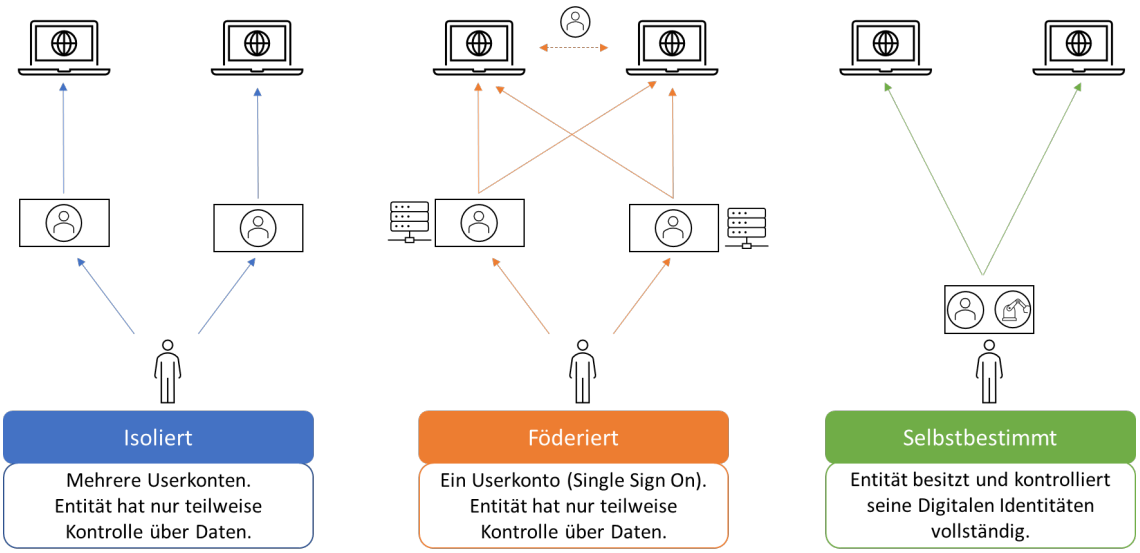
## 2.3 Identitäts- und Zugriffsmanagement Digitaler Identitäten

Weltweit nehmen bereits mehr als drei Milliarden Menschen digitale Identitätsdienste in Anspruch.[13] Laut Umfragen verwaltet ein Drittel der Deutschen bereits über 20 Digitale Identitäten, während andere Quellen sogar von rund 90 Digitalen Identitäten für einen durchschnittlichen Europäer sprechen.[14] Digitale Identitäten prägen somit unser

**12** Vgl. Anke, J., Richter, D. (2023).
**13** Vgl. McKinsey Global Institute (2019).
**14** Vgl. Begleitforschung Schaufenster Sichere Digitale Identitäten (2021); Bundesdruckerei (2020).

tägliches Leben. Diese werden mit Hilfe eines sogenannten **Identitäts- und Zugriffsmanagements** (IAM) verwaltet. In der Literatur finden sich unterschiedliche Modelle, die sich in den Methoden und zugeschriebenen Eigenschaften unterscheiden.[15] In dieser Studie führen wir nur die drei Modelle zum IAM auf, die jeweils prägend für eine der Entwicklungsphasen des World Wide Web sind. Wie in Abbildung 3 ersichtlich, handelt es sich bei den drei Modellen um isolierte Identitäten (Web 1.0), föderierte Identitäten (Web 2.0) sowie selbstbestimmte Identitäten (Web 3.0).

Abbildung 3: Vergleich von drei Modellen zum Identitäts- und Zugriffsmanagement Digitaler Identitäten




Quelle: WIK, eigene Darstellung in Anlehnung an Strüker, J., et al. (2021).

## Isolierte Identitäten

Beim Modell der isolierten Identitäten verwaltet und speichert ein Dienst (**Service Provider**) die Digitalen Identitäten der Entitäten, also der User, selbst.[16] Die Entität benötigt bei jedem Dienst einen eigenen Account, mit z. B. einem Usernamen als Identifier und einem Passwort zur Authentifizierung, der für jeden Dienst aufs Neue erstellt werden muss (s. Abbildung 3).[17]

Das Modell der isolierten Identitäten hat sich im Web 1.0 durchgesetzt und hat bis heute Bestand. Die Vorteile dieses Modells (insbesondere im Vergleich zu föderierten Identitäten, s.u.) liegen in der Unabhängigkeit von anderen Diensten. Sowohl der Service

15 Vgl. L'Amrani, H. et al. (2016).
16 In diesem Zusammenhang wird meist von Usern statt Entitäten gesprochen, da es sich ausschließlich um Digitale Identitäten für natürliche Personen handelt.
17 Vgl. Jøsang, A., Pope, S. (2005).

Provider, als auch die Entität, sind von Dritten unabhängig. Die Entität hat den Vorteil, dass ihre Aktivitäten nicht oder nur schwer Dienste-übergreifend nachverfolgt, in Korrelation gebracht und kontrolliert werden können.[18]

Für die isolierte Identität ergeben sich jedoch mehrere Nachteile. Jeder Account erfordert einen eigenen Usernamen und ein Passwort, was aufwendig ist und die Datensicherheit gefährdet. In der Realität werden dieselben Usernamen und Passwörter von einer Entität oft bei mehreren Diensten gleichzeitig verwendet, was zu Sicherheitslücken führt. Zudem ist jeder Service Provider selbst für die Datensicherheit verantwortlich. Bei einer Vielzahl an genutzten Diensten steigt damit auch die Wahrscheinlichkeit, dass Daten von unautorisierten Personen bei einem dieser Dienste eingesehen, gestohlen und anschließend missbraucht werden. Hinzu kommt, dass bei diesem Modell Digitale Identitäten nicht übertragbar sind. Alle benötigten Attribute müssen bei jedem Diensteanbieter wiederholt eingegeben werden, auch wenn es sich um die gleichen Attribute handelt.

**Föderierte Identitäten**

Beim Modell der föderierten Identitäten tritt zusätzlich zum Service Provider ein **Identity Provider** auf. Ein Identity Provider verwaltet und speichert Digitale Identitäten seiner User. Mit einem Account bei einem Identity Provider kann sich die Entität bei verschiedenen Service Providern registrieren, ohne dort separate Accounts erstellen zu müssen, vorausgesetzt dass die Service Provider in Verbindung mit den dem Identity Providern stehen. Der Identity Provider übernimmt dabei den Authentisierungs- und Authentifizierungsprozess. Bei diesem Modell verwaltet und speichert also ein Dienst die Digitale Identität der Entität für einen Verbund an Diensten, die in diesem Fall **Relying Party** genannt werden (s. Abbildung 3).[19] Man spricht dabei auch von **Single-Sign-On-Verfahren**. Der User erfährt insbesondere durch gesteigerte Usability Vorteile, da Registrierungsprozesse verkürzt bzw. nicht mehr benötigt werden. Die Service Provider können sich als sogenannte Relying Parties auf ihre eigentlichen Funktionalitäten und angebotenen Dienstleistungen wie z. B. den Verkauf von Waren oder Online-Services konzentrieren.

Im föderierten Modell kann es sowohl dedizierte Identity-Provider-Dienste geben, die sich nur um die Digitalen Identitäten und deren Sicherheit kümmern (also unabhängige Dienstleister), als auch Identity-Provider-Dienste von integrierten digitalen Plattformanbietern, wie Meta, Google usw., die sogenannte **Social-Login-Lösungen** anbieten.[20] In der Realität dominieren wenige digitale Plattformanbieter, die Social-Login-Lösungen anbieten, den Markt. [21]

Die Nachteile bei den föderierten Diensten liegen insbesondere in der mangelnden Datensouveränität der Entität. Der Identity Provider kann nachvollziehen, welchen Dienst

**18** Vgl. Ehrlich, T. et al (2021).
**19** Vgl. Jøsang, A., Pope, S. (2005).
**20** Vgl. Wiewiorra, L. et al. (2020).
**21** Vgl. ebd.

der User verwendet. Das Zusammenführen verschiedener Userdaten aus verschiedenen Diensten wird dem Identity Provider erleichtert und das generierte Wissen kann vom Identity Provider verwendet werden. Dies wird von Datenschutzrechtler:innen insbesondere für die Social-Login-Lösungen kritisch gesehen. Die Entität hat auch in diesem Modell nicht die vollständige Kontrolle über ihre Daten. Diese liegen zwar nur noch bedingt verteilt bei den einzelnen Service Providern, dafür aber zentralisiert bei den Identity Providern. Ein weiterer Nachteil von föderierten Identitäten ist, dass die Entität alle anderen Dienste beim Ausfall des Identity Providers gegebenenfalls nicht mehr oder nur eingeschränkt nutzen kann. Es ergibt sich auch ein Sicherheitsrisiko, wenn die Entität vom Schutz der Zugangsdaten eines einzelnen Dienstes (nämlich des Identity Providers) abhängig ist. Es ist darüber hinaus auch nicht anzunehmen, dass ein Identity Provider für alle Service Provider funktioniert, die eine Entität in Anspruch nehmen möchte. Zudem bestehen mögliche negative Konsequenzen für den Wettbewerb, wenn sich Service Provider in ein Abhängigkeitsverhältnis gegenüber weniger, marktbeherrschender Identity Provider begeben.

**Self-Sovereign Identities / selbstbestimmte Identitäten**

Im Modell der selbstbestimmten Identitäten hat die Entität bzw. die Identitätshalter:in die vollständige Kontrolle über ihre Daten bzw. über eine oder mehrere Digitale Identitäten (Subjekte) (s. Abbildung 3). Dies können personenbezogene Daten über die Entität selbst sein, aber auch Daten über andere Entitäten, für die die Identitätshalter:in verantwortlich oder bevollmächtigt ist (z. B. Eltern für ihre Kinder, Objekte im Besitz der Identitätshalterin, usw.).[22] Die Entität bzw. die Identitätshalter:in allein entscheidet, wann, wie und unter welchen Bedingungen diese Daten mit anderen geteilt werden. Diese Entscheidungsinstanz ist somit zentrale Verwalter:in der (Teil-)Identitäten. Damit einher geht, dass sie alleinige Entscheider:in über die der Entität zugeschriebenen Attribute ist. Dafür kann sie der Entität entweder selbst identitätsstiftende Attribute anlegen und diese bei Bedarf durch Dritte verifizieren lassen oder durch andere, ihr zugeschriebene identitätsstiftende Attribute selbst verifizieren.

Dabei gilt: Die Daten müssen gegenwärtigen Sicherheitsansprüchen genügen, um diese Prinzipien nicht zu verletzen. Hierfür zeichnet sich SSI entgegen konventionellen Ansätzen, personenbezogene Daten in zentralen Datenbanken zu sichern, durch die dezentrale Verwaltung und Haltung identitätsstiftender Nachweise aus, die ausschließlich bei der Entität selbst vorliegen.[23] Zur Verschlüsselung werden z. B. kryptographische Techniken wie digitale Signaturen sowie **Zero-Knowledge-Proofs** und **Public-Key-Infrastruktur** genutzt.[24] Christopher Allen formulierte in seinem Beitrag „The Path to Self-Sovereign Identity“ zehn Prinzipien zur Erfüllung dieser notwendigen Anforderungen, um

**22** Vgl. Begleitforschung Sichere Digitale Identitäten (2022).
**23** Vgl. Strüker, J. et al. (2021).
**24** Vgl. Schellinger, B. et al. (2022).

ein Rahmenwerk für SSI zu schaffen.[25] (s. Textbox *Zehn Anforderungen an SSI nach Christopher Allen*)

SSI stellt somit ein mögliches Konzept dar, um ein bisher stark fragmentiertes Ökosystem Digitaler Identitäten zu harmonisieren. Der dezentrale Ansatz schafft die Grundlage für einen weniger risikobehafteten Umgang mit sensiblen Daten und bezieht gleichzeitig die Nutzenden als zentrale Träger:innen ihrer persönlichen identitätsstiftenden Attribute mit ein.[26] Die genutzten Identitätsnachweise ((Verifiable Credentials, VCs) s. Kapitel 2.4) ermöglichen es, dass nahezu jeder Nachweis auch für juristische Personen z. B. Organisationen, Unternehmen und Objekte (z. B. im Internet of Things digital erfolgen kann (s. Abbildung 4)).[27]

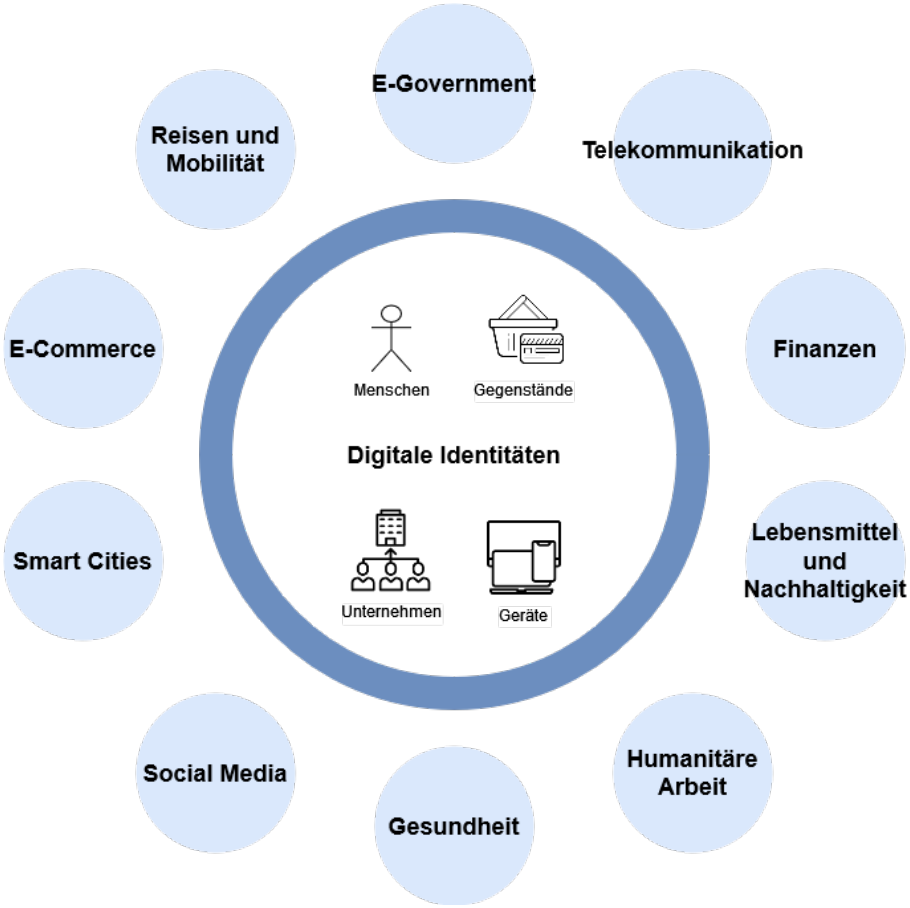
Zehn Anforderungen an SSI nach Christopher Allen (2016):*

1) **Existenz**: User müssen eine unabhängige Digitale Identität besitzen können.
2) **Kontrolle**: User sind in vollständiger Kontrolle ihrer Digitalen Identität.
3) **Einverständnis**: Für die Verwendung von Digitalen Identitäten bedürfen Entitäten der Zustimmung der identitätshaltenden User.
4) **Zugriff**: User müssen auf alle Aspekte ihrer Digitalen Identität zugreifen können, auch wenn Teilidentitäten von anderen Entitäten verwaltet werden.
5) **Transparenz**: Das Identitätsmanagementsystem muss für alle verfügbar und nutzbar sowie durch Open-Source-Code transparent sein.
6) **Übertragbarkeit**: Informationen und Daten einer selbstbestimmten digitalen Identität müssen interoperabel sein. Ändern sich Befugnisse von Entitäten durch Wegfall oder Regulierung ebendieser, obliegt die Hoheit der persönlicher Daten stets den Usern selbst.
7) **Interoperabilität**: Selbstbestimmte Identitäten müssen zwischen Anwendungsbereichen interoperabel nutzbar sein und somit unabhängig von Grenzen und existierenden Systemen sein.
8) **Minimalisierung**: Die Offenlegung von Daten muss minimiert werden, sodass personenbezogene Daten bei Verifizierungen von Digitalen Identitäten nur selektiv nach Ermessen der User geteilt werden.
9) **Schutz**: Die Rechte der User besitzen in jedem Anwendungsfall Priorität und werden im Konfliktfall am höchsten gewichtet.
10) **Langlebigkeit**: Die User bestimmen wie lange ihre jeweiligen Digitale Identitäten Bestand haben und gleichzeitig, wenn diese gelöscht werden sollen (Recht auf Vergessen).

* Vgl. Strüker, J. et al. (2021).

**25** Vgl. Allen, C. (2016).
**26** Vgl. Schellinger, B. et al. (2022).
**27** Vgl. Anke, J., Richter, D. (2023).

Abbildung 4: Anwendungsbereiche von SSI




Quelle: WIK, eigene Darstellung in Anlehnung an World Economic Forum (2023).

## 2.4 Einführung in Self-Sovereign Identity

Warum SSI grundsätzlich als digitales Identitätsmanagementsystem geeignet ist, wird im Folgenden veranschaulicht. Dazu werden der konzeptionelle Rahmen von SSI sowie mögliche Implementierungsverfahren dargestellt.

### 2.4.1 Akteure, Rollen und Funktionen

Im Gegensatz zu konventionellen, verschlüsselten Kommunikationsprotokollen wie **„http-over-Transport-Layer-Security** oder **„Secure-Socket-Layers“**, bei denen zentralisierte vertrauenswürdige Organisationen und Institutionen digitale Zertifikate ausstellen, um Personen, Unternehmen und andere digitale Entitäten zu verifizieren,

versprechen SSI-Lösungen Dezentralität und Datensouveränität.[28] Dennoch müssen bei SSI ebenfalls Vertrauensanker existieren, die einen sicheren Austausch zwischen allen beteiligten Parteien ermöglichen. Damit SSI die zehn Prinzipien nach Christopher Allen erfüllen, müssen drei wesentliche Bestandteile gegeben sein:[29]

1. **Dezentrale Identifikatoren** (**Decentralised Identifiers,** DIDs) bilden die Grundlage zur Authentifikation und dem Austausch von digital signierten Nachweisen. Sie können mit sogenannten **Uniform Resource Identifiers** realisiert werden. Diese bestehen aus einer bestimmten Zeichenfolge, die eindeutig einer Digitalen Identität (DID-Subjekt) zugeordnet ist. Das DID-Subjekt kann jede Entität sein: eine Person, eine Gruppe, eine Organisation oder ein Objekt. In der Zeichenfolge eines DIDs werden das URI-Schema, die DID-Methode sowie ein spezifischer DID-Identifikator definiert (s. Abbildung 5).

   Abbildung 5: DID-Schema, DID-Methode und DID-Identifikator


   Quelle: WIK, eigene Darstellung, in Anlehnung an W3C (2022a).

   DIDs werden als kryptografisch gesicherte Interaktion zwischen zwei Parteien verwendet und sind vergleichbar mit **X.509-Zerfikaten**[30], die bei Web- und Serverprotokollen eingesetzt werden. Sie können global eindeutig identifizierbare Adressen (s. Abbildung 6) für SSI stellen.

**28** Pohlmann, N. (2022).
**29** Vgl. Ehrlich, T. et al. (2021).
**30** Das X.509 Zertifikat enthält einen öffentlichen Schlüssel, digitale Unterschriften sowie Informationen zur Identität des Zertifikates als auch zu der jeweiligen Zertifizierungsstelle (CA). Vgl. SSL.com (2019).

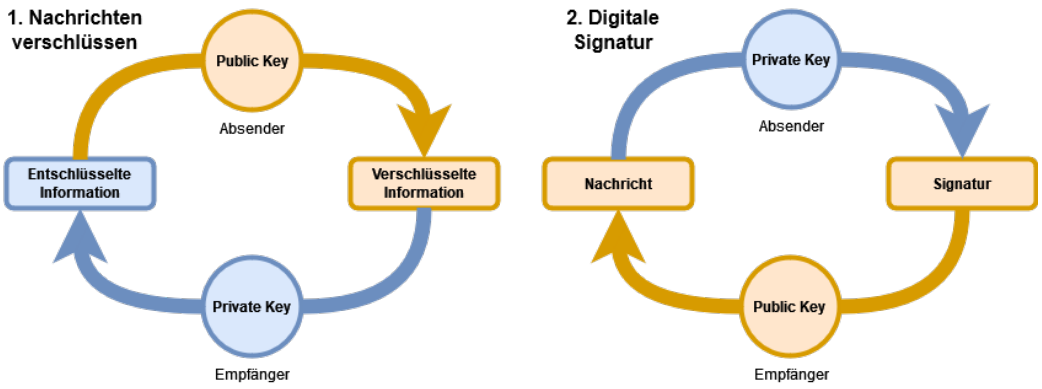
Abbildung 6: Öffentliche DIDs von Unternehmen und Organisationen

| Name der rechtlichen Einheit | Public:DID |
|---|---|
| IDunion SCE | did:sov:5CJcoPNuBpQHKtdEVXsM1M |
| mm1 Consulting GmbH | did:sov:BYWBUmMbVf6MronH8pL1Y3 |
| Deutsche Bahn AG | did:sov:PnAZpX85mnHNz8Xumqyqb6 |
| SBB – Schweizerische Bundesbahnen AG | did:sov:4ZUdBd9WedWVfDtntTUp83 |
| Robert Bosch GmbH | did:sov:Y7p6otrBDNowuCDRUabBxZ |
| neosfer GmbH | did:sov:5f95nKw1H5kXhYARxBorsJ |
| msg mySaveID GmbH | did:sov:3WDPV5zrNEWhAy9oRS2g8i |
| Bundesanzeiger Verlag | did:sov:DQFc11pkCqk6oi9X23RyRC |
| Siemens AG | did:sov:VaDkQ3ZMCfneZQXrNkP4fU |
| GS1 | did:sov:CisrppHJyZDD7VvDgrv2wf |
| SupplyOn AG | did:sov:URykoK85BAus7fXLZbhUNk |

Quelle: IDunion (2023a).

**2.** Des Weiteren bedarf es kryptografisch verschlüsselter Datenformate, um identitätsstiftende Attribute zu beschreiben. Viele SSI-Implementierungsansätze folgen der Methode der **asymmetrischen Kryptografie** oder Public-Key-Infrastruktur**.** Diese beruht auf sogenannten Schlüsselpaaren, einem privaten (vertraulichen) **Private Key** und einem öffentlichen (frei zugänglichen) **Public Key**, die zu einer Entität gehören. Mit diesen Schlüsselpaaren können Nachrichten verschlüsselt oder Dokumente signiert werden (s. Abbildung 7).

Abbildung 7: Verschlüsselungstechniken von Public-Key-Infrastruktur




Quelle: WIK, eigene Darstellung in Anlehnung an Diehl, A. (2023).

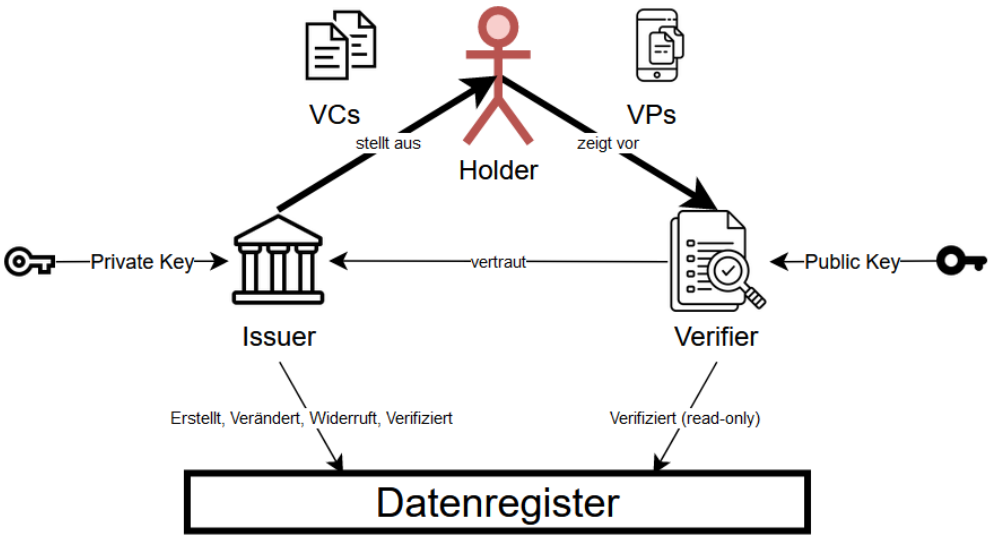
Public-Key-Infrastruktur kann genutzt werden, um Nachrichten zu verschlüsseln (links). Die Absender:in verschlüsselt die Nachricht mit dem öffentlichen Schlüssel der Empfänger:in, die diese mit ihrem privaten Schlüssel entschlüsseln kann. Um digitale Nachweise zu erstellen und verifizierbar zu machen, wird das Schlüsselpaar einer Absender:in benötigt (rechts). Diese signiert digitale Nachweise mit ihrem privaten Schlüssel. Die Gültigkeit und Korrektheit des signierten Dokumentes kann nun mithilfe des öffentlichen Schlüssels der Absender:in jederzeit aufgerufen und geprüft werden.

