Ehrlich, Tobias; Richter, Daniel; Meisel, Michael; Anke, Jürgen

Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten

HMD Praxis der Wirtschaftsinformatik

Provided in Cooperation with:
Springer Nature

Suggested Citation: Ehrlich, Tobias; Richter, Daniel; Meisel, Michael; Anke, Jürgen (2021) : Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten, HMD Praxis der Wirtschaftsinformatik, ISSN 2198-2775, Springer Fachmedien Wiesbaden, Wiesbaden, Vol. 58, Iss. 2, pp. 247-270,
https://doi.org/10.1365/s40702-021-00711-5

This Version is available at:
https://hdl.handle.net/10419/287632

HMD (2021) 58:247–270
https://doi.org/10.1365/s40702-021-00711-5

SCHWERPUNKT

Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten

Tobias Ehrlich · Daniel Richter · Michael Meisel · Jürgen Anke

Eingegangen: 30. November 2020 / Angenommen: 4. Februar 2021 / Online publiziert: 22. Februar 2021

Zusammenfassung In diesem Beitrag werden die Rolle digitaler Identitäten für eine funktionierende digitale Wirtschaft thematisiert und Anforderungen an das Management digitaler Identitäten abgeleitet. Bislang hat sich kein Ansatz für das Management digitaler Identitäten in der Breite etabliert, was zu einer Fragmentierung der ID-Landschaft sowie einer Vielzahl von Benutzerkonten für den Anwender führt. Mangels Standards ist zudem die Interoperabilität von digitalen Identitäten eingeschränkt. Dies führt zu einer Reihe von Problemen, die den effizienten und sicheren Umgang mit digitalen Identitäten behindern. Abhilfe verspricht das Konzept der Self-Sovereign Identities (SSI) und den damit verbundenen Standards „Verifiable Credentials“ und „Decentralized Identifiers“. Sie erlauben den flexiblen Austausch von manipulationssicheren digitalen Nachweisen zwischen Benutzern und Systemen und bilden damit die Grundlage für den Aufbau von Vertrauensbeziehungen im digitalen Raum. In diesem Beitrag werden das SSI-Paradigma vorgestellt und die Hürden diskutiert, die dem breitenwirksamen Einsatz dieses Konzepts entgegenstehen. Damit erhält der Leser einen kompakten Überblick verschiedener Ansätze für das Identitätsmanagement und die Potenziale selbst-souveräner Identitäten. Für die

T. Ehrlich · J. Anke (✉)
Hochschule für Technik und Wirtschaft (HTW) Dresden, Friedrich-List-Platz 1, 01069 Dresden, Deutschland
E-Mail: juergen.anke@htw-dresden.de

T. Ehrlich
E-Mail: tobias.ehrlich@htw-dresden.de

D. Richter
SAP Deutschland SE & Co. KG, Hasso-Plattner-Ring 7, 69190 Walldorf, Deutschland
E-Mail: daniel.richter@sap.com

M. Meisel
Fakultät CB, Hochschule Mittweida, Technikumplatz 17, 09648 Mittweida, Deutschland
E-Mail: meisel@hs-mittweida.de

Gestaltung digitaler Dienste in Wirtschaft und Verwaltung sollte dieser Ansatz stärker berücksichtigt werden, um von den damit verbundenen Vorteilen zu profitieren.

Schlüsselwörter Digitale Identität · Self-sovereign Identity · Verifiable Credentials · Identity Management

Self-Sovereign Identity as the Basis for Universally Applicable Digital Identities

Abstract This paper addresses the role of digital identities for a functioning digital economy and outlines requirements for their management. So far, no approach for the management of digital identities has been widely established, which leads to a fragmentation of ID services as well as a variety of user accounts. Due to the lack of standards, the interoperability of digital identities is also limited. This leads to several problems that prevent the efficient and secure handling of digital identities. The concept of Self-Sovereign Identities (SSI) and the associated standards "Verifiable Credentials" and "Decentralized Identifiers" is a promising approach to improve the situation. They allow the flexible exchange of tamper-proof digital proofs between users and systems. Therefore, they form the foundation for building trust relationships in the digital space. This paper introduces the SSI paradigm and discusses the barriers that prevent the wide-scale adoption of this concept. With that, the reader gets a compact overview of different approaches for identity management and the potentials of self-sovereign identities. For the design of digital services in business and administration, this approach should be given greater attention to benefit from the associated advantages.

Keywords Digital Identity · Self-sovereign Identity · Verifiable Credentials · Identity Management

1 Einleitung

1.1 Digitale Identitäten als Grundlage für Vertrauen im digitalen Raum

Mit zunehmender Digitalisierung von Wirtschaft und Verwaltung wächst das Angebot an digitalen Diensten. Um vertrauenswürdige Interaktionen mit solchen Diensten zu gewährleisten, müssen alle Beteiligten sicher digital identifiziert werden. Mit digitalen Identitäten können sich Personen, Organisationen oder Objekte gegenüber einem Softwaresystem ausweisen. Solche digitalen Identitäten sind im Kern eine Sammlung von verschiedenen, möglichst langlebigen Identifizierungsmerkmalen (Identitätsattributen) (Tsolkas und Schmidt 2017).

Bei der Entwicklung von digitalen Identitäten wurde zunächst pragmatisch vorgegangen. Dies führt dazu, dass Betreiber von Onlineservices und Anwendungen (Service Provider) die digitalen Identitäten ihrer Nutzer selbst verwalten müssen. Dadurch entstanden zahlreiche „Silos" mit einer Sammlung von Identitätsmerkma-

len und eigener Nutzerbasis. Die Anwender müssen in der Folge zahlreiche Nutzerkonten pflegen, deren gespeicherte Identitätsmerkmale vielfach redundant sind.

Eine Verbesserung erreicht das Modell der föderierten Identitäten, welches digitale Identitäten systemübergreifend nutzbar macht. Dabei werden zentrale Dienste, so genannte ID-Provider, eingesetzt, die Identitätsmerkmale und Authentifizierungsmethoden für die Nutzung einer Vielzahl von Anwendungen zentral bereitstellen. Somit kann der Fragmentierung der ID-Landschaft zum Preis der Zentralisierung von ID-Informationen bei einigen wenigen gewinnorientierten Unternehmen begegnet werden. Dies birgt wiederum neue Risiken. So können die ID-Provider beim Einsatz der Identitäten durch den Nutzer Daten aus unterschiedlicher Herkunft miteinander korrelieren und somit individuelle Profile von Nutzern erstellen. Diese Sammlung bietet die Grundlage sowohl für eigene wirtschaftliche Zwecke wie beispielsweise auf den Nutzer zugeschnittene Werbeanzeigen als auch für die möglicherweise unerwünschte Weitergabe persönlichen Daten an Dritte. Staatliche, elektronische Authentifizierungsmethoden versuchen die Fragmentierung der ID-Landschaft ebenfalls zu adressieren, indem sie einer Person ermöglichen, sich gegenüber einem Händler oder einer Behörde mit der eID auszuweisen. Die eID ist die elektronische Repräsentation des Personalausweises, die direkt im Ausweis eingebettet ist (BMI 2020a). Sie ist seit 2017 standardmäßig bei allen neu ausgestellten Personalausweisen aktiviert (Bundesregierung Deutschland 14.07.2017) und kann mittels geeigneter Apps, z. B. der AusweisApp2, per Smartphone ausgelesen und an einen berechtigten Anfrager übermittelt werden.

Auch Organisationen benötigen digitale Identitäten für die Kundenbetreuung, digitale Finanzverwaltung oder zum Nachweis der Rechtsform. In Deutschland übernehmen solche Registrierungen das Handelsregister, das Finanzamt, die Non-Profit Organisation GS1 Germany und andere Mitglieder der Global Legal Entity Identifier Foundation (GLEIF). Die ausgestellten Kennnummern sind jedoch nicht interoperabel. Dementsprechend ermöglicht der Handelsregistereintrag eine Identifizierung auf nationaler Ebene, während der Legal Entity Identifier (LEI) eine Identifizierung auf dem internationalen Finanzmarkt unterstützt.

Die Registrierung von technischen Produkten ist ein Sonderfall, denn anders als bei Personen übernimmt selten eine Behörde oder ein Konsortium die Speicherung der Identifikatoren. Ausnahmen bilden hier registrierungspflichtige Waren wie Fahrzeuge mit der Fahrzeug-Identifikationsnummer (FIN) aus der EU-Verordnung 19/2011 und Medizinprodukte mit der Unique Device Identification (UDI) aus der EU MDR2017/745. Hersteller unterhalten daher ihre eigenen Datenbanken mit den jeweiligen Kennnummern zur Identifizierung. Wenn ein Unternehmen seine Waren weltweit identifizierbar machen möchte, kann die GS1 hierfür eine zentral verwaltete Global Trade Item Number (GTIN) vergeben.

Vor dem Hintergrund der hohen Bedeutung digitaler Identitäten für die Digitalisierung der Wirtschaft soll der vorliegende Beitrag die bisherigen Herangehensweisen an den Umgang und die Verwaltung mit digitalen Identitäten bewerten und SSI als einen aussichtsreichen Lösungsweg vorstellen. Grundlage dafür sind Veröffentlichungen aus verschiedenen Quellen, vor allem Community- und Standardisierungsaktivitäten. Es ist festzustellen, dass es bislang nur wenige wissenschaftliche Arbeiten gibt, die sich insbesondere mit den neueren Entwicklungen rund um Self-

Sovereign Identity und den damit verbundenen Standards des World Wide Web Consortiums (W3C) auseinandersetzen. Der vorliegende Beitrag versucht diese Lücke zu schließen. Praktiker in Wirtschaft und Verwaltung sollen damit einen Einblick in aktuelle Entwicklungen bekommen, um diese in die Gestaltung von Systemen einfließen zu lassen. Für die Wissenschaft, insbesondere die Wirtschaftsinformatik, zeigt der Beitrag den aktuellen Stand der Technik in einem zunehmend wichtigen, aber bislang wissenschaftlich zu wenig beachteten Thema.

