Fraunhofer FIT

FRAUNHOFER-INSTITUT FÜR ANGEWANDTE INFORMATIONSTECHNIK FIT

Self-Sovereign Identity

Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten

Projektgruppe Wirtschaftsinformatik

Self-Sovereign Identity

Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten

Autoren

Prof. Dr. Jens Strüker, Prof. Dr. Nils Urbach, Tobias Guggenberger, Jonathan Lautenschlager, Nicolas Ruhland, Vincent Schlatt, Johannes Sedlmeir, Jens-Christian Stoetzer, Fabiane Völter

Die Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT vereint die Forschungsbereiche Finanz- und Informationsmanagement in Augsburg und Bayreuth. Die Expertise an der Schnittstelle von Finanzmanagement, Informationsmanagement und Wirtschaftsinformatik sowie die Fähigkeit, methodisches Know-how auf höchstem wissenschaftlichen Niveau mit einer kunden-, ziel- und lösungsorientierten Arbeitsweise zu verbinden, sind ihre besonderen Merkmale.

Fraunhofer-Institut für Angewandte Informationstechnik FIT
Projektgruppe Wirtschaftsinformatik
Wittelsbacherring 10
95444 Bayreuth

Acknowledgements

Wir danken unseren Mitarbeiter*innen Jannik Lockl, Benjamin Schellinger und Jonathan Schmid für die tatkräftige Unterstützung bei der Erstellung des White Papers.

Empfohlene Zitierweise

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.

Inhaltsverzeichnis


Dezentrales Identitäts-
management ermöglicht
interoperable und sichere
digitale Identitäten für
Menschen, Organisationen
und Maschinen.

Vorwort der Herausgeber

Innerhalb der letzten Dekaden hat sich unsere Welt durch technologischen Fortschritt noch schneller und fundamentaler verändert als zuvor. Viele Teilbereiche unseres gesellschaftlichen Lebens werden heute durch digitale Technologien bestimmt. Dabei rücken auch immer wieder Themen der Privatsphäre und Sicherheit im digitalen Umfeld in den Vordergrund. Diese Aspekte sind vor allem in der Nutzung von personenbezogenen Daten im Internet zunehmend wichtiger geworden. Die unberechtigte Weiterleitung von Nutzerdaten oder sog. Data Breaches infolge von Unachtsamkeit oder Hackerangriffen zeigen immer wieder die Anfälligkeiten des heutigen Umgangs mit sensiblen Daten auf. Dabei charakterisieren unsere persönlichen Daten unsere eigene digitale Identität und damit die Art und Weise, wie wir Dienstleistungen im Internet nutzen. Gleichzeitig werden das Verwalten der zahlreichen Accounts von Internetnutzer*innen mit unterschiedlichen Passwörtern und gegebenenfalls die technische Umsetzung von zusätzlichen Mechanismen für die Multi-Faktor-Authentifizierung immer komplexer.

Auch für Unternehmen sind die Gewährleistung einer reibungslosen digitalen Interaktion mit Kund*innen und das Verwalten von Zugangsberechtigungen von Mitarbeiter*innen zu einer erheblichen Herausforderung geworden. Diese Herausforderung entsteht durch den zentralistischen Ansatz, digitale Identitäten und persönliche Daten von Internet-nutzer*innen zu verwalten. Ein solcher Ansatz birgt für Nutzer*innen eine Vielzahl unterschiedlicher Nachteile, darunter Portabilitätsrestriktionen oder weitreichende Transparenz der digitalen Identität gegenüber zentralen Identitätsanbietern. Ein Beispiel hierfür sind Single Sign-on-Verfahren, die u. a. von sozialen Netzwerken angeboten werden. Die entsprechenden Dienstleistungen sind zwar komfortabel, jedoch sind Nutzeraktivitäten gegenüber den zentralen Identitätsanbietern vollkommen transparent und es besteht nur eine sehr beschränkte Portabilität der digitalen Identität. Während die Nutzung solcher Dienste für Privatpersonen nur eine Abwägung von Komfort und Privatsphäre darstellt, überwiegen für Unternehmen häufig die Befürchtungen, sich durch ein derartiges Identitätsmanagement von einem dominanten Marktakteur abhängig zu machen. Gleichzeitig wird unternehmensübergreifende Kollaboration im Identitätsmanagement für Dienstleister, die ihren Kunden ein hohes Maß an Flexibilität anbieten, zunehmend an Bedeutung gewinnen. Die heute vorhandenen Identitätsmanagementsysteme sind dabei kaum interoperabel. Plattformbasierte Lösungen haben entweder wegen ihrer hierarchischen Strukturen Akzeptanzprobleme oder müssen mit massiven regulatorischen Herausforderungen wie z. B. dem Datenschutz zu kämpfen.

Durch die Weiterentwicklung von kryptografischen Verfahren in Kombination mit der Blockchain-Technologie konnte in den letzten Jahren ein neues Paradigma an Aufmerksamkeit gewinnen, das wesentliche Nachteile des etablierten digitalen Identitätsmanagements beheben könnte. Das Konzept dieser portablen, von den Nutzer*innen kontrollierten selbstsouveränen Identitäten (engl.: Self-Sovereign Identities) sieht vor, dass die Nutzer*innen selbst über ihre domänenübergreifenden digitalen Identitäten bestimmen können. Insbesondere können selbstsouveräne Identitäten überprüfbare Nachweise über Eigenschaften und Berechtigungen erhalten und diese mittels interoperabler Standards domänenübergreifend in unterschiedlichen Interaktionen einfach nutzen. Selbstsouveräne Identitäten sind dabei nicht nur auf Personen, sondern auch auf Unternehmen oder vernetzte Gegenstände im Internet der Dinge anwendbar. So ergibt sich ein breites Feld an Anwendungen, in denen SSI ein großes ökonomisches Potenzial durch die Erhöhung der Sicherheit und der Effizienz von Prozessen entfalten kann.

Wir wollen in diesem White Paper zunächst die wichtigsten konzeptionellen und technologischen Grundlagen selbstsouveräner Identitäten skizzieren, bevor einige Anwendungsfälle im Detail vorgestellt werden. Im Anschluss daran werden sowohl das ökonomische Potenzial als auch die Herausforderungen von selbstsouveränen Identitäten näher beleuchtet. Wir wünschen viel Freude beim Lesen und möchten alle Leser*innen einladen, mit uns in einen Dialog zu treten. Gerne stehen wir für Fragen, Diskussionen und Anregungen zur Verfügung.

Hochschule Fresenius/ John M. John

Prof. Dr. Jens Strüker

Professor für Wirtschaftsinformatik und Digitales Energiemanagement

Universität Bayreuth

Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT

© Björn Seitz – kontender.Fotografie

Prof. Dr. Nils Urbach

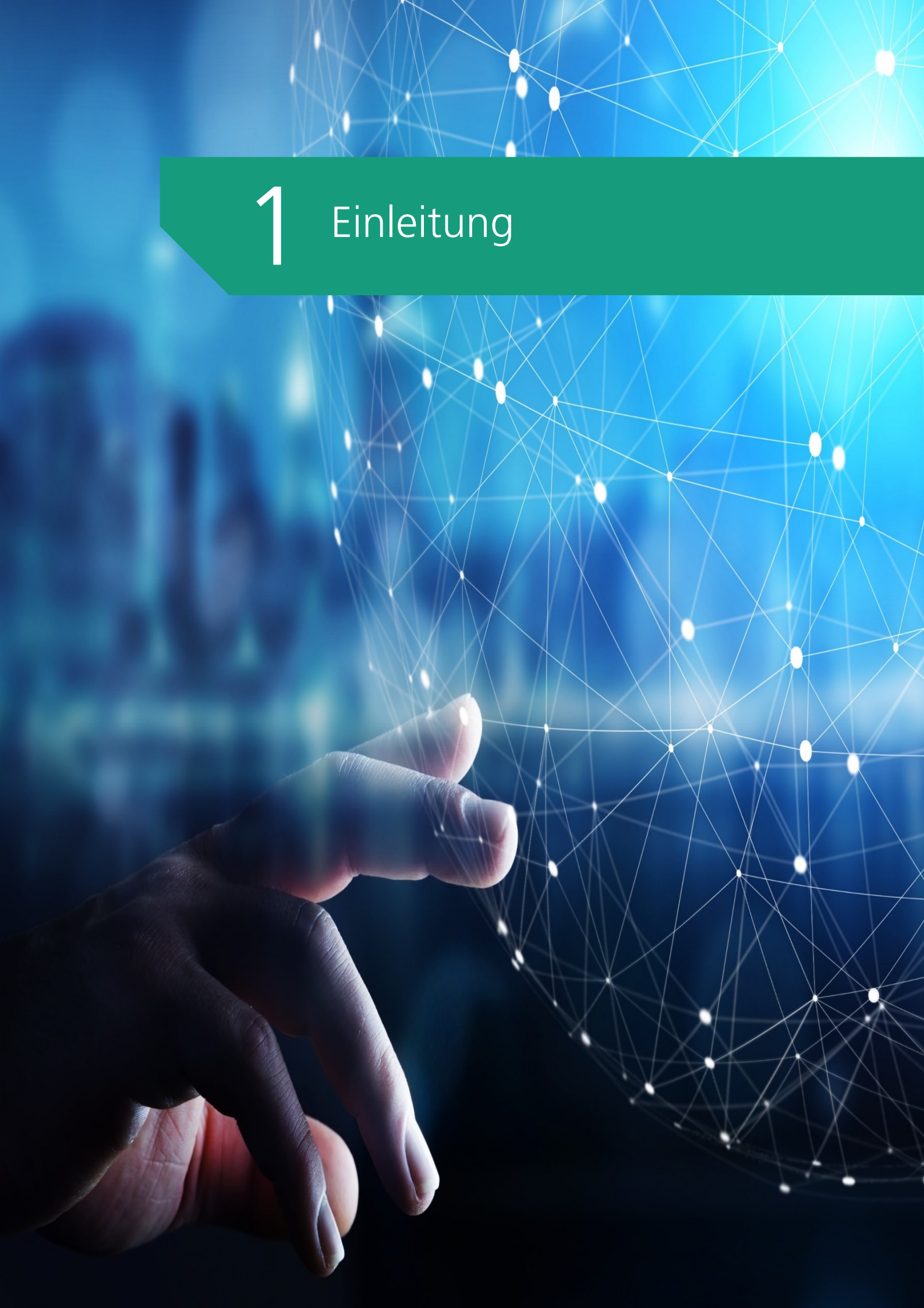
Professor für Wirtschaftsinformatik, Digital Business und Mobilität

Frankfurt University of Applied Sciences

Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT

Glossar

AML	Anti-Money Laundering
CA	Certificate Authority
DID	Decentralized Identifier
DKMS	Decentralized Key Management System
DLT	Distributed Ledger Technology
DSGVO	Datenschutz-Grundverordnung
ESSIF	European Self-Sovereign Identity Framework
EU	Europäische Union
IoT	Internet der Dinge
KYC	Know Your Customer
SSI	Self-Sovereign Identity
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier
VC	Verifiable Credential
VID	Vehicle Identity
VIN	Fahrzeugidentifikationsnummer
VP	Verifiable Presentation
ZKP	Zero-Knowledge Proof



1 Einleitung

Einleitung

Die Verbreitung des Internets hat zu tiefgreifenden Veränderungen in vielen Bereichen der Gesellschaft geführt. Das Internet ermöglicht es, eine Vielzahl digitaler Dienstleistungen zu nutzen, wie z.B. Informationen zu recherchieren, Kleidung und Essen zu bestellen sowie mit Freund*innen und Arbeitskolleg*innen über soziale Netzwerke zu kommunizieren. Als zentrale Herausforderung bei der Nutzung des Internets gilt bereits seit den frühen 90er-Jahren der Nachweis der eigenen Identität. So ist es nur sehr schwer möglich, in der Kommunikation über das Internet die eigene Identität oder zugehörige Attribute (beispielsweise Alter, Wohnort etc.) nachzuweisen. Der Cartoon „On the Internet, nobody knows you're a dog" von Peter Steiner beschreibt schon 1993 – und damit wenige Jahre nach Erfindung des Internets – dieses zentrale Problem.

Im Gegensatz zum Status quo des Identitätsmanagements im Internet sind Identitäten in der analogen Welt fast immer durch offizielle oder nicht offizielle Dokumente wie beispielsweise einen Ausweis oder eine Kundenkarte nachweisbar. In der Regel sind diese Dokumente zu einem gewissen Grad fälschungssicher gestaltet. Somit kann eine Person gegenüber einer anderen belegen, dass diese einen bestimmten Namen trägt oder ein bestimmtes Alter hat. Insofern kann in der analogen Welt jede/-r Nutzer*in die volle Kontrolle über die eigenen Ausweisdokumente und andere Nachweise haben, ohne bei einer dritten Partei oder dem Aussteller dieser Dokumente diesbezüglich um Erlaubnis bitten zu müssen oder die Dokumente an einer zentralen Stelle mit eingeschränkten Zugriffsmöglichkeiten abzulegen. Damit ist das Identitätsmanagement in der analogen Welt „selbstsouverän". Zum Beispiel basiert unsere analoge Ausweiskontrolle auf eben diesem selbstsouveränen Konzept. Das Vorzeigen des Personalausweises bietet in diesem Zusammenhang Interoperabilität und Sicherheit, weil er international anerkannt und in seiner Form standardisiert ist. Dadurch kann nahezu jede Partei, die der Verwaltung der Bundesrepublik Deutschland vertraut, den Personalausweis durch reines Vorzeigen verifizieren, ohne bei einer Behörde oder dergleichen nachfragen zu müssen. Darüber hinaus sind die persönlichen Daten von Nutzer*innen durch diese Konstruktion geschützt, da Daten „analog" auf dem Personalausweis abgespeichert" werden, die sich nur in der Geldbörse des/der Ausweiseigentümer*in befinden und nicht durch analoge Kopien an zahlreichen anderen Orten vorbehalten werden. Auch im Business-to-Business-Bereich wird diese Interoperabilität häufig verwendet, beispielsweise bei Kreditkarten, die von vielen Unternehmen akzeptiert werden, ohne dass ein unternehmensübergreifendes Identitätsmanagement nötig ist.