3. Schlussendlich bedarf es eines **Peer-to-Peer Protokolls** zur **Kommunikation** zwischen beteiligten Akteur:innen zur Ausstellung oder Verifizierung von digitalen Nachweisen. Für eine geschützte bilaterale Kommunikation zwischen den Akteur:innen werden diese von sogenannten **Digital Agents** (also Software wie bspw. digitale **Wallets** auf Endgeräten oder in der Cloud) als technische Endpunkte oder Treuhänder verwendet. Gleichzeitig werden die Digital Agents (z. B. Wallets) genutzt, um sensible private Informationen auf einem (mobilen) Endgerät oder in der Cloud zu bewahren. Dies können beispielsweise digitale Nachweise wie Verifiable Credentials (z. B. Ausweise) oder auch private Schlüssel sein. Im privatwirtschaftlichen Sektor existieren bereits Wallet-Formate, die zum automatisierten Austausch von Firmendaten wie Firmeninformationen, Adressen, Kontaktdaten, Bankkontodaten und Zertifikaten zwischen den Geschäftspartner:innen genutzt werden können.[31] Die Ausgestaltung einer europäischen Wallet für private Personen und Organisationen wird gegenwärtig diskutiert (s.A1 Die Ausgestaltung einer EUDI-Wallet).

Für die Umsetzung stehen drei Rollen (**Trust Triangle**) im Zentrum von SSI: 1) Aussteller/Herausgeber (**Issuer**), 2) Identitätshalter/Entität (**Holder**) und 3) Akzeptanzstelle/Verifizierer (**Verifier**), deren Beziehungsverhältnisse in Abbildung 7 dargestellt sind.[32]

**31** Vgl. das Organisation Wallet von Bosch (2023) oder das Enterprise-Identity-Wallet von dem Unternehmen Spherity (2023).
**32** Vgl. Ehrlich, T. et al. (2022).

Abbildung 8: Trust Triangle




Quelle: WIK, eigene Darstellung in Anlehnung an IDunion (2022a).

Das Trust Triangle funktioniert für die einzelnen Rollen nach folgendem Schema:

Der **Issuer** ist eine berechtigte[33] und vertrauenswürdige Entität, deren Aufgabe es ist, verifizierbare digitale Identitätsnachweise/Zertifikate auszustellen. Die Entität, auf die sich die Nachweise beziehen, wird auch als Subjekt eines Verifiable Credentials benannt. Das Subjekt muss nicht mit der Identitätshalter:in bzw. dem Holder identisch sein, sondern kann ein Objekt unter der Kontrolle der Identitätshalter:in sein (bspw. ihr Auto) oder eine Person, für die sie verantwortlich oder bevollmächtigt ist (bspw. Eltern für ihre Kinder). In der Regel beziehen sich aber die Nachweise auf die Identitätshalter:in selbst. Ein Verifiable Credential kann beispielsweise ein digitaler Personalausweis, Kontodaten oder ein Zeugnis sein, das vom Issuer verschlüsselt bzw. digital signiert und dessen Echtheit und das angewandte Signaturverfahren auf einem (dezentralen) Datenregister mit einem Vermerk versehen werden.

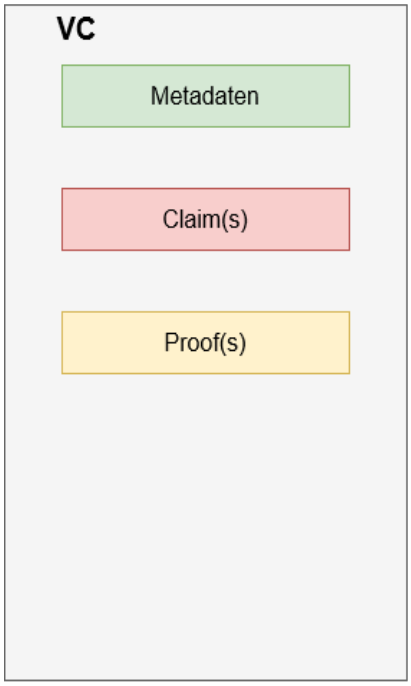
**Verifiable Credentials** sind vom Issuer mit seinem **Private Key** digital signierte Sammlungen von digitalen Nachweisen. Digitale Nachweise können identitätsstiftende Attribute (**Claims**) in kryptografisch gesicherter Form enthalten, die selbst oder durch Dritte attestiert wurden. Sie können auf ihre Korrekheit und Gültigkeit mithilfe des Public Key des Issuers geprüft werden, da er diese mit seinem Private Key beim Ausstellen signiert hat.

33 Wer berechtigt ist, ist gegenwärtig im eIDAS 2.0 Umsetzungsverfahren noch offen. Vgl. BMI(2023d).

Das Verifiable Credential Datenmodell basiert auf Standards, die vom World-Wide-Web-Consortium entwickelt wurden. Verifiable Credentials lassen sich in drei konstituierende Teile zerlegen. In Abbildung 9 ist beispielhaft der grundsätzliche Aufbau eines Verifiable Credentials und der zugehörige JSON-Quellcode eines (ungesicherten) Verifiable Credentials für ein universitäres Abschlussdokument dargestellt:

1. **Metadaten**, wie signierte Informationen zum Herausgeber, Typ, Datum oder einen Public Key für den Verifizierungsprozess, die Revokationsmethode, usw., die das Verifiable Credential beschreiben. Im Beispiel in Abbildung 9 wird der Identifikator des Verifiable Credential per HTTP Uniform-Resource-Locator identifiziert.
2. Einen **Beweis** (Proof), der die Echtheit/Integrität des Verifiable Credentials durch den Issuer garantiert (fehlt im Beispiel Abbildung 9, da eine ungesicherte Form dargestellt ist).
3. Eine **Sammlung von identitätsstiftenden Attributen** (Claims), die sich auf ein Subjekt beziehen, das im Beispiel in Abbildung 9 per DID identifiziert wird. In der Regel ist das Subjekt, auf das sich die Verifiable Credentials beziehen, auch der Identitätshalter/Holder.

Abbildung 9: Aufbau eines Verifiable Credentials und Quellcode eines (ungesicherten) Verifiable Credential eines Universitätsabschlusses.




```
{
    "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
    // Identifikator des VCs
    "id": "http://university.example/credentials/1872",

    // Welche Form hat das VC (welche Daten sind zu erwarten)
    "type": ["VerifiableCredential", "ExampleAlumniCredential"],

    // Die Entität, die das VC herausgegeben hat
    "issuer": "https://university.example/issuers/565049"

    // Wann das VC erstellt worden ist
    "validFrom": "2010-01-01T19:23:24Z",

    // Claims des Subjektes des VCs
    "credentialSubject": {

        // Identifikator des Subjekts des VCs
        "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
        "alumniOf": {

            // Identifikator der Universität
            "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
            "name": "Example University"
    }
  }
}
```

Quelle: WIK, eigene Darstellung in Anlehnung W3C (2023).

Die Rolle des **Holders** kann von jeder Entität eingenommen werden. In der Regel beziehen sich die Verifiable Credential **auf den Holder selbst,** können aber auch Entitäten referenzieren, die vom Holder verwaltet werden. Der Holder erhält Verifiable Credentials vom Issuer und kann diese beispielsweise in einem (digitalen) Wallet auf seinem Smartphone oder in der Cloud sichern. Er allein verfügt über die Verifiable Credentials und entscheidet, wann und mit wem er bestimmte Informationen ebendieser teilt.[34]

Der **Verifier bzw. die Akzeptanzstelle** kann eine virtuelle Anwendung, ein Onlineservice oder eine physische Stelle sein. Der Verifier erhält vom Holder das ursprüngliche Verifiable Credential in Form einer **Verifiable Presentation** (VP), wobei es sich nicht um die Vorlage des Verifiable Credentials selbst, sondern um eine für diesen Zweck gesonderte reduzierte Datenform handelt. Um die Stimmigkeit der Daten der Verifiable Presentations zu garantieren, wird ein mathematischer Beweis (Proof) eingesetzt. Eine weit verbreitete Form eines Proofs ist der **Zero-Knowledge-Proof** mit dem bestimmte Informationen verifiziert werden können, ohne die zugrundeliegenden Daten selbst vorweisen zu müssen. Teilermächtigungsverfahren wie **Selective Disclosure** ermöglichen hierbei, dass einzelne identitätsstiftende Attribute dem Verifier vom Holder selektiv freigegeben werden können und somit kein Zugriff auf die vollständigen Informationen der digitalen Nachweise stattfindet. So ist es möglich, personenbezogene Daten noch stärker zu schützen (beispielsweise das Alter, indem das konkrete Geburtsdatum nicht genannt wird). Es reicht also, dem Verifier für den Verifizierungsprozess eine Abwandlung der **digital signierten Verifiable Credentials** als **Verifiable Presentations** vorzulegen, ohne direkte Beteiligung eines Issuers dafür zu benötigen.

Die Echtheit einer Verifiable Presentation kann der Verifier prüfen, indem er mit den **Public Keys** des Issuers auf die gesicherten Informationen auf einem (dezentralen) vertrauenswürdigen Datenregister (VDR) zugreift. Auf einem VDR werden Informationen zu digitalen Nachweisen (bspw. öffentliche Metadaten von juristischen Personen) und wie diese abgerufen werden können, durch den Issuer und den Holder hinterlegt. Entscheidend dabei ist, dass beide Akteure Informationen auf einem VDR registrieren, aktualisieren, aber auch widerrufen können.[35] Personenbezogene Daten von natürlichen Personen hingegen, wie etwa individuelle Identitätsattribute, werden zu keinem Zeitpunkt auf einem VDR gespeichert.[36] Ein dezentraler Ansatz eines VDR ist beispielsweise die **Distributed-Ledger-Technologie** (DLT) wie Blockchain, die aktuell in vielen Pilotprojekten von digitalen Identitäten erprobt wird.[37] Eine besondere Eignung zur Implementierung von SSI wird DLT unter anderem wegen der hochverfügbaren und dezentralen Prüfstruktur für Identitätsnachweise sowie wegen eines hohen

**34** Vgl. Strüker, J. et al. (2021).
**35** Vgl. IDunion (2022a).
**36** Vgl. IDunion (2022b).
**37** Vgl. Schellinger, B. et al. (2022).

Datenschutzes nachgesagt.[38] Grundsätzlich ist es allerdings auch möglich, SSI ohne DLT zu realisieren, obwohl sie häufig gemeinsam gedacht werden.[39]

### 2.4.2 Implementierungsverfahren

Zunächst gehen wir auf zentrale Herausforderungen von technischen Implementierungsverfahren von SSI ein. Dafür setzen wir uns mit der Umsetzung von Blockchain als dezentrales Datenregister auseinander und legen dar, inwieweit dieses für SSI geeignet sein könnte. Im Anschluss stellen wir Identitätsmanagementsysteme vor, bei denen bereits gegenwärtig SSI-Konzepte Anwendung finden.

#### 2.4.2.1 SSI-Umsetzung mit Blockchain

Der strukturelle Aufbau von Distributed-Ledger-Technologie wie Blockhain-Technologien wird vielen Anforderungen von SSI an ein (dezentrales) Datenregister gerecht. DLT ermöglicht eine dezentrale Datenverwaltung durch das Einbinden von Netzwerkknoten (**Nodes**). Dies kann im Prinzip jeder (mobile) Computer sein, der mit dem Peer-to-Peer Netzwerk verknüpft ist. Nodes speichern Transaktionsdaten, verifizieren sie und leiten sie an andere Nodes weiter.[40] Blockchain ist eine Implementierungsform von DLT, in der Netzwerkblöcke Transaktionsinformationen beinhalten und von den Netzwerkknoten gespeichert werden, wobei jeder Block asymmetrische verschlüsselte Transaktionssignaturen und eine Referenz (**Hash**) zum vorher erstellten Block besitzt.[41] Die signierten Informationen ermöglichen die Verifizierung der Transaktionsherkunft.[42] Infolgedessen können Transaktionsinformationen nicht nachträglich verändert werden, ohne die gesamte Kette von Netzwerkblöcken zu manipulieren, da diese chronologisch miteinander verkettet sind. Dies würde nicht nur massive Rechenleistung erfordern, sondern auch eine flächendeckende Übernahme/Kontrolle von Knotenpunkten, da ein Konsensmechanismus aller Teilnehmenden darüber entscheidet, welche Netzwerkknoten einen neuen Block erstellen dürfen. Zusätzlich prüfen die Knoten, ob neu geschaffene Blöcke das korrekte semantische und syntaktische Format einhalten.[43] Eine dezentrale Verteilung von Knotenpunkten sorgt insbesondere durch dieses Verfahren für einen hohen Datenschutz und für Vertrauensbildung zwischen den einzelnen Teilnehmenden, ohne eine zentrale Prüfstelle oder vertrauenswürdige Drittpartei zu benötigen, da bereits alle Beteiligten diese Rolle gemeinsam erfüllen.[44]

---

**38** Vgl. IDunion (2022b).
**39** Vgl. ebd.
**40** Vgl. Pflanzner, T. et al. (2022).
**41** Public-Key-Infrastruktur wird auch für das Senden und Empfangen von Bitcoin-Transaktionen sowie anderen Kryptowährungen und digitale Datenübertragungen genutzt. Vgl. „Was ist asymmetrische Verschlüsselung“. Bitpanda (2023).
**42** Vgl. Babel, M. et al. (2023).
**43** Vgl. ebd.
**44** Vgl. ebd.

Blockchains existieren in privater und öffentlicher Form sowie mit einem uneingeschränkten oder beschränkten Benutzerkreis. Die wohl populärste Umsetzung einer Blockchain ist die Kryptowährung und Zahlungsnetzwerk Bitcoin. Andere Anbieter wie Ethereum beschränken sich nicht auf einzelne Anwendungsfälle, sondern ermöglichen das Speichern und Ausführen von jeglichem Programmiercode und damit eine Einbindung von sogenannten Smart Contracts.[45] Im Vergleich zu Kryptowährungsnetzwerken, die üblicherweise öffentlich und uneingeschränkt aufgebaut sind, bedarf es bei vielen SSI Umsetzungen besonderer Zugangsrechte, um auf die öffentliche Blockchain zu schreiben, da ausschließlich Issuer und Holder Schreibrechte besitzen sollen. Der SSI Aufbau mithilfe einer öffentlichen eingeschränkten Blockchain (Public Permissioned Blockchain) basierend auf dem Open-Source DLT Projekt Hyperledger Indy ist in Abbildung 10 veranschaulicht.[46]

Wie in Abbildung 10 zu sehen, betreuen die Issuer die Netzwerkknoten und garantieren somit den Fortbestand und die Konsistenz der Blockchain. Während Holder und Issuer dazu ermächtigt sind, Informationen auf die Blockchain zu schreiben, sind die Akzeptanzstellen bzw. Verifier ausschließlich dazu autorisiert, bestimmte Informationen auf der Blockchain abzurufen.[47] Informationen auf dem Ledger sollen, wie zuvor beschrieben, ausschließlich Daten von öffentlichen und privaten Organisationen, nicht aber von privaten Personen beinhalten. Grundsätzlich werden identitätsstiftende Informationen weder bei der Registrierung noch bei der Verifizierung von Nachweisen auf die Blockchain geschrieben. Stattdessen sollen diese ausschließlich selbstverwaltet vom Nutzenden in der persönlichen Wallet abrufbar sein. Dennoch bedarf es für Regulierungen und Verifizierungen eines geeigneten Vertrauenskonzepts (Governance), das die Authentizität der drei Akteure Issuer, Holder und Verifier sicherstellt. Dafür müssen Issuer personenbezogene Daten der Nutzenden auf ihren eigenen Datenbanken verarbeiten, speichern und kontrollieren. Eine zusätzliche Nutzung von Zero-Knowledge-Proofs verhindert, dass beim Prozess der Änderung und des Widerrufs von Attributen Kontakt zum Issuer und somit die Möglichkeit einer Profilbildung durch Rückschlüsse auf Personen entsteht.[48]

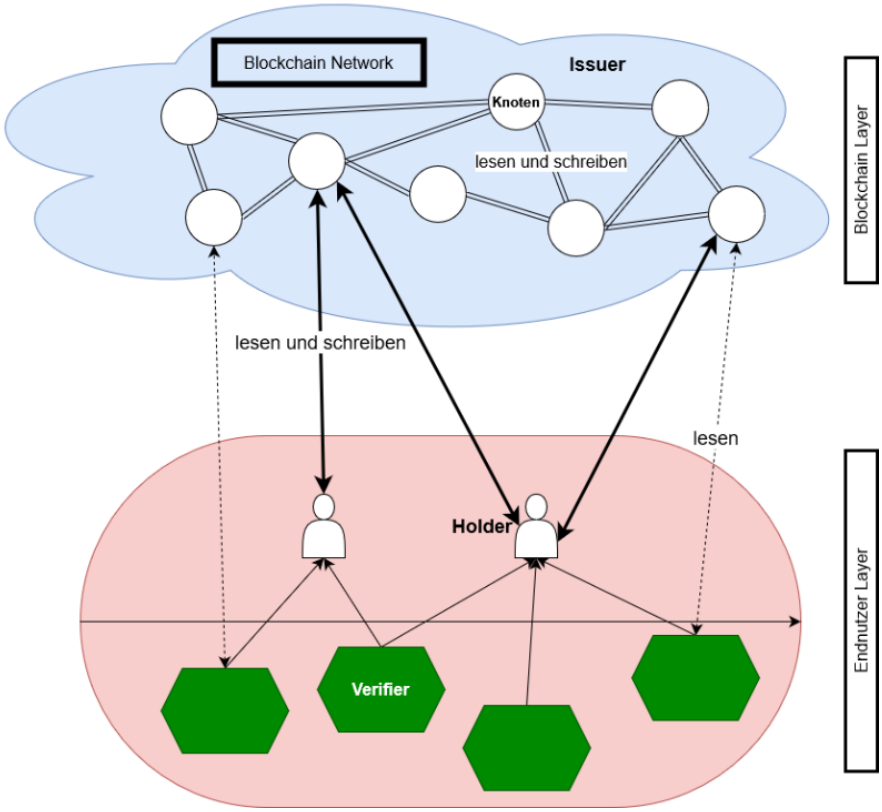
Möglicherweise anspruchsvoller gestaltet sich eine Bestimmung in der Datenschutzgrundverordnung (DSGVO), die die ausdrückliche Löschung personenbezogener Daten vorschreibt, sobald die betroffene Person dies verlangt. Die grundlegende Eigenschaft der Immutabilität des Ledgers in der Blockchain-Technologie impliziert, dass vergangene Transaktionsinformationen nicht rückwirkend modifiziert werden können, sondern lediglich überschrieben werden können. Dieses Prinzip steht im Widerspruch zu den Vorgaben der DSGVO. Hier gibt es bereits methodische Ansätze, die eine DSGVO-konforme Integration verfolgen, allerdings keine flächendeckende Lösung, die Planungssicherheit ermöglicht.[49] Mit der Hilfe von Revocation Registers können Informationen zur Aktualität

---

**45** Vgl. ebd.
**46** Vgl. ebd.
**47** Vgl. Schellinger, B. et al. (2022).
**48** Vgl. ebd.
**49** Vgl. Strüker, J., et al. (2021).

und Gültigkeit von Verifiable Credentials geprüft, geändert und widerrufen werden können – sogar dann, wenn kein Zugang zum Internet bestünde.[50]

Abbildung 10: Blockchain als vertrauenswürdiges Datenregister



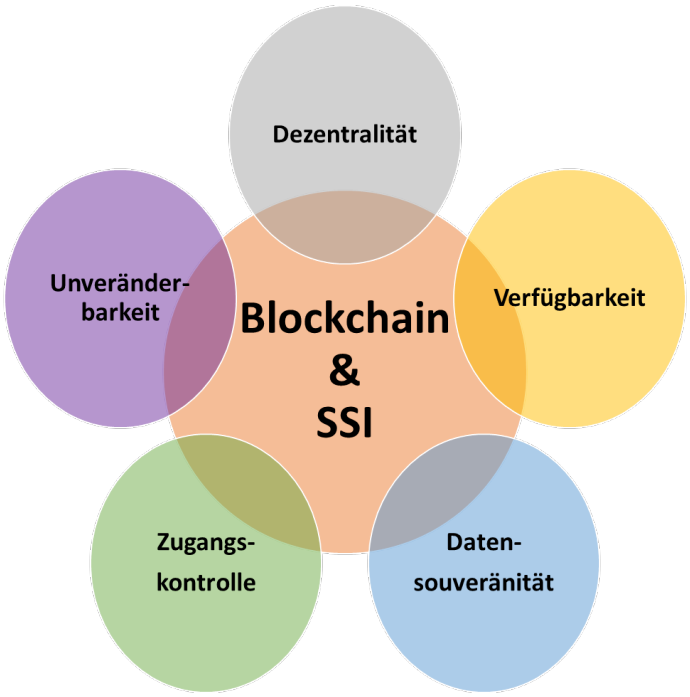

Quelle: WIK, eigene Darstellung in Anlehnung an Pflanzner, T. et al. (2022).

Die Überschneidungen der Anforderungen von SSI mit den Eigenschaften von Distributed-Legder-Technologie machen eine Umsetzung mit Blockchain besonders attraktiv (s. Abbildung 11). Insbesondere hinsichtlich Dezentralität, Unveränderbarkeit und Verfügbarkeit heben sich DLT-Lösungen von klassisch zentralisiert verwalteten Identitätsmanagementsystemen ab.[51] Durch die dezentrale Verwaltung wird das Risiko von „Single Points of Failure“ verringert und eine hohe Verfügbarkeit geschaffen, da die Ausfallwahrscheinlichkeit massiv reduziert wird. Auch hätten durch die Verkettung von Transaktionsblöcken Änderungen an einem Block Auswirkungen auf nachfolgsende Blöcke, was leicht nachweisbar ist. Beides garantiert ein hohes Maß an Sicherheit und Integrität der

**50** Vgl. ebd.
**51** Vgl. IDunion (2022b).

gespeicherten Daten. Verifizierte Informationen können schwer manipuliert werden, was die Zuverlässigkeit von Identitätsnachweisen verbessert.

Abbildung 11: Überschneidende Eigenschaften von Blockchain und SSI




Quelle: WIK, eigene Darstellung.

Die Korrektheit und Integrität der zu verifizierenden Daten spielen allerdings auch bei einer Umsetzung mit Blockchain eine zentrale Rolle. Zwar gelten Informationen, nachdem sie auf die Blockchain geschrieben wurden, als besonders manipulationssicher, die „Garbage In – Garbage Out"-Problematik bleibt jedoch auch bei einer Blockchain-Lösung bestehen (sogenanntes Oracle-Problem).Im SSI-Kontext kommt daher dem Issuer als vertrauenswürdigen Aussteller von digitalen Zertifikaten eine entscheidende Rolle zu, da er initial Entitäten und ihre Digitalen Identitäten authentifizieren und verifizieren muss.[52]

Ebenfalls birgt die Verwendung von Distributed-Ledger-Technologie als dezentrale Datenverwaltung in der bisherigen Form die Gefahr, gegen die Datenschutzgrundverordnung der EU zu verstoßen, die explizit das Recht auf die Löschung personenbezogener

[52] Die Immutabilität, also Unveränderlichkeit, der Blockchain sorgt dafür, dass Informationen, die einmal auf dieser gespeichert wurden, grundsätzlich nicht nachträglich gelöscht werden können. Daher werden zusätzliche Verfahren wie bspw. Widerruf-Register benötigt, die die Gültigkeit von digitalen Nachweisen festhalten. Zwar treten Austeller:innen von digitalen Nachweisen als vertrauenswürdige Instanzen auf, ein vollumfänglicher Schutz vor fehlerhaften Daten und Identitätsbetrug oder -missbrauch beim Authentifizieren und Verifizieren von Digitalen Identitäten kann aber dadurch nicht garantiert werden. Vgl. Babel, M., et al. (2023).