1.2 Beteiligte Akteure und ihre Rollen

Für eine systematische Betrachtung des Identitätsmanagements ist die Differenzierung verschiedener Rollen hilfreich. Der *Herausgeber (Issuer)* ist für das korrekte und vertrauenswürdige Erstellen von Identitäten bzw. dem Bestätigen der Korrektheit von behaupteten Identitätsmerkmalen zuständig. In der realen Welt sind das z. B. hoheitliche Dokumente, Urkunden oder Plastikkarten. Digital lassen sich diese in Form kryptografisch gesicherter, digitaler Nachweise repräsentieren. Der *Inhaber (Holder)* empfängt diese Nachweise und verwaltet sie in einer physischen Geldbörse oder digital in einer Wallet-App. Er hat die alleinige Verfügungsgewalt über diese Nachweise. Das *Subjekt* ist die Entität, auf die sich das Identitätsmerkmal bezieht. Das kann ein Objekt unter der Kontrolle des Inhabers sein oder eine Person, für die der Inhaber verantwortlich oder bevollmächtigt ist. In vielen Fällen ist das Subjekt jedoch mit dem Inhaber identisch. Die *Akzeptanzstelle (Verifier)* ist eine Anwendung, ein Onlineservice oder eine Stelle in der physischen Welt, der vom Inhaber Nachweise über bestimmte ID-Merkmale anfordert, um seine Identität oder Berechtigungen zu prüfen. Der Inhaber kann selbst entscheiden, welche Nachweise er präsentiert. Während in der realen Welt die Akzeptanzstelle durch Erfahrung und Fachwissen die Echtheit eines präsentierten Nachweises manuell prüfen muss, ist das bei Verwendung kryptografisch gesicherter, digitaler Nachweise automatisch möglich. Fälschungen sind dadurch deutlich schwieriger als bei physischen Dokumenten.

Akteure sind natürliche oder juristische Personen, die je nach konkreter Situation eine oder mehrere der genannten Rollen innehaben. Der Nutzer als natürliche Person hat in der Regel die Rolle Inhaber und meist auch Subjekt, da sich die Mehrzahl der von ihm verwalteten ID-Attribute auf ihn selbst bezieht. Auch juristische Personen (Organisationen) können Nutzer sein, da sie Teil von Rechtsgeschäften sind und eine nachweisbare Identität benötigen. Organisationen können darüber hinaus auch Betreiber von Anwendungen sein, mit denen Nutzer interagieren sollen. Je nach Ausprägung ist eine solche Anwendung Herausgeber und/oder Akzeptanzstelle. Anwendungen, die gegenüber dem Nutzer spezielle Eigenschaften nachweisen müssen, können ihrerseits auch Inhaber sein.

Um das Ausstellen, Speichern, Freigeben und Verifizieren von digitalen Identitätsmerkmalen praktisch zu realisieren, bedarf es technischer Infrastruktur und Softwarekomponenten, wie zum Beispiel die oben erwähnte digitale Wallet-App. Diese werden in der Regel von einem Hersteller oder einer Organisation bereitgestellt und im Folgenden unter der Bezeichnung „ID-Dienst“ zusammengefasst.

1.3 Anforderungen

Aus den vorgenannten Ausführungen lassen sich Anforderungen an ein verbessertes Identitätsmanagement ableiten. Aus Sicht der Inhaber ergeben sie sich vor allem aus breiter Anwendbarkeit und Kontrolle über die eigenen Daten:

- Datenschutzkonformität, d. h. nur notwendige Daten werden übertragen
- Portabilität von Identitätsmerkmalen zwischen ID-Diensten, um Lock-In Effekte zu vermeiden
- Hohe Benutzbarkeit (Usability), ohne die Sicherheit zu beschränken.
- Breite Anwendbarkeit, d. h. Identitätsdaten sollten in vielen Situationen einsetzbar sein
- Verfügungsmacht über eigene ID-Daten, um ungewünschte Verwertung durch Dritte zu verhindern

Für die Akzeptanzstellen ist vor allem wichtig, dass möglichst viele Nutzer einfach ihre Anwendung nutzen können und nicht von komplexen Registrierungsvorgängen abgeschreckt werden. Dennoch müssen Nutzer eindeutig identifiziert werden, um rechtssichere Transaktionen durchführen zu können:

- Einfacher Zugang für alle berechtigten Nutzer ohne zusätzliche Registrierung
- Eindeutige Identifikation von Nutzern für rechtssichere Transaktionen
- Geringer Aufwand für ID-Prüfung und Verwaltung personenbezogener Daten
- Geringe Kosten bei Einbindung und Verwendung eines ID-Dienstes

Die Anbieter von ID-Diensten sind für ihren Markterfolg vor allem darauf angewiesen, eine möglichst große Attraktivität für Nutzer und Anwendungen gleichermaßen zu besitzen. Dies drückt sich in einer großen Anzahl von Akzeptanzstellen aus, d. h. Anwendungen, die eine Authentifizierung mittels des jeweiligen Dienstes unterstützen. Dies ist in direkter Wechselwirkung mit der Anzahl der Nutzer, d. h. es entsteht ein positiver Netzwerkeffekt: Je mehr Akzeptanzstellen, desto attraktiver ist der Dienst für potenzielle Nutzer, und je mehr Nutzer ein Dienst hat, desto eher ist der Betreiber einer Anwendung bereit, diesen Dienst zu unterstützen. Um dies zu erreichen, ist wie bei allen Angeboten, die einen zweiseitigen Markt als Grundlage haben, entsprechend intensives Marketing notwendig. Daneben sind für den Markterfolg auch eine hohe Usability, Vertrauenswürdigkeit, Verfügbarkeit und Sicherheit erforderlich. Die EU-Verordnung für elektronische Identifizierung, Authentifizierung und Vertrauensdienste (eIDAS) enthält verbindliche Regelungen für elektronische Transaktionen im europäischen Binnenmarkt und deckt vor allem die Bereiche „Elektronische Vertrauensdienste“ und „Elektronische Identifizierung“ ab. Für den Einsatz in regulierten Domänen wie der öffentlichen Verwaltung müssen ID-Dienste dementsprechend eine Zertifizierung nachweisen, um für das eIDAS-Vertrauensniveau „substanziell“ oder „hoch“ zugelassen zu werden (BSI 2016).

2 Ansätze zum Management digitaler Identitäten

Im Laufe der Zeit wurden verschiedene Ansätze zur Erzeugung, Verwaltung und dem Einsatz digitaler Identitäten entwickelt. In diesem Abschnitt werden diese erläutert und verglichen.

2.1 Grundlagen des Managements digitaler Identitäten

2.1.1 Isolierte Identitäten

Das Modell der isolierten Identitäten ist am weitesten verbreitet und wird z. B. bei Routern, Webseiten und Onlineshops eingesetzt. Jeder Service verwaltet hierbei seine Benutzer in einer eigenen Nutzerdatenbank und führt Authentifizierungen selbst durch. Der Service ist damit Herausgeber und Akzeptanzstelle zugleich. Dies bringt den Vorteil, dass konkurrierende Organisationen nicht von Dritten abhängig sind, Daten optimal an ihre Bedürfnisse anpassen sowie verarbeiten können und die Aktivitäten der Nutzer nicht ohne Weiteres korreliert werden können. Weiterhin ermöglicht diese Flexibilität eine breite Anwendungsmöglichkeit von unterschiedlichen ID-Arten für Personen, Organisationen und technische Produkte. Jedoch müssen Service Provider potenzielle Nutzer zur Registrierung incentivieren. Damit steigt auch die Anzahl an Identitäten mit den dazugehörigen Authentifizierungsmethoden. Für den Nutzer endet das in der Herausforderung, diese Accounts auf effiziente und sichere Weise zu verwalten (Jøsang und Pope 2005). Aber auch Service Provider stehen von der Herausforderung, eine wachsende Zahl von Nutzerkonten datenschutzkonform zu speichern und vor Diebstahl zu sichern.

2.1.2 Föderierte Identitäten

Die föderierte Identität adressiert die beschriebenen Nachteile. Dem Nutzer wird ermöglicht, durch zentralisierte Identity Provider dieselbe digitale Identität bei verschiedenen Services zu verwenden, ohne sich neu registrieren zu müssen. Der Identity Provider fungiert dabei sowohl als Herausgeber und Inhaber, da er die Daten des Benutzerkontos verwaltet. Er verifiziert die Identität, wenn sich der Nutzer bei einem angeschlossenen Service anmelden will.

Unternehmen können Identitäten demnach mit geringerem Aufwand verwalten. Was aus administrativer Sicht sinnvoll ist, stellt für Privatanwender ein Problem dar, denn Identitäten verbleiben in den Händen der Identity Provider und der Nutzer ist von deren Fortbestand und Zugänglichkeit abhängig (Allen 2016). Die föderiert-zentralen ID-Verwaltung, in Verbindung mit der Nutzung unterschiedlicher Services, erleichtert die Zusammenführung von Informationen verschiedener Herkunft, um so ohne Kontrolle des Nutzers umfangreiche Profile anzufertigen. Die Menschen vertreten in der digitalen Welt verschiedene anonyme, pseudonyme oder rechtspersönliche Rollen. Je nach Anwendung differenzieren sie auch, wer welche Inhalte sehen darf. Da die individuellen Grundwerte schon immer Bestandteil des Identitätsmanagements sind, stellt die Korrelierbarkeit ein neues Problem dar. Werden die Informationen in einem falschen Kontext verarbeitet, können dem Nutzer finanzielle

oder soziale Nachteile entstehen (Priem et al. 2011). Die föderierten Identitäten beziehen sich vor allem auf Personenidentitäten. Technische Produkte oder Identitäten von Organisationen spielen in der Regel eine untergeordnete Rolle.

2.1.3 Elektronischer Personalausweis und andere staatliche Identitäten

Der elektronische Personalausweis (nPA) mit elektronischer ID (eID), der elektronische Aufenthaltstitel und der elektronische Reisepass gehören ebenfalls zu den föderierten Identitäten. Denn auch die Regierung hat das Interesse, personalisierte elektronische öffentliche Dienste bereitzustellen und Bürger vor Betrug und Sicherheitsrisiken zu bewahren (Priem et al. 2011). Diese Identität stellt einen Sonderfall dar, denn sie besitzt keinen ID-Managementansatz, sondern ist ein hoheitliches Authentisierungsmittel mit zusätzlicher digitaler Repräsentation. Anders als bei den bisher vorgestellten Modellen werden bei diesem Verfahren keine Identitätsdaten zentral verwaltet. Stattdessen wird eine dedizierte Infrastruktur (eID-Server) verwendet, mit der die eID-Daten vom Personalausweis zur Akzeptanzstelle übermittelt werden. Der Nutzer benötigt dazu sein elektronisches Ausweisdokument mit aktivierter eID-Funktion sowie mindestens die AusweisApp2. Der Identitätsbesitzer kann sich so digital authentisieren, ohne sich neu registrieren zu müssen (Pohlmann 2019a). Die Identifikation geschieht hierbei nach dem Prinzip der eIDAS-Vertrauensniveaus. Je nach Freigabe kann der Dienstleister den Nutzer nur vollständig pseudonym identifizieren, Daten teilweise oder vollständig auslesen. Bei einer pseudonymen Abfrage wird für jeden Online-Dienst eine eigene pseudonyme Kennung generiert (BMI 2020b).