Diese Verwendung solcher physischen, relativ fälschungssicheren Dokumente, die durch vertrauenswürdige Instanzen ausgestellt und dabei durch eine breite Zahl von Nutzer*innen einfach verifiziert werden können, ist in einer digitalen Umgebung in dieser Form heute nicht etabliert. Vielmehr entspricht das Identitätsmanagement im Internet einem „Flickenteppich". Nutzer*innen haben in der Regel zahlreiche Accounts bei vielen unterschiedlichen Dienstleistern, die sie verwalten müssen und bei denen sie kaum Möglichkeiten haben, einmal bestätigte Attribute – wie etwa einen Führerschein bei einem Carsharinganbieter oder eine gültige Bankverbindung bei einem Onlineversand – auch in anderen Kontexten verwenden zu können. Single Sign-on-Dienste wie Facebook oder Google können hier zwar zu einem gewissen Maße Abhilfe schaffen und Interoperabilität herstellen; dies geht jedoch auf Kosten der Datenhoheit und Privatsphäre und gibt diesen Unternehmen eine große Marktdominanz. Insgesamt müssen sich also Nutzer*innen heutzutage zwischen den Dimensionen Interoperabilität, Sicherheit und Datenschutz entscheiden und haben keine digitale Identität, die ähnlich wie ihre analoge Identität selbstsouverän ist.

Verschiedene technische und konzeptionelle Ansätze in den letzten Jahren haben versucht, Lösungen für den Nachweis von Identitäten in der digitalen Welt zu etablieren, die Probleme wie Datenschutz, mangelnde Interoperabilität und Sicherheit adressieren. Durch technologische Fortschritte im Bereich der Kryptografie und der dezentralen Datenspeicherung ist dabei das Konzept der selbstsouveränen Identität (engl. Self-Sovereign Identity, SSI) entstanden, welches sich zum Ziel gesetzt hat, Probleme bisheriger Identitätsmanagementsysteme zu lösen und neue Vorteile für Nutzer*innen zu bieten. Als Vorbild dient hierbei stets die Art und Weise, wie in der nicht digitalen Welt mithilfe von „Plastikkärtchen" gegenüber Dritten, die dem Aussteller der entsprechenden „Plastikkärtchen"

Einleitung

vertrauen, Attribute und Berechtigungen nachgewiesen werden können.

Eine Vielzahl unterschiedlicher Konsortien und Initiativen beschäftigt sich weltweit mit dem Konzept der SSI, insbesondere in Nordamerika und Europa. In der Folge liegen mittlerweile bereits zahlreiche Dokumentationen und Studien zu Pilotprojekten ebenso wie Veröffentlichungen in wissenschaftlichen Zeitschriften vor. Auch Standards und Open-Source-Implementierungen von Applikationen, die bilateral digitale Äquivalente dieser „Plastikkärtchen" zwischen universellen Smartphone-Apps und Applikationen austauschen, entwickeln sich aktuell sehr schnell weiter und zeigen eine wachsende Entwickler*innen-Community. Ziel dieses White Papers ist es daher, wesentliche Informationen zum Identitätsmanagement nach dem SSI-Paradigma in kompakter Form zusammenzutragen, um einem deutschsprachigen Publikum einen breiten Überblick über den aktuellen Stand der Forschung, der technologischen Entwicklungen und der praktischen Potenziale zu diesem Thema aufzubereiten.

Im Folgenden werden zunächst die Grundlagen zur Entwicklung von digitalen Identitäten vorgestellt. Danach erfolgt eine nicht-technische Einführung und Definition des Begriffs SSI. Ferner werden die technischen Grundlagen zu SSI dargestellt, bevor die Potenziale des neuartigen Konzepts näher betrachtet werden. Zuletzt erfolgt eine Zusammenfassung der Herausforderungen und Risiken von SSI.


Self-Sovereign Identity
ist die nächste
Entwicklungsstufe des
Digitalen
Identitätsmanagements.

2 Die Entwicklung des digitalen Identitätsmanagements

Die Entwicklung des digitalen Identitätsmanagements

Interoperables digitales Identitätsmanagement gewinnt zunehmend an Relevanz

Die Identität einer Person – unabhängig davon, ob analog oder digital – besteht aus mehreren Teilidentitäten. Eine oder mehrere Teilidentitäten können beispielsweise für die Arbeit, die Freizeit, die Nutzung von Internetservices oder den Besuch im Supermarkt verwendet werden. Jede Teilidentität enthält dabei Informationen, die sich mit anderen Teilidentitäten überschneiden können, aber nicht müssen (siehe Abbildung 1). In diesem Zusammenhang müssen auch nicht immer die gleichen Informationen verwendet

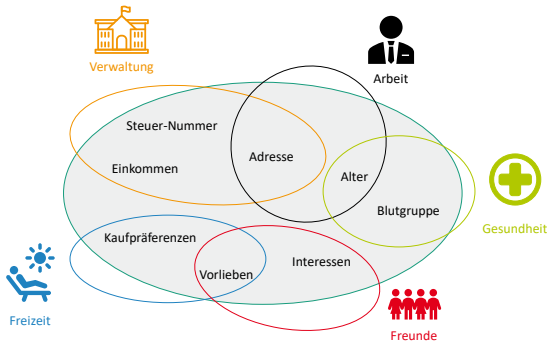


Abbildung 1: Teilidentitäten (basierend auf Clauß und Köhntopp 2001)

werden. So kann etwa der echte Name einer Person auf einer Website durch ein Pseudonym ersetzt werden. Die Nutzung dieser Teilidentitäten erfolgt fortlaufend im alltäglichen Leben und erfordert eine Portabilität der digitalen Identität, Interoperabilität mit unterschiedlichen Systemen und eine selbstbestimmte Verwaltung der Teilidentitäten. Diese Teilidentitäten besitzen wiederum mehrere Attribute, z. B. im Arbeitsleben Name, Adresse, Qualifikationen etc. Manche dieser Teilidentitäten identifizieren eine Person eindeutig, andere wiederum nicht. Abhängig von dem spezifischen Kontext und der Situation kann eine Person also durch verschiedene Teilidentitäten repräsentiert werden (Clauß und Köhntopp 2001).

Herausforderungen für das Identitätsmanagement im digitalen Zeitalter

Das Management von Identitäten gewinnt im digitalen Zeitalter aufgrund der stark ansteigenden Zahl digitaler Interaktionen zunehmend an Bedeutung. Physische Systeme sind dabei nicht oder nur bedingt in die digitale Welt übertragbar. Dennoch gilt es, die Vorteile der physischen Identitätsmanagementsysteme Systeme in ein digitales Äquivalent zu überführen. Ein digitales Identitätsmanagementsystem beschreibt ein System, durch das Nutzer*innen in der Lage sind, die Informationen ihrer Identität zu bestimmen, die mit Dritten geteilt werden (Clauß und Köhntopp 2001). Während in der analogen Welt die Identität häufig über ein physisches Objekt (z. B. Personalausweis, Führerschein oder Reisepass) ausgewiesen wird, ist dies in der digitalen Welt nicht ohne Weiteres möglich. Ein physisches Identitätsdokument ist dabei durch annähernd fälschungssichere Merkmale und Lichtbilder weitestgehend vor Missbrauch geschützt (Tönsing 2015). Klassischerweise wird dagegen im Internet die Nutzeridentität durch das Anlegen zahlreicher domänenspezifischer Nutzeraccounts, die meist durch die Kombination eines Benutzernamens und eines Passworts zugänglich sind, verwaltet. Diese Kombination sollte im besten Fall für jeden Account im Internet neu sein, was jedoch in der Praxis häufig nicht gegeben ist. Durchschnittlich besitzt ein/eine Internetnutzer*in 25 Accounts, für die oftmals individuelle Regeln zur Erstellung der Benutzername-Passwort-Kombination gelten. Aus Bequemlichkeitsgründen ist das Passwortmanagement dann oft nicht sicherheitskonform. Beispielsweise verteilen sich auf die durchschnittlich 25 Accounts im Mittel nur sechs bis sieben unterschiedliche Passwörter (Tönsing 2015). Durch die Kompromittierung eines einzigen Passworts wird dadurch häufig der Zugang zu gleich mehreren Diensten ermöglicht. Dies erhöht die Risiken für möglichen Missbrauch der Identität durch Dritte wesentlich. Die Verwendung von unterschiedlichen Passwörtern führt hingegen zu einer schnell wachsenden Komplexität im Management der Zugänge, da entweder spezielle Passwortmanager oder Notizen verwendet werden müssen, um sich die einzelnen Passwörter zu merken. So entsteht ein hoher Aufwand seitens der Nutzer*innen oder eine große Empfindlichkeit gegenüber Angriffen und damit einhergehende Sicherheitsrisiken.

Die durch Onlinedienste gespeicherten identitätsbezogenen Daten lassen sich zudem in den meisten Fällen nicht domänenübergreifend (wieder-) verwenden. Dies impliziert die Notwendigkeit von aufwendigen, wiederkehrenden Registrierungen bei verschiedenen Dienstanbietern. Die Identität von Nutzer*innen bezieht sich also

Die Entwicklung des digitalen Identitätsmanagements

bei dem heutigen digitalen, Account-basierten Identitätsmanagement nur auf den spezifischen Kontext der entsprechenden Anwendung. Die dort verwendeten Daten und Informationen sind meist außerhalb dieses spezifischen Kontextes nicht nutzbar oder bedeutungslos (Tobin und Reed 2017).

Entwicklungsstufen des digitalen Identitätsmanagements

Aktuell existieren verschiedene Arten des Identitätsmanagements in der digitalen Welt. Dabei können zentralisierte Identitäten, nutzerorientierte Identitäten, föderierte Identitäten und selbstsouveräne Identitäten (Allen 2016), wie in Abbildung 2 dargestellt, besonders hervorgehoben werden:

(1) Zentralisierte Identität

Eine zentralisierte Identität (engl.: Centralized Identity) wird auf Systemebene durch zentrale Parteien, wie z. B. Administrator*innen, verwaltet. Die Identität der Nutzer*innen ist demnach von den zentralen Teilnehmer*innen abhängig. Eine Löschung der Identität ist nur durch die jeweiligen Anbieter möglich, was für die Nutzer*innen kaum zu kontrollieren ist und ein Risiko der missbräuchlichen Nutzung darstellt. Weiterhin folgt aus der Abhängigkeit gegenüber den zentralen Teilnehmer*innen häufig eine mangelnde Interoperabilität. Daher muss die Identität durch die Nutzer*innen bei einem anderen Dienst ebenfalls neu angelegt werden, da sie nicht ohne Weiteres übertragen werden kann. Überdies werden die Nutzerinteraktionen für die zentralen Teilnehmer*innen transparent. Daneben ergibt sich zwangsläufig eine Redundanz in der Datenspeicherung bei verschiedenen Diensten, die die gleichen Informationen benötigen, wobei aber die Daten nicht synchronisiert werden.

(2) Nutzerorientierte Identität

Um den Nachteilen einer zentralisierten Identität entgegenzuwirken, wurde das Konzept der nutzerorientierten Identität entworfen. Dabei verwalten Nutzer*innen die Zugänge zu verschiedenen Diensten (und damit Teilidentitäten) selbst. Durch die Mehrfachverwendung von Passwörtern und mangelnden Wechseln der Zugangsdaten entstehen dabei jedoch Sicherheitsrisiken und eine mangelnde Nutzerfreundlichkeit. Einmal nachgewiesene Identitätsattribute (z. B. Fahrerlaubnis) müssen wiederholt für jeden Dienst einzeln nachgewiesen werden. Durch eine lokale Anwendung zur Speicherung und Verwaltung von Zugangsdaten zu verschiedenen Diensten können Nutzer*innen die unterschiedlichen Zugänge zu verschiedenen Diensten mit einem einzigen Passwort (oder Authentifizierungsschritt) verwenden. Die Daten über Attribute ihrer Teilidentitäten bleiben allerdings bei dem jeweiligen Anbieter gespeichert. Daher können diese auch zwischen verschiedenen Webdiensten weitergegeben werden (Tobin und Reed 2017; Allen 2016).