Daten vorsieht.[53] Die Ledger-Technologie verstößt zwar nicht grundsätzlich gegen die DSGVO, um sie einzuhalten muss allerdings die Unlöschbarkeit der Daten in einer Blockchain mittels Anonymisierung und Pseudonymisierung kompensiert werden.[54] Damit müssen Diskussionen zur Standardisierung und Verarbeitung von Transaktionen, zum einheitlichen Rollenverständnis durch klare Begriffsdefinitionen sowie zur Handhabung personenbezogener Daten geführt werden.[55] Die kryptografische Manipulationsresistenz der Blockchain-Technologie erfordert somit, dass aus datenschutzrechtlichen Gründen keine personenbezogenen Daten auf einer Blockchain gespeichert werden. Stattdessen sollte sie lediglich die Möglichkeit bieten, sensitive Daten auf ihre Gültigkeit zu prüfen, beispielsweise über ein Revocation Register.[56]

Bisher steht bei derzeitigen SSI-Implementierungen allerdings nur dem Issuer und nicht dem Holder die Möglichkeit offen, Verifiable Credentials zu widerrufen (via Revocation Register bzw. Proof of Non-Revocation bei Hyperledger Indy).[57] Zur Veranschaulichung wird in Abbildung 11 eine Übersicht von populären SSI-Umsetzungen differenziert nach DLT-Ansatz, DID-Methode und Interoperabilität sowie Selective Disclosure dargestellt.[58]

**53** Vgl. Strüker, J., et al. (2021).
**54** Vgl. European Parliamentary Research Service (2019).
**55** Vgl. Strüker, J. et al (2021).
**56** Vgl. ebd.
**57** Vgl. Abraham, A. et al. (2020).
**58** Vgl. Bai, Y. et al. (2022).

Abbildung 12: Identitätsmanagementsysteme mit DLT

| Projekt | DLT | Storage | DID-Method | Interoper-abilität | Selective-Disclosure |
|---|---|---|---|---|---|
| **ShoCard** | Blockchain (public) | Off-Chain | W3C compliant | Ja | Nein |
| **Weldentity** | FISCO-BLOCKCHAINOS (Blockchain Platform, public & private, permissioned & permissionless) | On/Off-Chain | W3C compliant | Nein | Nein |
| **Microsoft-DID** | Multi-chain Ledger | Keine Angabe | DID: ion-test/test | Nein | Keine Angabe |
| **Cambridge-Blockchain** | Privacy Blockchain | Off-Chain | Keine Angabe | Nein | Nein |
| **uPort** | Ethereum (blockchain & non-blockchain identity related uses cases) | Off-Chain | W3C compliant | Ja | Ja |
| **Sovrin** | Sorvin Ledger (Public-permissioned Blockchain) | On/Off-Chain | W3C compliant | Ja | Ja |

Quelle: WIK, eigene Darstellung in Anlehnung an Bai, Y. et al. (2022).

In der Europäischen Union (EU) treibt die Europäische Kommission (KOM) die Einrichtung einer gemeinsamen europäischen Blockchain-Infrastruktur (European Blockchain Services Infrastructure (EBSI)) voran. Seit 2020 hat EBSI ein Netzwerk von 362 Knotenpunkte (Nodes) in Europa eingerichtet, das Blockchain für sieben Anwendungsfälle nutzbar machen möchte, wobei SSI einen von mehreren Anwendungsfällen darstellt. EBSI hat zum Ziel, wertebasierte, vertrauenswürdige und User-orientierte grenzüberschreitende digitale Dienstleistungen im Public Sector innerhalb des Rechtsrahmens des Digitalen Binnenmarkts der EU zu ermöglichen und zu unterstützen.[59]

SSI-Anwendungsfälle von EBSI zeigen, dass spezifische technische Voraussetzungen für ein Revocation Register gegeben sein müssen, damit Blockchain-Lösungen der DSGVO entsprechen. Um dies zu verwirklichen, zeigt EBSI, dass eine unterschiedliche

**59** Vgl. Deutscher Bundestag (2022).

Ausgestaltung des Registers für private und juristische Personen möglicherweise von Nöten ist.[60] Dabei müssen folgende Punkte garantiert werden:

- Die Nachverfolgbarkeit bzw. Korrelation von Daten eines Holders darf nicht möglich sein (Eliminate the traceability of holders).
- Die Privatsphäre eines Holders muss geschützt sein (Protect holder privacy).
- Eine Speicherung oder Verarbeitung personenbezogener Daten auf der EBSI-Blockchain darf nicht stattfinden (Retain from storing or processing personal data on the EBSI blockchain).
- Es muss verhindert werden, dass Emittenten oder Dritte das Widerrufen von Verifiable Credentials eines Holder mit ebendiesem verknüpfen können (Prevent issuers or third parties from linking revocation checks to holders).

In Deutschland werden die Schaufensterprojekte ID-Ideal, IDunion, Once und SDIKA aus dem Innovationswettbewerb „Schaufenster Sichere Digitale Identitäten“ des Bundesministerium für Wirtschaft und Klimaforschung (BMWK) gefördert.[61] Gemeinsames Ziel ist der Aufbau eines offenen ID-Ökosystems mit einer dezentralen Identitätsverwaltung, das „weltweit nutzbar ist und sich an europäischen Werten und Regularien orientiert“.[62] Beispielsweise basiert IDUnion auf den Open-Source Blockchain-Technologien **Hyperledger Indy** und **Hyperledger Aries** und soll als Brücke zwischen eID und SSI fungieren, um so beide zu ergänzen.

#### 2.4.2.2 Weitere SSI-Implementierungsverfahren mit und ohne Distributed-Ledger-Technologie

Ein verbreiteter Irrtum ist, dass SSI ausschließlich mit Distributed-Ledger-Technologie wie Blockchain implementiert werden kann.[63] In einer Vielzahl von aktuellen europäischen Pilotprojekten ist dies zwar der Fall (s.o.); Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich allerdings sogar vorerst von einer Umsetzung von eID mit Distributed-Ledger-Technologie distanziert.[64] Grundsätzlich kann SSI auch ohne Ledger-Technologie oder als Hybrid-Lösung mit hoheitlichen und dezentralen Ansätzen realisiert werden.[65] Im Folgenden sollen alternative digitale Identitätsmanagementkonzepte wie OpenID for Verifiable Credentials**,** Keyless-Signature-Infrastructure, DID-Methoden wie did:peer, did:key und did:web sowie Interplanetary Filesystems, die sich

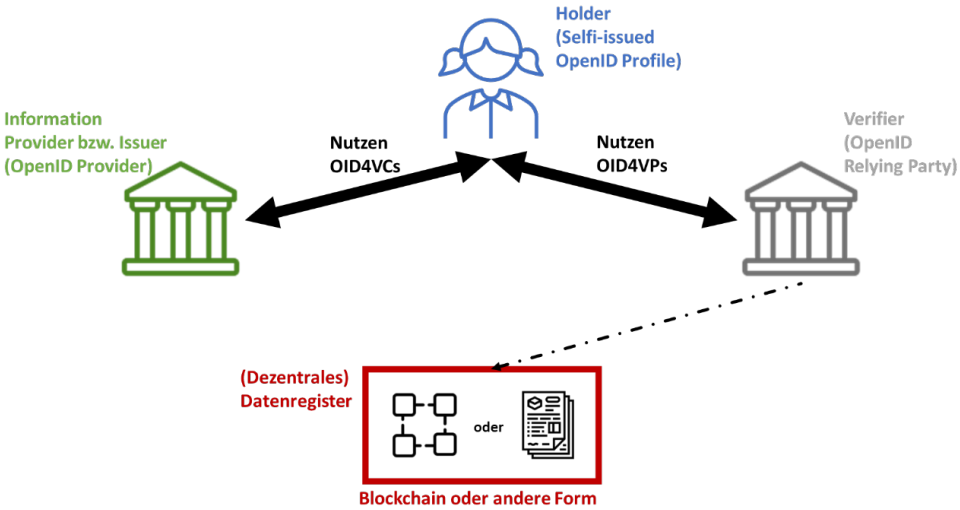
---

**60** Vgl. EBSI (2023).
**61** Vgl. Begleitung Sichere Digitale Identitäten (2023).
**62** Vgl. IDunion (2023b).
**63** Vgl. Schellinger, B. et al. (2022).
**64** Vgl. BSI (2021).
**65** „Dezentralität und hohe Verfügbarkeit eines Distributed Ledgers werden zwar oft als Vorteil genannt, sind aber kein Alleinstellungsmerkmal dieser Technologie. Auch andere Systeme, wie beispielsweise verteilte Datenbanken oder Verzeichnisdienste, können für das Datenregister in Betracht kommen.“ Vgl. BSI (2021).

teilweise an SSI-Leitgedanken orientieren und bereits Verwendung finden, kurz vorgestellt werden.

**OpenID for Verifiable Credentials** ist eine Form von OpenID Connect speziell für SSI-Anwendungen. OpenID for Verifiable Credentials ist ein interoperables Authentifizierungsprotokoll, das auf dem OAuth 2.0 Framework beruht und bereits für Single-Sign-On genutzt wird.[66] Die selbstsouveräne Version ermöglicht einen Verifizierungsprozess, ohne dass die Nutzenden einen persönlichen Zugang beim SSI OpenID for Verifiable Credentials Provider besitzen müssen. Somit werden keine persönlichen Daten bei zentralen Datenregistern gespeichert.[67] Das Verfahren wird bereits von 18 Wallets (Stand April 2023) im EBSI Projekt angeboten).[68] Der Verifizierungsprozess ist in **Fehler! Verweisquelle konnte nicht gefunden werden.** dargestellt.

Abbildung 13: OpenID for Verifiable Credentials Architektur




Quelle: WIK, eigene Darstellung in Anlehnung an Yasuda, K. und Lodderstedt, T. (2021).

**Keyless-Signature-Infrastructure** ist eine in Estland und dem Schweizer Kanton Jura verwendete dezentrale Infrastruktur für digitale Nachweise, die bereits für zahlreiche Verwaltungs- und Verifizierungsprozesse eingesetzt wird und dem Kerngedanken von SSI folgt. Sie kommt ohne kryptografische Schlüssel, wie sie bei konventionellen Public-Key-Infrastruktur-Methoden genutzt werden, aus. Stattdessen nutzt Keyless-Signature-Infrastructure Hashing-Algorithmen wie SHA256 sowie die Blockhain-Technologie, um Daten zu verschlüsseln. Der entscheidende Vorteil gegenüber „Proof of Work“ Blockchain-Anwendungen wie Bitcoin ist, dass Keyless-Signature-Infrastructure ausschließlich einen irreversiblen Hash-Wert statt vollständige Transaktionsinformationen auf das öffentliche

66 Vgl. Lux, Z. A. et al. (2020).
67 Vgl. Terbu, O. et al. (2023).
68 Vgl. Yasuda, K. et al. (2022).

Ledger schreibt, wodurch sich die Transaktionskosten massiv reduzieren. Während Bitcoin mehrere Minuten benötigt, um eine Transaktion zu verifizieren, sind es bei Keyless-Signature-Infrastructure unter einer Sekunde. Darüber hinaus skaliert es mit einer konstanten Rate von geschätzten 2GB pro Jahr – Bitcoin wächst hingegen mit der Anzahl an Transaktionen und ist bereits bei Wachstumsraten von 20-30GB (s. Abbildung 13).[69] Hash-Funktionen gelten zwar als resistent gegen Quantencomputer-Attacken, sind allerdings nicht vollständig davor sicher.[70]

Abbildung 14: KSI im Vergleich zu Bitcoin und RSA

| | KSI | Bitcoin | RSA |
|---|---|---|---|
| **Skalierbarkeit** | Global, linear zur Zeit | Global, linear zur Anzahl der Transaktionen | Lokal |
| **Transaktions-geschwindigkeit** | Unter 1 Sekunde | Nicht-deterministisch, 5-15 Minuten | Unter 1 Sekunde |
| **Datenschutz** | Transaktionsdaten bleiben unter Verschluss | Transaktionsdaten werden auf die Blockchain geschrieben | Transaktionsdaten bleiben unter Verschluss |
| **Verschlüsselung mit PKI** | n/a | n/a | Notwendig |
| **Gefahr der Entschlüsselung durch Quantencomputing** | Nein | Ja | Ja |

Quelle: WIK, eigene Darstellung in Anlehnung an Guardtime (2023).

**DID-Methoden wie did:peer**[71] **und did:key**[72] schaffen einen direkten und sicheren Kommunikationskanal zwischen zwei oder mehreren Parteien ohne Rückgriff auf Netzwerke, Datenbanken oder verteilte Dateiverwaltungssysteme. Sie kommen beispielsweise bereits bei IDunion Projekten zum Einsatz.[73] **Did:web**[74] baut auf Systemen im traditionellen Web-Framework auf. DID-Methoden sind grundsätzlich auch mit Ledger-Technologien oder anderen Systemen, die öffentliche Vertrauensregister nutzen, realisierbar. Statt wie üblich die öffentlichen Schlüssel beider Parteien auf einer Blockchain zu speichern, kann ein DID allerdings auch eingebunden in einem DID-Dokument von

69 Vgl. Buldas, A. et al. (2013); Martinovic, I. et al. (2017).
70 Vgl. Buldas, A. et al. (2017).
71 Vgl. Decentralized Identity Foundation (2023).
72 Vgl. W3C (2022b).
73 Vgl. IDunion (2022b).
74 Vgl. W3C (2022b).

einer Partei zur anderen versendet (**did:peer, did:key**) bzw. auf einer Domain veröffentlicht werden (**did:web**). Haben die Parteien Zugriff auf die jeweiligen Metadaten im DID-Dokument des anderen, können sie mit diesen die zugehörigen Informationen abrufen. Vorteil eines solchen Systems ist, dass keine Transaktionskosten entstehen und kein zentrales Datenregister existiert sowie kaum Sicherheitsrisiken vorliegen, sofern beide Parteien wissen, mit wem sie kommunizieren, da nur die involvierten Parteien die DIDs einsehen können.[75]

**Interplanetary Filesystem** ist ein Netzwerk und Protokoll zur **verteilten Datenverwaltung**. Es wurde mit dem Ziel entwickelt, dass auf Dateien zugegriffen werden kann, die auf einzelnen Knoten (Computern) im Netzwerk gesichert sind, unabhängig von wenigen Markt-dominierenden Cloud-Anbietern. Dafür werden üblicherweise das **Bitcoin Blockchain-Protokoll**, **Git** und **BitTorrent** genutzt, Interplanetary Filesystem kann allerdings auch ohne Bitcoin-Blockchain verwendet werden. Als sogenanntes **Peer-to-Peer** Dateisystem verbindet es alle Geräte mit demselben Klienten, um Dateien automatisch beim Upload auf verschiedene Netzwerkknoten zu verteilen. Mit eindeutig identifizierbarer Inhaltsadresse kann jede Datei anhand ihrer Kennung von anderen Usern im Netzwerk in Form eines kryptografischen Hash-Wertes (wie ein Fingerabdruck) gefunden und angefordert werden. Hierfür werden die nächstgelegenen Netzwerkknoten, die im Besitz der angeforderten Dateien sind, genutzt, was einen schnelleren Datenaustausch fördert (s. Abbildung 15). Interplanetary Filesystem kann somit beispielsweise zur dezentralen Sicherung von DIDs und kryptografisch verschlüsselten Verifiable Credentials genutzt werden.[76]

Wie gezeigt wurde gibt es unterschiedliche technische Umsetzungsmöglichkeiten für SSI-Konzepte, von denen einige bereits in Pilotprojekten wie dem „Schaufenster Digitale Identitäten“ auf ihre Praxistauglichkeit getestet werden.[77] Obwohl sich gegenwärtig die Umsetzung von SSI mit Ledger-Technologie als herausfordernd gestaltet, existieren bereits erfolgreiche SSI-Anwendungen, die diese nutzen, wie Keyless-Signature-Infrastructure in Lettland und der Schweiz. Grundsätzlich können auch DID-Methoden wie did:peer, did:key oder did:web oder die Weiterentwicklung bestehender Frameworks wie OpenID for Verifiable Credentials dazu dienen, die Leitkonzepte von SSI zu realisieren. Eine starke Fragmentierung von SSI-Lösungen steht allerdings dem Interoperabilitätsprinzip und einem harmonisierten digitalen Ökosystem entgegen. In Abbildung 15 sind die zentralen Merkmale zentralisierter, föderierter und dezentralisierter bzw. verteilter Identitätsmanagementsysteme und ihre spezifischen Charakteristika aufgeführt, die die potenziellen Vorzüge von SSI-basierten Ansätzen veranschaulichen sollen.

**75** Vgl. W3C (2022a).
**76** Vgl. IPFS (2023).
**77** Vgl. Begleitforschung Sichere Digitale Identitäten (2022).

Abbildung 15: Identitätsmanagementsysteme im Vergleich

| Identitäts-management-systeme | Zentralisiert  | Föderiert  | Dezentralisiert / Verteilt  |
|---|---|---|---|
| **Technologie** | • ID/Passwort<br>• Multifaktor-Authentifizierung<br>• SSO | • OAuth (2.0)<br>• OpenID Connect<br>• SAML | • Hyperleder Indy, Hyperledger Aries<br>• Did:key, did:web<br>• KSI<br>• IPFS<br>• OpenID Connect for SSI |
| **Charakteristika** | • Digitale Identitäten fragmentiert<br>• Datensouveränität nicht beim User<br>• Anfällig für Cyberattacken | • Weniger fragmentierte digitale Identitäten<br>• Datensouveränität nicht beim User<br>• Anfällig für Cyberattacken | • Identitäten sind interoperabel über Anbieter hinweg<br>• Datensouveränität beim User<br>• Dezentralität vermindert |

Quelle: Eigene Darstellung in Anlehnung an Bucci, D. (2022).

## 2.5 „Natürliche Grenzen“ von SSI

Bei SSI ist die Frage zu klären, wer oder was die erste Instanz ist, der vertraut wird; der sogenannte Root of Trust (Vertrauensanker). Es ist keine andere Art und Weise bekannt, um sicherzustellen, dass die ausstellende Stelle von Verifiable Credentials, der Issuer, tatsächlich die Stelle ist, die sie vorgibt zu sein.[78] Das gleiche gilt auch für die initiale Verifizierung der Holder. Infolgedessen wird es notwendig sein, entweder wie bisher auf staatliche Vertrauensanker und/oder -vermittler zurückzugreifen oder im dezentralen Modell dem Markt zu überlassen, sich selbst durchsetzende, vertrauenswürdige Akteure zu etablieren.[79] Im Fall staatlicher Vertrauensanker könnte dies für natürliche Personen beispielsweise das Einwohnermeldeamt sein, das Personalausweise ausstellt, oder das Standesamt, das Geburtsurkunden ausstellt. Im Falle von juristischen Personen böte sich beispielsweise das Gewerbeamt an, bei dem sich Unternehmen nach der Gründung anmelden. Da die meisten Ansätze auf zentralisierte Verwaltungsebenen mit Vertrauensankern und/oder -vermittlern setzen, erfüllen diese das SSI-Paradigma nur bedingt. In diesem Zusammenhang ist auch für die Entwickler:innen relevanter SSI-Komponenten (z. B. die Entwickler:innen der Wallets) notwendig, dass ihnen Vertrauen entgegen-

78 Vgl. Kubach, M. et al. (2020).
79 Vgl. Kubach, M., Roßnagel, H. (2021).

gebracht wird.[80] Dieser Gedanke kann weitergedacht werden und beispielsweise auf das Vertrauen in Hardwarehersteller oder Institutionen in den Ländern des Unternehmenssitzes der Hardwarehersteller erweitert werden, auf denen die Wallets installiert werden müssen.

Die vollständige Souveränität über Daten der Inhaber:innen ist im Kontext einer dezentralen Datenverwaltung aus vergleichbaren Gründen nicht uneingeschränkt realisierbar und unterliegt praktischen Einschränkungen. Die Erfassung und vorübergehende Speicherung sensibler, unternehmens- oder personenbezogener Daten ist zur Erstellung digitaler Nachweise, beispielsweise im Zusammenhang mit der Root-of-Trust oder dem Herausgeber jedes verifizierten Verifiable Credential, erforderlich. Zentralisierte Datenverwaltungen bergen grundsätzlich das Risiko von Datenlecks und Doxing[81], wodurch Informationen öffentlich zugänglich gemacht werden können. Zudem besteht die Möglichkeit, dass identitätsstiftende Daten zur Verifizierung von digitalen Nachweisen auch nach der Überprüfung behalten oder an Dritte weitergegeben werden. Nutzende haben zwar prinzipiell die Möglichkeit, die Offenlegung spezifischer Informationen zu verweigern, dies hat allerdings zur Folge, dass ihnen gegebenenfalls Dienstleistungen verwehrt bleiben. In dezentralen Datenverwaltungssystemen wie SSI kann im Grunde jede Entität Herausgebende (Issuer) und Verifizierende (Verifier) sein, wobei Issuer die Inhaber:in authentifizieren und autorisieren und sensible personen- oder unternehmensbezogene Daten zentral in eigenen Datenbanken speichern, kontrollieren und verwalten müssen. Daher ist ein hohes Maß an Vertrauen zwischen allen Parteien erforderlich. Personen- und organisationsbezogene Daten müssen sowohl technisch als auch datenschutzrechtlich angemessen geschützt werden. Daher sollten institutionelle Mandate umfassenden rechtlichen und regulatorischen Vereinbarungen unterliegen und durch unabhängige Aufsichtsgremien auf ihre Einhaltung überwacht werden.[82]

Im Kontext dezentraler Digitaler Identitäten liegt der Fokus auf der Entität, die vollständig die Verwaltung für ihre eigenen Daten übernimmt. Dies impliziert, dass bei einem Diebstahl des privaten Schlüssels oder eines unrechtmäßigen Zugangs zur persönlichen digitalen Wallet, gegebenenfalls potenziell nicht autorisierte (irreversible) Transaktionen getätigt werden können. Entitäten tragen daher eine gesteigerte Verantwortung für den Schutz ihrer personenbezogenen Daten. Eine Sensibilisierung für diese Verantwortung könnte unter anderem durch pädagogische Maßnahmen erreicht werden.[83]

---

**80** Vgl. Kubach, M. et al. (2020).
**81** Doxing bezeichnet einen Vorgang, bei dem personenbezogene Daten absichtlich von einem Dritten im Internet veröffentlicht werden, um die betroffene(n) Person(en) zu bestrafen, zu demütigen, zu bedrohen oder einzuschüchtern. Vgl. Douglas, David M. (2016).
**82** Vgl. World Bank (2019).
**83** Vgl. Ehrlich, T. et al. (2021).

## 2.6 Zwischenfazit

Im heutigen Umfeld haben Identity Provider oft die Kontrolle über die Identitäts- und Datenmanagementprozesse der User. Persönliche Daten werden dafür nicht selten in zentralen Datenbanken gespeichert und für kommerzielle Interessen der Plattformbetreiber genutzt. Als Gegenentwurf dazu ermöglichen dezentrale, selbstverwaltete Identitätsmanagementsysteme wie SSI den Nutzenden, die Hoheit über ihre Identitätsdaten zurückzugewinnen. Sie verfolgen das Ziel, dass User ihre Identitätsdaten selbst sicher speichern und verwalten können, wodurch sie zu einem integralen Bestandteil der Vision von Web 3.0 werden, das ein dezentralisiertes und interoperables Internetökosystem anstrebt.

In diesem Kapitel wurde aufgezeigt, dass Christopher Allens theoretische Anforderungen an SSI Kernkonzepte von Web 3.0 wie z. B. Dezentralisierung, Datenschutz sowie Interoperabilität anknüpfen, um Nutzenden zukünftig mehr Kontrolle über ihre Daten und genutzten Dienste zu verschaffen. Für eine Umsetzung von SSI gemäß des Trust Triangle bedarf es dezentraler Identifikatoren, kryptografischer Verschlüsselung und digitalen Brieftaschen (Wallets) sowie eines vertrauenswürdigen Datenregisters, das auf Ledger-Technologien basieren kann. Die Technologie für SSI, insbesondere basierend auf Blockchain, findet zwar bereits in mehreren europäischen Pilotprojekten und europäischen Ländern und Regionen Verwendung, allerdings fehlen einheitliche Standards, um eine flächendeckende interoperable Verbreitung zu ermöglichen. Verschiedene Initiativen und Organisationen (bspw. Decentralised Identity Foundation und World Wide Web Consortium) arbeiten an der Entwicklung solcher Standards, bisher fehlt es allerdings an universeller Adoption.[84]

Darüber hinaus bleiben auch mit dezentralen, selbstverwalteten Identitäten Probleme bestehen, die auf diesem Wege nicht gelöst werden können. Zwar können Anwender:innen grundsätzlich darüber entscheiden, mit wem sie ihre Daten teilen, allerdings nicht, was mit ihnen im Nachgang passiert.[85] Bei dem Registrieren und Abgleichen von personenbezogenen Daten ist man also weiterhin auf die Datensicherheit und den Datenschutz der Issuer-Stellen angewiesen. Gleichzeitig müssen die (öffentlichen, amtlichen oder akkreditierten) Issuer-Stellen prüfen und gewährleisten, dass die ihnen vorgelegten Informationen Gültigkeit besitzen (Oracle Problem). Somit bedarf es auch mit dezentralen, selbstverwalteten Identitäten Vertrauensanker (Roots-of-Trust), was den „libertären, staatsmisstrauenden Gedanken“[86] in Teilen der Web 3.0 Bewegung und des „Web-of-Trust“-Lösungsansatzes widerspräche.