Service Provider müssen zur Nutzung der eID zunächst eine Berechtigung beantragen und müssen dafür einen Dienst konzipieren, der vollständig DSGVO- und eIDAS-konform ist. Anschließend können sie nur die Daten auslesen, für die eine Genehmigung vorliegt. Werden weitere Daten benötigt, so müssen die Service Provider diese Informationen separat abfragen und verwalten (BSI 2017). Folglich haben die Bürger mit diesen Identitäten ein sehr hohes Sicherheitsniveau. Von der Privatwirtschaft werden vor allem die regulatorischen Hürden kritisiert, weswegen es gegenwärtig nur wenige Dienstleistungen gibt, die das eID-Verfahren verwenden. Ferner fehlen derzeit zur EU-weiten Anwendung grenzüberschreitende Standards: eID-Verfahren, die in einen Mitgliedsstaat zulässig sind, erfüllen die gesetzliche Bedingungen eines anderen Landes möglicherweise nicht (Winter et al. 2020). Zudem wird aus Nutzersicht die Usability dieses Verfahrens oft kritisiert, was die Verbreitung ebenfalls behindert (Kostic et al. 2016).

2.1.4 Self-Sovereign Identity

Ein neuer Ansatz für das Identitätsmanagement ist das auf dezentraler Organisation beruhende Paradigma „Self-Sovereign Identity“ (SSI). Dabei bekommt der Nutzer Identitätsmerkmale und Berechtigungen in Form von kryptografisch gesicherten digitalen Nachweisen („Verifiable Credentials“) ausgestellt und kann diese mittels einer digitalen Brieftasche („Wallet“) selbständig verwalten. Um sich gegenüber Akzeptanzstellen auszuweisen, genügt die Vorlage der geforderten Verifiable Cre-

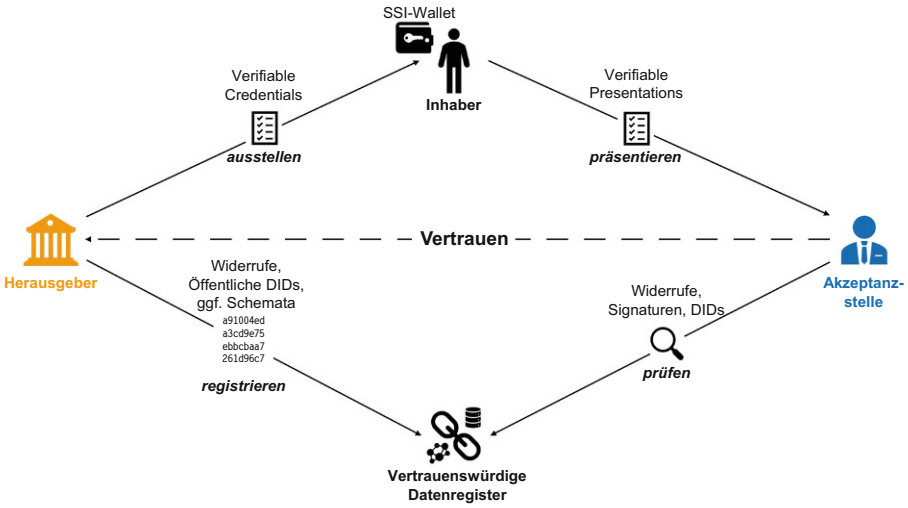


Abb. 1 SSI-Interaktionsschema, adaptiert von (Mühle et al. 17.07.2018)

dentials in Form von so genannten „Verifiable Presentations“, die ohne direkten Kontakt zum Herausgeber überprüfbar sind. Mittels geeigneter Protokolle ist die flexible Übermittlung solcher Verifiable Credentials und Presentations realisierbar (vgl. 3.1.3 DIDcomm). Dabei kann jeder Akteur eine oder mehrere Rollen annehmen und ein Vertrauensdreieck (vgl. Abb. 1) aufbauen (Windley 2018).

Für Christopher Allen ist die Unabhängigkeit eines Nutzers von einem zentralen ID-Provider das „Herzstück“ der Self-Sovereign Identity, anstatt nur den Nutzer ins Zentrum zu stellen. Er gilt als Vordenker im Bereich der SSI-Entwicklung und formulierte zehn Prinzipien, die seiner Meinung nach für SSI notwendig sind. Diesen zufolge muss der Benutzer die Möglichkeit haben, seine eigenen digitalen Identitäten zu erstellen, über mehrere Standorte hinweg mit voller Kontrolle zu verwenden und zu verwalten. Die Dienstleister müssen indes ihren Kunden Transparenz bieten, indem sie die Anwender zu den verwendeten Mitteln und zu der Datenverarbeitung informieren. Zusätzlich muss der Nutzer in der Lage sein, persönlich identifizierende Informationen oder Fakten minimalisiert und nur durch explizite Zustimmung einzusetzen. Auch sollte er selbst über die Verwendungsdauer der Verbindungen oder Informationen entscheiden (Allen 2016).

Dies begründet ein neues Paradigma für den Umgang mit digitalen Identitäten, in dem Benutzer in die Position von selbst-souveränen Verwaltern ihrer Identität gebracht werden. Diese Unabhängigkeit von Dritten ermöglicht zudem einen neuen Ansatz für die Interoperabilität verschiedener Dienste, vereinfacht die Handhabung personenbezogener Daten auf Seiten der Akzeptanzstellen und verbessert die Nutzererfahrung durch Wegfall von Passwörtern und vermeidet komplexe Registriervorgänge. Weiterhin wird durch eine Peer-to-Peer-Verbindung und dezentrale Verwaltung die Privatsphäre des Identitätsinhabers geschützt. Die Möglichkeiten zur Korrelation von Identitätsdaten zwischen unterschiedlichen Diensten und Service Providern werden vermindert. Gleichzeitig sinkt die Attraktivität für Angriffe auf

Tab. 1 Vergleich verschiedener Ansätze für das ID-Management

	Isoliert	Föderiert	eID/nPA	SSI
Sicherheit	Unklar	Hoch	Sehr hoch	Sehr hoch
Verbreitung	Hoch	Hoch	Gering	Sehr gering
Usability	Mittel	Hoch	Gering	(Potenziell) Hoch
Datenqualität	Unklar	Hoch	Sehr hoch	Hoch
Datenschutz	Unklar	Unklar	Hoch	Hoch
Standardisiert	Nein	Ja	Ja	Ja
Integrationsaufwand	Mittel	Gering	Sehr hoch	Implementationsabhängig
Primäre Nutzung	Beliebige Onlinedienste	Onlinedienste, Unternehmensanwendungen	V. a. in öffentlicher Verwaltung, online/offline	Beliebiger Einsatz, online/offline
ID-Attribute	Flexibel	Flexibel	Person	Flexibel

die Datenbestände von Akzeptanzstellen, da sie weniger lukrativ für Identitätsdiebstahl sind. Dennoch kann nicht technisch verhindert werden, dass Akzeptanzstellen eigene Datenbestände anlegen oder diese Informationen an Dritte weiterreichen.

2.2 Vergleich

Der Vergleich der verschiedenen Ansätze findet anhand von Kriterien statt, die auf den in Abschn. 1.3 genannten Anforderungen basieren. Dabei werden die Eigenschaften der einzelnen Ansätze aus den vorherigen Ausführungen genutzt und in einer konsolidierten Darstellung aufbereitet (Tab. 1).

Insgesamt lässt sich feststellen, dass die bisherigen Ansätze die Anforderungen an das Management digitaler Identitäten nur zum Teil erfüllen. Isolierte Ansätze sind sehr verbreitet und flexibel, aber nicht standardisiert und führen zu vielen verteilten Nutzerkonten. Föderierte Identitäten reduzieren zwar diese Zahl, führen aber zu einer Abhängigkeit der Nutzer von den Identity Providern, was diesen eine große Macht verschafft (Riedel 2019). Aufgrund der Nutzung für verschiedene Anwendungen stellen sie nicht nur ein attraktives Angriffsziel für Cyber-Kriminelle dar, sondern eignen sich auch für die Korrelation von Nutzeraktivitäten zur Erstellung von Kundenprofilen (Cyphers und Gebhart 2019). Hoheitliche Identitäten wie die eID des Personalausweises sind sehr sicher und datenschutzkonform. Wegen der niedrigen Usability und des hohen Aufwands für ihre Unterstützung auf Seiten der Anwendungen ist ihre Nutzbarkeit jedoch gering (Riedel 2019). Sie werden fast ausschließlich für das E-Government eingesetzt.

Der Ansatz der Self-Sovereign Identity verspricht hierbei Lösungen für viele der genannten Probleme. Allerdings ist die Verbreitung derzeit noch sehr gering. Dennoch werden sowohl die Standardisierung als auch die Implementierung nutzbarer Komponenten derzeit stark vorangetrieben. Um das Verständnis für die Funktionsweise und Potenziale von SSI zu schärfen, wird im Folgenden detaillierter auf Standardisierung, Einsatz und aktuelle Aktivitäten rund um SSI eingegangen.

3 Umsetzung von Self-Sovereign Identity

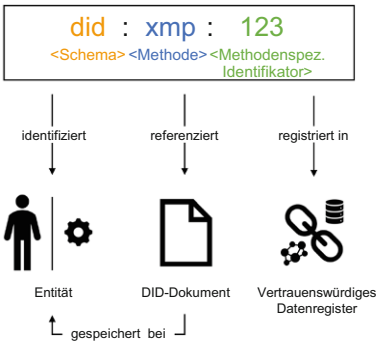
3.1 Elemente eines SSI-Systems

Für die Realisierung von SSI sind drei Bestandteile besonders relevant: (1) dezentrale Identifikatoren für beliebige Entitäten, (2) kryptografisch gesicherte Datenformate zur Beschreibung der Identitätsattribute sowie (3) ein Protokoll zur Peer-to-Peer Kommunikation zwischen den beteiligten Akteuren. Für diese drei Bestandteile sind mit Decentralized Identifiers, Verifiable Credentials und DIDcomm bereits Standardisierungsaktivitäten im Gange.

3.1.1 Decentralized Identifiers (DID)

Decentralized Identifiers sind einzigartige URIs, die nach dem Schema im RFC 3986 definiert sind. Eine DID identifiziert eine durch ihren Besitzer gewählte Entität (Reed et al. 2021). Die referenzierte Ressource ist ein DID-Dokument, das zum Beispiel als JSON-LD repräsentiert wird. Wie Abb. 2 zeigt, ist eine DID-URN dabei in drei Teile geteilt. Das Schema, welches den Bezeichner als DID-Ressource definiert, die Methode und der methodenspezifische Identifikator. Aktuell gibt es 82 produktive oder in der Entwicklung befindliche DID-Methoden (Steele und Sporny 2021).