(3) Föderierte Identität

Eine föderierte Identität (engl.: Federated Identity) stellt eine weitere Entwicklungsstufe einer digitalen Identität dar. Durch eine zentrale Log-in-Instanz (online oder offline) steht den Nutzer*innen die Möglichkeit offen, ihre Teilidentität mit anderen Anbietern zu teilen. Dieses Prinzip wird unter dem Begriff Single Sign-on vor allem in Unternehmen sowie von sozialen Netzwerken wie Facebook oder Google angeboten. Durch die Nutzung von Single Sign-on eines Identity Providers können die Nutzer*innen per Knopfdruck ihre Identität von einem Anbieter zu einem anderen transferieren. Die Weitergabe der Daten erfordert dabei stets Zugriff auf den zentralen Log-in-Dienst. Der Nachteil aus Sicht der Nutzer*innen ist die hohe Abhängigkeit von dem zentralen Log-in-Dienst als Identitätsanbieter. Dieser dient als kryptografischer Schlüssel zu allen Teilidentitäten und kann daher stets nachvollziehen, welche Dienste die Nutzer*innen mit ihren Teilidentitäten verwenden. Zudem steigt auch das Risiko durch eine missbräuchliche Verwendung der Identität, falls die Zugangsdaten

Abbildung 2: Entwicklung von digitalen Identitäten

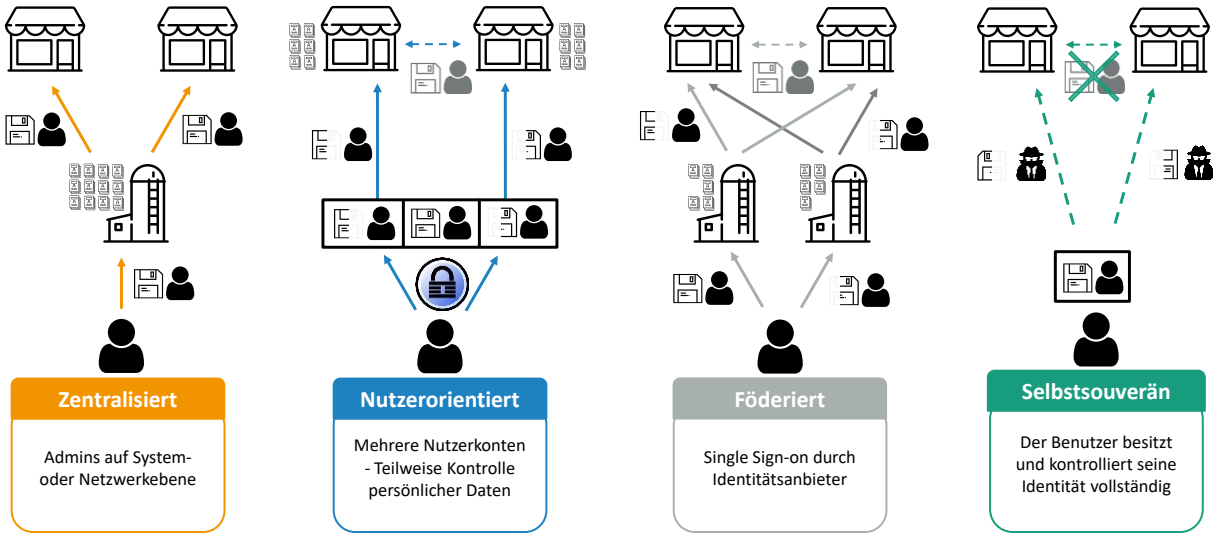


Abbildung 3: Vergleich verschiedener Identitätsmanagementsysteme

zu dem zentralen Log-in-Dienst an Dritte gelangen. Daher könnten diese mit dem Zugriff auf einen Dienst auch den Zugriff auf alle damit verbundenen Teilidentitäten kontrollieren.

Zusammenfassend lässt sich also festhalten, dass bisher existierende Ansätze zum Management von digitalen Identitäten diverse Nachteile wie z. B. mangelnde Interoperabilität oder eine Abhängigkeit von bestimmten Parteien aufweisen. Bisher hat es kein System geschafft, alle Probleme aktueller Identitätsmanagementsysteme und Bedürfnisse der Nutzer*innen zu adressieren.

Self-Sovereign Identity als neues Paradigma im Identitätsmanagement

Ausgehend von den im vorhergehenden Kapitel beschriebenen Herausforderungen hat sich innerhalb der letzten Jahre das Paradigma der SSI entwickelt. SSI soll die Herausforderungen und Probleme von existierenden digitalen Identitätsmanagementsystemen beheben und gilt dabei als die nächste Entwicklungsstufe digitaler Identitäten. Es existieren jedoch noch kein einheitliches Verständnis und keine allgemein akzeptierte Definition des Begriffs (Mühle et al. 2018). Tobin und Reed (2017) definieren SSI als finale Stufe der Entwicklung digitaler Identitäten. Diese soll dabei die individuelle Kontrolle, Sicherheit und volle Portabilität digitaler Identitäten über verschiedene Dienste hinweg sicherstellen. Allen (2016) definiert den/die Nutzer*in als zentralen Verwalter bzw. zentrale Verwalterin seiner/ihrer Identität, einschließlich aller existierender Teilidentitäten. Daher muss es Nutzer*innen möglich sein, über alle verschiedenen Dienste hinweg die Kontrolle über ihre Identität zu wahren und damit eine Autonomie in der Verwaltung dieser Dienste zu erzielen. Daraus folgt, dass eine SSI interoperabel und portabel sein muss. Nutzer*innen müssen in der Lage sein, Behauptungen über ihre Identität zu treffen, die durch die Bestätigung von Dritten zu verifizierten Attributen werden. Auch müssen Dritte in der Lage sein, Attribute zu einer Identität hinzuzufügen, die durch die Nutzer*innen bestätigt werden können. Das grundlegende Prinzip von SSI im Vergleich zu anderen Identitätsmanagementsystemen wird in Abbildung 3 dargestellt. Die Abgrenzung gegenüber anderen Identitätsmanagementsystemen wird durch die zehn Prinzipien von SSI (Allen 2016) verdeutlicht, die in Tabelle 1 aufgeführt sind.

Die Prinzipien von Allen basieren auf der Arbeit von Cameron (2005), der die Grundbedingungen für erfolgreiche digitale Identitätsmanagementsysteme skizzierte. Allen (2016) definierte die zehn Prinzipien von SSI als Reaktion auf die Nachteile bisheriger digitaler Identitätsmanagementsysteme, beschreibt damit jedoch keine spezifische technische Lösung. Daher wird zunächst das Prinzip von SSI technologieneutral erklärt.

Kontrollierbarkeit	Existenz	Nutzer*innen müssen die Möglichkeit haben, eine unabhängige digitale Identität zu besitzen.
	Kontrolle	Die Nutzer*innen einer SSI müssen die volle Befugnis und Kontrolle über ihre Identität haben. Dies muss durch sichere und gut erforschte Algorithmen geschehen, was allen Nutzer*innen die Möglichkeit gibt, seine/ihre Privatsphäre-Einstellungen so vorzunehmen, wie er/sie dies möchte.
	Einverständnis	Nutzer*innen müssen stets der Verwendung ihrer Identität durch eine Entität zustimmen. Da das System von SSI darauf beruht, dass Informationen mit Entitäten geteilt werden, ist die Zustimmung der Nutzer*innen für jede Weiterleitung von Daten notwendig.
	Zugriff	Nutzer*innen müssen in der Lage sein, auf alle Aspekte ihrer Identität zuzugreifen, auch wenn einzelne Teilidentitäten von anderen Entitäten verwaltet werden.
Portabilität	Transparenz	Jede SSI muss in ihren Systemen und Algorithmen ausreichend Transparenz bieten. Dabei sollte das System für alle verfügbar, nutzbar und durch Open-Source-Code ebenfalls untersuchbar sein, um Vertrauen in die Technologie herzustellen.
	Übertragbarkeit	Die Informationen und Daten einer SSI müssen stets übertragbar sein. Damit soll sichergestellt werden, dass Identitäten nicht verloren gehen und stets in der Hoheit der Nutzer*innen liegen, wenn Entitäten im Zeitverlauf verschwinden oder sich Regulierung und Systeme ändern.
	Interoperabilität	Eine SSI muss in so vielen verschiedenen Anwendungsbereichen wie möglich nutzbar sein und daher unabhängig von Grenzen und existierenden Systemen arbeiten.
Sicherheit	Minimalisierung	Die Offenlegung von Daten muss minimiert werden. Bei jeder Offenlegung von (Teil-)Identitäten müssen so wenig Daten wie möglich offengelegt werden, also nur so viele, wie unbedingt für die Erfüllung der Aufgabe notwendig sind. Als Beispiel für dieses Prinzip gilt der Einkauf von alkoholhaltigen Getränken: Die Nutzer*innen müssen nachweisen, dass sie das gesetzliche Mindestalter für den Erwerb erreicht haben, aber dabei nicht ihr genaues Geburtsdatum offenlegen.
	Schutz	Die Rechte der Nutzer*innen müssen in jedem Anwendungsfall geschützt sein. Falls dabei die Notwendigkeiten des Netzwerks den Rechten der Nutzer*innen konfliktär gegenüberstehen, sollten die Rechte der Nutzer*innen höher gewichtet sein.
	Langlebigkeit	Die einzelnen, durch die SSI verwalteten Identitäten müssen so lange nutzbar sein, wie es die betreffenden Nutzer*innen wünschen. Auch wenn sich die zugrunde liegenden Algorithmen eventuell verändern, müssen die Informationen und damit die Identität im besten Fall unangetastet bleiben. Gleichzeitig besteht die zwingende Notwendigkeit des Rechts auf Vergessen. Daher muss die SSI sicherstellen, dass Nutzer*innen ihre Identität löschen und damit die bisher erteilten Rechte unbrauchbar machen können.

Tabelle 1: Zehn Prinzipien von SSI (Allen 2016)


Self-Sovereign Identities sollen Kontrollierbarkeit,
Portabilität und Sicherheit ermöglichen.

3 Technologische Grundlagen von Self-Sovereign Identity

Die zehn Prinzipien von SSI fungieren als Anforderungskatalog für die Umsetzung einer SSI-Lösung. Daher ist es notwendig, neben den zehn Prinzipien von SSI zu verstehen, wie eine SSI-Lösung technisch implementiert werden kann. Damit kann nachvollzogen werden, welche verschiedenen Grundbestandteile von SSI mit bereits bekannten Technologien umsetzbar sind und in Kombination eine SSI-Lösung bilden können. Deshalb werden im Folgenden die Funktionsweisen der einzelnen Grundbestandteile und der beteiligten Schlüsseltechnologien erklärt.

Grundbestandteile: die elementaren Bausteine eines SSI-Systems

Die Bestandteile einer SSI-Lösung, die in ihrer Kombination das Fundament einer SSI-Architektur bilden, können in fünf Hauptartefakte aufgeteilt werden: Verifiable Credentials (VCs), Rollen (Issuer, Holder und Verifier), Identifier, Digital Wallets sowie Agents und Hubs.

Der zentrale Baustein jeder SSI-Lösung sind digitale Zertifikate (folgend engl.: Credentials). Diese Credentials können entweder selbstattestierte Identitätsattribute enthalten oder solche, die durch Dritte attestiert wurden. Attestierte Credentials werden als VCs definiert (1), für die bereits ein Standard existiert, der vorgibt, wie ein solches Zertifikat aufgebaut ist. Darüber hinaus bilden VCs die zentralen Artefakte zum Nachweis von Identitätsattributen zwischen den zentralen Rollen einer SSI-Lösung (2). Diese Rollen bilden im Rahmen der Issuer-Holder-Verifier-Beziehung das Grundgerüst der Interaktion. Jedes VC wird von einem Issuer erstellt, von einem Holder aufbewahrt und darin enthaltene Informationen dem Verifier gegenüber präsentiert.

Zur Gewährleistung möglichst sicherer Kommunikationswege und zum Schutz der Privatsphäre ermöglicht der DID-Standard (3) den Parteien Informationen zum Herstellen einer Ende-zu-Ende-verschlüsselten, bilateralen Kommunikation auf unterschiedlichen Infrastrukturen. Im Gegensatz zu derzeitigen verschlüsselten Kommunikationsprotokollen wie „http over Transport Layer Security (TLS)“, bei dem mindestens eine der Kommunikationsparteien ein von einer Certificate Authority (CA) ausgestelltes SSL-Zertifikat benötigt, ermöglicht der DIDComm Standard Ende-zu-Ende verschlüsselte Kommunikation auch ohne diese Zertifizierung und ist damit weniger abhängig von CAs. Die einzelnen VCs sowie kryptografische Schlüssel werden dabei in digitalen Äquivalenten einer Geldbörse, sog. Digital Wallets (4), aufbewahrt. Als Anknüpfungspunkte von bilateraler Kommunikation werden in diesem Zusammenhang Agents und Hubs (5) als technische Endpoints und Treuhänder für den Identifier benötigt. Sie stellen die geschützte Kommunikation zwischen einzelnen Identitäten sicher und sollten analog zu E-Mail-Servern durchgehend erreichbar sein. Diese fünf Grundbausteine (1–5, siehe Tabelle 2) ergeben die Kernarchitektur einer technischen SSI-Lösung und werden daher im Folgenden umfassend erklärt.