Die Einführung von SSI wirft zusätzlich regulatorische Fragen auf, vor allem im Hinblick auf Einhaltung der DSGVO. Regulierungsbehörden müssen ein rechtliches Rahmenwerk entwickeln, um sicherzustellen, dass SSI-Implementierungen den gesetzlichen

84 Vgl. Strüker, J., et al. (2021); Babel, M., et al. (2023).
85 Vgl. Strüker, J., et al. (2021).
86 Vgl. IDunion (2022b).

Anforderungen entsprechen, beispielsweise hinsichtlich der Ausgestaltung von digitalen Wallets, in denen persönliche Identitätsdaten gespeichert und verwaltet werden. Im folgenden Kapitel soll aus diesem Grunde auf zentrale offene Fragen eingegangen werden, um diesbezüglich staatliche Handlungsbedarfe und -optionen abzuleiten.

# 3 Chancen und Herausforderungen Web 3.0-konformer Digitaler Identitäten für die Wirtschaft

Im folgenden Kapitel sollen die Potenziale Web 3.0-konformer Digitaler Identitäten in Deutschland vor dem Hintergrund gegenwärtiger Herausforderungen für die Wirtschaft eingehend untersucht werden. Dazu erfolgt eine Analyse möglicher Chancen und Herausforderungen unter Berücksichtigung unterschiedlicher Marktteilnehmer:innen. Die Diskussion wird durch eine detaillierte Untersuchung konkreter Anwendungsmöglichkeiten vertieft.

## 3.1 Aktuelle Entwicklungen zu eIDAS 2.0

Gegenwärtig fehlt es in Europa und damit auch in Deutschland an einem rechtlichen Rahmen für SSI-Lösungen, da die derzeitige eIDAS-Verordnung[87] hauptsächlich auf staatliche eIDs ausgerichtet ist. Die Aktualisierung der eIDAS-Verordnung (eIDAS 2.0) soll den Geltungsbereich der ursprünglichen Verordnung um weitere Arten elektronischer Vertrauensdienste erweitern. Ziel ist die Schaffung einer Digitalen Identität, die Erleichterungen für EU-Bürger:innen und Unternehmen bieten soll.[88] Das darin angedachte, User-zentrierte Identitätsmodell beinhaltet auch eine europäische digitale Wallet, die den Bürger:innen die Kontrolle über ihre Daten ermöglichen soll, ohne dass sie – wie bisher – auf Identifikationsdienste angewiesen sind.[89] Die sogenannte **EUDI-Wallet** soll nicht nur Dienstleistungen aus dem öffentlichen Sektor nutzbar machen. Auch private Dienstleister:innen sollen – oder müssen gegebenenfalls sogar – die europäische Wallet-Lösung für Digitale Identitäten als Authentifizierungsmethode akzeptieren können.[90] Expert:innen gehen davon aus, dass eIDAS 2.0 somit erhebliche Auswirkungen auf die europäische Wirtschaft haben wird.[91]

Mit Abschluss dieser Studie, Stand Anfang Dezember 2023, ist die eIDAS 2.0-Verordnung noch nicht in Kraft getreten, da EU-Rat und -Parlament sie noch formell verabschieden müssen. Mit dem **Architektur- und Referenzrahmen** (European Digital Identity Architecture and Reference Framework (ARF)) stellte die EU mit Version 1.1.0 allerdings bereits eine Reihe von Spezifikationen zu Verfügung, die für die Entwicklung einer interoperablen EUDI-Wallet-Lösung auf der Grundlage gemeinsamer Standards und Praktiken erforderlich sind. Der ARF dient der Referenzimplementierung eines EUDI-Wallets sowie den Konsortien der Large Scale Pilots (LSP). Es stellt damit den aktuellen Stand der laufenden Arbeiten der eIDAS-Sachverständigengruppe dar, impliziert aber keine formelle Vereinbarung über den Inhalt oder den Gesetzesvorschlag.[92] Zudem wurde Ende November 2023 im Rahmen des Konsultationsprozesses des Bundesministerium des

**87** Vgl. Europäische Union (2014).
**88** Vgl. KOM (2021).
**89** Vgl. Schwalm, S., Alamillo-Domingo, I. (2021).
**90** Vgl. KOM (2023a).
**91** Vgl. PwC und DLA Piper (2021).
**92** Vgl. Europäische Union (2023).

Innern und für Heimat (BMI)[93] das sogenannte „Architecture Proposal for the German eIDAS Implementation“ in Version 1 für eine deutsche EUDI-Wallet veröffentlicht. Das Dokument erhebt laut eigenen Angaben allerdings keinen Anspruch auf Vollständigkeit oder Endgültigkeit und soll zu Beginn des Jahres 2024 finalisiert werden.[94]

Die im folgenden getätigten Aussagen beziehen sich somit auf den zurzeit öffentlich verfügbaren Kenntnistand. Sie können, müssen sich allerdings nicht auf tatsächliche Chancen beziehen, die durch eIDAS 2.0 eröffnet werden. Vielmehr sollen sie die Chancen aufzeigen, die Web 3.0-konforme Digitale Identitäten bieten können.

## 3.2 Welche Chancen bieten Web 3.0-konforme Digitale Identitäten für die Wirtschaft?

Die Art und Weise, wie Identitäten online verwaltet werden, wird voraussichtlich grundlegende Veränderungen in den Beziehungen zwischen Staat, Bürgern und dem privatwirtschaftlichen Sektor herbeiführen. Laut einer Studie von 2019 könnten Verbesserungen im Bereich Digitaler Identität in entwickelten Volkswirtschaften bis zum Jahr 2030 einen wirtschaftlichen Nutzen generieren, der etwa drei bis vier Prozent des Bruttoinlandsprodukts entspricht.[95] Im Folgenden werden Potenziale aufgezeigt, die dezentrale, selbstverwaltete Digitale Identitäten gegenüber gegenwärtigen IAMs bieten und mit konkreten Anwendungsszenarien veranschaulicht.

### 3.2.1 Verbesserte Informationssicherheit

Trotz gesetzlicher Vorgaben und steigendem Bewusstsein erfolgt sowohl bei Endnutzer:innen als auch Service Providern kein ausreichender Schutz von Identitätsdaten. Neben nachlässigem Verhalten verschärfen insbesondere isolierte und föderierte Identitäts- und Zugangsmanagements die Gefahrenlage. SSI könnten eine Lösung sein, um potenzielle Angriffspunkte zu reduzieren, Datenlecks zu minimieren und die Informationssicherheit zu optimieren. Sie kommen durch Verschlüsselung und dezentrale Datenspeicherung dem Wunsch und Bedarf nach Sicherheit nach und beugen Wohlstandsverluste durch Cyberkriminalität vor.

Das BSI konstatierte in seinem Lagebericht 2023, dass sich die bereits zuvor angespannte Lage im Cyber-Raum im zurückliegenden Jahr weiter zuspitzte und so hoch war wie nie zuvor.[96] Verlässliche Daten zu den tatsächlichen Schadensereignissen und den dadurch entstandenen Kosten für die deutsche Wirtschaft und Privatpersonen sind allerdings schwer zu erheben und daher auch in der Literatur selten zu finden.[97] Studien

**93** Vgl. BMI (2023c).
**94** Vgl. BMI (2023a).
**95** Vgl. McKinsey Global Institute (2019).
**96** Vgl. BSI (2023).
**97** Vgl. Dreißigacker, A. et al. (2020).

gehen aktuell von bis zu über 200 Mrd. Euro jährlichem Schaden für Unternehmen allein in Deutschland aus.[98] Informationssicherheit ist für Unternehmen somit ein bedeutender Erfolgsfaktor. Ein nicht unerheblicher Teil der Schäden entsteht im Zusammenhang mit Identitätsdaten. Allein bei Betrugsvorfällen mit Bezug zu Verbraucher:innen bzw. Endkund:innen betragen die Kosten für Unternehmen im E-Commerce in Deutschland geschätzt mehrere Milliarden Euro pro Jahr.[99] Datenschutz und Datensicherheit spielen im Zusammenhang mit Digitalen Identitäten also eine wichtige Rolle. Unternehmen sind schließlich daran interessiert, die entstehenden Verluste durch Kriminalität möglichst gering zu halten.

Diese Absicht verfolgen auch gesetzliche Anforderungen wie die DSGVO, die Unternehmen dazu verpflichtet, Datenschutzmaßnahmen für personenbezogene Informationen zu implementieren. Bei Nichteinhaltung müssen sie mit erheblichen finanziellen Sanktionen rechnen. Gleichzeitig wächst bei Privatpersonen das Bewusstsein für den Schutz ihrer (Identitäts-)Daten im Internet. Empirische Erhebungen zeigen, dass bereits im Jahr 2016 etwa ein Drittel der Befragten Erfahrungen mit Identitätsdiebstahl gemacht bzw. entsprechende Vorfälle realisiert haben. Der monetäre Schaden, welcher unmittelbar aus derartigen Verletzungen resultiert, kann mehrere Hundert Euro pro individuellem Fall und betroffener Person betragen.[100] Überdies sind weitere potenzielle Schäden nicht auszuschließen. Andere, jüngere Umfrageergebnisse unterstreichen die erhebliche Bedeutung, die Individuen dem Schutz ihrer Daten beimessen.[101]

Trotz alldem lässt die Verwaltung und der Schutz von Identitätsdaten, sowohl seitens der Endnutzer:innen[102] als auch der Service Provider[103], auf ein scheinbar nachlässiges Verhalten im Umgang mit diesen Daten schließen. Viele User unterlassen notwendige Sicherheitsmaßnahmen zum Schutz ihrer Accounts. Gleichzeitig zeigen auch zahlreiche Service Provider unzureichende Anstrengungen hinsichtlich angemessener Sicherheitskonzepte bei der Datenverwaltung.[104] Dieser Widerspruch im Vergleich zu den DSGVO-Vorgaben sowie den Äußerungen der User zur Wichtigkeit ihrer Daten lässt sich, neben inkonsistentem Verhalten, jedoch auch auf die gegenwärtigen Gegebenheiten des isolierten und föderierten Identitäts- und Zugriffsmanagements zurückführen.[105] Die notwendige Offenlegung bzw. Sammlung umfassender Daten ist derzeit unabdingbar, um zahlreiche Online-Dienstleistungen überhaupt in Anspruch nehmen zu können. Die Speicherung persönlicher Daten bei einer Vielzahl von Dienstleister:innen erhöht zwangsläufig die Angriffsfläche für Cyberkriminelle, was wiederum die Wahrscheinlichkeit eines erfolgreichen Angriffs erhöht.

---

**98** Vgl. Bitkom (2023a).
**99** Vgl. Schunck, C. H. et al. (2021).
**100** Vgl. PwC (2016).
**101** Vgl. eco (2022); PwC (2021).
**102** Vgl. BSI (2022).
**103** Vgl. BSI (2023).
**104** Vgl. Zwitter, A. J. et al. (2020).
**105** Vgl. Ehrlich, T. et al (2021).

Durch die ausschließliche Übermittlung von Daten in Form von Verifikationspunkten mittels Verifiable Presentation zur Nutzung von Dienstleistungen im SSI-Ansatz werden potenzielle Angriffspunkte erheblich reduziert. Infolge dieser Praxis sind Identitätshalter:innen, sprich Entitäten, nicht mehr gezwungen, den Service Providern alle ihre Daten in „Klarform“ offenzulegen. Die Notwendigkeit und Möglichkeit zur Erstellung von Datensilos mit umfassenden Informationen über individuelle Entitäten wird dadurch erheblich reduziert. Im Falle eines erfolgreichen Hackerangriffs auf eine Kund:innendatenbank könnten erheblich weniger oder sogar überhaupt keine verwertbaren Datensätze beim Service Provider erbeutet werden. Dies würde dazu betragen, Schäden durch Datenlecks bei den Service Providern zu minimieren und somit die gesamtwirtschaftlichen Schäden, die durch kriminelle Aktivitäten verursacht werden, zu verringern.

Zudem können Service Provider, die aktuell Daten aufbewahren (müssen), durch die Umsetzung eines SSI-Ansatzes im Zusammenhang mit ihren Pflichten entlastet werden. Die Speicherung und der Schutz von Daten stellen für Service Provider einen substantiellen Kostenfaktor dar, insbesondere in Situationen, in denen sensible Daten (z. B. Ausweisdaten) für betriebliche Abläufe angefragt werden.[106] Gegenwärtig erfordern gewisse Prozesse z. B. die Vorlage einer Kopie des Personalausweises des Nutzenden, dessen Daten der Service Provider nach Erfassung entweder löschen oder adäquat schützen muss.[107] Die Übermittlung der Daten durch den Holder in Form eines Verifiable Presentation würde es dem Service Provider ermöglichen, zahlreiche Daten, insbesondere durch selektive Offenlegung, überhaupt nicht mehr in ihrer (ungeschützten) Form einsehen und speichern zu können. Daten, die beim SP nicht vorliegen, müssen dort auch nicht geschützt werden. Selbst im Falle von Datenpannen beim Service Provider würden somit erheblich weniger oder sogar überhaupt keine verwertbaren Daten preisgegeben werden.

Das SSI-Konzept kann auch innerhalb von Unternehmensstrukturen die Informationssicherheit optimieren. Durch die Einführung einer dezentralen, selbstverwalteten Digitalen Identität für jede:n Mitarbeiter:in oder Besucher:in, die individuelle Attribute wie Zugriffs- und Zugangsrechte aufweist, können aufwendige Datensilos, in denen diese Informationen bislang zentral vom Unternehmen verwaltet werden müssen, abgelöst werden. Zusätzlich entfällt für die Mitarbeiter:innen die Verantwortung, eine Vielzahl von Accounts für jede Anwendung zu verwalten und mit Passwörtern zu sichern.[108] Diese Anwendungsmöglichkeiten können in sämtlichen Unternehmensbereichen umgesetzt werden, die einer umfassenden Sicherung bedürfen, wie beispielsweise im Kontext des Geländezugangs bei Unternehmen der kritischen Infrastruktur oder bei der Gewährleistung von Netzwerkzugriffen für beauftragte Softwareunternehmen.

**106** Vgl. Strüker, J. et al. (2021).
**107** Vgl. Bitkom (2020).
**108** Vgl. Bitkom (2023b); Strüker, J. et al. (2021); Bitkom (2020).

### 3.2.2 Verbesserte Vertrauensbeziehungen

Die Herstellung von Vertrauensbeziehungen gestaltet sich in der digitalen Welt oftmals schwer. Qualifizierte Vertrauensdienste gemäß der eIDAS-Verordnung erweisen sich als aufwendig, kostenintensiv und teilweise nicht mehr sicher. User und Service Provider verzichten darum oft auf die Erbringung eines qualifizierten Vertrauensnachweises. SSI könnte als Ansatz dienen, um klare Informationen bereitzustellen und Datenschutz durch selektive Offenlegung zu ermöglichen, wodurch Vertrauensbeziehungen verbessert werden könnten. Durch das Trust-Triangle werden Misstrauen und Informationsasymmetrien in der Prinzipal-Agent-Beziehung abgebaut, wodurch Service Provider und Entitäten tiefere und vertrauensvolle Beziehungen zueinander aufbauen können.

Vertrauen „*ist die Erwartung, nicht durch das Handeln anderer […] geschädigt zu werden; […]*“.[109] Es erleichtert daher Beziehungen, wie beispielsweise alltägliche Transaktionen zwischen zwei Parteien oder ist sogar eine Grundvoraussetzung dafür. In der analogen Welt können Vertrauensbeziehungen u. a. durch die Vorlage äußerst fälschungssicherer Dokumente, wie z.B. Personalausweis, gestärkt werden. Das Vertrauen beruht dabei weniger auf der spezifischen Entität, die das Dokument vorlegt, als vielmehr auf der als vertrauenswürdig eingeschätzten Institution, die das Dokument ausgestellt hat.[110]

Der Aufbau und die Stärkung von Vertrauensbeziehungen in der digitalen Welt gestalten sich – allein durch das Fehlen des physischen Gegenübers – als weitaus herausfordernder. Mithilfe qualifizierter Vertrauensdienste gemäß den Bestimmungen der eIDAS-Verordnung wird versucht, Grundlagen für ähnliche Vertrauensbeziehungen in der digitalen Welt zu ermöglichen. Als qualifizierter elektronischer Vertrauensdienst wird z. B. eine Signatur auf Basis qualifizierter Zertifikate bezeichnet, die „*die elektronischen Validierungsdaten mit einer natürlichen oder juristischen Person verknüpft und mindestens den Namen oder das Pseudonym dieser Person bestätigt*“.[111] Diese Vertrauensdienste umfassen qualifizierte elektronische Signaturen und Siegel sowie (theoretisch) qualifizierte Validierungsdienste und Bewahrungsdienste.[112] Diese Verfahren laufen allerdings nur bedingt rein digital ab. Außerdem sind sie für natürliche Personen lediglich in Verbindung mit physischen Dokumenten, wie beispielsweise dem Personalausweis, anwendbar. In Deutschland wird dies beispielsweise durch die AusweisApp[113] oder die Anwendung eines Video-Identifizierungsverfahrens realisiert, bei dem der Service Provider oder eine beauftragte Dienstleister:in mittels Videotelefonie Sicherheitsmerkmale des Ausweises der betreffenden Entität überprüft. Dies führt dazu, dass die Identifizierung im digitalen Raum anhand offizieller Dokumente für beide Parteien üblicherweise äußerst aufwendig ist. Für das Video-Ident-Verfahren wurden darüber hinaus Möglichkeiten zum Betrug

**109** Vgl. Gabler Wirtschaftslexikon (2021).
**110** Vgl. Anke, J., Richter, D. (2023).
**111** Vgl. Bundesnetzagentur (2022a).
**112** Vgl. Bundesnetzagentur (2022b). Stand 20.11.2023 werden keine Anbieter für qualifizierte Validierungsdienste und Bewahrungsdienste aufgeführt, da es nach Angabe der Quelle noch keine Anbieter gibt.
**113** Vgl. BMI (2023b).

nachgewiesen[114] und das automatisierte Identifikationsverfahren eingestellt. Im Kontext juristischer Personen gestaltet sich der Identitätsnachweis in der digitalen Welt erheblich anspruchsvoller, da diese von den genannten Verfahren ausgeschlossen sind.[115]

Als Alternative zu den qualifizierten Online-Verfahren wird daher in der Regel auf angemessene Vertrauensnachweise verzichtet. Entitäten müssen sich bei den meisten geschäftlichen Transaktionen nur mit einer E-Mail-Adresse und Angaben zu ihrer Person registrieren. Nur in Einzelfällen werden Sicherheitsmaßnahmen, wie beispielsweise eine Kopie des Personalausweises, verlangt. Diese alternativen Methoden weisen jedoch erheblich weniger oder gar keine robusten Sicherheitsmerkmale auf. Zusätzlich geben die User mit diesen Verfahren viele persönliche Informationen Preis. Service Provider neigen in Folge der aufwendigen bzw. fehlenden Verfahren zur Vertrauensbildung dazu, auf privatwirtschaftliche Siegel und Zertifikate als Vertrauensnachweis zurückzugreifen. Diese Methoden sind jedoch mit Unsicherheiten und Nachteilen behaftet und generieren zusätzliche Kosten.[116] Bei vielen wirtschaftlichen Transaktionen wird dem Gegenüber aufgrund des Aufwandes für beide Seiten darum ein Vertrauensvorschuss gewährt. Ein solcher Vertrauensvorschuss begünstigt jedoch Identitätsdiebstahl und Internetbetrug.[117]

Gegenwärtig manifestiert sich der Prozess des Vertrauensnachweises mit geringerer Qualität in der Regel außerdem zu Ungunsten der Entität, der dabei oft eine einseitige Belastung auferlegt wird. Während die Entität ihre Identität durch die zuvor beschriebenen Verfahren nachweisen muss und dabei viele Informationen über sich Preis gibt, kann sie sich beim Service Provider meist nur auf privatwirtschaftliche Siegel und Zertifikate verlassen. Diese asymmetrischen Informationsverhältnisse führen zu unausgewogenen Vertrauensbeziehungen[118] Insgesamt haben Service Provider und Entitäten gegenwärtig daher nur begrenzte bis gar keine Möglichkeiten, ihre Vertrauensbeziehungen in der digitalen Welt in dem Maße zu gestalten, wie es in der analogen Welt der Fall ist.

SSI trägt zur Optimierung von Vertrauensbeziehungen für beide Vertragsparteien bei, indem klare Informationen darüber bereitgestellt werden, mit wem sie in geschäftlicher Interaktion stehen. Zusätzlich ermöglicht SSI den Entitäten einen verbesserten Datenschutz durch selektive Offenlegung. Ein konkretes Anwendungsszenario ist die Ausstellung von E-Rezepten durch Ärzt:innen (Issuer) für Patient:innen (Holder), die diese in Apotheken (Verifier) einlösen. Dabei kann die Apotheke sicherstellen, dass die Patient:in autorisiert ist, ein bestimmtes Medikament zu beziehen, während diese keine Sorge haben muss, dass die Apotheke mehr als die erforderlichen Informationen aus dem E-Rezept von ihr erhält.[119] Potenzielle Arbeitnehmer:innen müssen in Bewerbungsprozessen bei Arbeitgebenden beispielsweise Dokumente vorweisen, die ihre Verlässlichkeit und Fähigkeiten bestätigen (z. B. Zeugnisse, Zertifikate, Arbeitsbescheinigungen, …).

**114** Vgl. CCC (2022).
**115** Vgl. BaFin (2017).
**116** Vgl. Puhl, P. et al. (2021).
**117** Vgl. Schellinger, B. et al. (2022).
**118** Vgl. Akerlof, G. A. (1970).
**119** Vgl. Strüker, J. et al. (2021).

Digitale Ausführungen dieser Dokumente weisen aktuell lediglich eingeschränkte bis keinerlei Fälschungssicherheit auf. Durch den Einsatz von Verifizierungspräsentationsnachweisen (Verifiable Credentials) könnten Bewerber:innen jedoch im Besitz solcher fälschungssicheren Dokumente sein, bei denen die potenziellen Arbeitgebenden darauf vertrauen können, dass sie von vertrauenswürdigen Herausgebenden stammen.[120]

Neben solchen Fällen, in denen ein hohes Vertrauensniveau notwendig ist (QEAA), sind aber insbesondere auch Anwendungsfälle mit niedrigerem Vertrauensniveau denkbar (EAA), die in der Wirtschaft deutlich häufiger zur Anwendung kommen dürften. Dies tritt insbesondere dann auf, wenn keine Verknüpfung mit personenbezogenen Identitätsdaten notwendig ist, wie beispielweise bei Eintrittskarten.

Auch im Kontext der Integration von Elementen des Internet of Things können SSI zu einer Optimierung von Vertrauensbeziehungen beitragen.[121] Ein exemplarisches Szenario sind Fahrzeuge, denen mittels ihrer Fahrzeugidentifikationsnummer eine Vehicle Identity zugeordnet wird. Durch diese Vehicle Identity können Fahrzeuge eigenständig, unabhängig von der Fahrer:in, mit verschiedenen Instanzen wie z. B. dem Kraftfahrtbundesamt, Prüfstellen wie dem TÜV, Tankstellen oder Werkstätten interagieren. Dabei bleiben Fahrzeugattribute, darunter z. B. Einträge im Fahrzeugschein und -brief, Haupt- und Abgasuntersuchung, Serviceplan bzw. Scheckheft oder Tachostand, vor Manipulation geschützt.[122]

### 3.2.3 Mehr Datensouveränität

Isolierte Digitale Identitäten und die Geschäftsmodelle vieler Identity Provider, insbesondere bei Social Logins, führen zu einem Kontrollverlust über persönliche Daten der User. SSI können durch dezentrale Datenverwaltung und selektive Offenlegung der Daten dagegen gewährleisten, dass Daten nur für autorisierte Zwecke genutzt werden und sparsam in den Umlauf kommen. SSI können somit die Datensouveränität der Entitäten steigern und zugleich Abhängigkeitsverhältnisse vorbeugen.