Ziel des W3C ist es, DIDs als weltweiten Standard für kryptografisch unabhängige, verifizierbare Identifikatoren zu etablieren, die keiner Kontrolle zentraler Verwaltungen unterliegen. Der Nutzer, der die DID erzeugt und dem sie anschließend gehört, entscheidet selbst über die Lebensdauer (Reed et al. 2021). Jedes DID-Dokument kann Informationen zu kryptografischen Verifizierungsmethoden und Service Endpoints enthalten, die es einem DID-Besitzer ermöglichen, die Kontrolle über die DID nachzuweisen (Reed et al. 2021). Außerdem ist es möglich, durch DIDs Parameter an einen Service-Endpunkt zu übertragen. Zusätzlich bieten sie der Akzeptanzstelle die Möglichkeit, die gleichen Methoden zur Verifizierung der Credentials zu nutzen.




```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:xmp:123",
  "verificationMethod": [
    {
      "id": "did:xmp:123#ZC2jXTO6t4R501bfCXv3RxarZyUbdP2w_psLwMuY6ec",
      "type": "Ed25519VerificationKey2018",
      "controller": "did:xmp:123",
      "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
    },
    {
      "id": "did:xmp:123#zQ3shP2mWsZYWgvgM11nenXRTx9L1yiJKmkf9dfX7NaMKb1pX",
      "type": "EcdsaSecp256k1VerificationKey2019",
      "controller": "did:xmp:123",
      "publicKeyBase58": "d5cW2R53NHTTkv7EQSYR8YxaKx7MVCcchjmK5EgCNXxo",
    }
  ],
  "service": [{
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21#showexample",
    "type": "ExampleService",
    "serviceEndpoint": "https://example.com/endpoint/1928374657"
  }]
}
```


Abb. 2 Beziehung zwischen DID, DID-Dokument (mit JSON-LD Repräsentation), DLT und Entität

Die jeweiligen DID-Methoden definieren, wie eine DID im Netzwerk registriert, aufgelöst, aktualisiert und widerrufen wird. Schon heute gibt es DID-Methoden die Bitcoin und Ethereum als vertrauenswürdiges Datenregister verwenden. Aufgrund der dezentralen Speicherung des Public Keys als Verifizierungsschlüssel in einem DID-Dokument kann der Inhaber bei Verbindungsaufbau seinen Key direkt an den Kommunikationspartner übermitteln, ohne dass eine zentrale Einheit benötigt wird (Tobin 2018). Wegen der Vielzahl dieser Methoden ist auf Implementierungsebene keine Interoperabilität bezüglich der Auflösung eines DIDs zu einem DID-Dokument – also der Leseoperation der jeweiligen DID-Methoden – gewährleistet. Zur Lösung dieses Problems ist von der Decentralized Identity Foundation (DIF) ein sogenannter Universal Resolver entwickelt worden (Hardman 2020b). Dieser arbeitet auf der Basis von Treibern und kann für die unterstützten DID-Methoden entsprechende DID-Dokumente bei Eingabe eines DIDs zurückgeben. Dieser universelle Ansatz erleichtert die Adaption von SSI-Ansätzen auf Seiten von Service Providern, da diese die unterstützten DID-Methoden verschiedener Anbieter nicht selbstständig implementieren müssen. Die DIF erhebt keinen Anspruch auf Standardisierung des Konzepts des Universal Resolver, stellt aber die derzeit am weitesten fortgeschrittene Implementierung mit 38 unterstützten von 82 im DID-Methoden-Register gelisteten Methoden bereit (DIF 2020).

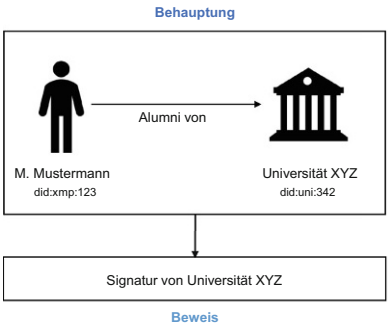
Doch nicht nur der gesicherte Datenaustausch und Datenminimierung schafft dem Nutzer einen starken Schutz seiner Privatsphäre. So wird bei der Entwicklung des SSI-Netzwerks Sovrin die DSGVO als Verordnung für den Datenschutz wird als fester Bestandteil berücksichtigt (The Sovrin Foundation 2020). Bei Sovrin besteht eine Verbindung zwischen Kommunikationspartnern lediglich aus paarweise pseudonymisierten DIDs, alle weiteren Informationen sind Bestandteil von Verifiable Credentials (Reed und Windley 2018). Jeder Nutzer hat die Möglichkeit, pseudonyme DIDs privat zu speichern oder über einen Trust Anchor/Transaction Endorser im zugrundeliegenden Register zu veröffentlichen.

Ein Herausgeber, z. B. eine Hochschule, kann mit seinem veröffentlichten DID öffentlich verifizierbare Verifiable Credentials, z. B. Studentenausweise, ausstellen und signieren. Außerdem dient sie als öffentlicher Zugangspunkt, über den andere Nutzer eine Kontaktaufnahme anfordern können. Ebenfalls sind Verbindungen zu einem Service-Login-Server denkbar. Anschließend verwendet der Nutzer die privaten DIDs für die direkte Kommunikation oder den Austausch von Credentials.

3.1.2 3.1.2 Verifiable Credentials (VC)

Im Zuge der Entwicklung des Self-Sovereign Identity Paradigmas ist der Standard „Verifiable Credentials“ entstanden (Sporny et al. 2019). Vereinfacht gesagt lassen sich damit Aussagen über ein Subjekt in einem kryptografisch gesicherten Format abbilden. Verifiable Credentials können beliebige Datenstrukturen aufnehmen und somit eine Vielzahl verschiedener Anwendungsszenarien unterstützen. (Abb. 3).

Schon im realen Leben weisen die Menschen sich mit unterschiedlichen Dokumenten aus. Der Personalausweis oder die Firmen-ID-Karte werden verwendet, um die persönliche Identität nachzuweisen, der Führerschein dient als Nachweis, dass die Identität in der Lage ist, ein Kraftfahrzeug zu bedienen, und Zeugnisse




```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://htwexample.edu/credentials/1234",
  "type": ["VerifiableCredential", "AlumniCredential"],
  "issuer": "https://example.edu/hochschulen/sachsen/12345",
  "issuanceDate": "2020-01-01T19:73:24Z",
  "credentialSubject": {
    "id": "did:xmp:123",
    "alumniOf": {
      "id": "did:uni342",
      "name": "Universität XYZ"
    }
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2017-06-18T21:19:10Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://example.edu/issuers/keys/1",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmF...PAYuNzVBAh4vGHSrQyHUdBBPM"
  }
}
```


Abb. 3 Anwendungsbeispiel Verifiable Credential inkl. JSON-LD Repräsentation

beglaubigen den Bildungsabschluss. VCs adaptieren dieses Prinzip und lassen sich in drei konstituierende Teile gliedern. Im Zentrum eines VCs stehen eine oder mehrere Behauptungen bezüglich des Subjekts des VCs. Bei der zweiten Komponente handelt es sich um einen Graphen von Metadaten mit Herausgeber, Typ, Datum und weiteren Datenfeldern, welche das VC beschreiben. Diese können vom Herausgeber signiert sein, um ein erhöhtes Maß an Vertrauen zu gewährleisten. Sowohl der Herausgeber als auch das Subjekt des VCs können mithilfe von DIDs referenziert werden. Dies erlaubt eine eindeutige Identifikation dieser Rollen. Die ersten beiden Komponenten bilden einen in sich geschlossenen Graphen, zu welchem die dritte Komponente des digitalen Beweises zugeordnet wird. Dieser stellt sicher, dass die zugehörige Behauptung tatsächlich vom Herausgeber des VCs aufgestellt wurde. In der Regel werden hierfür gängige Signaturverfahren verwendet.

Mit VCs lassen sich also Behauptungen bezüglich bestimmter Subjekte aufstellen, wobei die Integrität des Inhalts, des Herausgebers und des Subjekts kryptografisch sicher nachgewiesen werden können. Die vorigen Beschreibungen liefern bereits einen Einblick in zwei der drei Rollen innerhalb eines Nachweisaustausches: den Herausgeber eines VCs sowie dessen Subjekt. In der Regel handelt es sich beim Subjekt eines VCs auch um den Inhaber, welcher die Kontrolle über das VC ausübt und es in Interaktionen verwendet. Um die Behauptungen innerhalb des VCs in Interaktionen geltend zu machen, muss die Akzeptanzstelle diese mit geeigneten Mitteln überprüfen. Es wird davon ausgegangen, dass die Akzeptanzstelle dem Herausgeber des VCs und damit der Korrektheit seiner Behauptungen gegenüber Vertrauen aufbringt. Dabei erhält die Akzeptanzstelle nicht das VC selbst, sondern eine als „Verifiable Presentation“ bezeichnet Datenstruktur, die für die Interaktion benötigten Daten aus verschiedenen VCs enthält.

Eine Verifiable Presentation beinhaltet neben dem ursprünglichen VC weitere Metadaten wie Nutzungsbedingungen und einen weiteren Beweis, welcher die Datenstruktur absichert. Ein Spezialfall dieses Beweises ist der sogenannte Zero-Knowledge-Proof. Dieser ermöglicht den mathematisch-abgesicherten Nachweis über den Besitz bestimmter Informationen, ohne die zugrundeliegenden Daten selbst vorweisen zu müssen. Das Vorweisen mittels Zero-Knowledge-Proofs abgesicherter Prä-

sentationen in Verbindung mit DIDs stellt die konsequente Erfüllung der Prinzipien von SSI dar. Auf diese Weise bleiben nicht nur die kontextspezifischen Identifikatoren im persönlichen Kontrollbereich des Subjekts, sondern auch die zugehörigen Attribute, welche in ihrer Gesamtheit die eigene digitale Identität ausmachen.

3.1.3 DIDcomm

DIDs stellen einen ersten Schritt in die Etablierung eines dezentralen, von den Nutzern kontrollierten Identitätssystems dar. Die zweite Komponente des identitätsbezogenen Metasystems stellt daher ein auf DIDs basierendes Kommunikationsprotokoll dar. In Zusammenarbeit mit dem Hyperledger-Projekt Aries arbeitet die DIF unter der Bezeichnung „DIDComm Messaging“ an der Erstellung eines Standards für ein solches Protokoll (Hardman 2020b). Dieses stellt eine wichtige Komponente in der Architektur sogenannter Agenten dar. Bei Agenten handelt es sich um Software, welche den Inhabern von Identitäten beim Management ebendieser und den Beziehungen zu anderen Identitätsinhabern unterstützen. Weiterhin können Agenten im Namen der Inhaber Interaktionen durchführen. Da Agenten üblicherweise auf Geräten mit beschränkter Netzwerkverbindung wie Smartphones ausgeführt werden, bestehen in den Mechanismen des Nachrichtenversands bei DIDcomm Unterschiede zu herkömmlicher Kommunikation im Web. Der Austausch von Nachrichten bei DIDcomm Messaging basiert auf Asynchronität und Simplexbetrieb. Dies bedeutet, dass eine Antwortnachricht weder sofort noch über denselben Kanal wie die Ausgangsnachricht übermittelt werden muss. Der Standard erhebt den Anspruch die Grundlage aller SSI-basierten Interaktionen zu sein. Daher soll er unabhängig vom in der Implementierung gewählten Transportprotokoll eingesetzt werden können (Hardman 2020b).