(1) Verifiable Credentials	Standard für SSI-Architekturen Digital signierte Sammlung von Attributen
(2) Rollen (Issuer, Holder, Verifier)	Protagonisten der SSI-Lösung (stehen in Beziehung zueinander)
(3) Decentralized Identifiers (DID)	Standard, der es ermöglicht, verschiedene Identifier für Ende-zu-Ende-verschlüsselte Kommunikation zu nutzen (Schutz der Privatsphäre, Anonymisierung)
(4) Digital Wallets	Software zur Aufbewahrung von privaten Schlüsseln, VCs und gegebenenfalls DID-Dokumenten für den Holder
(5) Digital Agents und Hubs	Technische Endpoints und Treuhänder für Identifier (stellen Kommunikation zwischen Identitäten sicher)

Tabelle 2: Bausteine des SSI-Konzepts

Verifiable Credentials

Digitale Zertifikate unterliegen der Vertrauensbeziehung einer Partei zu einer dritten, neutralen Autorität. Konkret müssen Nutzer*innen in aktuellen Umsetzungen des Zertifikatsmanagements einer oder mehreren CAs vertrauen (Goodell und Aste 2019). CAs ordnen mittels eines signierten Zertifikats einer Identität

bestimme Eigenschaften zu. Die Rolle der CA kann jede vertrauenswürdige Partei einnehmen. Dabei existieren verschiedene Organisationen, die sich ausschließlich um die Ausstellung von Zertifikaten bemühen. Dennoch bestehen aktuell nur begrenzt Ansätze, die es anderen Organisationen erlauben, Zertifikate selbst auszustellen und diese mittels übergreifender Infrastrukturen überprüfbar zu machen. So wird die Entstehung weitreichender Ökosysteme aus Identitätszertifikate ausstellenden Parteien verhindert.

Dies stellt auch insofern ein Problem dar, dass aktuell zwei miteinander kommunizierende Parteien in der Regel von der Integrität der entsprechenden CAs abhängig sind: Das System unterliegt der Annahme, dass CAs immer vertrauenswürdig sind und nicht kompromittiert werden. Die CA ist somit die Schwachstelle, die das System bei korrupten Betreibern und unzureichenden Sicherheitsvorkehrungen anfällig macht (Goodell und Aste 2019). Zudem ist die Zertifizierung durch eine CA mit einem entsprechenden Zeit- und Kostenaufwand verbunden, was den Prozess umständlich macht. In einer SSI-Architektur nehmen diese CAs aufgrund von VCs keine derartig zentrale Rolle mehr ein (McKenna et al. 2020). Dies liegt in erster Linie daran, dass bei den im selbstsouveränen Identitätsmanagement verwendeten VCs die Kopplung von Identifiern und Public Keys (die kryptografisch oder durch öffentliche Selbstattestierung erfolgen kann) getrennt von der Kopplung von Attributen an die Identifier (dies geschieht in der Regel durch das Ausstellen von Zertifikaten durch vertrauenswürdige Institutionen) erfolgen kann. Zudem gibt es Architekturen, in denen das Identitätsmanagement von Organisationen in einem öffentlichen Register (Distributed Ledger) selbst verwaltet wird, was eine Alternative zu CAs darstellt.

Definition: Verifiable Credentials

Im Rahmen des Identitätsmanagements ist eine Identität die Abbildung einer Entität in einem bestimmten Kontext. Zum einen besteht diese aus Identifiern, also Identifikatoren zur eindeutigen Bestimmung einer Organisation, eines Objekts oder einer Person. Zum anderen besteht sie aus den Attributen der Entität, wie beispielsweise einem Passwort oder demografischen Daten. Zusammen bilden diese Komponenten das eingangs beschriebene „digitale Plastikkärtchen".

Diese Attribute dienen dem Zweck, gegenüber Dritten nachweisbar zu sein. Je sensibler die Attribute sind, desto wichtiger ist die Gewährleistung der Datensouveränität der jeweiligen Entität. Zur Schaffung weitreichender Ökosysteme eines digitalen Identitätsmanagements muss es zudem einer Vielzahl an Organisationen möglich sein, Attribute für Entitäten zu attestieren und entsprechende Credentials zum Nachweis auszustellen. Die Überprüfung dieser Credentials muss Dritten sicher, effizient und strukturiert ermöglicht werden. Das bedeutet konkret, dass interoperable Systeme, ein holistisches Vertrauensverhältnis zwischen den Akteuren und den CAs sowie die Gewährleistung der Privatsphäre der Nutzer*innen sichergestellt werden müssen. Dazu sind Standards und interoperable Systeme notwendig.

VCs sind durch das W3C-Konsortium mit dem Ziel standardisiert digitales Vertrauen aufzubauen, um die Privatsphäre der Nutzer*innen mit den Vorteilen von digitalen Zertifikaten in Einklang zu bringen. VCs sorgen dabei für einen verifizierbaren digitalen Austausch von Berechtigungs- und Eigenschaftsnachweisen über einen beliebigen Kommunikationskanal, z. B. klassisch mittels TLS und sind daher trennscharf von DIDs zu unterscheiden. DIDs ermöglichen das Erstellen eines sicheren bilateralen Kommunikationskanals und sorgen für eine Ende-zu-Ende-verschlüsselte Verbindung zwischen den beteiligten Akteuren (z. B. Verifier und Prover), ohne dabei von einer CA abhängig zu sein. Darüber hinaus sind im Rahmen eines DID ebenfalls Aspekte der Nutzungsberechtigung definiert – z. B. von NFC- oder potenziellen Bluetooth-Lösungen. Letztlich besteht hier insbesondere der Unterschied darin, dass VCs das Ziel verfolgen, digitales Vertrauen aufzubauen, während DIDs dafür einen sicheren Kommunikationskanal schaffen.

Zur vereinheitlichten Nutzung von digitalen Zertifikaten wird das Erstellen digitaler Signaturen aktuell beispielsweise mittels des weitverbreiteten X.509-Standards oder des JWS-Standards (JSON Web Signature Standard) umgesetzt. VCs verwenden dagegen häufig die Erweiterung JSON-LD (JSON-basierte Serialisierung für verlinkte Daten) in Verbindung mit etablierten oder auch neuen Signaturverfahren, um fälschungssichere VCs bzw. „digitale Plastikkärtchen" gewährleisten zu können. Beide Standardisierungen ermöglichen es, die Integrität von Informationen in einem hochgradig serialisierten

und maschinenlesbaren Format nachzuweisen. Sie bescheinigen demnach, dass es sich bei einem signierten VC um Informationen handelt, die sich seit der Unterzeichnung nicht geändert haben. Die Umsetzung mittels JSON-LD ermöglicht zusätzlich eine semantische Interoperabilität (einheitliche Semantik des maschinellen Codes).

Darüber hinaus benötigt Interoperabilität auch einen „offenen" Zugriff auf Revocations, was mit aktuellen X.509-Zertifikaten nur bedingt funktioniert. Dementsprechend stellen sogenannte Zero-Knowledge Proofs (ZKPs) eine interoperablere, sicherere und auf mehr Privatsphäre ausgelegte Lösung dar. Diese ermöglichen durch fortgeschrittene Signaturverfahren das selektive und (abgesehen vom Wert des Attributs selbst) unkorrelierbare Nachweisen von in Zertifikaten bestätigten Attributen. Die Wahl des geeigneten digitalen Signaturverfahrens und der in einer Interaktion vorzuzeigenden Attribute ist dabei oft eine Abwägung zwischen Authentizität und Datenschutz.

Dabei bedeutet die Interoperabilität von Systemen aus rein technischer Sicht jedoch noch nicht, dass das Identitätsmanagement funktioniert. Im Identitäts- und Accessmanagement großer Unternehmen, die eine Vielzahl von Softwareapplikationen nutzen, werden zwar in der Regel hoch standardisierte Verfahren für föderiertes Identitätsmanagement wie Open ID Connect als Erweiterung von OAuth 2.0 genutzt. Dennoch haben die dort ausgestellten Zertifikate außerhalb der jeweiligen Domäne keine Bedeutung, weil es kein domänenübergreifendes Identitätsmanagement für die jeweiligen Organisationen gibt und Nutzer*innen ihre „Token" jeweils nur kontextgebunden einsetzen können.

Diese Herausforderungen versucht das Paradigma von SSI zu lösen. SSI verfolgt dabei einen nutzerzentrierten Ansatz, sodass die Hoheit und Kontrolle über Identitätsdaten bei ihren jeweiligen Nutzer*innen liegen. Gleichzeitig soll Nutzer*innen ein hohes Maß an Komfort für Aktivitäten im Kontext ihrer digitalen Identität ermöglicht werden. Zur Umsetzung eines solchen nutzerzentrierten Ansatzes, bei dem keine dritte Partei benötigt wird, müssen Credentials sicher gestaltet und durch Dritte einfach überprüfbar (verifiable) werden. Damit geht aber auch einher, dass ohne eine bestehende zentrale Instanz zwingend Standards geschaffen werden müssen. Erst durch eine einheitliche Standardisierung werden VCs interoperabel anwendbar und müssen nicht für jeden Kontext neu ausgestellt werden. Im Zuge dessen hat die internationale Gemeinschaft zur Standardisierung von Webinhalten (W3C) einen Standard definiert, der digitale Credentials, die diesem Konzept entsprechen, als VC klassifiziert (Sporny et al. 2019). Darüber hinaus besitzen diese VCs verschiedene Charakteristika, die für die technische Funktionsweise notwendig sind. Diese Bestandteile und Charakteristika werden im Folgenden vorgestellt.

Bestandteile und Charakteristika von VCs

SSI basiert auf dem Konzept der asymmetrischen Kryptografie (Public Key Cryptography), beruhend auf Private-Public-Key-Paaren (Keys). Der VC-Ersteller, der im Folgenden Issuer genannt wird, erstellt mit seinem geheimen Schlüssel (Private Key) für das VC eine digitale Signatur. Diese hängt er als eine Art digitale Unterschrift dem VC an. Nun kann jeder mithilfe des öffentlichen Schlüssels des Issuers (Public Key) überprüfen, dass die Signatur mittels des zugehörigen Private Keys berechnet wurde, ohne diesen Private Key jemals gesehen zu haben. Damit kann die Integrität des VCs bestätigt werden, sofern der Verifier davon überzeugt ist, dass der Issuer seinen Private Key geheim hält.

Dafür besteht ein VC aus einer Reihe von Behauptungen (Claims) über die Eigenschaften einer Entität. VCs können auch Metadaten zur Beschreibung von Eigenschaften des VCs enthalten, wie z. B. den Aussteller, das Ablaufdatum, einen öffentlichen Schlüssel für Verifizierungszwecke oder einen Widerrufsmechanismus (Sporny et al. 2019). Darüber hinaus kann kryptografisch durch die Verwendung eines öffentlichen Schlüssels zur Signatur der VCs belegt werden, wer das VC ausgestellt hat und welchen Inhalt das VC bei der Ausstellung hatte. Die typischen Inhalte eines VCs sind in Abbildung 4 dargestellt.

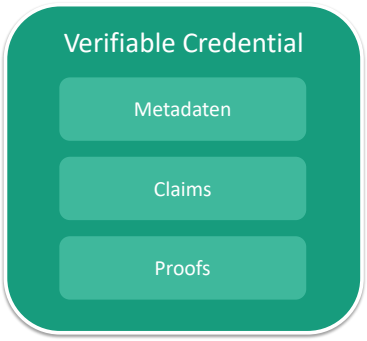


Abbildung 4: Bestandteile eines VCs

VCs werden durch verschiedene Eigenschaften charakterisiert. Die wichtigsten vier werden im Folgenden näher erläutert.

(1) Charakteristikum der Privatsphäre

Eines der zentralen Ziele der SSI-Architektur ist, persönliche Daten zu schützen und nur so viele Daten über das Subjekt des VCs preiszugeben, wie unbedingt notwendig sind. So ist es am Einlass einer Diskothek für den Sicherheitsdienst nicht notwendig, den vollständigen Personalausweis mit allen Angaben zu prüfen. Ihm würden zwei Informationen reichen: ein Beleg, dass der Partygast wirklich das Subjekt des Zertifikats ist (in dem Fall abgebildet durch das Lichtbild in dem Ausweisdokument, die Augenfarbe und Körpergröße), und ein Beweis, dass der Gast mindestens 18 Jahre alt ist. Genau das ist mit der SSI-Architektur umsetzbar: Die SSI-Architektur ermöglicht einen domänenübergreifenden Austausch von verifizierbaren Daten zwischen Verifier und Holder, ohne dass der Issuer an der Interaktion beteiligt sein muss. Das allein schafft bereits einen Mehrwert für Effizienz (wiederholte und hochautomatische Nutzung von bestehenden Zertifikaten) und Privacy (der Issuer erfährt nicht jede Interaktion, im Gegensatz zu föderiertem Identitätsmanagement, in dem der Identitätsprovider als Issuer und Holder eines innerhalb der Domäne universellen Identity-Zertifikats betrachtet werden kann).

Diese Informationen können durch Signaturverfahren auf Echtheit überprüft werden. Möglich wird dies durch ZKPs, mit denen z. B. gezeigt werden kann, dass eine Person über 18 Jahre alt ist, ohne das Geburtsdatum preiszugeben.