In Deutschland besteht tendenziell ein höheres Vertrauen gegenüber hiesigen beziehungsweise europäischen Hersteller:innen und Dienstleistungsanbieter:innen im Vergleich zu ihren nicht-europäischen Pendants. Insbesondere Plattformanbieter:innen, die häufig als Identity Provider im Kontext des föderierten Identitäts- und Zugiffsmanagements operieren, wird ein geringes Vertrauen im Umgang mit persönlichen Daten entgegengebracht.[123] Die Ursache für dieses Misstrauen liegt unter anderem in den Geschäftsmodellen zahlreicher Identity Provider.[124] Anbieter:innen von Single-Sign-On-Diensten, sprich Identity Provider, erhalten Informationen über die Nutzung verbundener

**120** Vgl. Strüker, J. et al. (2021); World Economic Forum (2020); Bitkom (2020).
**121** Vgl. Babel, M. (2023).
**122** Vgl. Bitkom (2023b); MOBI (2019); Strüker, J. et al. (2021).
**123** Vgl. Bitkom (2021).
**124** Vgl. PwC (2018); Wiewiorra, L. et al (2020).

Dienste und Webseiten von Entitäten. Im Fall von Plattformanbieter:innen besteht die Geschäftspraxis u. a. darin, User-Profile ihrer Kund:innen durch die Verknüpfung mit neuen Informationen anzureichern. [125] Die Angebote für Single-Sign-On durch Plattformanbieter:innen erweisen sich zwar als nutzerfreundlich im Sinne der Praktikabilität, führen jedoch aus Sicht der Entitäten zu einem Kontrollverlust über ihre eigenen Daten.

Die EU-Verordnung für eine Stärkung von transparenten und fairen digitalen Märkten (Digital Markets Act (DMA)) verfolgt das Ziel, die marktbeherrschende Stellung von solchen sogenannten Gatekeepern (Betreiber:innen zentraler Plattformdienste)[126], insbesondere im Bereich der Identifikationsdienste, aufzubrechen.[127] Gatekeeper konnten bisher von externen Unternehmen, die ihre Dienstleistungen auf ihren Plattformen anbieten, verlangen, einen Identifizierungsdienst des Gatekeepers zu nutzen, anzubieten oder mit diesem zu interoperieren.[128] Der DMA verschiebt zwar die Entscheidungsgewalt über Digitale Identitäten von den Gatekeepern zu den Dienstanbieter:innen, dennoch besteht nach wie vor die Gefahr, dass Diensteanbieter:innen und insbesondere ihre User durch Lock-in-Effekte in eine Abhängigkeit von wenigen Gatekeepern geraten, was potenziell die Preisgabe von Daten (sogenanntes Hold-up-Problem) zur Folge haben kann.[129] Zudem findet ein Kontrollverlust der Daten von Usern nicht nur über Gatekeeper, sondern auch durch zahlreiche andere Identity Provider und Service Provider statt. Entitäten, sowohl Privatpersonen als auch Unternehmen, laufen somit weiterhin Gefahr, die Kontrolle über ihre Daten zu verlieren. Gegenwärtig sind sie auf die Speicherung ihrer Daten durch Service Provider oder Identifizierungsdienste angewiesen und haben keinen Einfluss darauf, wo und wie ihre Identitätsdaten gespeichert werden.

Im Kontext des SSI-Konzepts, das eine dezentrale, selbstverwaltete Identitätsverwaltung ohne eine zentrale Rolle des Identity Providers anstrebt, haben Entitäten die Gewissheit, dass ihre Daten ausschließlich für die von ihnen autorisierten Zwecke genutzt werden. Für natürliche Personen bedeutet dies beispielsweise, dass sie Dienstleistungen in Anspruch nehmen können, ohne sich bei jedem einzelnen Service Provider oder einem Identity Provider separat anmelden zu müssen. Die erforderlichen Daten wurden bereits von einem oder mehreren Issuern erstellt und liegen den Entitäten vor. Diese können, auch in selektierter Form mittels Selective Disclosure, bei Bedarf an den jeweiligen Service Provider weitergegeben werden. Entitäten müssen somit nur die Daten offenlegen, die für den spezifischen Geschäftsprozess unerlässlich sind. Als Beispiel lässt sich die Altersverifikation anführen, die etwa beim Mieten von Fahrzeugen oder dem Erwerb von Tabak und Alkohol relevant ist. Während bisher das Alter durch die Übermittlung des vollständigen Geburtsdatums auf dem Personalausweis verifiziert werden musste –

**125** Vgl. Wiewiorra, L. et al (2020).
**126** Damit sind – Stand 06.09.2023 – die Unternehmen Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft mit ihren Identifizierungsdiensten gemeint, die „*zusammen mit oder zur Unterstützung von zentralen Plattformdiensten*“ erbracht werden und „*eine Überprüfung der Identität von Endnutzern oder gewerblichen Nutzern ermöglich[en], unabhängig von der verwendeten Technologie*“. (vgl. Art. 2 Nr. 19 DMA).
**127** Vgl. Europäische Union (2022).
**128** Vgl. Yildiz, H. et al. (2023).
**129** Vgl. Yildiz, H. et al. (2023); Tagesschau (2023); Ehrlich, T. et al. (2021).

wobei auch für den jeweiligen Prozess irrelevante Informationen wie z. B. Augenfarbe und Geburtsort übermittelt wurden – ermöglicht die Selective Disclosure nunmehr die Übermittlung lediglich der unbedingt erforderlichen Information (beispielsweise älter als 18 Jahre).

Für juristische Personen sind analoge Prozesse vorstellbar, die vermeiden, dass ihre Daten nicht bei diversen Service Providern zentral gespeichert werden. Ein exemplarisches Modell für einen solchen datenschutzorientierten Ansatz ist Gaia-X.[130] In diesem Datenraum haben Unternehmen die Möglichkeit, anderen Unternehmen Dienstleistungen oder Produkte anzubieten, wobei der Erwerb dieser Angebote nur unter bestimmten Voraussetzungen erfolgen kann, wie beispielsweise unter Nachweis bestimmter Zertifizierungen.[131] Somit erfolgt nur ein minimaler Datenaustausch und dieser auch nur dann, wenn geforderte Bedingungen erfüllt sind.

Im Zusammenhang mit der Datensouveränität können auch Service Provider von den Potenzialen von SSI profitieren. Hierzu gehört beispielsweise die Möglichkeit, jederzeit den Nachweis über die Freigabe der von einer Entität übermittelten Daten zu erbringen zu können, insbesondere im Kontext rechtlicher Anforderungen wie beispielsweise der DSGVO.[132]

### 3.2.4 Effizientere Prozesse und neue Geschäftsmodelle

Die ineffiziente Verwaltung zahlreicher Digitaler Identitäten stellt sowohl für Service Provider als auch für Entitäten ein Problem dar. Die bisherigen Prozesse sind ineffizient, kostenintensiv und aufwendig. Durch die Verwendung von SSI können sowohl Service Provider als auch Entitäten Prozesse optimieren und somit signifikante Einsparungen in Bezug auf Zeit und Kosten realisieren. Darüber hinaus eröffnet die Einführung neuer digitaler Identitätsformen für juristische Personen und Objekte die Chance, innovative Geschäftsmodelle zu entwickeln und zu nutzen.

Bei der Nutzung verschiedener Digitaler Identitäten ist ein zentrales Problem, dass sie für alle Beteiligten äußerst ineffizient ist.[133] Insbesondere für Service Provider gestaltet sich die Verwaltung einer Vielzahl von Accounts als umständlich, aufwendig und kostspielig. Ein Beispiel hierfür sind die Know-Your-Customer-Prozesse (KYC), die vor allem von Banken durchgeführt werden, um die Legitimation neuer Kunden zu prüfen und Geldwäsche zu verhindern.[134] Studien beziffern die Kosten für einzelne Unternehmen aus dem Finanzsektor pro KYC-Prozess auf 10 bis 100 britische Pfund,[135] bzw. insgesamt

**130** Vgl. Maier, B., Pohlmann, N. (2022).
**131** Vgl. Verein Industrie 4.0 Österreich (2022).
**132** Vgl. Strüker, J. et al. (2021).
**133** Die Interessen der Identity Provider, insbesondere der Anbieter von Social-Logins, sind hiervon natürlich ausgenommen.
**134** Vgl. World Economic Forum (2020).
**135** Vgl. Ogunsola, F. (2017).

zwischen 60 und 500 Millionen US-Dollar pro Jahr.[136] Laut PwC betrugen die weltweiten Kosten für KYC-Prozesse in der Finanzbranche zwischen 2015 und 2019 allein 23,2 Milliarden Euro. Eine erhebliche Reduzierung dieser Kosten wäre durch die Einführung anerkannter Datenstandards und die Möglichkeit eines sicheren und grenzübergreifenden Datenaustauschs mittels geeigneter digitaler Lösungen möglich.[137] Im Finanzwesen könnten die Kosteneinsparungen durch eine Reduzierung der Ausgaben für Onboarding-Prozesse jährlich zwischen 860 Millionen und 1,7 Milliarden US-Dollar liegen, was etwa fünf bis zehn Prozent der Gesamtausgaben für diesen Zweck ausmacht. Gleichzeitig könnten durch eine Verringerung von Betrugsfällen in diesem Sektor zwischen 1,1 Milliarden und 4,3 Milliarden Euro eingespart werden.[138] Vereinfachte Legitimationsprüfungen könnten jedoch auch für Service Provider in anderen Branchen von Interesse sein, um die notwendigen Identitätsmerkmale ihrer Kund:innen effizienter zu erfassen.[139]

Auf der anderen Seite ist es für Entitäten ebenso umständlich und aufwendig, eine Vielzahl von Accounts zu erstellen und zu verwalten. Laut einer Umfrage verwaltet ein Drittel der Deutschen bereits über 20 Digitale Identitäten, während andere Quellen sogar von rund 90 Digitalen Identitäten für einen durchschnittlichen Europäer sprechen.[140] Die Mehrheit der User von Online-Diensten verwendet dabei bis zu zwölf Onlinedienste pro Woche, wobei ein Großteil auf "klassische" Anmeldeverfahren zurückgreift und nur ein relativ kleiner Anteil Single-Sign-On-Lösungen nutzt. Werden diese Single-Sign-On-Lösungen genutzt, erfolgt dies häufig über Social-Logins bei den Gatekeepern.[141] Aufgrund des Verwaltungsaufwands und des Abflusses individueller Daten versuchen Entitäten oft, die Anzahl der Accounts möglichst gering zu halten. Bedingungen wie beispielsweise die Notwendigkeit zur Erstellung eines Kundenkontos führen bei rund einem Viertel der Befragten einer KPMG-Umfrage zum Thema Online-Shopping zum Abbruch.[142]

Aus Sicht der Anbieter:innen und User ermöglicht SSI effizientere Authentifizierungsprozesse. Entitäten können dabei ihre Digitale Identität eigenständig bei verschiedenen Diensten nutzen, ohne sich anmelden zu müssen oder auf marktbeherrschende Identity Provider angewiesen zu sein. Ein konkretes Beispiel aus Usersicht stellt die Reisebranche dar. Während bei einem Urlaub derzeit sowohl für den Check-In der Fluggesellschaft als auch im Hotel sowie zum Ausleihen eines Mietwagens persönliche Daten jeweils aufs Neue angegeben werden müssen, wäre dies mithilfe einer SSI-Wallet-Lösung auf verhältnismäßig sparsame Weise in einem einzigen Schritt möglich. Durch diesen Prozess müssen Reisende vor dem Flug, im Hotel und bei der Mietwagenfirma keine (oder

**136** Vgl. Reuters (2016).
**137** Vgl. PwC (2022).
**138** Vgl. PwC und DLA Piper (2021).
**139** Vgl. World Economic Forum (2020); Bitkom (2020).
**140** Vgl. Begleitforschung Schaufenster Sichere Digitale Identitäten (2021).
**141** Vgl. Wiewiorra, L. et al. (2020).
**142** Vgl. KPMG (2021).

weniger) Formulare ausfüllen und persönliche Daten preisgeben, während die Anbieterseite nicht mit der Verwaltung dieser Daten belastet ist.[143]

Abgesehen von Lösungen für Privatpersonen können Angebote für Unternehmen, die auf dezentralen, selbstverwalteten Digitalen Identitäten basieren, die Prozesse effizienter gestalten – insbesondere, wenn sie bei verschiedenen Service Providern oder Diensten anwendbar sind. Dies könnte beispielsweise durch die Nutzung einer Organisationswallet bzw. Organisationsidentitäten ermöglicht werden. Ein Anwendungsfall ist die Erstellung von Unternehmenskonten bei verschiedenen Service Providern oder das digitale Onboarding von Kunden oder Lieferanten im Business-to-Business-Bereich.[144] Solche Lösungen könnten Unternehmen nicht nur dabei unterstützen, effizienter miteinander zu interagieren, sondern auch bei der Erfüllung von Berichtspflichten, bei denen Unternehmen bestimmte Eigenschaften oder die Einhaltung von Anforderungen nachweisen müssen (z. B. im Rahmen des Lieferkettensorgfaltsgesetzes, der Export Compliance, Environmental, Social and Governance (ESG)-Berichtspflichten usw.).[145] Eine unkomplizierte und nutzerfreundliche Abwicklung digitaler Datentransaktionen kann auf Seiten der Anbieter:innen zeitaufwändige Dokumenten- und Nachweisverifikationen sowie manuelle Nachbearbeitung und Pflege von Stammdaten eliminieren. Dies führt zu einer Entlastung der Mitarbeiter:innen und Einsparungen von Arbeitszeit.[146]

Die skizzierten, neuartigen und optimierten Geschäftsmodelle schaffen ebenfalls einen Markt für die erforderliche Infrastruktur und die entsprechenden Dienstleistungen. Dies umfasst unter anderem die Bereitstellung von Cloud Agents, Digital Wallets sowie den Betrieb der technischen Infrastruktur, wie beispielsweise Blockchain-Knotenpunkte.[147]

## 3.3 Welche Herausforderungen gehen mit Web 3.0-konformen Digitale Identitäten einher?

Wie in Kapitel 3.2 ausgeführt, bieten SSI eine Vielzahl von Anwendungsmöglichkeiten, um den Herausforderungen im Hinblick auf Identitäts- und Zugriffssystemen zu begegnen. Sowohl Unternehmen als auch Bürger:innen zeigen ein ausgeprägtes Interesse an diesen potenziellen Anwendungsfeldern. Gemäß einer Umfrage von eco Verband e.V. erkennen die meisten Unternehmen die Bedeutung sicherer Digitaler Identitäten für ihre Geschäftsmodelle.[148] Im Rahmen von SSI ist zudem zu erwarten, dass eine verstärkte Nutzung digitaler Dienste seitens der Bevölkerung erfolgen wird.[149] Dennoch ist

**143** Ergänzend sei an dieser Stelle gesagt, dass ein Projekt zum digitalen Hotel-Check-in im Rahmen des Innovationswettbewerbs "Schaufenster Sichere Digitale Identitäten" des BMWK in der tatsächlichen Umsetzung gescheitert ist. Die verantwortlichen Gründe stehen allerdings nicht im Gegensatz zur Machbarkeit eines solchen Verfahrens. Vgl. BMWK (2023a); Bundeskanzleramt (2021).
**144** Vgl. Heinig, M. (2023).
**145** Vgl. Bitkom (2023c).
**146** Vgl. Biedermann, B. et al. (2023).
**147** Vgl. Strüker, J. et al (2021).
**148** Vgl. eco (2022).
**149** Vgl. ebd. (2022).

ungeachtet des vorhandenen Interesses und der praktischen Anwendung von SSI die flächendeckende Verbreitung bislang begrenzt.[150]

Digitale Identitäten, die dezentral und selbstverwaltet organisiert sind, müssen in Bezug auf Einfachheit, Sicherheit und Benutzerfreundlichkeit mindestens gleichwertig zu ihren physischen Pendants sein. Nur so können digitale Prozesse datensparsam, fälschungssicher und datenschutzfreundlich gestaltet werden, um ausreichend Nutzende anzuziehen. In der gegenwärtigen Entwicklungsphase erweisen sich diese Anforderungen jedoch oft als noch nicht vollständig überwunden. Dies lässt sich zum Teil darauf zurückführen, dass das Konzept dezentraler, selbstverwalteter Digitaler Identitäten vergleichsweise neuartig ist. Im Nachfolgenden sollen demnach wesentliche Herausforderungen präsentiert werden, die mit dezentralen, selbstverwalteten Digitalen Identitäten im Kontext des Web 3.0 einhergehen.

### 3.3.1 Gesetzliche und regulatorische Fragen

Die Entwicklung von Lösungen für komplexe rechtliche und regulatorische Fragestellungen im Kontext der Ausgestaltung eines Governance-Frameworks für das digitale Ökosystem dezentraler, selbstverwalteter Digitaler Identitäten gestaltet sich als herausfordernd. Hierbei kommen Fragen bezüglich Datenschutz, Haftung, der rechtlichen Anerkennung digitaler Identitäten, Zugriffs- und Kontrollrechte, der Harmonisierung unterschiedlicher Gesetze sowie der internationalen Zusammenarbeit besondere Bedeutung zu. Die bevorstehende Verabschiedung der eIDAS-2.0-Verordnung und ihre anschließende Umsetzung sollen einen rechtlichen Rahmen für SSI-Lösungen schaffen. Ein zentraler Aspekt der Verordnung ist die Verpflichtung jedes EU-Mitgliedstaats, den Bürger:innen ein EUDI-Wallet bereitzustellen, das von öffentlichen Stellen, kritischen Infrastrukturen und Internetgroßkonzernen anerkannt werden muss und, womöglich, auch privaten Issuern zur Verfügung stehen könnte.[151]

Die eIDAS-2.0-Verordnung umfasst erstmals auch Regelungen für digitale Nachweise und Vorgaben für Maschinenidentitäten, die in der bisherigen eIDAS-Verordnung nicht enthalten waren.[152] Trotz dieser Fortschritte bestehen im Zusammenhang mit eIDAS 2.0 noch einige Detailfragen, deren Klärung entscheidend ist, um eine umfassende Planungssicherheit für Unternehmen und Bürger:innen zu gewährleisten. Für aktuelle Herausforderungen verweisen wir an dieser Stelle auf den gegenwärtigen Umsetzungsstand (s. Kapitel 3.1).

Die Überarbeitung der eIDAS-Verordnung wird voraussichtlich erhebliche Auswirkungen auf bestehende Gesetzgebungen haben, insbesondere in Bezug auf Identifizierungsverfahren wie den Personalausweis.[153] In diesem Zusammenhang müssen Gesetze mit den

**150** Vgl. Ehrlich, T. et al. (2021).
**151** Vgl. KOM (2021).
**152** Vgl. IDunion (2022a).
**153** Vgl. Schwalm, S., Alamillo-Domingo, I. (2021).

Anforderungen und Bestandteilen des SSI-Konzepts (z. B. Wallets, Verifiable Credentials, usw.) in Einklang gebracht werden.[154] Darüber hinaus erfordert die Schaffung eines kohärenten Ökosystems die Harmonisierung verschiedener Gesetze. Verdeutlicht werden kann dies an Service Providern aus dem Bankensektor, die aufgrund verschiedener Gesetze verpflichtet sind bestimmte Identifikationsmerkmale ihrer Kunden wie Namen und Geburtsdatum aber zum Teil auch die Staatsangehörigkeit oder den Geburtsort zu erheben. Die sektorspezifischen Regelungen des Geldwäschegesetzes (GwG), des Onlinezugangsgesetzes (OZG) und des Telekommunikationsgesetzes (TKG) weisen dabei Gemeinsamkeiten in den zu erhebenden Informationen auf (z. B. die Erhebung von Name und Geburtsdatum), aber auch Unterschiede in den zu erhebenden Informationen (z. B. die Erhebung von Staatsangehörigkeit und Geburtsort). Die Wiederverwendung von einmal erfassten Identifikationsmerkmale kann dadurch erschwert oder verhindert werden.[155]

Eine der häufig diskutierten rechtlichen Herausforderungen im Zusammenhang mit dezentralen, selbstverwalteten Digitalen Identitäten betrifft die Frage, inwiefern die technische Umsetzung mit der DSGVO in Übereinstimmung gebracht werden kann (s. Kapitel 2.4.2.1). Aktuell wird intensiv darüber diskutiert, wie eine solche Vorgabe mit den Eigenschaften der Blockchain-Technologie vereinbar sein kann.[156]

Nicht nur der Gesetzgeber, sondern auch Unternehmen sehen sich mit juristischen Fragen konfrontiert, wenn sie sich mit dem Thema SSI befassen. Die aktuellen rechtlichen Unklarheiten erschweren es ihnen z. B., passende Geschäftsmodelle zu entwickeln. Diese umfassenden Hürden werden voraussichtlich auch weiterhin eine Herausforderung für viele Unternehmen darstellen, insbesondere aufgrund der vielschichtigen Bandbreite an Gesetzen, die sie möglicherweise beachten müssen. In vielen Unternehmen könnte es auch nach Inkrafttreten oder der Anpassung entsprechender Gesetze an Expert:innen für rechtliche Fragestellungen mangeln.[157]

### 3.3.2 Interoperabilität (offene Governance-, Standardisierungs- und Technologiefragen)

Das SSI-Konzept beschränkt sich nicht nur auf die in Kapitel 2.4 beschriebenen Akteure, Rollen, Funktionen und Implementierungsverfahren, sondern beschreibt auch verschiedene Schemata, Datenmodelle, Protokolle, APIs, usw..[158] SSI ist aufgrund der in Abstimmung befindlichen Standardisierungsarbeit allerdings noch kein vollständig standardisiertes Ökosystem. Trotz erster Standards gibt es zudem – durch den weiterhin bestehenden Gestaltungsfreiraum innerhalb der Grenzen der Standards – eine Vielzahl an Implementierungsvarianten (für z. B. DID-Methoden) oder Protokolle für das Ausstellen,

**154** Vgl. IDunion (2022a).
**155** Vgl. Tenner, T. (2021).
**156** Vgl. Strüker, J. et al. (2021).
**157** Vgl. eco (2022).
**158** Vgl. Bitkom (2023b); Yildiz, H. et al. (2023).

Transferieren und Präsentieren von Verifiable Credentials.[159] Um Interoperabilität zu gewährleisten, sind noch mehrere offene Governance-, Standardisierungs- und Technologiefragen zu klären.

Um föderierte Identitätsdienste zu harmonisieren und flächendeckende Normen sowie Standards zu etablieren, gewinnen EU-Pilotprojekte im Rahmen von eIDAS 2.0 (wie die Large Scale Pilots (LSP))[160] neben nationalen Bestrebungen wie der eID-Infrastruktur in Deutschland (Schaufenster Sichere Digitale Identitäten)[161] an Relevanz. Gleichzeitig streben zahlreiche private Anbieter:innen danach, ihre Lösungen im Markt zu positionieren. Das wirft die Frage nach einheitlichen Governance-, Standards- und Technologielösungen sowie nach Interoperabilität auf. Während beispielsweise die LSP (DC4EU, EWC, NOBID, POTENTIAL) untereinander interoperabel sind,[162] fehlt diese Interoperabilität zwischen den vier nationalen Schaufensterprojekten (ID-Ideal, IDunion, ONCE, SDIKA). Service Provider müssten demnach entweder mehrere SSI-Stacks in ihrer eigenen Infrastruktur implementieren oder Entitäten wären gezwungen, verschiedene Wallets aus diversen SSI-Stacks zu verwenden.[163]

Governance-, Standards- und Technologiefragen sind im Zusammenhang mit dem eIDAS 2.0-Prozess, Stand Anfang Dezember 2023, noch nicht abschließend gelöst. Dies wird besonders bei der Implementierung des Vertrauensdienstregisters (VDR) deutlich: Die aktuelle Version 1.1.0 des Architektur- und Referenzrahmens (ARF) enthält keine spezifischen Einschränkungen bezüglich der Infrastruktur.[164] Das European Digital Identity Wallet Ecosystem (EUDIW), PIDs und QEAAs könnten demnach sowohl mit als auch ohne den Einsatz von DLT wie Blockchain realisiert werden.[165] Während mehrere europäische Ausarbeitungen der LSP auf Blockchain setzen,[166] hat sich Deutschland vorerst gegen eine solche Umsetzung entschieden.[167] Aufgrund der Verpflichtung jedes LSP-Konsortiums, Interoperabilität zu den anderen Konsortien herzustellen, muss zwischen den Anwendungen dieser Konsortien Interoperabilität sowohl zwischen DLT und Non-DLT als auch zwischen den unterschiedlichen technologischen Ansätzen gewährleistet sein.[168] Die divergierenden technologischen Perspektiven, beispielsweise zwischen dem BSI[169] bzw. dem Bundesministerium des Innern und für Heimat (BMI)[170] und dem EBSI[171] müssen daher in Einklang gebracht bzw. es müssen Lösungen gefunden werden, die eine nahtlose Interoperabilität ermöglichen.

---

**159** Vgl. Yildiz, H. et al. (2023).
**160** Vgl. KOM (2023b).
**161** Vgl. BMWK (2023b).
**162** Vgl. KOM (2023a).
**163** Vgl. Yildiz, H. et al. (2023).
**164** Vgl. Europäische Union (2023).
**165** Vgl. Schwalm, S. (2023a).
**166** Vgl. hierzu die Ausführungen in Kapitel 2.4.2.1.
**167** Vgl. Deutscher Bundestag (2023a); Deutscher Bundestag (2023b).
**168** Vgl. Schwalm, S. (2023b).
**169** Vgl. BSI (2021).
**170** Vgl. BMI (2023c).
**171** Vgl. Deutscher Bundestag (2022).