3.1.4 Vertrauenswürdiges Datenregister

Zur Registrierung, Aktualisierung, Widerrufung und Beschreibung von Verifizierungsverfahren und Schemata von Decentralized Identifiers und Verifiable Credentials werden, wie oben beschrieben, häufig dezentrale Datenregister verwendet. Die kontemporäre Literatur zu SSI vermittelt oftmals den Eindruck, dass Distributed-Ledger-Technologien wie Blockchains daher ein notwendiger Bestandteil der neuen Lösungen sind. Tatsächlich stellen diese aber nur eine Möglichkeit der Umsetzung dar und werden zum Beispiel für reine Peer-to-Peer Verbindungen nicht benötigt, da in diesem Fall die Verwaltung und er Austausch der DIDs und VCs direkt von den Wallets der Kommunikationspartner vorgenommen werden. Sobald jedoch VCs, die von Dritten herausgegeben wurden, verifiziert werden müssen, benötigen die Akzeptanzstellen einen Vertrauensanker zur Überprüfung. Dabei dienen die Datenregister als Speicher für die öffentliche DID des Herausgebers, den Informationen zum Verifizierungsmechanismen zur Überprüfung der VCs, den VC-Schemata zur Beschreibung der VC-Attribute und den Gültigkeitsdefinitionen. An dieser Stelle können neben Blockchains auch andere unveränderbare Datenspeicher eingesetzt werden. Damit ein hohes Vertrauensniveau erreicht werden kann, müssen diese Datenregister zum einen ähnlich der DNS-Resolver zur Auflösung von IP-Adressen

eine hohe Verfügbarkeit und Skalierbarkeit vorweisen und zum anderen resistent gegen Manipulationsversuche sein (Ferdous et al. 2019). Daher stellen Blockchains aktuell eine häufig verwendete technologische Implementierung für ein vertrauenswürdiges Datenregister dar und werden dementsprechend oft in Verbindung mit SSI genutzt.

3.2 Anwendung der Standards in einem Softwaresystem für SSI

Das Zusammenspiel der Standards DID, VC und DIDcomm ermöglicht die Realisierung von SSI-Lösungen. Weltweit gibt es verschiedene Ansätze zur Umsetzung des Self-Sovereign Identity Paradigmas. So wurde das Sovrin Netzwerk von Grund auf neu entwickelt und verwendet eine neue Netzwerkinfrastruktur speziell für digitale Identitäten. Andere Lösungen, wie der DIF Sidetree oder Blockstack, bauen auf bestehende Infrastrukturen auf. Für die Schaffung von Interoperabilität von SSI-Lösungen müssen drei wesentliche Festlegungen getroffen werden (Reed und Windley 2018):

- Format für kryptografisch signierte Dokumente
- Verfahren zur Überprüfung kryptografisch signierter Dokumente
- Kommunikationskanal als Ersatz für die physische Anwesenheit

Alle identitätsbezogenen Informationen, wie Name, Besitz, Alter, etc., werden in Verifiable Credentials gespeichert. Diese Dokumente kann jeder Inhaber nach der Ausstellung in ein Wallet, in der Cloud oder auf ein privates Speichermedium unabhängig von einem zentralen ID-Provider speichern (Reed und Windley 2018). Der Inhaber kann mit einer Reihe von Credentials eine Beweiskette aufbauen, um sich damit zu identifizieren oder sein Eigentum nachzuweisen (Abb. 1). Die Vertrauenswürdigkeit hängt davon ab, welches Maß an Vertrauen die Akzeptanzstelle dem Herausgeber entgegenbringt. Folglich stellt sich die Frage: *Wie kann eine Akzeptanzstelle einen solchen Nachweis verifizieren?*

Dieses Problem wird durch die Decentralized Identifiers mit den zugehörigen DID-Dokumenten gelöst. Sie dienen zum einen zur Identifizierung einer Identität und fungieren zum anderen als Ressourcenbezeichner für die angesprochenen DID-Dokumente. Beide sind unabhängig von ID-Providern und unterliegen der vollen Kontrolle des Erstellers. Durch die Verbindungen zwischen DIDs und die Beschreibung der Besitztümer, Authentifizierungs- und Autorisierungsdaten in Verifiable Credentials ist unter anderem eine Umleitung einer Public-DID zu einem Cloud-Agent oder eine direkte Peer-to-Peer-Verbindung ohne Zwischenhändler möglich. Wenn zum Beispiel ein Nutzer seine Eigentumsverhältnisse gegenüber Dritten nachweisen soll, so können diese die Echtheit der vom Nutzer bereitgestellten Credentials nicht verifizieren. Externe Speicher können die benötigten Informationen zur Verifizierung bereitstellen. Wie an der Rolle der Identity Provider im föderierten Modell gezeigt wurde, können zentralisierte Systeme keine Unabhängigkeit bei der Identitätsverwaltung herstellen. Daher werden in SSI-Systemen auf der untersten Ebene Identitätsregister verwendet (vgl. Abb. 1), um dezentralisierte Identifikatoren zu registrieren. Für diese werden in den meisten Implementierungen Distributed-Ledger-Technologie (DLT)-Ansätze verwendet (van Bokkem et al. 2019). Die Unveränder-

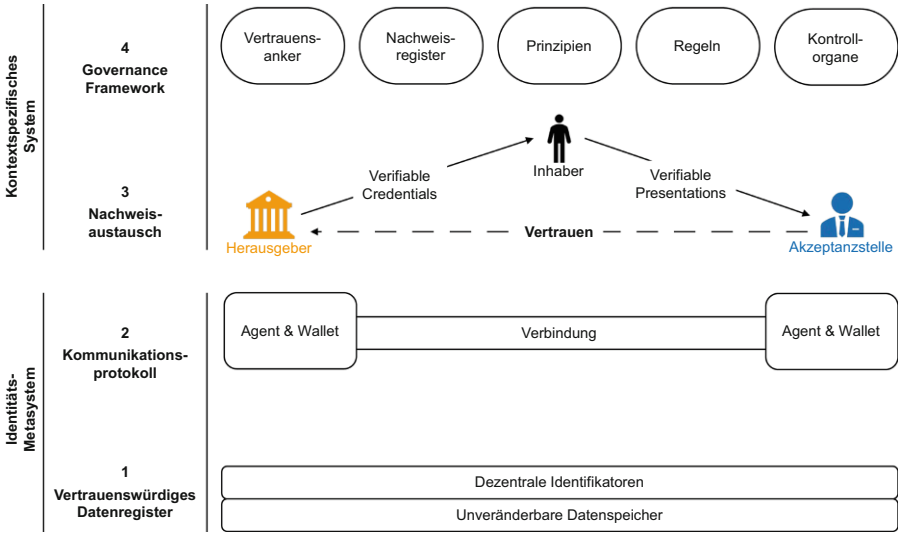


Abb. 4 Technisches Gesamtkonzept als Vier-Ebenen-Modell, modifiziert nach (Windley 2020)

lichkeit (Immutabilität) der Transaktionen bei DLT-basierten Registern erlaubt die Etablierung einer gemeinsamen Vertrauensbasis, ohne eine zentrale Autorität oder Behörde einsetzen zu müssen (Steele und Sporny 2021). Darauf folgt die Schicht der Kommunikationsprotokolle, welche einen grundlegenden dezentralisierten Austausch von Nachrichten erlauben. Dazu lässt sich auch der standardisierte Austausch überprüfbarer Nachweise (VCs) zählen, welcher im Kern des SSI-Ökosystems steht. Innerhalb der Schicht des Nachweisaustauschs werden kontextspezifische Identitätssysteme definiert, welche etwa in Geschäftsnetzwerken oder in Interaktion mit staatlichen Behörden entstehen (Abb. 4).

Zu jedem SSI-Ökosystem gehört ein Governance Framework, das Standard-Prozesse und Vorgaben wie Datenmodelle im jeweiligen Kontext regelt. Dabei müssen sich die Beteiligten im Vorfeld des Systemaufbaus auf eines solches Regelwerk einigen, um reibungslose Interaktionen zu gewährleisten. Während die Verwendung kryptografisch abgesicherter Informationen Vertrauen herstellen kann, sind Rollenverteilungen und die Festlegung bestimmter Geschäftsregeln Aktivitäten, welche auch unter dem Paradigma SSI in jedem Kontext separat abgestimmt werden müssen. Ein wichtiger Punkt zur gegenseitigen Abstimmung auf der Ebene der Governance sind klar definierte Prozesse, denn die Interoperabilität von Identitäten allein genügt nicht, um interoperable Geschäftsprozesse zu realisieren. Die „Trust Over IP Foundation“ erarbeitet eine Framework-Schablone, die bei der Entwicklung anderer Self-Sovereign-Identity-Systeme helfen soll, unterschiedliche Aspekte für die Beeinflussung in Technologie und Rechtesystem zu beachten. Das Framework ist dabei in vier Ebenen (Layer Stack) unterteilt. Die zugrundeliegenden Richtlinien der Ebenen können sich dabei je nach Nutzung, Geschäftsmodell, Rechtsmodell und technischer Architektur von denen einer Organisation oder zwischen Organisationen unterscheiden (Davie et al. 2019; Hardman 2020a).