(2) Charakteristikum des (aktiven) Berechtigungsnachweises

VCs haben jedoch das Charakteristikum, dass sie immer nur einen „aktiven" Berechtigungsnachweis darstellen. Somit können VCs Nutzer*innen niemals in ihren Handlungen einschränken, sondern müssen Befugnisse oder Vorteile für das Subjekt des Credentials ermöglichen. Beispielsweise ist es leicht möglich, mittels einer verifizierten Vereinsmitgliedschaft nachzuweisen, dass man als Privatperson Mitglied eines Vereins ist. Jedoch ist es nur schwer bzw. nicht möglich nachzuweisen, dass eine Privatperson nicht Mitglied eines Vereins ist. Konkret kann mittels des Einsatzes von Zertifikaten nicht bewiesen werden, dass eine gewisse Eigenschaft (z. B. eine Vereinsmitgliedschaft) nicht vorliegt, da Holder nicht gezwungen werden können, entsprechende Zertifikate aus ihrer digitalen Wallet vorzuzeigen (Tobin 2019).

(3) Charakteristikum der Vereinheitlichung

Zur einheitlichen Nutzung von VCs müssen sich alle Parteien über den Aufbau des VCs einig sein, wodurch die Standardisierung von VCs entscheidend ist. Ferner müssen aber auch alle Parteien ein gemeinsames Verständnis davon haben, wie jedes spezifische VC auszusehen hat. Nur wenn alle Teilnehmenden ihre Berechnungen auf Basis der gleichen Struktur durchführen, kann es schlussendlich zu einem Konsens über die Zulässigkeit des VCs kommen. Aus diesem Grund ist in jedem VC ein nach Möglichkeit standardisiertes Credential-Schema referenziert, das angibt, wie ein solches VC strukturiert sein muss. Das Schema kann dabei allen Parteien zugänglich sein, was die Verwendbarkeit des VCs durch alle Beteiligten sicherstellt. Der Vorteil eines umfassenden Zugriffs aller Parteien ist dementsprechend eine erhöhte Interoperabilität (Hardman 2019a).

(4) Charakteristikum der Authentifizierung

Jedes VC muss eindeutig an eine Person, eine Institution, ein Tier oder einen Gegenstand gebunden sein. Damit der Holder aber später unter verschiedenen Pseudonymen auftreten kann, muss das VC an das Subjekt als Ganzes gebunden sein – und nicht nur an das Pseudonym, unter dem das Subjekt einer Identität bekannt ist. Kryptografische Verfahren ermöglichen es, die Kontrolle von Berechtigungsnachweisen an ein nur dem/der Besitzer*in bekanntes Geheimnis,

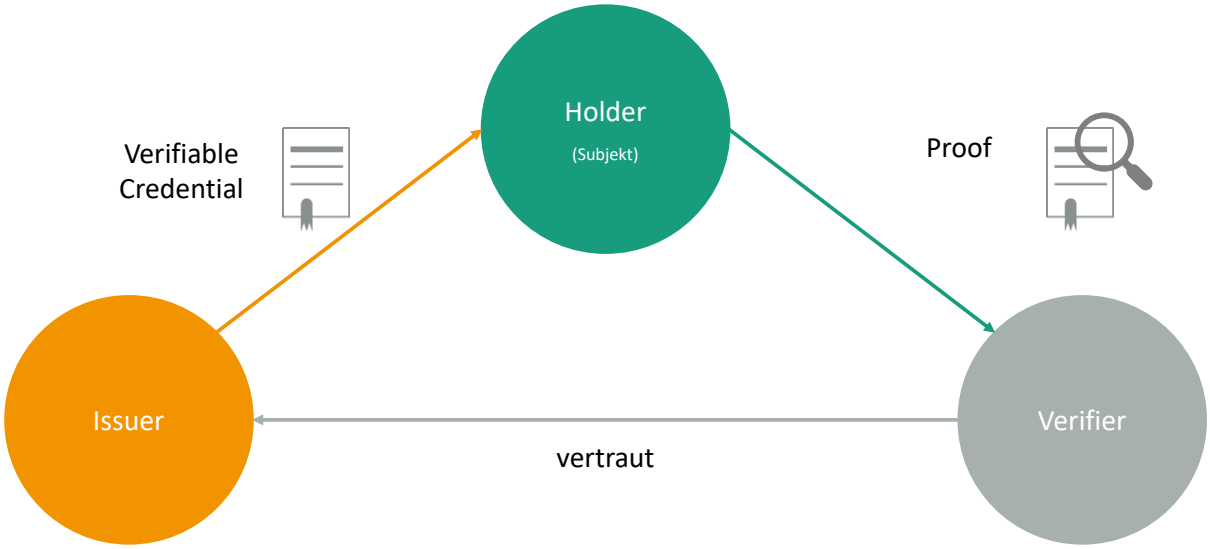


Abbildung 5: Rollen in einem SSI-System

das Link Secret (oftmals auch Master Key genannt), zu knüpfen. Ähnlich wie bei einem Private Key handelt es sich um eine zufällig generierte Zahl, die aber immer geheim bleibt. Es dient dazu, verschiedene digitale Zertifikate aneinander und damit an eine Person binden zu können, ohne es im Klartext vorzeigen zu müssen.

Zusammenfassend lässt sich festhalten, dass VCs aus einer Reihe belegbarer Attribute bestehen, die kryptografisch signiert sind und auf Basis von VC-Schemata interpretiert und geprüft werden können (Sporny et al. 2019).

Rollen in einem SSI-System: Issuer, Holder und Verifier

VCs bestehen aus individuell belegbaren Claims, die von einer Partei kryptografisch signiert und damit bestätigt wurden. Zudem besitzen sie, abhängig vom jeweiligen Kontext, einen spezifischen Überprüfer. Im Folgenden werden die Rollen, die im Kontext von Interaktionen mit VCs auftreten, vorgestellt und definiert:

(1) Issuer

Die Rolle des Issuers übernehmen vertrauenswürdige Parteien, deren Identität und damit einhergehend deren Public Key öffentlich einsehbar sind. Ob ein Issuer vertrauenswürdig ist oder nicht, wird vom jeweiligen Verifier selbst bewertet. Ein Issuer kann eine öffentliche Institution wie beispielsweise eine Hochschule sein. Der Issuer erstellt ein VC, das beliebige Attribute des jeweiligen Identitätsinhabers bestätigt, z. B. ein Hochschulzeugnis. Schließlich signiert der Issuer das VC digital. Die so entstehenden digitalen Dokumente werden den Holdern, etwa den Studierenden, ausgestellt, die in der Regel das Subjekt des VCs sind und dieses auf ihrem privaten Speicher ablegen (Sporny et al. 2019).

(2) Holder

Der Holder ist der Besitzer, der die Claims auf Basis erworbener VC geltend machen kann. Der Holder eines VCs kann ein Mensch, eine Organisation oder ein Ding sein. Neben diesen miteinander agierenden Parteien gibt es noch eine weitere Rolle: das Subjekt des Zertifikats. Das Zertifikat bescheinigt dem Subjekt ein Attribut. In SSI-Lösungen ist oftmals der Holder das Subjekt des Zertifikats. Das VC muss jedoch nicht an den Holder gebunden sein (Sporny et al. 2019). So ist der Fahrzeugschein oder die TÜV-Plakette eines Fahrzeugs nicht an den Fahrzeughalter, sondern an das Fahrzeug selbst gebunden, jedoch würden aktuell die wenigsten Fahrzeuge in der Lage sein, ihre VCs selbst in ihrer eigenen digitalen Wallet zu speichern und zu verwalten.

(3) Verifier

Der Verifier fragt Identitätsinformationen bzw. Attribute bei deren jeweiligem Holder an. Er erhält diese in Form einer Verifiable Presentation (VP) auf Basis zuvor von ihm festgelegter Anforderungen durch einen oder mehrere Claims

sowie einen Beweis von deren Korrektheit. Der Verifier bestimmt also mittels dieser Anfrage, eines sogenannten Proof Requests, welche Informationen nachgewiesen werden müssen. Der Proof Request selbst ist eine Nachricht an den Holder, die die zu überprüfenden Claims und entsprechenden Bedingungen beschreibt, die der Holder erfüllen muss (Nauta und Joosten 2019). Dazu können z. B. auch Nachweise über die Gültigkeit der VCs zu einem gewissen Zeitpunkt bzw. die ausstellende Organisation zählen.

Zur Verdeutlichung soll folgendes Beispiel dienen:

Ein Holder möchte ein neues Bankkonto erstellen. Beim Eröffnen eines Bankkontos benötigt die Bank den vollen Namen und weitere persönliche Informationen des Subjekts zur vollständigen Eröffnung des Kontos. Somit beantragt die Bank mittels eines Proof Requests die erforderlichen Informationen bei dem Holder. Der Holder, der nun als Prover agiert, kann die Anforderungen dann akzeptieren und die zugehörige VP dem Verifier übermitteln.

Zum Vergleich benötigt das Beispiel des Eintrittes in die Diskothek lediglich eine Link-Secret-Referenz[1], die im Rahmen des ZKP einen höheren Grad an Privatsphäre garantiert. Letztlich gilt: Der Verifier muss einen für den Anwendungsfall angemessenen Proof Request zur Authentifizierung ausstellen. Ein Verifier kann eine Polizeibeamtin, eine Website, bei der sich der Holder anmelden will, oder auch das Sicherheitspersonal einer Diskothek sein. Wichtig ist nur, dass der Verifier dem Issuer, der Identität des Issuers und dessen Berechtigung zur Ausstellung eines solchen Zertifikats vertraut. Darüber hinaus braucht der Verifier keine aktive Verbindung zum Issuer, da durch die kryptografische Signatur auch ohne direkten Kontakt zum Issuer überprüft werden kann, ob das Zertifikat gefälscht wurde (Sporny et al. 2019).[2] Nur der Signaturschlüssel des Issuers muss dem Verifier bekannt sein.

Zusammenfassend lassen sich die interagierenden Rollen von SSI wie folgt beschreiben:

(1) Der Issuer stellt das VC mit den im Credential-Schema festgelegten Attributen aus.
(2) Der Holder/ Prover verwaltet das VC und präsentiert dieses gegenüber dem Verifier im Rahmen der VP.
(3) Der Verifier prüft, ob die Attribute des VCs bestimmten Anforderungen entsprechen.

Diese drei Rollen interagieren im Prozess von SSI stetig miteinander und werden Triangle of Trust genannt. Sowohl Issuer und Holder als auch Holder und Verifier stehen im Laufe des Lebenszyklus eines VCs im direkten Austausch. Zwischen Issuer und Verifier besteht zum Zeitpunkt der VP nicht notwendigerweise ein direkter Kontakt, jedoch ein Vertrauensverhältnis des Verifiers gegenüber dem Issuer. Bei der VP ist insbesondere keine Interaktion des Issuers mit dem Holder oder dem Verifier erforderlich. Dieses Schema ist in Abbildung 5 dargestellt.

Zur Verdeutlichung soll folgendes Beispiel dienen: Bei föderierten Identitätsstrukturen, bei denen Identity Provider die Identitäten der Nutzer*innen verwalten, übernimmt ein Identity Provider die Rolle des Issuers und des Holders. Die Nutzer*innen, die sich bei einer Website anmelden wollen, sind nur das Subjekt des Zertifikats, nicht der Holder. Die Nutzer*innen bitten den Identity Provider nur, einer Website die Daten zugänglich zu machen, sind dabei aber komplett vom Identity Provider abhängig. Die Website ist in diesem Konstrukt eine Art Verifier, muss sich aber selbst auch vorher beim Identity Provider registriert haben und diesem zusätzlich vertrauen.

SSI-Lösungen versuchen, in einer neuen Architektur die Benutzerfreundlichkeit der föderierten Architektur mit einem nutzerzentrischen Ansatz zu verknüpfen.

[1] Verifier, die vom Holder die Vorlage der Attribute mehrerer von verschiedenen Issuern ausgestellter verlangen, benötigen einen Nachweis, dass diese VCs tatsächlich für ein und denselben Holder ausgestellt wurden. Holder können diesen Nachweis erbringen, indem sie die Issuer auffordern, eine maskierte Version ihres privaten verbindlichen Geheimnisses (Link Secret) in ein von ihnen ausgestelltes VC aufzunehmen; sie können dann für jede beliebige Kombination von VCs einen Nachweis erstellen, der beweist, dass sie alle eine maskierte Version desselben verbindlichen Geheimnisses enthalten (ohne das verbindliche Geheimnis selbst preiszugeben).

[2] Dies ist zwar auch beispielsweise beim X.509-Zertifikat der Fall, jedoch benötigen SSI-Lösungen keine dritte Partei (CA), zu der ein beidseitiges Vertrauensverhältnis bestehen muss.

Decentralized Identifiers

Zur Gestaltung von interoperablen SSI-Lösungen zwischen Identitätsinhabern wurde ein Standard festgelegt, mit dem Identitäten eindeutig sogenannten DIDs zugeordnet werden. Ein DID ist ein Universally Unique Identifier (UUID)[3] mit speziellen Eigenschaften und ermöglicht dem Controller des DID somit eine universell einsetzbare Kennzeichnung seiner Informationen.

DIDs sind eine neue Art von Identifikatoren, die eine überprüfbare, dezentralisierte digitale Identität ermöglichen. Ein DID identifiziert ein beliebiges Subjekt (z. B. eine Person, eine Organisation, eine Sache, ein Datenmodell usw.), über dessen Identifizierung der Controller des DID entscheidet (Reed et al. 2020). Ein DID besteht dabei aus dem URL-Schema DID, gefolgt von einer DID-Methode[4] und einem DID-methodenspezifischen Identifier (siehe Abbildung 6).