Es stehen zusätzlich technologische Herausforderungen bevor, für die noch Lösungen etabliert werden müssen. Ein exemplarisches Beispiel ist die langfristige Nachweisfähigkeit. Während auf der Grundlage der PKI bereits Verfahren etabliert sind, die bis zum Ende einer festgelegten Aufbewahrungsfrist die Authentizität, Integrität und Nachvollziehbarkeit digitaler Nachweise gewährleisten können, fehlen derzeit entsprechende Lösungen für dezentrale PKI, die auf Blockchain basiert.[172]

Die Ursachen für die bisherige mangelnde Interoperabilität liegen, wie bei der Entstehung von Standards üblich, im Entwicklungsprozess. Die verschiedenen Interessengruppen und Beteiligten bringen Vorschläge ein, die untereinander nicht kompatibel sind.[173] Diese fehlende Interoperabilität und die ungeklärten Technologiestandards beeinträchtigen jedoch die Verbreitung von SSI-Lösungen. Bevor Entwickler:innen, Herausgeber:innen und Akzeptanzstellen interoperable Anwendungen oder Geschäftsmodelle implementieren können, müssen sie sich auf ein System einigen. Dieser Prozess erfordert derzeit erheblichen Aufwand, und selbst nach einer Entscheidung besteht die Unsicherheit, ob die Interoperabilität zu anderen Konsortien gewährleistet ist, die möglicherweise andere Entscheidungen getroffen haben.[174] Dieser Aufwand, gepaart mit der Unsicherheit über den Erfolg des Ergebnisses, kann insbesondere kleine und mittlere Unternehmen (KMU) davon abhalten, sich zu engagieren, da sie in der Regel über weniger Ressourcen als Großunternehmen für derartige Herausforderungen verfügen.

### 3.3.3 Skalierbarkeit und Ausweitung der Anwendungsfälle

Im Kontext der Diskussion um SSI gewinnt die Bedeutung konkreter Anwendungsfälle zunehmend an Relevanz. Trotzdem sind flächendeckende Verbreitung und praktische Anwendung von SSI-Lösungen bisher gering geblieben.[175] Daher werden neben privatwirtschaftlichen Anbietern, die erste Lösungen entwickeln, auch öffentlich geförderte Projekte umgesetzt, die konkrete Anwendungsfälle aufzeigen sollen. Das Bundeswirtschaftsministerium begründet die Notwendigkeit dieser im Jahr 2020 ins Leben gerufener Projekte damit, dass *„keine der existierenden ID-Lösungen […] bislang die für eine breite Anwendung notwendige kritische Masse erreichen [konnte]. […] Mit dem „Schaufenster Sichere Digitale Identitäten“ sollen deutsche eIDAS-Lösungen zugänglich gemacht werden, die gleichermaßen nutzerfreundlich, vertrauenswürdig und wirtschaftlich sind: Für Verwaltung, Wirtschaft – insbesondere KMU – und die Bevölkerung.“*[176] In den Schaufensterprojekten sind nach eigenen Angaben mehr als 100 Anwendungsmöglichkeiten sicherer digitaler Identität entstanden.[177] Im Zuge von eIDAS 2.0 wurden 2023 zudem vier sogenannte LSPs gestartet, die in Zukunft die Möglichkeiten einer digitalen Wallet plastisch darstellen sollen. Dabei sollen nicht nur die Funktionalitäten getestet, sondern

172 Vgl. IDunion (2022a).
173 Vgl. van der Veer, H., Wiles, A. (2008).
174 Vgl. Ehrlich, T. et al. (2021).
175 Vgl. ebd.
176 Vgl. BMWK (2023a).
177 Vgl. Begleitforschung Sichere Digitale Identitäten (2021).

auch deren Mehrwert anhand von diversen Anwendungsfällen potenziellen Usern nähergebracht werden.[178]

Die erfolgreiche Umsetzung Digitaler Identitäten ist maßgeblich von ihrer Ausgestaltung abhängig. Diese muss den technischen sowie gesellschaftlichen Rahmenbedingungen und Anforderungen gerecht werden. Der organisatorische und finanzielle Aufwand für die Implementierung neuer Technologien in der Datenverwaltung und den Aufbau von Fachwissen stellt insbesondere für kleine und mittlere Unternehmen erhebliche Investitionen und Aufwände dar. Aktuell steht dem jedoch entgegen, dass der Mehrwert solcher Geschäftskonzepte und -prozesse noch nicht eindeutig nachgewiesen wurde bzw. skaliert werden kann.[179] Es ist zu befürchten, dass viele Unternehmen sich daher trotz der bevorstehenden Umsetzung der eIDAS 2.0-Verordnung zurückhaltend zeigen. Dies birgt die Gefahr, dass es ihnen nicht nur jetzt, sondern auch zukünftig an Kenntnissen über mögliche Geschäftsmodelle fehlt.[180]

### 3.3.4 Fehlendes Bewusstsein und mangelnde User-Akzeptanz

Viele User zeigen ein Bewusstsein hinsichtlich der Probleme, die mit zentralen und föderierten Identitäts- und Zugriffsmanagementsystemen auftreten können. Sie zeigen sich jedoch bei der Nutzung alternativer Verfahren, wie z. B. der eID, noch sehr zurückhaltend. Zum Großteil liegt das an Bedenken zur Informationssicherheit sowie der Usability. Die mit der eIDAS 2.0-Verordnung angestrebten Digitalen Identitäten könnten viele dieser Bedenken zerstreuen, werden in der derzeitigen Umsetzungsphase von vielen Bürgerrechtler:innen jedoch noch kritisch gesehen.

Eine beträchtliche Anzahl potenzieller Anwender:innen begegnet zentralen Digitalen Identitäten häufig mit Skepsis.[181] Sie würden stattdessen die Vorteile von SSI vorziehen, die ihnen die eigenständige Verwaltung ihrer Identitätsdaten ermöglichen.[182] Es scheint jedoch, dass vielen potenziellen Anwender:innen die Existenz solcher Lösungsmöglichkeiten noch nicht bewusst ist. Gemäß einer Umfrage von eco Verband aus dem Jahr 2022 haben nur etwa die Hälfte der Unternehmen und lediglich ein Fünftel der Bürger:innen bereits vom Konzept der SSI gehört.[183]

Neben einem fehlenden Bewusstsein mangelt es weiterhin auch an einer breiten Nutzungsakzeptanz für geeignete Lösungen. Ein Grund dafür ist vermutlich auch die Gewohnheit an bestehende Systeme. Beispielsweise kann sich über die Hälfte der Befragten einer repräsentativen Studie zum Thema Digitale Identitäten nicht vorstellen, Dokumente in einer „elektronischen Brieftasche“ auf dem Smartphone abzulegen.[184] In einer weiteren Untersuchung gibt ein nicht unerheblicher Teil der Befragten für diese ablehnende Haltung an, dass sie nicht ständig auf das Smartphone angewiesen sein

**178** Vgl. BMI (2022).
**179** Vgl. Ehrlich, T. et al. (2021).
**180** Vgl. eco (2022).
**181** Vgl. ebd.
**182** Vgl. Begleitforschung Schaufenster Sichere Digitale Identitäten (2021).
**183** Vgl. eco (2022).
**184** Vgl. Begleitforschung Schaufenster Sichere Digitale Identitäten (2021).

möchten.[185] Dies ist jedoch – neben Softwarelösungen auf einem Computer – eine zentrale Anforderung, um sie überhaupt nutzen zu können.
Die eingeschränkte User-Akzeptanz resultiert auch aus der Tatsache, dass insbesondere Bürger:innen oft Bedenken hinsichtlich möglicher Zusatzkosten äußern.[186] Wenn jedoch die Verwendung von Daten als Zahlungsmittel wegfällt, müssen alternative Finanzierungsmodelle in Betracht gezogen werden. Die Bereitschaft der User, diese Kosten zu tragen, ist noch Gegenstand weiterer Untersuchungen.

Doch auch eine generell zurückhaltende oder ablehnende Haltung der Bürger:innen gegenüber der Digitalisierung sowie ein mangelndes Vertrauen in neue Technologien stellen die Implementierung dezentraler, selbstverwalteter Digitaler Identitäten vor erhebliche Herausforderungen. Die wirtschaftlichen Vorteile durch Effizienzgewinne unterliegen den Datenschutz- und Sicherheitsbedenken.[187] In einer repräsentativen Umfrage der Wirtschaftsprüfungsgesellschaft PwC zu den eID-Funktionen werden unter anderem Bedenken hinsichtlich der Informationssicherheit sowie Ängste vor Datenverlusten und Hackerangriffen und die daraus resultierenden Identitätsdiebstähle, geäußert.[188] Andere Umfragen, wie die von eco, kommen zu ähnlichen Ergebnissen und zeigen, dass Datenschutzbedenken und mangelndes Vertrauen in die Technologie und die dahinterliegenden Dienste zu einer ablehnenden Haltung führen.[189]

Auch bei potenziellen Anwenderunternehmen zeigen sich Herausforderungen durch Unsicherheiten gegenüber neuer Technologien. In einer Umfrage von eco äußern viele Unternehmen Bedenken hinsichtlich der möglicherweise unsicheren Verwaltung der Digitalen Identitäten.[190] Es bleibt jedoch noch offen, inwieweit User gegenüber SSI aufgeschlossen sein werden. Eine Umfrage zeigt, dass ein Großteil der Befragten digitale Dienste auch mit SSI-Lösungen nicht oder nicht häufiger nutzen würden.[191]

Das Thema Informationssicherheit, insbesondere Datenschutz, wird auch von Aktivist:innen, die sich den Freiheitsrechten widmen, im Zusammenhang mit der eIDAS 2.0-Verordnung oft kritisch betrachtet. Dabei wird häufig, aber nicht ausschließlich, kritisiert, dass die Ausgestaltung „zertifizierte Unsicherheiten“ und eine Online-Überwachung durch den Staat ermöglichen könnte.[192] Darüber hinaus werden auch Bedenken hinsichtlich potenzieller sozialer Risiken geäußert. Diese bestehen unter anderem darin, dass viele User ihre Credentials nicht mit der nötigen Sorgfalt schützen (können) und diese unbedarft oder unwissentlich teilen.[193] Die Diskussion findet bislang vor allem auf

185 Vgl. PwC (2021).
186 Vgl. eco (2022).
187 Vgl. ebd. (2022).
188 Vgl. PwC (2021).
189 Vgl. eco (2022).
190 Vgl. ebd. (2022).
191 Vgl. ebd. (2022).
192 Vgl. Leisegang, D. (2023).
193 Vgl. Wittmann, L. (2022).

Expert:innenebene statt, aber die genannten Kritikpunkte könnten auch vor dem Hintergrund der zuvor genannten Zurückhaltung, von (größeren) Teilen der Bevölkerung geteilt werden.

# 4 Diskussion zu Handlungsbedarf und Schlussbemerkung

Im abschließenden Kapitel werden regulatorische Implikationen und potenzielle (staatliche) Handlungsbedarfe und -optionen aus den zuvor genannten Herausforderungen abgeleitet, um die Chancen, die die eIDAS-2.0-Verordnung bietet, nutzen zu können.

## 4.1 Staatliche Handlungsbedarfe und -optionen

SSI sind, wie in den Kapiteln 2.4 und 2.5 gezeigt, aus technologischer Sicht geeignet, das Fundament des Web 3.0 zu bilden. Die erfolgreiche Implementierung und die damit verbundenen Chancen (s. Kapitel 3.2) hängen jedoch von einer Reihe an Faktoren ab (s. Kapitel 3.3), die durch staatliche Handlung (mit-)beeinflusst werden können. Um einen allgemein akzeptierten Einsatz von dezentralen, selbstverwalteten Digitalen Identitäten zu gewährleisten, sind noch weitgehende rechtliche und regulatorische Anpassungsbedarfe von Nöten. Ebenso ist die Ausgestaltung einer Governance-Struktur mit einheitlichen Verfahrens- und Organisationsregeln sowie Technologiestandards noch nicht abgeschlossen. Auch die zu klärenden rechtlichen und regulatorischen Fragestellungen, stellen unvollendete Herausforderungen dar, die seitens des Gesetzgebers und weiterer politischer Institutionen in Kooperation mit nicht-staatlichen Akteuren umzusetzen sind. Parallel dazu sollten wirtschafts- und gesellschaftspolitische Überlegungen Berücksichtigung finden, um staatliche Handlungsbedarfe und -optionen zu evaluieren und somit die Akzeptanz seitens Bürgerinnen und Bürgern sowie Unternehmen zu fördern.

### 4.1.1 Rechtliche und regulatorische Rahmenbedingungen sowie Klarheit schaffen

Die aktuell fehlenden rechtlichen und regulatorischen Grundlagen sowie bestehende Unklarheiten im rechtlichen Kontext wirken als Hemmnis für die rechtssichere Entwicklung von Lösungen im Bereich selbstbestimmter Digitaler Identitäten und deren weitreichende Verbreitung. Dies betrifft insbesondere die Fortschritte bezüglich der Verabschiedung, Inkraftsetzung und Umsetzung der eIDAS-2.0-Verordnung. Gleichzeitig wird die Notwendigkeit erkennbar, nationale Gesetze an ein potenzielles "Recht auf und an Digitalen Identitäten" anzupassen, was weitere Unsicherheiten mit sich bringen könnte. Um ein geeignetes Ökosystem für Digitale Identitäten zu schaffen, ist daher vor allem regulatorische Verbindlichkeit zu schaffen. Dafür müssen zum einen neue Gesetze erlassen und zum anderen aktuell noch divergierende rechtliche und regulatorische Vorgaben harmonisiert werden. Dies ist zwingend notwendig, um die Nutzung von Digitalen Identitäten nach einheitlichen Regeln zu gestalten.[194]

Auf nationaler und europäischer Ebene sollte daher eine proaktive Herangehensweise verfolgt werden, um eine zeitnahe Klärung rechtlicher und regulatorischer Vorgaben

**194** Vgl. Tenner, T. (2021).

sowie etwaiger offener Fragen zu erreichen. Hierbei stellt die Zusammenarbeit mit relevanten Institutionen und Interessengruppen ein zentrales Element dar, um sicherzustellen, dass Anpassungen an den rechtlichen Rahmen sowohl sachgemäß als auch praxisorientiert erfolgen und dabei die Interessen der Bürger:innen angemessen berücksichtigt werden.

### 4.1.2 Offene Standards und Technologiefragen in Einklang bringen

Für eine erfolgreiche und flächendeckende Umsetzung muss darüber hinaus eine Governance entwickelt werden, mit der Digitale Identitäten nicht nur universell gültig, sondern auch interoperabel und nutzerzentriert sind. Wesentlicher Bestandteil der Governance sind Standardisierungen für die Erstellung, Übertragung und Verifikation von Digitalen Identitäten. Im Zuge der Interoperabilität erfordert es unter anderem Entscheidungen in Bezug auf Technologien, Datenformate und Kommunikationsprotokolle. Diese Entscheidungen sollten im Sinne einer konsistenten und effizienten Gestaltung auf europäischer Ebene harmonisiert werden - auch in den Bereichen, in denen den EU-Mitgliedsstaaten gewisse Handlungsspielräume offenstehen könnten. Nur so ist eine uneingeschränkte Nutzung Digitaler Identitäten über verschiedene Plattformen und Systeme hinweg möglich. Bei der Entscheidungsfindung sollte der Fokus auf den Bedürfnissen der User liegen. Im Verlauf der aktuellen Diskussionsrunden sollten ebenso die kritischen Stimmen sowie vulnerable Gruppen gehört und angemessen berücksichtigt werden. Eine transparente und aktive Einbindung aller Beteiligten ist daher unverzichtbar. Um die genannten Punkte umzusetzen, empfehlen sich folgende Herangehensweisen:

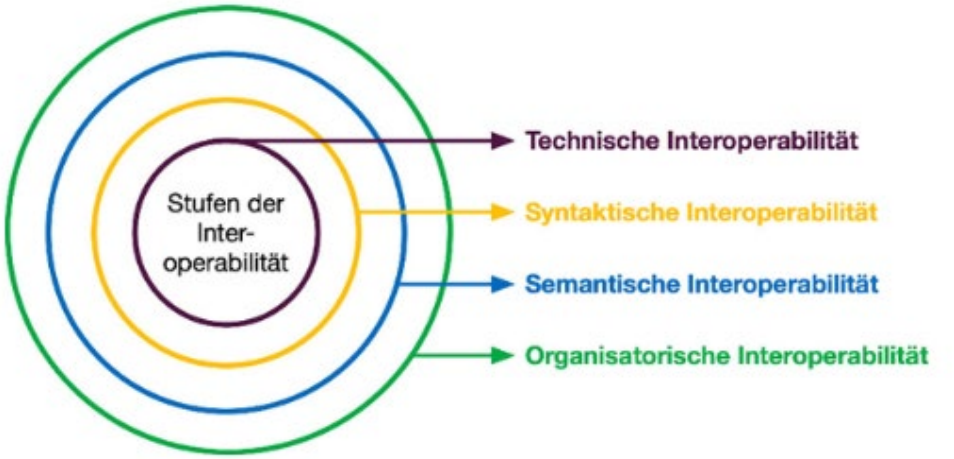
- Für alle beteiligten Akteur:innen sollten, wie im offenen Konsultations- und Architekturprozess des BMI im Rahmen des „GovLabDE Digitale Identitäten“ bereits geschehen[195], Austauschplattformen geschaffen werden. Auf diesen Plattformen können verschiedene Interessensgruppen – einschließlich staatlicher Institutionen, Forschung Unternehmen und Zivilgesellschaft, offene Standard- und Technologiefragen diskutieren. Dabei sollte besonders darauf geachtet werden, dass auch die Akteur:innen einbezogen werden, die von den Entscheidungen betroffen sind, im Konsultationsprozess bisher aber nur bedingt teilnehmen (z. B. durch fehlende Technologieaffinität). Dabei sollten nicht nur technische Aspekte, sondern auch die persönlichen Bedürfnisse und Anliegen der User Berücksichtigung finden. Der kontinuierliche Austausch fördert nicht nur die Einigung auf Standards und Technologien, sondern auch das Verständnis, das Vertrauen und die Akzeptanz (s. u.).

**195** Vgl. BMI (2023d).

- Auf nationaler Ebene sollte bei der Findung geeigneter Standards und Technologien auf das Prinzip der Technologieoffenheit gesetzt werden. Keine Technologie, die auf europäischer Ebene umgesetzt oder angestrebt wird, sollte von vornherein ausgeschlossen werden. Dies trägt maßgeblich zur Harmonisierung der unterschiedlichen Systeme bei. Nach aktuellem Stand betrifft das insbesondere die ablehnende Haltung gegenüber der Blockchain-Technologie.[196] Diese ist zwar, wie das BSI richtigerweise feststellte, keineswegs zwingend,[197] kann aber eine von mehreren Lösungen sein, wie bspw. als Hybridmodell, und Vorteile gegenüber anderen Technologien bieten.[198] Dabei sind insbesondere die Unveränderbarkeit und eine „echte Dezentralität mit gleichberechtigten Knotenpunkten mittels Konsensus-Protokoll“ zu nennen.[199] Die Arbeiten auf Basis von DLT/Blockchain in mehreren anderen europäischen Ländern, den Large Scale Pilots (DC4EU, EWC) sowie am EBSI und dem European Self-Sovereign Identity Framework (ESSIF), sollten Anlass geben, im Sinne der europäischen Harmonisierung, DLT/Blockchain nicht auszuschließen und als Vertrauensdienst einzustufen. Selbst wenn ein deutsches Wallet nicht auf DLT bzw. Blockchain basieren sollte, ist es dennoch erforderlich, dass sämtliche deutsche Behörden sowie kritische Infrastrukturen Lösungen aus dem Ausland anerkennen. Hierfür sind natürlich detaillierte Prüfungen und Zertifizierungen notwendig, die eine Praxistauglichkeit gewährleisten.[200]
- Um Interoperabilität für SSI zu ermöglichen, müssen sich die unterschiedlichen Stakeholder auf ein gemeinsames Verständnis einigen. Grundlage dafür könnte z. B. ein Rahmenwerk des European-Telecommunications-Standards-Institute (ETSI)[201] sein, dass Interoperabilität in vier aufeinander aufbauende Stufen bzw. Schichten unterscheidet (s. Abbildung 16).[202]

**196** Vgl. BMI (2023c).
**197** Vgl. BSI (2021).
**198** Vgl. ENISA (2022).
**199** Vgl. IDunion (2022b).
**200** Vgl. Kudra, A. (2022).
**201** Vgl. van der Veer, H. und Wiles, A. (2008).
**202** Vgl. Yildiz, H. et al. (2023).

Abbildung 16: Interoperabilität in vier Stufen




Quelle: van der Veer, H. und Wiles, A. (2008).

### 4.1.3 Ausgestaltung der deutschen Wallet-Lösung

Klärungsbedarf besteht außerdem beim „Ökosystem Wallet“. Für dieses sind weiterhin drei Szenarien denkbar: ein staatliches Wallet, mehrere privatwirtschaftliche Wallets oder eine Kombination beider Varianten. Prinzipiell steht es den EU-Staaten frei eine der drei Varianten zu wählen. Im Falle einer Koexistenz verschiedener Wallet-Anbieter müssten die einzelnen (geplanten oder bestehenden) Wallets mit den EU-Vorgaben harmonisiert und zertifiziert werden. Die Zertifizierung könnte sowohl von staatlicher Stelle erfolgen als auch von ihr beauftragt werden.[203] Bei der Auswahl zwischen den drei Varianten ist eine Abwägung zwischen möglichen Vor- und Nachteilen zu treffen, die u. a. in den Positionspapieren des BMI-Konsultationsprozesses dargestellt wurden.[204]

Bei der Entwicklung einer Wallet-Lösungen ist es von entscheidender Bedeutung, Informationssicherheit und Datensparsamkeit als oberste Prinzipien zu berücksichtigen und sie so zu gestalten, dass eine hohe Akzeptanz unter Usern gegeben ist, auch bei jenen, die kein technisches Wissen über die Systemarchitektur mitbringen. Bei der Konzeption sollten daher die Prinzipien Privacy und Security-by-Design sowie Privacy und Security-by-Default grundlegend gelten. Dadurch würden Sicherheits- und Datenschutzaspekte im gesamten Entwicklungsprozess mitgedacht und integriert werden. Zudem würden User automatisch, ohne manuelle Einstellungen vornehmen zu müssen, von vorgegebenen Sicherheits- und Datenschutzeinstellungen bei der Nutzung profitieren. Bei der Entwicklung sollte zudem darauf geachtet werden, dass eine Multifunktionalität der Wallet Lock-in-Effekte verhindert und User eine maximale Flexibilität zwischen verschiedenen

**203** Vgl. BMI (2023c).
**204** Vgl. BMI (2023e).

Lösungen bietet. Die Integration verschiedener Anwendungsbereiche ermöglicht es den Usern, die Wallets für eine Vielzahl an Anwendungen zu nutzen, wodurch ihre Abhängigkeit von einer speziellen Lösung minimiert wird. Dabei sollten Wallets, um die Akzeptanz zu erhöhen, möglichst viele Anwendungsfelder abdecken und sich nicht nur auf hoheitliche Anwendungsfelder beschränken. Daraus folgen diese Maßnahmen:

- Um den vielfältigen, individuellen Bedürfnissen potenzieller User gerecht zu werden, sollte eine Kombination aus staatlicher Infrastruktur und privatwirtschaftlich angebotenen Wallets möglich sein. Während der Kern der Infrastruktur sowie eine nutzbare Referenzimplementierung von staatlicher Seite bereitgestellt wird, kann daneben die Entwicklung von kompatiblen Brieftaschen von allen Marktteilnehmern erfolgen. Dabei sollten aus den gleichen Gründen auch Anwendungsfälle unterschiedlicher Vertrauensniveaus ermöglicht werden. Dabei würde durch Zertifizierungen die Sicherheit sichergestellt werden und zeitgleich Raum für Innovation geboten werden.
- Im Ausgestaltungsprozess sollten weiterhin relevante Interessensgruppen einbezogen werden. Um herauszufinden, welche Eigenschaften besonders zur Akzeptanz beitragen, sollten im Vorfeld zusätzlich empirische Studien unter den relevanten Zielgruppen durchgeführt werden. Dies würde die tatsächlichen Bedürfnissen und Erwartungen der User einbeziehen. Zudem würden mögliche Bedenken und Kritikpunkte, die zurzeit insbesondere Qualified Website Authentication Certificates (QWAC), potenzielle Möglichkeiten zur Überwachung durch staatliche Behörden und potenzielle Möglichkeiten zur Umgehung des Zero-Knowledge-Proofs und damit der Pseudonymität betreffen, berücksichtigt werden.[205] Inwiefern diese Kritikpunkte noch aus dem Weg geräumt werden können, ist offen. Möglichkeiten bestehen für die Politik noch durch Spezifikationen im Architektur- und Referenzrahmen (ARF) sowie in der nationalen Ausgestaltung.