3.3 Aktuelle Aktivitäten, Projekte und Initiativen

3.3.1 Bestehende Dienste, Infrastrukturen und Komponenten

Auch wenn noch nicht alle Standards vollständig ausformuliert sind, gibt es bereits Dienste und Komponenten zur Umsetzung von SSI. Erste funktionsfähige Identity-Netzwerke werden z. B. von Sovrin und uPort bereitgestellt. SSI-Wallet-Entwickler wie Jolocom zeigen mit ihrer Avalon Testumgebung wie SSI in Zukunft aussehen könnte (Jolocom 2019). Zusätzlich konnten Interessierte im September 2019 an der Präsentation von Telekom Xride teilnehmen, die auf ein speziell entwickeltes Blockchain-Betriebssystem für IoT-Ökosysteme aufbaut (Habel 2019). Mit der Bundesdruckerei entstand im Januar 2020 die erste staatliche SSI-Demo-Umgebung (Jolocom 2020). Auch uPort zeigt mit der Demo-Anwendung zu ihrer Wallet was bereits mit dem entstandenen Netzwerk möglich ist. Wallets der eSatus AG, der Lissi Initiative oder Evernym (Connect.Me) unterstützen das Sovrin Netzwerk und können zur Entwicklung eigener Use Cases eingesetzt werden. Zum Beispiel stellt die Global Legal Entity Identifier Foundation (GLEIF) die ersten Legal Entity Identifier (LEIs) in Form von Verifiable Credentials aus (Sopek 2020) und die eSatus AG schlägt mit ihrer SeLF Plattform eine Brücke zwischen den klassischen Enterprise Identity- and Access Management und der SSI-Verwaltung (ESATUS AG 2019). Blockchain-Entwickler und Knotenbetreiber, wie unter anderen Evan, Hyperledger, Multichain, SAP oder die Deutsche Telekom, beteiligen sich an verschiedenen Projekten und können damit ihre Erfahrungen weitergeben sowie neuen Projekten zum Erfolg verhelfen.

3.3.2 Aktivitäten der Europäischen Union

Aufgrund des wachsenden Interesses an einer dezentralen Datenverwaltung haben sich 29 europäische Staaten zu einer Blockchain-Partnerschaft zusammengeschlossen und die „European Blockchain Services Infrastructure“ (EBSI) gegründet. Ziel ist es, EU-weit grenzüberschreitende Dienstleistungen auf Basis von Blockchains bereitzustellen. Zusammen mit Self-Sovereign Identity ist es möglich, rechtsverbindliche digitale Dienstleistungen zwischen EU-Bürgern, EU-Institutionen und nationalen Behörden anzubieten (CEF Digital 2020b). 2019 starteten die Next Generation Internet Initiative und die niederländische Organisation für Angewandte Naturwissenschaftliche Forschung (TNO) das „eSSIF-Lab“ Projekt zur Förderung und Spezifizierung von europäischen Self-Sovereign-Identity-Lösungen (van Deventer 2019). In dieser Zusammenarbeit laufen derzeit mehrere Projekte, wie die Unterstützung einer SSI-eID-Lösung (vgl. Domingo 2020) und die eIDAS Bridge.

Die 2014 verabschiedete eIDAS-Verordnung reduziert eine Vielzahl analoger und bürokratischer Hemmnisse, damit Behörden, Gewerbe und Verbraucher einen besseren Zugang zum europäischen Markt erhalten (BDR 2018). Die eIDAS Bridge ist hierbei nicht direkt im Self-Sovereign-Identity-Ökosystem verwoben. Das ermöglicht zum einen eine flexible Anwendung und Erweiterung der eSealing/eSignature-Funktionen, zum anderen sind Wallet-Anbieter nicht gezwungen, vollständige eIDAS-konforme digitale Brieftaschen zu entwickeln. Folglich werden weitere bü-

rokratische Hürden abgebaut. Wo früher nahezu jede interessierte juristische Entität die eIDAS-Notifizierung durchführen musste, soll die eIDAS Bridge für jeden zugänglich sein, auch wenn weiterhin nur Trusted Service Provider[1] die Berechtigung zu eSignature-Funktionen haben. Die EU-Kommission empfiehlt dementsprechend eine Bereitstellung des Qualified Electronic Certificate Public Keys in einer öffentlichen DID, sowie die Ausstellung einzelner W3C konformer Verifiable Credentials. Die eIDAS Bridge nimmt selbst einen Hash oder ein ganzes Verifiable Credential entgegen (Vila 2020).

Die EBSI Blockchain und die eSealing/eSignature-Funktion der eIDAS Bridge ermöglichen es, Verifiable Credentials grenzübergreifend rechtskonform zu signieren. Behörden können somit eIDs als Verifiable Credential verteilen, notarielle Beglaubigungen speichern und ausstellen, oder Informationen sicher austauschen (CEF Digital 2020a).

3.3.3 Aktivitäten in Deutschland

Im Jahr 2019 startete das Bundesministerium für Wirtschaft und Energie (BMWi) im Rahmen des Förderrahmens „Entwicklung digitaler Technologien" den Innovationswettbewerb „Sichere Digitale Identitäten" (BMWi 25.01.2021). Ziel war dabei, die in Deutschland vorhandenen Kompetenzen zu bündeln und innovative Ansätze für den Umgang mit digitalen Identitäten voranzubringen. Dabei wurde explizit auf einen möglichst universellen Einsatz geachtet: Nicht nur sollten verschiedene Anwendungsdomänen wie Kommunalverwaltung, Logistik, Banken und Gesundheitswesen betrachtet werden, sondern neben Personen auch Organisationen und Objekte mit ihren Identitäten in digitalen Interaktionen berücksichtigt werden. Insgesamt bewarben sich elf Konsortien in der Ende 2020 beendeten Wettbewerbsphase mit ihren Umsetzungskonzepten. Von diesen wurden vier ausgewählt und zur Antragstellung aufgefordert. Die Umsetzung über einen Zeitraum von bis zu drei Jahren verspricht die Entstehung interessanter Schaufenster in verschiedenen Regionen sowie die Schaffung von Grundlagen für die Interoperabilität von ID-Lösungen unterschiedlicher Modelle. Damit könnte auch der Self-Sovereign Identity der Weg für den breitenwirksamen Einsatz gebahnt werden.

4 Hindernisse für den Einsatz

Die konzeptionellen Vorteile als auch die weltweiten Standardisierungs- und Entwicklungsaktivitäten zur Etablierung von Self-Sovereign Identity unterstreichen die Relevanz dieses Ansatzes. Dennoch bleibt festzustellen, dass die Verbreitung und praktische Nutzung bislang sehr gering sind. In diesem Abschnitt werden einige der Schwierigkeiten bei der Etablierung von dezentralen Lösungen vorgestellt.

[1] Ein Trusted Service Provider ist ein eIDAS-notifizierter Aussteller der EU für eSealing/eSignature-Funktion.

4.1 Organisatorische Hürden

Föderierte und isolierte Identitäten mit den dazugehörigen Identitätsmanagementsystemen waren bislang die Basis für neue Soft- und Hardwareprodukte. Durch Self-Sovereign Identity werden nicht nur neue Technologien, sondern auch ein komplett neues Paradigma zur Datenverwaltung eingeführt. Durch die Umorientierung in der Datenverwaltung und die fehlenden Erfahrungen benötigen die Entwickler, Herausgeber, Inhaber und Akzeptanzstellen mehr Zeit, um neue Produkte als auch neue Geschäftsmodelle auf den Markt zu bringen oder diese zu akzeptieren. Entsprechend entstehen daher bei der Planung an dieser Stelle oftmals Diskussionen über fehlende technische Standards oder regulatorische Hürden, wie die DSGVO und eIDAS (Doerk et al. 2020).

Im Kern ist es erforderlich, dass grundlegend neue Geschäftskonzepte, Prozesse sowie Kooperationen entstehen. Im direkten Vergleich mit dem Aufwand, den Organisationen benötigen, um eine dezentrale Verwaltung umzusetzen, könnten einige Marktteilnehmer zurückschrecken. Denn alle Beteiligten müssen die Einsatzbereiche für eine Dezentralisierung individuell prüfen. Hierbei gilt es zunächst zu klären, welches Problem von SSI gelöst und welcher Mehrwert erreicht werden soll. Des Weiteren sollten Organisationen die Verantwortung des Betriebs der Blockchain-Knoten an mehrere Netzteilnehmer verteilen. Was bei großen Konzernen ein geringeres Problem darstellt, ist bei kleinen oder mittelständischen Unternehmen schwierig umsetzbar. Konkurrierende Unternehmen dürfen keine Möglichkeit erhalten, die Daten zu manipulieren oder Transaktionen zu behindern. Damit stellt sich die Frage: Wohin einzelne Knoten verteilen und wer ist für die Objektregistrierung verantwortlich? Zudem können für Blockchain-Konsortien länderübergreifende Einrichtungsprozesse als Hürden mit sich bringen. Folglich müssen auch außerhalb von Softwareentwicklungen neue Partnerschaften entstehen, die Verwaltungsarbeiten übernehmen. Schlussendlich müssen Entwickler ebenso Konzepte für Prozesse zur Verbesserung der Selbstverantwortlichkeit der Nutzer, Bedienungsfreundlichkeit und Skalierbarkeit schaffen.

4.2 Unklare Mehrwerte

Obwohl Blockchain-Entwickler wie Hyperledger oder MultiChain einige Problematiken reduziert haben und Intermediäre den Prozess der Konsensbildung für eine gemeinsame Governance beschleunigen und gegebenenfalls die Verwaltung der Knoten übernehmen, sprechen sowohl die GS1 Germany als auch Greenspan davon, dass Organisationen immer noch stark zur Dezentralisierung motiviert werden müssen. Bisher waren die beiden wesentlichen Triebkräfte das Misstrauen gegenüber anderen Organisationen und die Notwendigkeit zur Umsetzung von Regularien (Compliance). Zum einen möchte niemand von einer zentralen Behörde abhängig sein oder seine Daten einem Konkurrenten anvertrauen und zum anderen erfordern gerade globale Standards oder Regularien eine effektive Zusammenarbeit. (Greenspan 13.05.2019; Uhde 2018). Die Regelung der MDR2017/745 wird sowohl in Europa als auch in ähnlicher Weise in den Vereinigten Staaten umgesetzt. Jedoch übernehmen in der EU zentrale Behörden die Überwachung, in den USA nicht. Die

Food and Drug Administration (FDA) legt lediglich die Regularien fest, für die jeweilige Umsetzung sind anschließende die Konzerne auf sich gestellt. Da niemand die eigenen Daten einem Konkurrenten anvertrauen möchte und diese Regularien wiederum einen gemeinsamen Mittelweg erfordern, müssen sie eine ähnliche dezentrale Lösung entwickeln (Greenspan 13.05.2019).

4.3 Technische Hürden

In Literatur finden sich vor allem technische Hürden. Allen voran die unzureichende Netzinfrastruktur im Bereich Internet und Mobilfunk. In einer dezentralen Verwaltung benötigen alle Nutzer Mobilfunkgeräte mit einer Anbindung an das Internet. In Europa ist jedoch die Netzabdeckung nicht flächendeckend. Während Unternehmen ihren Mitarbeitern die Möglichkeit bieten, die Geräte in das WLAN-Netz einzubinden, sind z. B. die Fahrer der Logistikunternehmen auf den Mobilfunk angewiesen. Aus technischer Sicht steht einem Gastzugang in ein WLAN-Netz nichts im Weg, grundsätzlich verbieten viele Unternehmen aus Sicherheitsgründen externe Mobilgeräte oder die notwendigen Freigabeprozeduren sind im Vergleich zum Nutzen zu aufwändig (Freda 2019).