Mit DIDs werden Teilnehmer*innen identifiziert. Dabei können Nutzer*innen beliebig viele verschiedene DIDs besitzen, denn jede einzelne Interaktion könnte durch einen separaten DID abgebildet werden. Durch diese Vielfalt kann die Privatsphäre der einzelnen Nutzer*innen geschützt werden, da mit jedem einzelnen DID ein eigener Kommunikationskanal eröffnet wird (Reed et al. 2020).

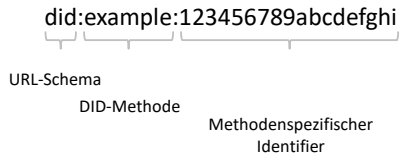


Abbildung 6: Bestandteile eines DID

Mit einem DID-Resolver (siehe Abbildung 7) wird eine DID-Auflösungsfunktion ausgeführt, die einen DID als Eingabe nimmt und ein sogenanntes DID-Dokument zurückgibt. DID-Dokumente spezifizieren, auf welche Weise mit dem DID-Subjekt interagiert werden kann. Das Subjekt sind die jeweiligen Teilnehmer*innen, die durch den DID identifiziert und durch das DID-Dokument beschrieben werden. Jedes DID-Dokument referenziert genau auf einen DID. Dagegen werden Teilnehmer*innen, die in der Lage sind, Änderungen an einem DID-Dokument vorzunehmen, DID-Controller genannt. Ein DID kann dabei mehr als einen DID-Controller haben. Ein DID-Controller kann gleichzeitig aber auch das DID-Subjekt sein (Reed et al. 2020).

Auf welcher technischen Infrastruktur die DID-Dokumente gespeichert werden, wird bei den verschiedenen DID-Methoden unterschiedlich

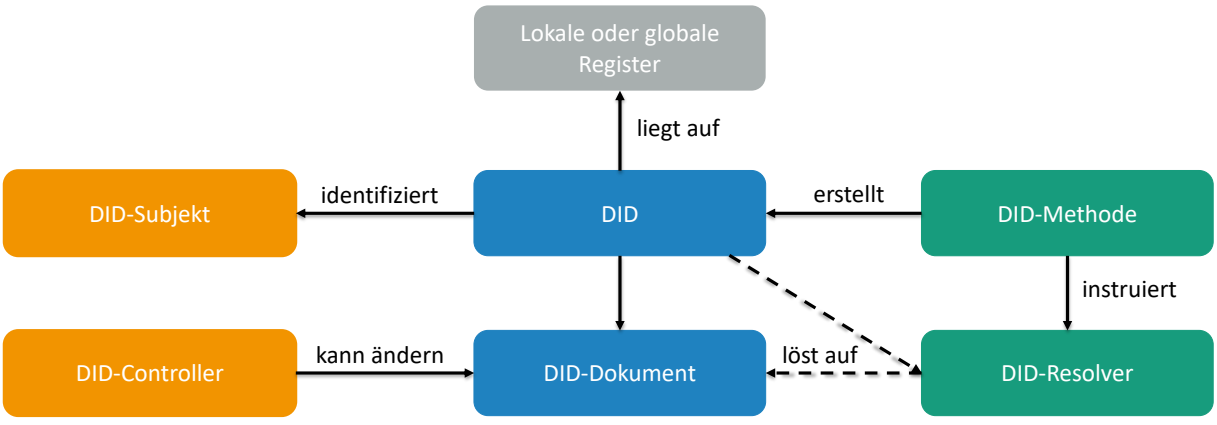


Abbildung 7: DID-Architektur

3 UUID entsprechen einer 128-Bit-standardisierten Identifikationsnummer, die dazu verwendet wird, ein einzigartiges Identifikationsmerkmal zur Kennzeichnung von Informationen abzubilden.

4 Eine Definition, wie ein bestimmtes DID-Schema auf einem bestimmten überprüfbaren Datenregister implementiert werden kann. Programmierer wählen designspezifisch, mit welcher Recheninfrastruktur sie arbeiten wollen (z. B. Blockchain, Distributed Ledger, Decentralized File System, Distributed Database, Peer-to-Peer Network). Die Spezifikation für einen bestimmten Typ von DID wird als DID-Methode bezeichnet.