### 4.1.4 Nutzungsakzeptanz bei Bürger:innen und Unternehmen schaffen

Die Förderung der Akzeptanz dezentraler, selbstverwalteter Digitaler Identitäten unter den Usern ist von essenzieller Bedeutung für ihre weitreichende Verbreitung. Hierbei steht im Fokus, die Mehrwerte solcher Identitäten, wie beispielsweise verbesserte Informationssicherheit, Selbstbestimmung, Datensouveränität, Interoperabilität und Effizienzgewinne, für potenzielle User transparent und verständlich zu kommunizieren. Diese Kommunikation sollte insbesondere diejenigen erreichen, die bisher kritisch gegenüber Digitalen Identitäten eingestellt sind oder die Vorteile noch nicht kennen oder verstanden haben. Im Zusammenhang damit ist die Schaffung konkreter Anwendungsfälle und die Förderung ihrer Entstehung von entscheidender Relevanz. Gleichzeitig bedarf es Maßnahmen zum Schutz der User vor potenziellen Missbräuchen oder Fehlverhalten, die

**205** Vgl. Leisegang, D. (2023); Koch, M.-C. (2023).

trotz der Vorteile dezentraler, selbstverwalteter Digitaler Identitäten auftreten können. Um dies zu erreichen, sollten folgende Punkte umgesetzt werden:

- In Anbetracht der noch begrenzten Bekanntheit dezentraler, selbstverwalteter Digitaler Identitäten und ihrer Mehrwerte wird die Empfehlung ausgesprochen, gezielte Werbe- und Informationskampagnen zu starten, um diese Aspekte herauszustellen. Hierbei sollten nicht nur die Vorteile, sondern auch konkrete Anwendungsbeispiele aus verschiedenen Lebensbereichen adressiert werden. Gleichzeitig ist es ratsam, Informationsangebote für Bürger:innen sowie KMU zu etablieren, um einen sicheren Umgang mit (dezentralen, selbstverwalteten) Digitalen Identitäten zu fördern. Zur Intensivierung der Wahrnehmung und Verbreitung von Anwendungsfällen im Bereich des E-Government sollten kontinuierlich und nachhaltig solche Anwendungsfälle entwickelt werden. Anwenderfreundliche Szenarien können nicht nur das Vertrauen der Bürger:innen stärken, sondern auch die Akzeptanz in der breiten Bevölkerung fördern.
- Um die Verbreitung auf unternehmerischer Ebene weiter zu fördern, sollten Organisationsidentitäten im Rahmen der deutschen Wallet-Lösung zeitnah aktiv unterstützt werden. Dies ermöglicht es Unternehmen, von den in Abschnitt 3.2 identifizierten Chancen zu profitieren und gleichzeitig ihren Mitarbeitenden die praktischen Vorteile näherzubringen.

## 4.2 Schlussbemerkung

Die Erfahrungen aus den Phasen des Web 1.0 und Web 2.0 haben eindeutig aufgezeigt, dass ein grundlegender Paradigmenwechsel in der Verwaltung Digitaler Identitäten essenziell ist. Sowohl im Kontext isolierter als auch föderierter Digitaler Identitäten verlieren die User die Kontrolle über die Verwaltung ihrer Daten und damit ihre Datenhoheit. Die Implementierung einer dezentralen, selbstverwalteten und interoperablen Digitalen Identität wird als entscheidendes Grundgerüst für die Funktionalität des Web 3.0 betrachtet. Insbesondere SSI werden als Schlüsselkomponente angesehen, um Datensouveränität und Datenschutz künftig effektiver zu gewährleisten. Die Sicherstellung eines vertrauenswürdigen Miteinanders zwischen Wirtschaft, Verwaltung und Endnutzer:innen legt dabei den Grundstein für einen langfristig nachhaltigen gesellschaftlichen und ökonomischen Mehrwert.

Mit der Aktualisierung der eIDAS-Verordnung soll die Schaffung einer dezentralen, selbstverwalteten Digitalen Identität für alle EU-Bürger:innen dazu beitragen, zuvor genannte Potenziale zu heben. In der Praxis wird deutlich, dass gegenwärtige Entwicklungen im Kontext der eIDAS-2.0-Verordnung möglicherweise nicht in vollem Umfang mit dem oben genannten Leitgedanken konform gehen. Insbesondere die divergierenden Ansätze der EU-Mitgliedsstaaten in Bezug auf technologische und Governance-Fragen können die Interoperabilität erschweren. Darüber hinaus verdeutlicht Kritik von Bürgerrechtsaktivist:innen, dass es weiterhin Bedarf an Kommunikation und Einigung gibt,

insbesondere hinsichtlich der Ausgestaltung von Anforderungen an Datensouveränität und der Sicherstellung des Datenschutzes.

Es bleibt abzuwarten, inwiefern eIDAS 2.0 letztendlich den Prinzipien der SSI gerecht wird. Aktuelle Entwicklungen deuten darauf hin, dass sich zwar Digitale Identitäten abzeichnen, die wichtige Elemente der Dezentralität und Selbstverwaltung aufgreifen, jedoch nicht zwangsläufig in vollständiger Übereinstimmung mit den zehn Prinzipien von Christopher Allen stehen werden. In diesem Zusammenhang sollte jedoch beachtet werden, dass Christopher Allen nach eigener Aussage nur einen Dialog zu einer neuen Form der Digitalen Identität beginnen wollte, indem er eine Definition und eine Reihe von Prinzipien als Ausgangspunkt vorschlägt.[206] Die Prinzipien sollten darum vielmehr als Leitbild fungieren, deren Wortlaut im Einzelfall nicht dogmatisch gefolgt werden kann. Wichtiger ist, dass das eigentliche Kernanliegen nicht außer Acht gelassen wird: Nämlich dass den Usern eine eigenständige und selbstbestimmte Kontrolle über ihre Digitalen Identitäten gegeben werden sollte, die negative Begleiterscheinungen gegenwärtiger Digitaler Identitäten für sie und die Gesellschaft entgegenwirkt.

Um User wieder in den Mittelpunkt zu rücken, die Datensouveränität und Datensicherheit zu stärken sowie wirtschaftliche Potenziale zu erschließen, steht ein beträchtlicher Kraftakt bevor. Der entscheidende Paradigmenwechsel wird letzten Endes von der Akzeptanz und Nutzung dieser innovativen Identitätsmanagement-Lösungen abhängen. Dies erfordert verstärkte staatliche Bemühungen, um die Interoperabilität zu fördern und die Praxistauglichkeit der Anwendungen zu gewährleisten, damit die Potenziale von SSI vollumfänglich ausgeschöpft werden können.

**206** Vgl. Allen, C. (2016).

## Literaturverzeichnis

Abraham, A., More, S., Rabensteiner, C., Hörandner, F. (2020): Revocable and offline-verifiable self-sovereign identities. In G. Wang, R. Ko, M. Z. A. Bhuiyan, & Y. Pan (Eds.), Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020 (pp. 1020-1027). [9343191] (Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020). https://doi.org/10.1109/TrustCom50675.2020.00136.

Akerlof, G. A. (1970): The Market for „Lemons“: Quality Uncertainty and the Market Mechanism, in: The Quarterly Journal of Economics, 84. Jg. (1970), Nr. 3, S. 488-500

Anke, J., Richter, D. (2023): Digitale Identitäten - Status Quo und Perspektiven, in: HMD Praxis der Wirtschaftsinformatik 60.2 (2023): 261-282. DOI: 10.1365/s40702-023-00965-1.

Allen, C. (2016): The Path to Self-Sovereign Identity. Online abrufbar unter: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (zuletzt abgerufen am 01.11.2023).

Babel, M., Gramlich, V., Guthmann, C., Schober, M., Körner, M.-F., Strüker, J. (2023): "Vertrauen durch digitale Identifizierung: Über den Beitrag von SSI zur Integration von dezentralen Oracles in Informationssysteme.", in: *HMD Praxis der Wirtschaftsinformatik* 60.2 (2023): 478-493. DOI: 10.1365/s40702-023-00955-3.

BaFin (2017): Rundschreiben 3/2017 (GW) – Videoidentifizierungsverfahren. Online abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1703_gw_videoident.html (zuletzt abgerufen am 10.11.2023).

Y. Bai, H. Lei, S. Li, H. Gao, J. Li and L. Li, "Decentralized and Self-Sovereign Identity in the Era of Blockchain: A Survey," 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 2022, pp. 500-507, doi: 10.1109/Blockchain55522.2022.00077.

Begleitforschung Schaufenster Sichere Digitale Identitäten (2021): Umfrage zu digitalen Identitäten: viele Identitäten, wenig professionelle Hilfsmittel, Vorrang für dezentrale Lösungen, 18. Oktober 2021. Online abrufbar unter: https://digitale-identitaeten.de/meinungsumfrage_zu_sicheren_digitalen_identitaeten (zuletzt abgerufen am 13.11.2023).

Begleitforschung Sichere Digitale Identitäten (2022): Ansätze zum Management von (digitalen) Identitäten – Das kleine 1x1 der sicheren digitalen Identitäten, 9. Dezember 2022. Online abrufbar unter: https://digitale-identitaeten.de/ansaetze-zum-management-von-digitalen-identitaeten-das-kleine-1x1-der-sicheren-digitalen-identitaeten/ (zuletzt abgerufen am 10.11.2023).

Begleitung Sichere Digitale Identitäten (2023): Schaufensterprojekte. Aktuelle Technologieprogramme. Online abrufbar unter: https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/projekte_umsetzungsphase.html (zuletzt abgerufen am 12.12.2023).

Biedermann, B, Handke, S., Jürgenssen, O., Orta, E., Schindler, C., Schröder, R., Schroll, L., Sonne, F. (2023): Nutzen und Grenzen von SSI für Verwaltung und öffentliche Institutionen. Betrachtung am Beispiel des Projektes ID-Ideal, einem im Rahmen des Innovationswettbewerbs „Schaufenster Sichere Digitale Identitäten“ des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) geförderten Projektes, *HMD Praxis der Wirtschaftsinformatik* (2023) 60.2: 437-457, https://doi.org/10.1365/s40702-023-00953-5.

Bitkom (2020): Self Sovereign Identity Use Cases – von der Vision in die Praxis. Online abrufbar unter: https://www.bitkom.org/sites/default/files/2020-07/200703_lf_self-sovereign-identity-use-cases.pdf (zuletzt abgerufen am 01.12.2023).

Bitkom (2021): Vertrauen und Sicherheit in der digitalen Welt, Berlin, Juli 2021. Online abrufbar unter: https://www.bitkom.org/sites/main/files/2021-07/bitkom_vertrauenitsicherheit2021.pdf (zuletzt abgerufen am 01.12.2023).

Bitkom (2023a): Wirtschaftsschutz 2023, Berlin, 1. September 2023. Online abrufbar unter: https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf (zuletzt abgerufen am 01.12.2023).

Bitkom (2023b): Vertrauen stärken, Praktischer Leitfaden zu digitalen Identitäten, SSI & DLT. Online abrufbar unter: https://www.bitkom.org/sites/main/files/2023-09/bikom-leitfaden-digitale-identitaeten.pdf (zuletzt abgerufen am 01.12.2023).

Bitkom (2023c): Digitale Identitäten juristischer Personen, Organisationsidentitäten als Katalysator für nachhaltige Finanzen. Online abrufbar unter: https://www.bitkom.org/sites/main/files/2023-10/digitaliserung-von-identitaeten-teil-3-juristische-personen.pdf (zuletzt abgerufen am 24.11.2023).

Bitpanda (2023). Was ist asymmetrische Verschlüsselung? Online abrufbar unter: https://www.bitpanda.com/academy/de/lektionen/was-ist-asymmetrische-verschlusselung/ (zuletzt abgerufen am 12.12.2023).

BMI (2022): EU-Kommission bewilligt den Large-Scale-Pilot für die EUDI-Wallet, MELDUNG 14.12.2022. Online abrufbar unter: https://www.personalausweisportal.de/SharedDocs/kurzmeldungen/Webs/PA/DE/2022/12_large_scale_pilot.html (zuletzt abgerufen am 16.11.2023).

BMI (2023a): Architecture Proposal for the German eIDAS Implementation Version 1. Online abrufbar unter: https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept-v1/-/blob/main/architecture-proposal.md (zuletzt abgerufen am 01.12.2023).

BMI (2023b): Der Online-Ausweis, Ihren Ausweis für die digitale Welt können Sie mit immer mehr Smartphones nutzen. Online abrufbar unter: https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/online-ausweisen/online-ausweisen-node.html;jsessionid=9762A8836A20C7714F71E59E080A1B6E.2_cid504 (zuletzt abgerufen am 06.11.2023).

BMI (2023c): Beyond EU Digital Identity Wallet – Diskussionspapier zur Erarbeitung einer prototypischen eIDAS 2.0-konformen Infrastruktur für Digitale Identitäten in Deutschland, Information zu Zielen, Rahmenbedingungen, ersten Überlegungen sowie zum Start des öffentlichen Konsultationsprozesses zu einem Konzept der deutschen Ausgestaltung von EUdi-Brieftaschen, 07. Juni 2023. Online abrufbar unter: https://gitlab.opencode.de/bmi/eidas2/-/blob/main/Beyond_EUDIW_Diskussionspapier.pdf?ref_type=heads (zuletzt abgerufen am 21.11.2023).

BMI (2023d): eIDAS 2.0 Architekturprozess. Online abrufbar unter: https://bmi.usercontent.opencode.de/eidas2/start/ (zuletzt abgerufen am 01.12.2023).

BMI (2023e): eIDAS2 / Positionspapiere. Online abrufbar unter: https://gitlab.opencode.de/bmi/eidas2/-/tree/main/Positionspapiere?ref_type=heads (zuletzt abgerufen am 29.11.2023).

BMWK (2023a): Schaufenster Sichere Digitale Identitäten. Online abrufbar unter: https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html (zuletzt abgerufen am 09.11.2023).

BMWK (2023b): Schaufenster Sichere Digitale Identitäten. Online abrufbar unter: https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html (zuletzt abgerufen am 13.11.2023).

Bosch (2023): Organisationswallet. Online abrufbar unter: https://orgwallet.de/ (zuletzt abgerufen am 12.12.2023).

BSI (2021): Eckpunktepapier für Self-sovereign Identities (SSI) unter besonderer Berücksichtigung der Distributed-Ledger-Technologie (DLT). Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 10.11.2023).

BSI – Bundesamt für Sicherheit in der Informationstechnik (2022): DIGITALBAROMETER, Bürgerbefragung zur Cyber-Sicherheit 2022, Kurzbericht zur Studie der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2022.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 17.11.2023).

BSI (2023): Die Lage der IT-Sicherheit in Deutschland 2023. Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=7 (zuletzt abgerufen am 24.11.2023).

Bucci, D. (2022): The Global Open Health Movement: Empowering People and Saving Lives by Unlocking Data, Status: Working Draft, Date: June 21, 2022. Online abrufbar unter: https://openid.net/wordpress-content/uploads/2022/06/OIDF-and-the-Health-Whitepaper-June-21.pdf (zuletzt abgerufen am 09.11.2023).

Bundesnetzagentur (2022a): Fragen zu elektronischen Vertrauensdiensten. Online abrufbar unter: https://www.bundesnetzagentur.de/EVD/DE/Nutzer/Infothek/Fragen/start.html (zuletzt abgerufen am 20.11.2023).

Bundesnetzagentur (2022b): Übersicht aller elektronischen Vertrauensdienste, Online abrufbar unter: https://www.bundesnetzagentur.de/EVD/DE/Uebersicht_eVD/start.html (zuletzt abgerufen am 20.11.2023).

Buldas, A., Kroonmaa, A., Laanoja, R. (2013): Keyless signatures' infrastructure: How to build global distributed hash-trees. *Nordic Conference on Secure IT Systems*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. DOI: 10.1007/978-3-642-41488-6_21.

Buldas, A., Laanoja, R., Truu, A. (2017): Keyless signature infrastructure and PKI: hash-tree signatures in pre-and post-quantum world. International Journal of Services Technology and Management 23.1-2 (2017): 117-130. DOI: 10.1504/IJSTM.2017.081881.

Bundeskanzleramt (2021): Digitale Identität, Wie ein Ökosystem digitaler Identitäten zu einem selbstbestimmten und zugleich nutzerfreundlichen Umgang mit dem digitalen Ich beitragen kann. Online abrufbar unter: https://www.bundesregierung.de/resource/blob/992814/1898280/d9819a40553a9543b9e8f3acb620b0c2/digitale-identitaet-neu-download-bundeskanzleramt-data.pdf (zuletzt abgerufen am 09.11.2023).

Bundesdruckerei (2020): Digitale Identitäten: So entwickeln sie sich weiter, Veröffentlicht am 02.06.2020. Online abrufbar unter: https://www.bundesdruckerei.de/de/innovation-hub/digitale-identitaeten-so-entwickeln-sie-sich-weiter (zuletzt abgerufen am 21.11.2023).

Cameron, K. (2005): The Laws of Identity. Online abrufbar unter: https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (zuletzt abgerufen am 31.08.2023).

J. L. Camp, "Digital identity," in IEEE Technology and Society Magazine, vol. 23, no. 3, pp. 34-41, Fall 2004, DOI: 10.1109/MTAS.2004.1337889.

CCC – Chaos Computer Club (2022): Chaos Computer Club hackt Video-Ident, 2022-08-10 09:59:21, erdgeist. Online abrufbar unter: https://www.ccc.de/de/updates/2022/chaos-computer-club-hackt-video-ident (zuletzt abgerufen am 06.11.2023).

Decentralized Identity Foundation (2023): Peer DID Method Specification, Specification Status: v1.0 Draft. Online abrufbar unter: https://identity.foundation/peer-did-method-spec/ (zuletzt abgerufen am 10.11.2023).

Deutscher Bundestag (2022): Aufbau einer European Blockchain Services Infrastructure – EBSI, Initiativen und Rahmenbedingungen. Online abrufbar unter: https://www.bundestag.de/resource/blob/890570/2ba0a50d8a8450aa6f80e534f905cca3/PE-6-012-22-pdf-data.pdf (zuletzt abgerufen am 10.11.2023).

Deutscher Bundestag (2023a): Drucksache 20/8040, Kleine Anfrage der Fraktion der CDU/CSU, Stand der Umsetzung der eIDAS-2.0-Verordnung. Online abrufbar unter: https://dserver.bundestag.de/btd/20/080/2008040.pdf zuletzt abgerufen am 13.11.2023).

Deutscher Bundestag (2023b): Drucksache 20/8201, Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der CDU/CSU, Drucksache 20/8040, Stand der Umsetzung der eIDAS-2.0-Verordnung. Online abrufbar unter: https://dserver.bundestag.de/btd/20/082/2008201.pdf (zuletzt abgerufen am 13.11.2023).

Deutscher Bundestag (2023c). Drucksache 20/8183, Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion CDU/CSU, Vergabe von eindeutigen Personenkennziffern hinsichtlich der Entwicklung einer EUdi-Wallet. Online abrufbar unter: https://dip.bundestag.de/vorgang/vergabe-von-eindeutigen-personenkennziffern-hinsichtlich-der-entwicklung-einer-eudi-wallet/303333?f.deskriptor=E-Government&rows=25&pos=17 (zuletzt abgerufen am 12.12.2023).

Diehl, Andreas (2023): Blockchain einfach erklärt – Wie funktioniert die Blockchain?, 11. April 2023. Online abrufbar unter: https://digitaleneuordnung.de/blog/blockchain-erklaerung/ (zuletzt abgerufen am 16.11.2023).

Douglas, D. M. (2016): Doxing: a conceptual analysis. Ethics and information technology 18, 199 - 210 (2016). DOI: https://doi.org/10.1007/s10676-016-9406-0.

Dreißigacker, A. et al (2020): Cyberangriffe gegen Unternehmen in Deutschland, Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019. Online abrufbar unter: https://kfn.de/wp-content/uploads/Forschungsberichte/FB_152.pdf (zuletzt abgerufen am 01.12.2023).

EBSI (2023): Revocation by EBSI, EBSI's Credential Status Framework and how to choose a revocation method when using W3C Verifiable Credentials (and more). Online abrufbar unter: https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/What+to+do+when+good+Verifiable+Credentials+go+bad. (zuletzt abgerufen am 12.12.2023).

eco (2022): Security & digitale Identitäten in einer digitalisierten Welt. Online abrufbar unter: https://norbert-pohlmann.com/wp-content/uploads/2022/11/eco-studie_security-und-digitale-identitaeten-in-einer-digitalisierten-welt-prof-norbert-pohlmann.pdf (zuletzt abgerufen am 17.11.2023).

ENISA (2022): DIGITAL IDENTITY, Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust, JANUARY 2022. Online abrufbar unter: https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust (zuletzt abgerufen am 23.11.2023).

Ehrlich, T., Richter, D., Meisel, M., Anke, J. (2021): Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. *HMD Prax. Wirtsch.* 58.2: 247-270. DOI: 10.1365/s40702-021-00711-5.

KOM (2021): Digitale Identität für alle Europäer/innen, Eine persönliche digitale Brieftasche für alle Menschen in der EU. Online abrufbar unter: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_de (zuletzt abgerufen am 13.11.2023).

KOM (2023a): European Digital Identity – Questions and Answers, Brussels, 8 November 2023. Online abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_2664 (zuletzt abgerufen am 01.12.2023).

KOM (2023b): Digitale Identität der EU: 4 Projekte zur Erprobung der EUDI-Brieftasche, DIGIBYTE | Veröffentlichung 23 Mai 2023. Online abrufbar unter: https://digital-strategy.ec.europa.eu/de/news/eu-digital-identity-4-projects-launched-test-eudi-wallet (zuletzt abgerufen am 13.11.2023).

European Parliamentary Research Service (2019): Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law? Scientific Foresight Unit (STOA), PE 634.445 – July 2019. Online abrufbar unter: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (zuletzt abgerufen am 20.11.2023).

Europäische Union (2014): VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, Amtsblatt der Europäischen Union. Online abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910 (zuletzt abgerufen am 10.11.2023).

European Union (2022): VERORDNUNG (EU) 2022/1925 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), Amtsblatt der Europäischen Union. Online abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R1925 (zuletzt abgerufen am 01.12.2023).

Europäische Union (2023): The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework – The European Digital Identity Wallet Architecture and Reference Framework, April 2023, Version 1.1.0. Online abrufbar unter: https://www.identrust.eu/wp-content/uploads/2023/03/ARF_v100_for_publication.pdf (zuletzt abgerufen am 20.11.2023).

EWC (2023): EU Digital Identity Wallet Consortium, Online abrufbar unter: https://eudiwalletconsortium.org/ (zuletzt abgerufen am 04.12.2023).

Gabler Wirtschaftslexikon (2021): Definition Vertrauen, Revision von Vertrauen vom 25.08.2021 - 11:36. Online abrufbar unter: https://wirtschaftslexikon.gabler.de/definition/vertrauen-50461/version-384763 (zuletzt abgerufen am 17.11.2023).

Gallersdörfer, U., Matthes, F.: TeSC: TLS/SSL-certificate endorsed smart contracts. In: 2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), pp. 95–100 (2021). DOI: https://doi.org/10.1109/DAPPS52256.2021.00016.

Grassi, P., Garcia, M. E., Fenton, J. L. (2017): Digital Identity Guidelines, NIST Special Publication 800-63-3. https://doi.org/10.6028/NIST.SP.800-63-3.

Guardtime (2023): Keyless Signature Infrastructure™, Massive-Scale System Integrity, Online abrufbar unter: https://m.guardtime.com/files/KSI_data_sheet_201509.pdf (zuletzt abgerufen am 08.11.2023).

Heinig, M. (2023): Zusammenarbeit von Unternehmen in einer volatilen Welt. Online abrufbar unter: https://news.sap.com/germany/2023/04/unternehmen-in-einer-volatilen-welt-digitale-identitaeten/ (zuletzt abgerufen am 08.11.2023).

IDunion (2022a): Whitepaper – Einsatz der SSI-Technologie bei der Implementierung der OZG-Nutzerkonten. Online abrufbar unter: https://govpart.de/wp-content/uploads/2023/03/V1.3_WP_SSI_und_OZG_Nutzerkonten.pdf (zuletzt abgerufen am 01.12.2023).