Wallets müssen hohe Sicherheitsanforderungen erfüllen, damit Angreifer keine Möglichkeit erhalten, unbemerkt Agents, Off-Chain Storages oder Blockchains zu übernehmen. Gleichzeitig müssen sie dem Nutzer komfortabel Zugänge zu unterschiedlichen Blockchain-Netzwerken bieten. Auch die flexible Verwaltung von Credentials und Präsentationen sowie deren Inhalten ist ein essenzieller Bestandteil. Dieser Umstand geht einher mit einem weiteren oft genannten Punkt, dem partiellen Kontrollverlust. Nutzer sind ab diesem Zeitpunkt selbst für die Daten verantwortlich und müssen technologisch sowie pädagogisch sensibilisiert werden. Aktuelle Demo-Wallets bieten oftmals nur eine Akzeptieren-Abbruch-Funktion. Die ist zwar einfach zu verstehen, jedoch vermittelt sie dem Nutzer nicht das Gefühl von Kontrolle. Folglich ist diese Funktion eher vergleichbar mit den Lizenzbestimmungen von Software oder Cookie-Informationen und baut nicht genügend Vertrauen auf.

Eine weitere technische Hürde ist die Datenverfügbarkeit. Organisationen sind gewohnt, beliebig auf Informationen zuzugreifen. Mit einer dezentralen Aufbewahrung samt Erlaubniseinforderung werden die gewohnten Arbeitsprozesse unterbunden. Dies führt vor allem zum Problem, wenn sich der Service Provider in einer anderen Zeitzone befindet als der Dateninhaber. Hierbei können Identity Hubs oder entsprechend konfigurierte Agents Abhilfe schaffen, um auf Basis von Regeln selbständig Freigaben zu erteilen.

4.4 Mangelndes Bewusstsein

Eine weitere Hürde ist das öffentliche Marketing. Self-Sovereign Identity soll dem Nutzer die Kontrolle über seine Daten wiedergeben. In Kombination mit der Komplexität der Blockchains ist es ratsam, diese Nutzer frühzeitig in derartige Projekte zu integrieren (Wunsch 2018). Beispielsweise ermöglicht die CEF Digital es zwar allen Mitgliedsländern des European Blockchain Partnerships, an verschiedenen Tests zur EBSI teilzunehmen, jedoch bewerben die EU oder die jeweiligen Mitgliedsländer

die Plattform nicht (CEF Digital 2020c). Europa sollte seine Bemühungen zur eigenen digitalen Souveränität bewerben und die Erkenntnisse somit auch für andere Interessengruppen, wie für Journalisten und die breite Öffentlichkeit, zugänglich machen (Courcelas et al. 2020). In der Vergangenheit berichteten öffentlich-rechtliche Medien von den Bestrebungen aus der Privatwirtschaft. Die Dokumentarfilme stellen die Vorteile der Blockchain-Technologie nur einseitig dar (Prinzler 2019). Die Autoren behandeln darin oftmals nur überblicksmäßig den wirtschaftlichen Nutzen, während die Vorteile für die Nutzer oder Self-Sovereign Identity als Thematik keine Beachtung fanden. Eine umfangreiche Berichterstattung kann die Vorurteile in der Öffentlichkeit reduzieren und infolgedessen die Akzeptanz des neuen Identitätsmanagements fördern.

5 Diskussion

Vor dem Hintergrund der hohen Bedeutung digitaler Identitäten für die digitale Transformation von Wirtschaft und Gesellschaft sollen die gewonnenen Erkenntnisse in diesem Abschnitt aus verschiedenen Perspektiven reflektiert werden. Dabei wird insbesondere auf die Auswirkung von Self-Sovereign Identity auf die bislang vorherrschenden Modelle von isolierten und föderierten Identitäten eingegangen.

5.1 Sicherheit

Wie in Abschn. 2.2 gezeigt, sind föderierte Identitäten weit verbreitet und in vielen Organisationen fest verankert. Vor allem die populärsten werden jedoch zunehmend zum Angriffsziel für Cyber-Kriminelle (Pohlmann 2019b; Bleich 15.02.2019), die mit den gestohlenen Identitätsdaten u. a. im Darknet Handel betreiben (Ries 18.10.2019). Hierdurch steigen die Kosten für die Systemsicherheit, ohne einen länger andauernden Mehrwert zu erhalten. Des Weiteren müssen sie regelmäßig die Nutzer zwingen, sich neue schwierigere Passwörter zu merken. Mit der eID wollte die Europäische Union eine echte Alternative schaffen. Hohe Onboarding-Hürden, ungleichmäßige Ausübung verschiedener Regularien in den Mitgliedsstaaten und eine schlechte Usability machten diese Hoffnungen jedoch weitgehend zunichte.

Der Ansatz von Self-Sovereign Identity hat einen neuen Impuls in diese Problematik gebracht. So erlaubt der in diesem Umfeld entstandene W3C-Standard DID den Aufbau einer Peer-to-Peer-Verbindung, die Kommunikations- und die Systemsicherheit zwischen beiden Partnern nachhaltig verbessert. Aber auch andere Inhalte, wie eine Governance, könnten dazu beitragen, dass Nutzer ein größeres Vertrauen zu Service Provider aufbauen. Sollte es dennoch zu illegalen Netzwerkzugriffen kommen, so ermöglichen die neuen Standards ein weiteres Vordringen zu verhindern. Selbst wenn Angreifer an Teilinformationen gelangen oder sich Zugriff mit DID-Spoofing verschaffen wollen, können sie keinen nennenswerten Schaden anrichten. Die DID-to-DID-Kommunikation mit den zugehörigen Public Keys sorgt bereits für ein hohes Sicherheitsniveau, welches durch spezielle Definitionen, mehrere Credentials oder verschlüsselte Inhalte verstärkt werden kann. Überdies ist es

unwahrscheinlich, dass die meisten Nutzer einen Status als Trust Anchor besitzen und somit keine Credentials über den privaten Gebrauch hinaus ausstellen können.

5.2 Datensouveränität

Weiterhin führt das föderierte ID-Management zu einem Verdrängungswettbewerb durch die großen Plattformen, die durch Netzwerkeffekte ihre Marktmacht ausbauen und Nutzer in zunehmende Abhängigkeiten bringen. Dies trifft insbesondere dann zu, wenn sie wie Google, Microsoft, Apple oder Facebook keine reinen ID-Provider sind, sondern eigene Inhalte und Services anbieten. Damit sind Nutzer gezwungen, digitale Identitäten dieser Provider zu nutzen und begeben sich damit in deren Abhängigkeit, wenn sie ihre IDs bei anderen Services verwenden. Ein aktuelles Beispiel ist die Blockade von Apple für die Nutzung seiner ID beim Spieleanbieter Epic Games (Kwan 10.09.2020). Mit einer dezentralen Verwaltung in Verifiable Credentials könnte Apple zwar immer noch den Zugang zu den Spielen sperren, jedoch hätte Epic Games einen größeren Handlungsspielraum, um seinen Kunden alternative Lösungen anzubieten. So kann das Unternehmen weiterhin den Credentials vertrauen, auch wenn sie von Apple als „nicht mehr vertrauenswürdig“ markiert wurden. Im Regelfall müssten sich jetzt staatliche Stellen mit der Problematik auseinandersetzen und neue Gesetze schaffen. Bei einer korrekten Anwendung von Self-Sovereign Identity sind jedoch keinerlei Änderungen in Gesetzestexten erforderlich. Folglich sollte es keine regulatorischen Hürden geben neue nutzerfreundliche Services anzubieten.

Ferner kann SSI zu einer Demokratisierung der digitalen Identitäten beitragen, da die Identifier (DIDs) sowie die ausgetauschten Nachweise (VCs) unter der Kontrolle des Nutzers stehen. Er ist damit in der Lage, seine Identität gegenüber Dritten unabhängig von staatlichen Stellen und Wirtschaftsunternehmen nachzuweisen. Die Übermittlung von Daten an Dritte unterliegt ebenso ausschließlich der Kontrolle des Nutzers. Die damit entstehende Datensouveränität realisiert das Prinzip der informationellen Selbstbestimmung, die Datenschutzgesetzgebungen zugrunde liegt. Auch für die Betreiber von Onlinediensten und Anwendungen (Service Provider) bringt dieser Ansatz Vorteile. Sie müssen sich nun nicht mehr von einem oder mehreren spezifischen ID-Providern abhängig machen, sondern müssen nur den Herausgebern von ID-Merkmalen vertrauen. Mit welcher Software ein Nutzer seine Identitätsmerkmale durch VCs zugänglich macht, ist unerheblich. Damit kann eine größere Vielfalt kompatibler Dienste in Koexistenz bestehen.

6 Zusammenfassung

Zusammengefasst lässt sich feststellen, dass SSI und seine damit verbundenen Standards trotz ihres frühen Entwicklungsstadiums zweifellos das Potenzial besitzen, die Erzeugung, Verwaltung und Nutzung digitaler Identitäten zu revolutionieren. Verifiable Credentials sind für eine Vielzahl von Situationen einsetzbar, um kryptografisch gesicherte Daten zu übermitteln. Mit den neuen Standards können Organisationen den Verwaltungsaufwand signifikant reduzieren und zugleich präzise zeitlich be-

grenzte organisationsübergreifende Logins ermöglichen. Zugleich ermöglicht diese Verwaltung die Auslagerung von IT-Infrastrukturen, was wiederum zur Kostensenkung beiträgt. Darüber hinaus sind Arbeitnehmer in der Lage, den Vorteil zu nutzen, sich und ihre Organisation zu jeder Zeit bei einem Kunden zu authentifizieren. Die Nutzer hingegen erhalten die Kontrolle über ihre digitalen Identitäten zurück, müssen sich keine langen Passwörter merken und entscheiden selbst, welche Daten sie preisgeben. Darüber stellt Self-Sovereign Identity eine nie dagewesene Durchgängigkeit für Identitäten bereit, die für Personen, Organisationen und technische Objekte gleichermaßen angewendet werden kann. Damit ist es in einer Vielzahl von Anwendungsszenarien möglich, einen rechtssicheren digitalen Raum zu schaffen. In diesem können die Vorteile der Digitalisierung genutzt und dabei gleichzeitig die Datensouveränität der Akteure gestärkt werden.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Allen C (2016) The path to self-sovereign identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. Zugegriffen: 15.04.2020

BDR (2018) Die eIDAS-Verordnung – die Basis für ein starkes digitales Europa; Effizientere Prozesse, geringere Kosten, mehr Kundenzufriedenheit. Bundesdruckerei, https://www.bundesdruckerei.de/de/whitepaper/download/859/whitepaper-eIDAS.pdf.pdf. Zugegriffen: 20.08.2020