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "controller": "did:example:123456789abcdefghi",
  "authentication": [{
      "id": "did:example:123456789abcdefghi#keys-1",
      "type": "RsaVerificationKey2020",
      "controller": "did:example:123456789abcdefghi",
      "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "service": [{
      "id": "did:example:123456789abcdefghi#vcs",
      "type": "VerifiableCredentialService",
      "serviceEndpoint": "https://example.com/vc/"
  }]
}
```

Abbildung 8: Beispiel für ein DID-Dokument (JSON-LD)

gehandhabt. DID-Dokumente sind typischerweise im JSON-LD-Format geschrieben und werden in Abbildung 8 gezeigt (Reed et al. 2020).

Zum Verständnis des Aufbaus eines DID-Dokuments werden im „@context"-Abschnitt ein oder mehrere Uniform Resource Identifier (URI)[5] referenziert. Das DID-Subjekt wird unter „id" aufgeführt. Die DID-Controller werden im Abschnitt „controller" bestimmt. Wer im Namen dieses DID kommunizieren darf, wird im „authentication"-Abschnitt aufgeführt. Mit den angegebenen Public Keys und dem entsprechenden Authentifizierungsalgorithmus kann nachgeprüft werden, ob der zur Authentifizierung angegebene Beweis gültig ist. Neben „authentication" gibt es noch weitere Methoden, auf die hier jedoch nicht tiefer eingegangen werden soll. Diese und weitere Bestandteile eines DID-Dokuments werden detailliert im DID-W3C-Standard (Reed et al. 2020) beschrieben. Im Abschnitt „service" können die verschiedenen Endpoints definiert werden, mit denen das DID-Subjekt angesprochen werden kann. Je nachdem, welcher Service in Anspruch genommen werden soll, können unterschiedliche Endpoints existieren. Jedoch können Endpoints, die auf die gleiche Domain referenzieren, Möglichkeiten zur Korrelation zwischen verschiedenen DID-Dokumenten und damit DIDs bieten.

Mithilfe von digitalen Signaturen können DID-Dokumente überprüft werden. Die Signaturen offenbaren dabei nicht direkt die aktuellen Besitzverhältnisse des DID, da die Keys im Laufe der Zeit geändert werden können. Es muss vielmehr eine gültige Kette an Änderungen vorgelegt werden, die jeweils mit dem dazu befähigten Key signiert wurden. Erst so können aktuelle Besitzverhältnisse klargestellt werden. Der Besitz des Private Keys kann aber auch für jeden anderen Zeitpunkt nach Erstellung des DID-Dokuments abgefragt werden.
Dem Besitzer der DID wird dabei über einen im DID-Dokument angegebenen Service Endpoint eine Anfrage geschickt, die beispielsweise eine mit dem Public Key verschlüsselte Nonce (Zufallszahl) beinhaltet (Reed et al. 2020). Erst mit der korrekten Antwort kann der Besitz bewiesen werden.

Wer und wie viele Teilnehmende in einem Netzwerk einen bestimmten DID und das zugehörige DID-Dokument kennen, ist dabei vom Anwendungsfall abhängig. Daher gibt es verschiedene Ansätze für Datenregister, wie DIDs und DID-Dokumente abgespeichert werden. Die zwei wichtigsten Ansätze werden im Folgenden erläutert.

(1) Microledger

Aus Sicht des Datenschutzes, insbesondere zur Einhaltung von Datenschutzbestimmungen wie der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU), ist die ideale Kennung ein paarweiser, pseudonymer DID. Dieser DID (und das zugehörige DID-Dokument) ist nur den

5 Uniform Resource Identifier (URI) sollen abstrakte oder physische Ressourcen im Internet ansprechen. Was für Ressourcen das sein sollen, kann sich je nach Situation unterscheiden. Es kann sich dabei beispielsweise um Websites handeln, aber ebenso können auch Sender oder Empfänger von E-Mails per URI identifiziert werden. Anwendungen nutzen die eindeutige Identifikation, um mit einer Ressource zu interagieren oder Daten der Ressource abzufragen.

beiden Parteien in einer Beziehung bekannt. Die Parteien haben also einen eigenen privaten Kommunikationskanal, man spricht hier von einem Microledger. Über das Microledger muss eine formelle Verbindung aufgebaut werden können und DID-Dokumente müssen ausgetauscht und aktualisiert werden können. Die Peer-DID-Methode ist der wohl bekannteste Ansatz für diese Architektur (Reed et al. 2019). Sie besitzt die folgende Form:

did:peer:abcdefghi1234

Die DID-Dokumente werden an einem privaten Ort abgelegt, der nur der anderen Partei bekannt ist. Eine initiale Prüfung, wer sich hinter einem DID befindet (DID-Authentifizierung), kann auf Basis eines VCs oder eines bestehenden Kommunikationskanals geschehen.

(2) Public/Private Ledger

Im unternehmensspezifischen Kontext kann es sinnvoll sein, dass ein gesamtes (Unternehmens-) Netz den Identifier kennt. Der DID kann dann in einem am besten dezentral bereitgestellten Register aufgenommen werden. Je nach Anforderung kann dieses Register öffentlich (public) oder nur einer bestimmten Gruppe zugänglich sein (private). Distributed-Ledger-Technologien (DLT), insbesondere Blockchains, weisen hier viele Vorteile auf, weswegen sie in vielen SSI-Lösungen zu diesem Zweck verwendet werden. Die so entstehende Architektur lässt sich gut mit einem Telefonbuch vergleichen: Ähnlich wie Telefonnummern ins Telefonbuch geschrieben werden, können DIDs in einen dezentralen Speicher aufgenommen werden, um einen allgemeingültigen Identifier zur Kontaktaufnahme bereitzustellen.

Obwohl bei SSI oftmals die initiale Kontaktaufnahme zwischen zwei Peers mittels eines öffentlichen DID erfolgt, werden für die weitere Interaktion auf Basis dieser vertrauten Verbindung dann wiederum eigene Peer-DIDs ausgetauscht (Preukschat 2019).

Digital Wallets

Für die Speicherungen von SSI-relevanten Informationen werden sogenannte Digital Wallets benötigt. Diese dienen dazu, die gängigsten Arten von Interaktion mit anderen Self-Sovereign Identities abzuwickeln. Darunter fallen das Signieren von Nachrichten, die Authentifizierung (DID-Auth) oder die Verwaltung der VCs (Vescent et al. 2018). Eine Digital Wallet speichert Keys und Secrets und kann darüber hinaus als Adressbuch verwendet werden, um verschiedene Kontakte und Belege zu vergangenen Interaktionen im SSI-Kontext zu speichern.

Mit dem Decentralized Key Management System (DKMS) wird ein Standard konzipiert, der für die Verwaltung der Private Keys zuständig ist. Ziel dieses Standards ist es, Lock-in-Effekte bei Digital Wallets zu vermeiden (Reed et al. 2019). Neben der Speicherung ist es für den Alltagsgebrauch auch notwendig, Keys wiederherstellen zu können. Beim Verlust einer Digital Wallet (beispielsweise Verlust des Smartphones) dürfen die Keys und damit im schlimmsten Fall der Zugang zur Identität nicht verloren sein, sondern müssen wiederhergestellt werden können. Das DKMS bietet diese zwei Ansätze zur Key-Wiederherstellung:

(1) Offline Recovery

Ein von DKMS unterstützter Lösungsansatz ist die Offline Recovery. Dabei wird ein verschlüsseltes Back-up der Wallet in einer Cloud-Infrastruktur gespeichert. Das verschlüsselte Back-up kann nur mit dem sogenannten Recovery Key entschlüsselt werden. Dieser Key wird an einem sicheren Ort verwahrt und garantiert so, dass die Wallet mit den entsprechenden Keys wieder entschlüsselt werden kann (Reed et al. 2019). Das verhindert zwar, dass bei Verlust des Smartphones und der darauf gespeicherten Wallet die zugehörigen Keys verloren gehen. Jedoch muss, ähnlich wie bei einer Bitcoin-Wallet, über längere Zeit ein Key aufbewahrt werden und darf nicht verloren gehen. Dieser Ansatz allein schützt also nicht vor einem Verlust des Keys, sondern lediglich einer lokal genutzten technischen Infrastruktur.

(2) Social Recovery

Ein zweiter Ansatz ist die Social Recovery. Dabei werden ein oder mehrere vertrauenswürdige Identitäten benannt, die Daten verwahren, die die Wiederherstellung ermöglichen. Ein Beispiel für Social Recovery ist das Shamir-Secret-Sharing-Verfahren. Dabei wird nur eine zuvor festgelegte Teilmenge aller vertrauenswürdigen Identitäten benötigt, um die kryptografischen Keys wiederherzustellen. Das Verfahren ist vergleichbar mit einer in Stücke gerissenen Schatzkarte, bei der jedoch nur eine bestimmte Anzahl an Stücke benötigt wird und keines der Stücke essenziell zur Wiederherstellung ist.

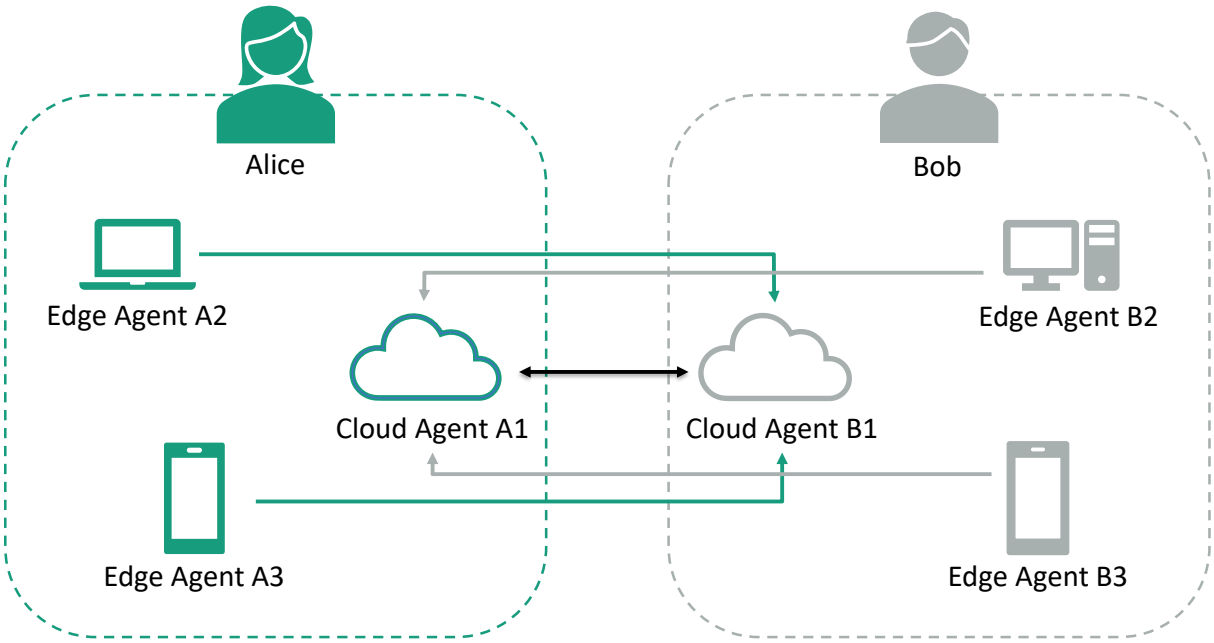


Abbildung 9: Agent-zu-Agent-Kommunikation

So könnte beispielsweise ein Minimum von drei bis fünf vertrauenswürdigen Signaturen notwendig sein, um die Key-Wiederherstellung zu ermöglichen (Reed et al. 2019).

Digital Agents und Hubs

Damit Nutzer*innen möglichst sicher und ohne Ausfallzeiten mit einem SSI-Netzwerk interagieren können, gibt es sogenannte Agents. Diese aktualisieren Kontaktdaten zu anderen Identitäten (Vescent et al. 2018) und können als Service Endpoint auf Anfragen im Kontext einer Identität eingehen. Ein Agent für SSI-Lösungen sollte drei grundlegende Eigenschaften besitzen (Hardman 2019b):

(1) Er fungiert als Treuhänder im Namen eines einzelnen Identitätsinhabers.
(2) Er enthält kryptografische Keys, die ihm zu Ersterem autorisieren.
(3) Er interagiert mit interoperablen DID-Protokollen. Die DIDComm Working Group hat sich das Ziel gesetzt, diese Interaktion mit dem DIDComm-Protokoll zu standardisieren (DID Communication Working Group 2019).

Agents bilden das Bindeglied zwischen den Digital Wallets ihrer Nutzer*innen sowie gegebenenfalls zur Kommunikation zwischen Digital Wallets und Distributed Ledgern. Damit agieren die Agents als ein wichtiges Element der Interaktion zwischen Holder, Issuer und Verifier.

Es wird zwischen zwei Arten von Agents entsprechend ihrer jeweiligen Ausführungsumgebung unterschieden (Preukschat 2019). Der Edge Agent läuft auf einem lokalen Gerät, das im Besitz des Identitätsinhabers ist. Edge Agents müssen nicht dauerhaft online sein. Im Gegensatz dazu läuft der Cloud Agent auf einer dem Identitätsinhaber zugänglichen Cloud und bildet so einen dauerhaft zugänglichen Endpoint. Zudem ermöglicht er die Kommunikation zwischen verschiedenen Edge Agents. Dieser Sachverhalt ist in Abbildung 9 dargestellt. Hubs sind eine spezielle Art von Agents, die viele Daten und Services bereitstellen und verwalten, die andernfalls von den Endnutzer*innen gespeichert und betrieben werden müssten (Vescent et al. 2018). Hubs konzentrieren sich primär auf Aspekte des Datenaustausches von Identitäten (Hardman 2019b).

Weiterführende Technologien und Konzepte zur Nutzung von SSI

Neben den grundlegenden Bausteinen sind noch weitere Technologien und Konzepte zur Erweiterung von SSI-Lösungen relevant. Diese können eine erhöhte Sicherheit, höhere Privatsphäre, Konzepte zur klaren Authentifizierung von Identitäten und Schutz bei Geräte- und Key-Verlust ermöglichen.

Key Rotation

Keys sollten in regelmäßigen Abständen geändert werden, um Sicherheitsrisiken vorzubeugen. Bei einer Key Rotation werden die vorherigen Keys widerrufen und neue Keys hinzugefügt. Neben der Rotation gibt es die Möglichkeit, Keys endgültig zu widerrufen. Es reicht nicht, einen Key einfach zu vergessen, da dies nicht vor einer Kompromittierung schützt. Bei einem Smartphone-Diebstahl und dem damit verbundenen Verlust eines Edge Agents muss die Berechtigung des Geräts widerrufen werden können. So ist der Datenwert für den Dieb gering, auch wenn es ihm gelingt, den Agent zu kompromittieren (Reed et al. 2019).

Key Rotations in regelmäßigen Abständen haben folgende Vorteile (Reed et al. 2019):

(1) Technologischer Wandel: Verschlüsselungstechnologien werden ständig weiterentwickelt. Mit der Rotation der Keys kann auch die Verschlüsselungstechnologie geändert werden. Die SSI-Lösung wird dadurch sicherer.
(2) Unrentable Attacken: Selbst wenn Keys von einem Angreifer gestohlen werden können, werden sie durch die Key Rotation schnell unbrauchbar. Attacken sind dadurch weniger rentabel.
(3) Sich ändernde Bedürfnisse: Nach der Beendigung bestimmter Tätigkeiten werden auch die dazugehörigen Keys nicht mehr benötigt. Durch das Ablaufen der Keys werden diese automatisch nach einer gewissen Zeitspanne ungültig.

Key Rotations der DID-Keys brauchen je nach Bestimmung des DID-Dokuments die Zustimmung von einem oder mehreren Agents. Nachdem die Zustimmung der Agents eingeholt wurde, müssen die aktualisierten Keys den Kontakten der Nutzer*innen mitgeteilt werden. Dies geschieht über eine bestehende Microledger-Verbindung der anderen Teilnehmer*innen oder über die Aktualisierung des DID-Dokuments im Distributed Ledger.

Distributed-Ledger-Technologie (DLT)

Ein Prinzip von SSI ist es, möglichst wenig persönliche Daten der Öffentlichkeit zugänglich zu machen, um die Privatsphäre der Nutzer*innen zu schützen. Aus diesem Prinzip ergeben sich die folgenden zwei Problemstellungen:

Erstens ist es in manchen Fällen notwendig, Daten der Öffentlichkeit preiszugeben. So ergibt es beispielsweise für Issuer Sinn, den öffentlichen Identifier und den zugehörigen Service Endpoint im DID-Dokument der Öffentlichkeit zugänglich zu machen, um als vertrauenswürdig zu gelten.

Zweitens ist nicht jedes Credential für unbegrenzte Dauer gültig. Daher muss es eine Möglichkeit für den Issuer geben, Credentials und die damit verbundenen Attribute widerrufen zu können. Man spricht hier von sogenannten Revocations. Bei nachgewiesener Trunkenheit am Steuer sollte z. B. das Führerschein-Credential wieder entzogen werden können. Der Holder kann technisch nicht gezwungen werden, das VC zu löschen. Deswegen muss es eine Möglichkeit geben, die Aktualität des VCs durch den Verifier nachvollziehen zu können.

Theoretisch könnte ein Verifier direkt eine Aktualitätsanfrage an den Issuer des VCs stellen. Ein Ansatz wäre ein zu diesem Zweck betriebener Service Endpoint des Issuers. Die Bereitstellung und Anfrage der Daten muss jedoch dabei in Bezug auf das Datenformat und Protokoll standardisiert sein, zudem unterläuft eine solche Lösung die Bemühung von SSI, eine direkte Interaktion von Issuer und Verifier zu vermeiden. Plattformen können eine sinnvolle Alternative sein, da diese ein gewisses Maß an Standardisierung mit sich bringen und zudem den Vorteil der Ausfallsicherheit bieten.

Diese Plattformen müssen dabei folgende Funktionen erfüllen (Hardman 2019b):

(1) Die Veröffentlichung von DIDs, um diese einer möglichst großen Anzahl von Identitäten bekannt zu machen, was besonders für Issuer wichtig ist.
(2) Ein Revocation Register bereitstellen, das eine Möglichkeit zur Überprüfung der Aktualität von VCs darstellt.

(3) Die Veröffentlichung von Credential-Schema-Definitionen, da die zugehörigen Schemata öffentlich zugänglich sein müssen, um die semantische Interoperabilität der VCs zu gewährleisten.
(4) Die Veröffentlichung der Agent-Autorisierung, damit neben VCs auch die Autorisierung von Agents widerrufen werden kann.