IDunion (2022b): Stellungnahme zum SSI Eckpunktepapier des BSI. Online abrufbar unter: https://idunion.org/2022/03/15/idunion-stellungnahme-zum-ssi-eckpunktepapier-des-bsi/ (zuletzt abgerufen am 10.11.2023).

IDunion (2023a): Organisations ID – Die Firmenidentität der Zukunft. Online abrufbar unter: https://idunion.org/piloten/orgid/ (zuletzt abgerufen am 30.11.2023).

IDunion (2023b): Eine offenes Ökosystem für vertrauensvolle Identitäten. Was wir machen. Online abrufbar unter: https://idunion.org/ (zuletzt abgerufen am 12.12.2023).

IPFS (2023): A Universe of Uses. Online abrufbar unter: https://ipfs.tech/ (zuletzt abgerufen am 12.12.2023).

ISO/IEC (2019): ISO/IEC 24760-1:2019 – IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts. Online abrufbar unter: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-2:v1:en (zuletzt abgerufen am 09.09.2023).

Jøsang, A., Pope, S. (2005): User Centric Identity Management: Centralised User Identity Models und Federated User Identity Model. Online abrufbar unter: https://folk.universitetetioslo.no/josang/papers/JP2005-AusCERT.pdf (zuletzt abgerufen am 2.10.2023).

KPMG (2021): Online-Shopping, Einkaufsverhalten – wer kauft was, wann, wie, Analyse zu Trends und Potenzialen im E-Commerce in der DACH-Region, April 2021. Online abrufbar unter: https://assets.kpmg.com/content/dam/kpmg/ch/pdf/studie-online-shopping-kpmg-2021.pdf (zuletzt abgerufen am 20.11.2023).

Kubach, M., Schunck, C. H., Sellung, R., Roßnagel, H. (2020): Self-sovereign and Decentralized identity as the future of identity management?, Open Identity Summit (2020), Lecture

Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020. Online abrufbar unter: https://dl.gi.de/server/api/core/bitstreams/aaa640a1-f8dd-4514-ad72-b809932072cc/content (zuletzt abgerufen am 20.11.2023).

Kubach, M., Roßnagel, H. (2021): A lightweight trust management infrastructure for selfsovereign identity, Open Identity Summit (2021), Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021. Online abrufbar unter: https://dl.gi.de/server/api/core/bitstreams/746a78bd-b94d-45d0-8a27-510eb32ee4cc/content (zuletzt abgerufen am 20.11.2023).

Kudra, A. (2022): Self-Sovereign Identity (SSI) in Deutschland, Datenschutz Datensich 46, 22–26 (2022). DOI: https://doi.org/10.1007/s11623-022-1555-1.

Koch, M.-C. (2023): Hunderte Experten warnen vor staatlichen Root-Zertifikaten, Abrufbar unter: https://www.heise.de/news/Hunderte-Wissenschaftler-warnen-vor-staatlichen-Root-Zertifikaten-9355165.html (zuletzt abgerufen am 22.11.2023).

L'Amrani, H., Berroukech, B. E., El Bouzekri El Idrissi, Y., Ajhoun, R. (2016): Identity management systems: Laws of identity for models 7 evaluation 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, Morocco, 2016, pp. 736-740, DOI: 10.1109/CIST.2016.7804984.

Leisegang, D. (2023): eIDAS-Reform: Digitale Brieftasche mit Ausspähgarantie. Online abrufbar unter: https://netzpolitik.org/2023/eidas-reform-digitale-brieftasche-mit-ausspaehgarantie/?via=nl#netzpolitik-pw (zuletzt abgerufen am 15.11.2023).

Lux, Z. A., Thatmann, D., Zickau, S., Beierle, F. (2020): Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials. 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 2020, pp. 71-78, DOI: 10.1109/BRAINS49436.2020.9223292.

Maier, B., Pohlmann, N. (2022): Gaia-X-sichere und vertrauenswürdige Ökosysteme mit souveränen Identitäten, Entwicklung eines dezentralen, benutzerzentrierten und sicheren Cloud-Ökosystems. Online abrufbar unter: https://www.gxfs.eu/de/ssi-white-paper/ (zuletzt abgerufen am 15.11.2023).

Martinovic, I., Kello, L., Sluganovic, I. (2017): Blockchains for governmental services: Design principles, applications, and case studies. Center for Technology and Global Affairs, University of Oxford (2017). Online abrufbar unter: https://www.politics.ox.ac.uk/sites/default/files/2022-03/201712-CTGA-Martinovic%20I-Kello%20L-blockchainsforgovernmentalservices.pdf (zuletzt abgerufen am 01.12.2023).

McKinsey Global Institute (2019): Digital Identification, A key to inclusive growth, April 2019. Online abrufbar unter: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20identification%20a%20key%20to%20inclusive%20growth/mgi-digital-identification-report.pdf (zuletzt abgerufen am 23.11.2023).

MOBI (2019): Vehicle Identity Standard, Mobility Open Blockchain Initiative, VID Working Group, Version 1.0 Online abrufbar unter: https://dlt.mobi/wp-content/uploads/2019/09/MOBI-Vehicle-Identity-Standard-v1.0-Preview.pdf (zuletzt abgerufen am 08.11.2023).

Nath, K., Dhar, S., Basishtha, S. (2014): "Web 1.0 to Web 3.0 - Evolution of the Web and its various challenges"; 2014 International Conference on Reliability Optimization and Information Technology (ICROIT), Faridabad, India, 2014, pp. 86-89, DOI: 10.1109/ICROIT.2014.6798297.

Ogunsola, F., Pannifer, S. (2017): AMLD4/AMLD5 KYCC, Know Your Compliance Costs, June 2017. Online abrufbar unter: https://www.fstech.co.uk/fst/mitek/Hyperion-Whitepaper-Final-for-Release-June2017.pdf (zuletzt abgerufen am 08.11.2023).

Pflanzner, T., Baniata, H., Kertesz, A. (2022): Latency Analysis of Blockchain-Based SSI Applications. Future Internet 14.10, 282. DOI: https://doi.org/10.3390/fi14100282.

Pohlmann, N. (2023): Glossar Cybersicherheit, Digitale Identität, Was ist eine digitale Identität?. Online abrufbar unter: https://norbert-pohlmann.com/glossar-cyber-sicherheit/digitale-identitaet/ (zuletzt abgerufen am 08.09.2023).

Puhl, P., Stuck, J., Hillebrand, A. (2021): Vertrauen in Datenverarbeitung – Kurzstudie, Bad Honnef, Dezember 2021. Online abrufbar unter: https://www.wik.org/fileadmin/files/_migrated/news_files/WIK-Studie_Vertrauen_in_Datenverarbeitung_2021.pdf (zuletzt abgerufen am 27.11.2023).

PwC (2016): Identitätsklau – die Gefahr aus dem Netz, 2016. Online abrufbar unter: https://www.pwc.de/de/handel-und-konsumguter/cyber-security-identitaetsdiebstahl-2016.pdf (zuletzt abgerufen am 17.11.2023).

PwC (2018): Vertrauen in Medien, 2018. Online abrufbar unter: https://www.pwc.de/de/technologie-medien-und-telekommunikation/pwc-studie-vertrauen-in-medien-2018.pdf (zuletzt abgerufen am 17.11.2023).

PwC (2021): Der Online-Ausweis auf dem Smartphone und die digitale Brieftasche, Oktober 2021. Online abrufbar unter: https://www.pwc.de/de/branchen-und-markte/oeffentlicher-sektor/pwc-studie-der-online-ausweis-auf-dem-smartphone-und-die-digitale-brieftasche.pdf (zuletzt abgerufen am 01.12.2023).

PwC (2022): KYC bietet hohes Einsparpotenzial für Banken. Online abrufbar unter: https://www.strategyand.pwc.com/ch/de/presse/2022/kyc.html (zuletzt abgerufen am 08.11.2023).

PwC und DLA Piper (2021): Study to support the impact assessment for the revision of the eIDAS regulation, Final Report. Online abrufbar unter: https://op.europa.eu/de/publication-detail/-/publication/9ce0f9e5-03bb-11ec-8f47-01aa75ed71a1 (zuletzt abgerufen am 27.11.2023).

Reuters (2016): Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity. Online abrufbar unter: https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html (zuletzt abgerufen am 08.11.2023).

Schellinger, B., Sedlmeir, J., Willburger, L., Strüker, J., Urbach, N. (2022): Mythbusting Self-Sovereign Identity (SSI) – Diskussionspapier zu selbstbestimmten digitalen Identitäten. Online abrufbar unter: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Whitepaper_Mythbusting_Self-Sovereign_Identity.pdf (zuletzt abgerufen am 01.12.2023).

Schunck, C. H., Sellung, R., Rossnagel, H. (2021): KI zur Verhinderung von Identitätsbetrug – Von der Kundenidentifikation zur Prävention von Verbraucherbetrug. Online abrufbar unter: https://publica-rest.fraunhofer.de/server/api/core/bitstreams/1da2b9c5-a80b-40d8-83a4-b83e5c3480c4/content (zuletzt abgerufen am 01.12.2023).

Schwalm, S., Alamillo-Domingo, I. (2021): Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of eIDAS 2.0, in European Review of Digital Administration & Law – Erdal, 2021, Volume 2, Issue 2, pp. 89-108. DOI: 9791259947529 10.

Schwalm, S. (2023a): Das EU-Digital Wallet -der Schlüssel für (rechts)sichere dezentrale Identitäten in Europa? SSI zwischen ARF, eIDAS 2.0 und Large Scale Pilots. DOI: 10.13140/RG.2.2.36300.59523.

Schwalm, S. (2023b): Die Rolle der vier EU Large Scale Pilots, Interview geführt von Benjamin Burde und Kordula Kiefer-Kempf von esatus AG. Online abrufbar unter: https://i-dunion.org/2023/07/17/interview-large-scale-pilots/ (zuletzt abgerufen am 13.11.2023).

Soltani, R., Nguyen, U. T., An, A. (2020): A Survey of Self-Sovereign Identity Ecosystem, Security and Communication Networks, vol. 2021, Article ID 8873429, 26 pages, 2021. https://doi.org/10.1155/2021/8873429.

Spherity (2023): Das Enterprise-Identity-Wallet. Online abrufbar unter: https://www.spherity.com/enterprise-identity-wallet (zuletzt abgerufen am 12.12.2023).

Strüker, J., Urbach, N., Guggenberger, T., Lautenschlager, J., Ruhland, N., Schlatt, V., Sedlmeir, J., Stoetzer, J.-C., Völter, F. (2021): Self-Sovereign Identity – Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Bayreuth. Online abrufbar unter: https://www.fim-rc.de/wp-content/uploads/2021/06/Fraunhofer-FIT_SSI_Whitepaper.pdf (zuletzt abgerufen am 01.12.2023).

SSL.com (2019): Was ist ein X.509-Zertifikat?. Online abrufbar unter: https://www.ssl.com/de/faq/Was-ist-ein-x-509-Zertifikat%3F/#:~:text=Anwendungen%20von%20X.-,509-Zertifikaten%20sind%3A%20SSL%20%2FTLS%20und%20HTTPS%20f%C3%BCr%20authentifiziertes,der%20Regierung%20ausgestellter%20elektronischer%20Ausweis (zuletzt abgerufen am 10.11.2023).

Tagesschau (2023): Digital Markets Act, Volltreffer gegen die Big-Tech-Übermacht? Stand: 05.07.2022 18:32 Uhr, Online abrufbar unter: https://www.tagesschau.de/wirtschaft/verbraucher/digital-markets-act-eu-regulierung-techkonzerne-wettbewerb-gatekeeper-messenger-bussgelder-101.html (zuletzt abgerufen am 09.11.2023).

Telekom (2023): Beyond EU Digital Identity Wallet, Positionspapier der Deutschen Telekom zum BMI-Diskussionspapier zur Erarbeitung einer prototypischen eIDAS 2.0-konformen Infrastruktur für Digitale Identitäten in Deutschland. Online abrufbar unter: https://gitlab.opencode.de/bmi/eidas2/-/blob/main/Positionspapiere/Telekom.pdf (zuletzt abgerufen am 16.11.2023).

Tenner, T. (2021): Digitale Identitäten – Schritte auf dem Weg zu einem ID-Ökosystem, 18.03.2021, Positionspapier. Online abrufbar unter: https://bankenverband.de/digitalisierung/digitale-identitaeten-schritte-auf-dem-weg-zu-einem-id-oekosystem/ (zuletzt abgerufen am 21.11.2023).

Terbu, O., Lodderstedt, T., Yasuda, K., Look, T. (2023): OpenID for Verifiable Presentations – draft 18. Online abrufbar unter: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html (zuletzt abgerufen am 10.11.2023).

van der Veer, H., Wiles, A. (2008): ETSI White Paper No. 3, Achieving Technical Interoperability -the ETSI Approach, 3rd edition - April 2008. Online abrufbar unter: https://www.etsi.org/images/files/ETSIWhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf (zuletzt abgerufen am 14.11.2023).

Verein Industrie 4.0 Österreich (2022): Digitale Identitäten und ihre Bedeutung für den Datenaustausch. Online abrufbar unter: https://plattformindustrie40.at/blog/2022/12/17/digitale-identitaeten-und-ihre-bedeutung-fuer-den-datenaustausch/ (zuletzt abgerufen am 09.11.2023).

VSDI (2020): „SICHERE DIGITALISIERUNG ERFORDERT SICHERE DIGITALE IDENTITÄTEN“ THESENPAPIER DES VERBANDS SICHERE DIGITALE IDENTITÄT e. V. (VSDI). Online abrufbar unter: https://vsdi.de/wp-content/uploads/2020/06/20-05-11_Thesenpapier-des-Verbands-Sichere-Digitale-Identit%C3%A4t.pdf (zuletzt abgerufen am 05.10.2023).

W3C (2022a): Decentralized Identifiers (DIDs) v1.0, Core architecture, data model, and representations, W3C Recommendation 19 July 2022. Online abrufbar unter: https://www.w3.org/TR/did-core/ (zuletzt abgerufen am 10.11.2023).

W3C (2022b): The did:key Method v0.7, A DID Method for Static Cryptographic Keys, Unofficial Draft 02 September 2022. Online abrufbar unter: https://w3c-ccg.github.io/did-method-key/ (zuletzt abgerufen am 10.11.2023).

W3C (2023): Verifiable Credentials Data Model v2.0, W3C Working Draft 02 December 2023. Online abrufbar unter: https://www.w3.org/TR/vc-data-model-2.0/#credentials (zuletzt abgerufen am 04.12.2023).

walt.id (2023): DID Web. Online abrufbar unter: https://docs.walt.id/v/ssikit/concepts/did-web (zuletzt abgerufen am 10.11.2023).

Wiewiorra, L., Liebe, A., Taş, S. (2020): Die wettbewerbliche Bedeutung von Single-SignOn- bzw. Login-Diensten und ihre Relevanz für datenbasierte Geschäftsmodelle sowie den Datenschutz. Online abrufbar unter: https://www.wik.org/fileadmin/user_upload/Unternehmen/Veroeffentlichungen/Diskus/2022/WIK_Diskussionsbeitrag_Nr_462.pdf (zuletzt abgerufen am 01.12.2023).

Winfield, A (2017): How Blockchain's 'Web of Value' Could Oust the New Big Media. Online abrufbar unter: https://www.forbes.com/sites/sap/2017/11/20/how-blockchains-web-of-value-could-oust-the-new-big-media/?sh=73c66eb79271 (zuletzt abgerufen am 01.12.2023).

Wittmann, L. (2022): Stellungnahme zum Fragenkatalog des Ausschusses für Digitales in der Sache „Web 3.0 und Metaverse von Lilith Wittmann, Deutscher Bundestag Ausschuss für Digitales, Ausschussdrucksache 20(23)113, 13.12.2022. Online abrufbar unter: https://www.bundestag.de/resource/blob/926420/fe19d8b8a49a11bc7e05e1700b52403c/Stellungnahme-Wittmann-data.pdf (zuletzt abgerufen am 15.11.2023).

World Bank (2019): ID4D Practitioner’ Guide: Version 1.0 (October 2019). Washington, DC: World Bank. License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO). Online abrufbar unter: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf (zuletzt abgerufen am 20.11.2023).

World Economic Forum (2020): Reimaging Digital Identity: A Strategic Imperative. Online abrufbar unter: https://www3.weforum.org/docs/WEF_Digital_Identity_Strategic_Imperative.pdf (zuletzt abgerufen am 10.11.2023).

World Economic Forum (2023), Reimaging Digital ID – Insight Report, June 2023. Online abrufbar unter: https://www3.weforum.org/docs/WEF_Reimagining_Digital_ID_2023.pdf (zuletzt abgerufen am 01.12.2023).

Yasuda, K., Lodderstedt, T., Chadwick, D., Nakamura, K., Vercammen, J. (2022). OpenID for Verifiable Credentials, A Shift in the Trust Model Brought by Verifiable Credentials. Online abrufbar https://openid.net/wordpress-content/uploads/2022/05/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials_FINAL_2022-05-12.pdf (zuletzt abgerufen am 12.12.2023).

Yasuda, K., Lodderstedt, T. (2021): OpenID Connect for SSI. Online abrufbar unter: https://openid.net/wordpress-content/uploads/2021/09/OIDF_OIDC4SSI-Update_Kristina-Yasuda-Torsten-Lodderstedt.pdf (zuletzt abgerufen am 10.11.2023).

Yildiz, H., Philipp, A., Schulte, A., Küpper, A., Göndor, S., Garzon, S. R. (2023): Interoperable Selbstsouveräne Identitäten: Ein Digital Markets Act für Endnutzer?. HMD 60, 405–421 (2023). https://doi.org/10.1365/s40702-023-00947-3.

Zavratnik, J. (2022): Analysis of Web3 Solutions Development Principles. Online abrufbar unter: https://upcommons.upc.edu/bitstream/handle/2117/379908/171754.pdf?sequence=1 (zuletzt abgerufen am 30.11.2023).

Zwitter, A. J., Gstrein, O. J., Yap, E. (2020): Digital Identity and the Blockchain: Universal Identity Management and the Concept of the “Self-Sovereign” Individual. Front. Blockchain 3:26. DOI: 10.3389/fbloc.2020.00026.

# Anhang

## A1 Die Ausgestaltung einer EUDI-Wallet

Die Europäische Union strebt das Ziel an, dass bis zum Jahr 2030 80% der EU-Bürger:innen Zugang zu digitalen Wallets in Anlehnung an EUDI-Wallet haben sollen.[207] Die EUDI Wallet soll es EU-Bürger:innen ermöglichen, ausgewählte Attribute ihrer Identität, Daten und Zertifikate mit Dritten, sowohl Behörden als auch privaten Akteuren, zu teilen. Dies schließt die Möglichkeit ein, dass digitale Nachweise von staatlichen und nicht-staatlichen Organisationen ausgestellt werden können, um elektronische Attribute zu bestätigen. Hierbei erfolgt eine Unterscheidung zwischen Trust Service Providers und Qualifizierten Trust Service Providers, die dazu befugt sind, digitale Nachweise gemäß spezifischer Anforderungen auszustellen:

- **Qualified Electronic Attestation of Attributes** müssen bestimmte Anforderungen erfüllen. So dürfen sie nur von einem autorisierten **Qualifizierten Trust Service Provider** ausgegeben werden. Qualifizierte Daten sind beispielsweise Zeugnisse.
- **Qualified Electronic Signatures** umfassen qualifizierte elektronische Signaturen und Siegel.
- **Non-qualified Electronic Attestation of Attributes** können von jeder (privaten) Organisation ausgestellt werden und sind nicht-qualifizierte Daten wie Reisetickets oder Mitgliedschaftsausweise.
  Alle Nachweise sollen gemeinsam in der EUDI aufgeführt werden. Eine eindeutige Definition des Ökosystems einer deutschen EUDI-Wallet steht noch aus.

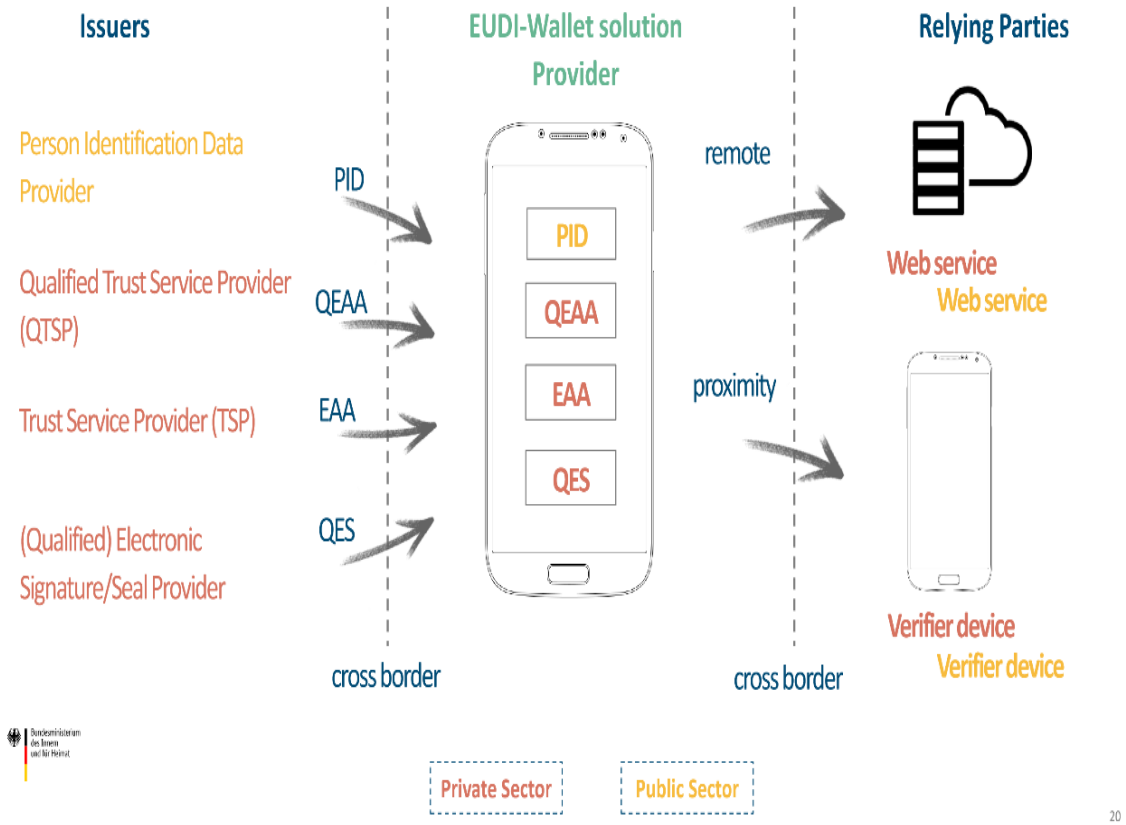
Die Identifizierung eines Users geschieht auf qualifiziertem Niveau beispielsweise durch **Personenidentitätsdaten**[208], wie sie bereits bei der eID-Infrastruktur genutzt werden, wobei die Verifizierung über eine Schnittstelle zum relevanten staatlichen Datenregister vollzogen werden muss. Eine Anonymisierung der Daten kann allerdings nur garantiert werden, wenn Verifiable Credentials–**nicht** mit **Personenidentitätsdaten** verbunden sind, sondern **DID**-Konzepte nutzen. Dies verhindert, dass durch Korrelation Rückschlüsse auf die identitätshaltende Entität gezogen werden können.

Die EU-Mitgliedsstaaten werden voraussichtlich dazu verpflichtet, jeder juristischen Person eine Organisations-Wallet (angelehnt an EUDI-Wallet) auszustellen.[209] Diese soll

**207** Vgl. EWC (2023).
**208** PIDs sind eine nicht-anonymisierte Identifikatoren-Form und sollen als eindeutige Personenkennziffern in EUDI-Wallets Verwendung finden. Vgl. Deutscher Bundestag (2023c).
**209** Vgl. EWC (2023).

dazu verwendet werden, überprüfbare Berechtigungsnachweise zu speichern, die von Anbietern von Qualified Electronic Attestation of Attributes für die jeweilige juristische Person ausgestellt werden (bspw. ein Organisationsausweis, ein Handelsregisterauszug oder eine Bankkarte). Die Wallets sollen dazu in der Lage sein, sichere Verbindungen untereinander (zwischen den Geschäftspartnern) herzustellen, um verifizierbare Anmeldeinformationen zwischen den Teilnehmenden auszutauschen und so Daten verifizieren zu lassen. Die Organisationen, die eine Wallet besitzen, nehmen gleichzeitig die Rolle eines Issuers und die eines Verifiers ein, um sich gegenseitig Berechtigungsnachweise vorzulegen und um diese zu überprüfen.[210]

Abbildung 17: Ausgestaltung einer EUDI-Wallet




Quelle: BMI (2023a).

**210** Vgl. IDunion (2023b); EWC (2023).

**ISSN 1865-8997**