Bleich H (2019) Identitätsklau nimmt zu und wird raffinierter. https://www.heise.de/hintergrund/Identitaetsklau-nimmt-zu-und-wird-raffinierter-4305746.html. Zugegriffen: 28.01.21

BMI (2020a) Der Personalausweis. https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/der-personalausweis/der-personalausweis-node.html. Zugegriffen: 28. Nov. 2020

BMI (2020b) FAQ – eID Diensteanbieter werden. https://www.personalausweisportal.de/SharedDocs/faqs/Webs/PA/DE/Dienstanbieter-werden/Diensteanbieter-werden.html. Zugegriffen: 26. Nov. 2020

BMWi (2021) Schaufenster Sichere Digitale Identitäten. http://www.schaufenster-sdi.de/. Zugegriffen: 25. Jan. 2021

van Bokkem D, Hageman R, Koning G, Nguyen L, Zarin N (2019) Self-sovereign identity solutions: the necessity of Blockchain technology. arXiv e-prints:arXiv:1904.12816

BSI (2016) Elektronische Identifizierung. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/Elektronische_Identifizierung/Elektronische_Identifizierung_node.html. Zugegriffen: 01.08.2020

BSI (2017) eIDAS-Notifizierung der Online-Ausweisfunktion. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeIdentitaeten/

Online-Ausweisfunktion/eIDAS-Notifizierung/eIDAS-Notifikation_node.html. Zugegriffen: 26.11.2020
Bundesregierung Deutschland (2017) Gesetz zur Förderung des elektronischen Identitätsnachweises. http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2310.pdf. Zugegriffen: 28.11.2020
CEF Digital (2020a) EBSI documentation home. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/EBSI+Documentation+home. Zugegriffen: 29.08.2020
CEF Digital (2020b) European Blockchain Services Infrastructure (EBSI). https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI. Zugegriffen: 20.08.2020
CEF Digital (2020c) Get Started EBSI. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Get+Started+EBSI. Zugegriffen: 12.09.2020
Courcelas L, Lyons T, Timsit K (2020) Conclusions and reflections. In: EU Blockchain Observatory and Forum 2018–2020
Cyphers B, Gebhart G (2019) Behind the one-way mirror: a deep dive into the technology of corporate surveillance. https://www.eff.org/wp/behind-the-one-way-mirror. Zugegriffen: 28.01.2021
Davie M, Gisolfi D, Hardman D, Jordan J, O'Donnell D, Reed D, van Deventer O (2019) Aries RFC 0289: Trust over IP Stack. HYPERLEDGER. https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0289-toip-stack. Zugegriffen: 03.08.2020
DIF (2020) Universal resolver. https://github.com/decentralized-identity/universal-resolver. Zugegriffen: 27.11.2020
Doerk A, Hansen P, Jürgens G, Kaminski M, Kubach M, Terbu O (2020) Self Sovereign Identity Use Cases – von der Vision in die Praxis. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., https://www.bitkom.org/Bitkom/Publikationen/Self-Sovereign-Identity-Use-Cases. Zugegriffen: 30.07.2020
Domingo IA (2020) SSI eIDAS legal report; how eIDAS can legally support digital identity and trustworthy DLT-based transactions in the digital single market. https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf. Zugegriffen: 28.08.2020
ESATUS AG (2019) Identity & Access Management (IAM) – Realisiert mit Self-Sovereign Identity (SSI). https://esatus.com/files/whitepapers/Whitepaper-IAM-realisiert-mit-SSI-201908.pdf. Zugegriffen: 18.08.2020
Ferdous MS, Chowdhury F, Alassafi MO (2019) In search of self-sovereign identity leveraging blockchain technology. IEEE Access 7:103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173
Freda D (2019) Am seidenen Faden unseres Digitalisierungsniveaus. GS1 Innovation. https://www.gs1-germany.de/innovation/blockchain-blog/peer-to-peer-netzabdeckung-als-show-stopper/. Zugegriffen: 04.08.2020
Greenspan G (2019) Multichain: ten enterprise blockchains. That actually work. Hilton Midtown, New York
Habel P (2019) Xride: Erstes Blockchain-basiertes Elektromobilitätsprojekt seiner Art. https://www.telekom.com/de/medien/medieninformationen/detail/xride-erstes-blockchain-basiertes-elektromobilitaetsprojekt-seiner-art-580924. Zugegriffen: 12.09.2020
Hardman D (2020a) Aries RFC 0430: machine-readable governance frameworks. Trust Over IP Foundation. https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0430-machine-readable-governance-frameworks. Zugegriffen: 10.08.2020
Hardman D (2020b) DIDComm Messaging specification. Decentralized Identity Foundation. https://identity.foundation/didcomm-messaging/spec/. Zugegriffen: 22.11.2020
Jolocom (2020) Jolocom SSI in Bundesdruckerei's e-government proof of concept. https://jolocom.io/blog/jolocom-self-sovereign-identities-at-work-in-bundesdruckerei-proof-of-concept-for-e-government/. Zugegriffen: 30.11.2020
Jolocom (2019) Test drive your self-sovereign identity – Jolocom. Jolocom, https://stories.jolocom.com/test-drive-your-self-sovereign-identity-9a8b2566aa1b. Zugegriffen: 30.11.2020
Jøsang A, Pope S (2005) User centric identity management. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.1563&rep=rep1&type=pdf. Zugegriffen: 25.11.2020
Kostic S, Heinemann A, Margraf M (2016in) Usability-Untersuchung eines Papierprototypen für eine mobile Online-Ausweisfunktion des Personalausweises. In: Mayr HC, Pinzger M (Hrsg) Informatik 2016. Tagung vom 26.–30. September 2016 in Klagenfurt. Gesellschaft für Informatik e.V., Bonn, S 519–527
Kwan C (2020) Epic Games to lose Apple ID sign on for accounts. ZDNet, https://www.zdnet.com/article/epic-games-to-lose-apple-id-sign-on-for-accounts/. Zugegriffen: 28.11.2020

Mühle A, Grüner A, Gayvoronskaya T, Meinel C (2018) A survey on essential components of a self-sovereign identity. https://arxiv.org/pdf/1807.06346. Zugegriffen: 30.11.2020
Pohlmann N (2019a) Identifikation und Authentifikation. In: Pohlmann N (Hrsg) Cyber-Sicherheit. Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von CyberSicherheitssystemen in der Digitalisierung. Springer, Wiesbaden, S 151–211
Pohlmann N (2019b) Sichtweisen auf die Cyber-Sicherheit. In: Pohlmann N (Hrsg) Cyber-Sicherheit. Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von CyberSicherheitssystemen in der Digitalisierung. Springer, Wiesbaden, S 1–42
Priem B, Leenes R, Kosta E, Kuczerawy A (2011) The identity landscape. In: Camenisch J, Leenes R, Sommer D (Hrsg) Digital privacy. PRIME—privacy and identity management for Europe. Springer, Berlin, S 33–51
Prinzler HL (2019) Internet.Macht.Zukunft: Wie die Vernetzung die Mobilität revolutioniert. https://www.imdb.com/title/tt12993446/. Zugegriffen: 12.09.2020
Reed D, Sporny M, Longley D, Allen C, Grant R, Sabadello M, Holt J (2021) Decentralized identifiers (DIDs). https://www.w3.org/TR/did-core/. Zugegriffen: 18.01.2021
Reed D, Windley P (2018) Sovrin; a protocol and token for self-sovereign identity and decentralized trust. https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf. Zugegriffen: 13.07.2020
Riedel J (2019) Identitäten als Schlüsselfaktor für medienbruchfreie digitale Prozesse. In: Schmid A (Hrsg) Verwaltung, eGovernment und Digitalisierung. Springer, Wiesbaden, S 23–30
Ries U (2019) Studie zu Darknet-Preisen: Daten von Europäern sind teuer. https://www.heise.de/newsticker/meldung/Studie-zu-Darknet-Preisen-Daten-von-Europaeern-sind-teuer-4560072.html. Zugegriffen: 28.01.2021
Sopek M (2020) New services for LEI owners. https://lei.info/portal/new-services-for-lei-owners/. Zugegriffen: 29. Aug. 2020
Sporny M, Longley D, Chadwick D (2019) Verifiable credentials data model 1.0. https://www.w3.org/TR/vc-data-model/#lifecycle-details. Zugegriffen: 13.08.2020
Steele O, Sporny M (2021) DID specification registries—DID methods. https://w3c.github.io/did-spec-registries/#did-methods. Zugegriffen: 18.01.2021
The Sovrin Foundation (2020) Innovation meets compliance; data privacy regulation and distributed ledger technology. https://sovrin.org/wp-content/uploads/GDPR-Paper_V1.pdf. Zugegriffen: 28.01.2021
Tobin A (2018) Sovrin: what goes on the ledger. https://www.evernym.com/wp-content/uploads/2017/07/What-Goes-On-The-Ledger.pdf. Zugegriffen: 13.07.2020
Tsolkas A, Schmidt K (Hrsg) (2017) Rollen und Berechtigungskonzepte. Springer, Wiesbaden
Uhde T (2018) Technologische Erwägungen für den weiterführenden Einsatz. SAP. https://www.gs1-germany.de/index.php?id=5193. Zugegriffen: 4.08.2020
van Deventer O (2019) EU Project eSSIF-Lab, aimed at faster and safer electronic transactions via the internet as well as in real life, open for start-ups and SMEs. https://www.tno.nl/en/about-tno/news/2019/12/essif-lab/. Zugegriffen: 29.08.2020
Vila X (2020) eIDAS Bridge. Use cases and technical specifications. https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI%20eIDAS%20Bridge%20-%20Use%20 cases%20and%20Technical%20Specifications%20v1.pdf. Zugegriffen: 11.08.2020
Windley P (2018) Multi-source and self-sovereign identity. https://www.windley.com/archives/2018/09/multi-source_and_self-sovereign_identity.shtml. Zugegriffen: 13.08.2020
Windley P (2020) The Sovrin SSI stack. https://www.windley.com/archives/2020/03/the_sovrin_ssi_stack.shtml. Zugegriffen: 19.08.2020
Winter H, Gerling J, Roth K (2020) Nutzung elektronischer Identifzierungsmittel (eIDs) im elektronischen Zahlungsverkehr und bei der Kontoeröffnung. https://www.bundesbank.de/resource/blob/820850/8f7ff5fca3fe5d823f7f10a30752b31f/mL/bericht-eids-elekronischer-zahlungsverkehr-data.pdf. Zugegriffen: 27.11.2020
Wunsch A (2018) Nagelprobe Praxistest: Erkenntnisse aus dem echten Leben. https://www.gs1-germany.de/innovation/blockchain-blog/nagelprobe-praxistest-erkenntnisse-aus-dem-echten-leben/. Zugegriffen: 04.08.2020