Die Verwendung einer zentralen Plattform würde dabei Abhängigkeiten gegenüber ebendiesen schaffen. Mit DLT, also dezentralen, verteilten Systemen, können genau diese Probleme einer zentralen Plattform umgangen werden. Blockchains, die ein Teilgebiet der DLTs darstellen, werden in bekannten SSI-Lösungen wie Hyperledger Indy benutzt. Blockchains sind verteilte Datenstrukturen, die es erlauben, in Blöcken gruppierte Transaktionen transparent, chronologisch und manipulationssicher zu speichern (Lockl et al. 2020). DLTs und insbesondere Blockchains verbinden mehrere Vorteile, die auch für die SSI-Architektur notwendig sind.

(1) Zuverlässigkeit: Durch die dezentrale, redundante Architektur einer Blockchain ist sie ausfallsicherer als eine zentrale Serverstruktur.
(2) Unveränderlichkeit: Einmal in eine Blockchain geschrieben, können die Transaktionen und die damit auf der Blockchain gespeicherten Daten nicht mehr ohne großen Aufwand verändert oder manipuliert werden.
(3) Transparenz: In der Regel können alle Teilnehmenden im Netzwerk gleichermaßen alle Transaktionen sehen. Statusänderungen wie neue Identifier werden somit direkt architekturbedingt allen Teilnehmenden des Netzwerks gleichzeitig zur Verfügung gestellt.
(4) Kryptografische Signatur: Transaktionen müssen von dem/der Transaktionsersteller*in signiert werden. Dadurch kann der Ursprung der Daten in der Transaktion direkt einem/einer Teilnehmenden zugeordnet werden.
(5) Zeitchronologische Anordnung: Durch die Blockarchitektur einer Blockchain, die die einzelnen Blöcke kryptografisch aufeinander bezieht, entsteht eine verkettete Liste. Damit werden die Blöcke und somit auch die einzelnen Transaktionen automatisch zeitchronologisch angeordnet. Die Aktualität der Daten, etwa die Aktualität des Revocation Registers, kann also einfach nachgeprüft werden.

Für die Implementierung einer Blockchain-Lösung als Teil einer SSI-Lösung gibt es aber auch Restriktionen. So sollten zur Vermeidung von Skalierungsengpässen möglichst wenige Daten auf einer DLT gespeichert werden. Zudem sollten keine personenbezogenen Daten auf einem solchen Ledger im Klartext abliegen. Darüber hinaus wird selbst die verschlüsselte Speicherung von personenbezogenen Daten auf einem gemeinsam genutzten Ledger als unvorteilhaft angesehen, da zukünftige technische Fortschritte (z. B. Quantencomputing) im Zuge deren Weiterentwicklung diese Kryptografie brechen könnten, obwohl sie derzeit noch als nicht manipulierbar gilt (Vescent et al. 2018). Die DSGVO schreibt außerdem in Deutschland vor, dass personenbezogene Daten berichtigt bzw. gelöscht werden müssen, falls die betreffende Person dies fordert (Datenschutz-Grundverordnung 2018). Da Blockchains die Eigenschaft der kryptografischen Manipulationsresistenz aufweisen, dürfen personenbezogene Daten aus rechtlichen Gesichtspunkten nicht auf der Blockchain gespeichert werden.

Credential Revocation

Wie im vorherigen Kapitel beschrieben, braucht es also ein öffentlich zugängliches Gültigkeitsregister, mit dem VCs von den Issuern widerrufen werden können. Erst auf diese Weise können Issuer auf Betrug oder Fehlverhalten reagieren. Aber auch unveränderliche, dauerhafte VCs müssen widerrufen werden können, wenn sie irrtümlich ausgestellt wurden. So muss beispielsweise in seltenen Fällen selbst eine Geburtsurkunde widerrufen und ausgebessert werden können, wenn sie einen Tippfehler aufweist. Die Möglichkeit zur Revocation muss dementsprechend für eine Vielzahl an VCs gegeben sein.

Das Revocation Register sollte bei SSI-Lösungen in der Art implementiert sein, dass folgende Anforderungen erfüllt sind (Hardman 2018):

(1) Performance: Die Prüfung auf Widerruf sollte möglichst unkompliziert und performant ablaufen.
(2) Privacy: Die Prüfung und Veröffentlichung im Revocation Register sollte die Privatsphäre aller Beteiligten wahren.

(3) Contactless: Es sollte möglich sein, auch ohne direkte Kontaktaufnahme mit dem Issuer den Status des VCs zu überprüfen.

Aufgrund der Anforderungen an das Revocation Register setzen SSI-Architekturen häufig auf DLTs. Im Folgenden soll das Revocation Register an dem Beispiel der Blockchain Hyperledger Indy erklärt werden.

Indy benutzt das Prinzip von kryptografischen Akkumulatoren. Ein kryptografischer Akkumulator ist eine Ein-Weg-Zugehörigkeitsfunktion, mit der gezeigt werden kann, dass ein Eintrag Teil des Akkumulators ist, jedoch die anderen Teile dazu nicht offengelegt werden müssen. Man kann sich einen Akkumulator als Zahl vorstellen, die sich als Produkt vieler sehr großer Primzahlen ergibt. Es ist mit großem Rechenaufwand verbunden, einzelne Primfaktoren aus diesem Produkt zu errechnen. Der Beweis, dass eine Primzahl aber Teil des Akkumulators ist, ergibt sich jedoch aus einer einfachen Division. Performante, in der Praxis eingesetzte kryptografische Akkumulatoren können neue Werte zum Akkumulator hinzufügen, ohne seine Länge zu erhöhen. Gemeinsam mit dem Akkumulator wird durch den Issuer eines VCs ein Tails-File publiziert, das alle möglichen Faktoren für das Produkt (den Akkumulator) enthält. Jeder Eintrag in diesem Dokument ist einem VC einer bestimmten Definition zugewiesen. Dem Besitzer eines VCs ist der jeweilige Eintrag bekannt. Durch einen Rest, der sich aus dem Witness-Delta, das gemeinsam mit dem Akkumulator durch den Issuer eines VCs publiziert und aktualisiert wird, ergibt, kann nachgewiesen werden, dass man einen gültigen Faktor für das Produkt besitzt. Das Tails-File muss ebenfalls durch den Issuer eines VCs publiziert werden.

In einem „positiven" Akkumulator werden dann nur die VCs referenziert, die noch nicht widerrufen wurden. So kann die Gültigkeit einfach nachgeprüft werden, ohne den Issuer direkt kontaktieren zu müssen. Dieser Vorgang wird auch Proof of Non-Revocation genannt. In Hyperledger Indy wird der Proof of Non-Revocation erbracht, indem der Holder dem Verifier nachweist, dass er den Wert des Akkumulators unter Verwendung des ihm bekannten Faktors des VCs und allen anderen Faktoren ableiten kann. Der Verifier kann damit prüfen, dass der Holder zum richtigen Ergebnis kam, da die Antwort auf dem Ledger steht, kennt aber die Details der Berechnung nicht (Hardman 2018). So kann die Privatsphäre aller Beteiligten beim Prüfungsprozess gewahrt werden. Man spricht deshalb von einem ZKP.

Zero-Knowledge Proofs

ZKPs sind eine entscheidende Komponente in dem SSI-Paradigma. Sie spielen eine wichtige Rolle zwischen dem Prover und dem Verifier und lösen damit ein Dilemma zwischen diesen beiden Parteien. Die Privatsphäre der einzelnen Nutzer*innen verlangt, dass persönliche Informationen anderen verborgen bleiben. ZKPs ermöglichen die Wahrung der Privatsphäre, da nur die nötigsten Informationen einem Verifier präsentiert werden. In der Regel herrscht ein Zielkonflikt zwischen Minimierung der bereitgestellten Informationen (Privatspähre) und dem oft berechtigten Interesse des Verifiers zur Prüfung von Berechtigungen und Eigenschaften des Holders. ZKPs sind eine kryptografische Lösung für das Spannungsfeld zwischen der persönlichen Privatsphäre des Provers und der Integrität des Verifiers, wobei Letztere so durchgesetzt wird, dass Erstere möglichst wenig kompromittiert wird (Ben-Sasson et al. 2018).

Erklärung eines einfachen Zero-Knowledge Proofs

Stellen Sie sich vor, ihr Freund Bob sei farbenblind. Sie verfügen über zwei Billardkugeln; eine ist rot, eine grün. Ansonsten sind die beiden Kugeln identisch. Da Sie Bob schon öfter hinters Licht geführt haben, bezweifelt er, dass beide Kugeln tatsächlich unterscheidbar sind. Wie beweisen Sie ihm also ohne eine dritte Partei, dass seine Vermutung falsch ist?

Hier kommt der ZKP ins Spiel. Sie geben Bob beide Kugeln, eine in die linke Hand, die andere in die rechte. Bob nimmt nun beide Hände hinter seinen Rücken. Er darf die Kugeln austauschen oder in der Hand behalten. Nachdem dies geschehen ist, holt Bob beide Kugeln wieder hervor und Sie müssen nun „raten", ob die Kugeln vertauscht wurden oder nicht. Dadurch, dass Sie den Unterschied zwischen den beiden Farben erkennen können, können Sie sofort sagen, ob Bob die Kugeln hinter seinem Rücken vertauscht hat oder nicht. Wären die Kugeln nicht unterscheidbar, könnten Sie allerdings ebenfalls mit einer Wahrscheinlichkeit von 50 Prozent richtig raten. Um einen möglichen Zufallstreffer auszuschließen, wiederholen Sie das

Experiment n-mal, bis die Wahrscheinlichkeit, dass die korrekte Zuordnung nur Glück war, für Bob klein genug ist. Bob weiß nun also, dass die Kugeln unterschiedliche Farben haben, allerdings nicht, welche, und nicht einmal, auf welche Art und Weise man die Kugeln unterscheiden kann: ein ZKP.

SSI und Zero-Knowledge Proofs

Der ZKP in dem Beispiel erfordert ein hohes Maß an Interaktion, da immer wieder Informationen zwischen beiden Parteien unter Hinzunahme eines willkürlichen Bestandteils hin- und hergeschickt werden müssen. Man nennt diesen ZKP deswegen einen interaktiven ZKP. Praktisch wird der ZKP aber erst als nicht-interaktiver ZKP, bei dem mehrere Nachrichten auf eine einzelne Nachricht heruntergebrochen werden und deshalb keine stabile Kommunikation über einen längeren Zeitraum notwendig ist.

ZKPs, die bei SSI-Lösungen verwendet werden, haben die Aufgabe, zu beweisen, dass der Holder über spezielles Wissen verfügt. Er muss zeigen können, dass er im Besitz der Signatur des Issuers ist, die ein bestimmtes Attribut bestätigt. Das wird mit einem ZKP mittels VCs bewiesen, ohne dass der Prover dem Verifier die Signatur vorzeigen muss. Konkret bedeutet das, dass mit VCs selektiv Informationen eines Credentials offengelegt werden können, ohne den Inhalt des gesamten Credentials preiszugeben.

Zudem sollten verschiedene Arten von Beweisen ermöglicht werden (Nelson 2018):

(1) Range Proof: Ist eine Person zwischen 18 und 40 Jahre alt?
(2) Membership: Ist eine Person Staatsbürger*in von Deutschland?
(3) Comparison: Stimmt die Identität der Subjekte zweier VCs überein?
(4) Computational Integrity: Sind die Ergebnisse von Berechnungen richtig?

ZKPs im SSI-Kontext sind in der Regel vergleichsweise wenig rechenaufwändig. Der wohl am häufigsten eingesetzte und auch beispielsweise bei Sovrin[6] implementierte ZKP ist ein Beweis, der auf sogenannten Camenisch-Lysyanskaya-Signaturen (CL) basiert (Camenisch und Lysyanskaya 2002). Viele grundlegende Designentscheidungen bestehender SSI-Konzepte sind eben durch diesen ZKP-Ansatz entscheidend geprägt worden.

Statt die einzelnen Attribute des Credentials in einer kollisionsresistenten Hash-Funktion zu einer einzigen Nachricht zusammenzufassen, werden sie bei CL so signiert, dass jede Teilmenge dieser Attribute zusammen mit einer gültigen Signatur gekoppelt und präsentiert werden kann. Der Vorteil besteht darin, dass Informationen selektiert werden können und nicht alle Informationen dem Verifier offenbart werden müssen (Abramson 2019). Dieser Vorgang wird als Selective Disclosure definiert.

Durch ZKPs wird es darüber hinaus möglich, verschiedene Zertifikate beliebig zu kombinieren. Das bedeutet, dass jede Teilmenge der Attribute der in der VP zusammengestellten VCs zusammen mit einer gültigen Signatur präsentiert werden kann. Da die VCs nachweislich auf zwei übereinstimmende Link Secrets ausgegeben wurden, muss auch keine weitere verbindende Referenz wie der Name auf beiden Zertifikaten offengelegt werden. Das macht die Übertragung einer Sammlung verschiedenster Attribute nicht nur sicherer, sondern ist auch für beide Parteien mit einem kleineren Verwaltungsaufwand verbunden (Hardman 2019a).

Konzepte der Authentifizierung

Im Folgenden werden zwei Konzepte vorgestellt, die die Authentifizierung von Nutzer*innen ermöglicht.

(1) Link-Secret-Authentifizierung

Ein Link Secret ist eine Zufallszahl, die niemand kennt, außer der Holder selbst. Das Link Secret wird vom Holder erstellt und in einer nicht einsehbaren, verhüllten Form dem Issuer übermittelt, der es neben verschiedenen Claims in das VC einbettet und signiert. Die Signatur des VCs schließt den identitätsspezifischen Teil (blinded Link Secret) und mehrere klar einsehbare Attribute ein. In späteren Schritten kann dann bewiesen werden, dass zwei VCs an die gleiche Identität ausgestellt wurden. Aus einem blinded Link Secret kann das Link Secret nicht extrahiert werden. Es kann nur kryptografisch bewiesen werden, dass mehrere blinded Link Secrets das gleiche Link Secret als Ursprung haben. Daher können die VCs, die über eine Verbindung

6 Die Sovrin-Foundation ist eine internationale Non-Profit-Organisation mit dem Ziel, ein Ökosystem von SSI-Netzwerken zu etablieren.

(Issuer – Holder) ausgegeben werden, in einer anderen Verbindung ohne Verlust der Privatsphäre durch wechselbare Pseudonyme überprüft werden. Somit kann dem Verifier gezeigt werden, dass mehrere VCs auf das gleiche Link Secret und somit vermutlich auf den gleichen Nutzer bzw. die gleiche Nutzerin ausgestellt wurden (Abramson 2019).

Die Verhinderung der willentlichen Weitergabe (bspw. Verkaufs) des Link Secrets muss jedoch möglichst erschwert werden, da damit die vollständige Identität einer anderen Person angenommen werden kann. Dies kann beispielsweise durch die Nutzung von sicherer Hardware in Mobiltelefonen erreicht werden.

(2) Biometrische Authentifizierung

Ein weiterer Ansatz sieht vor, eine Variation des Link Secrets an die physische Nutzeridentität mittels biometrischer Verfahren zu koppeln, sodass biometrische VCs erstellt werden können. Biometrie stellt die Identität auf der Grundlage von Verhaltens- und körperlichen Merkmalen wie Fingerabdrücken, Gesicht, Iris, Stimme und Gang fest (Hardman et al. 2019). Biometrie spielt in vielen Identitäts-Use-Cases eine wichtige Rolle, da sie in der Lage ist, ein Individuum und dessen Einzigartigkeit zu identifizieren. Die Verwendung hängt jedoch von einer Vielzahl von Faktoren wie der Abgleichgenauigkeit und Privatsphäre ab (Callahan et al. 2019).

Die Angabe biometrischer Attribute birgt ein Spannungsverhältnis: Die vollständige Biometrie (z. B. vollständiger Scan der Iris) ist ein perfekter Korrelator und greift somit stark in die Privatsphäre der Bezugsperson ein. Unvollständige Biometrie führt jedoch zu einer unvollständigen und eventuell unzureichenden Authentifizierung (z. B. Augenfarbe).

Biometrie kann den Betrug mit VCs erheblich verringern, indem sie es dem/der falschen Inhaber*in sehr schwer macht, die VCs unter falscher Identität zu benutzen. Die Vorteile der Biometrie kommen jedoch nicht ohne negative Aspekte (Hardman et al. 2019). Es muss darauf geachtet werden, Prozesse zu entwerfen, die je nach Anwendungsfall Rechte und Verantwortlichkeiten definieren. Dabei müssen sowohl die Privatsphäre geschützt als auch eine ausreichend sichere Identitätsprüfung sichergestellt werden (Hardman et al. 2019):

(1) Bei einem direkten biometrischen Abgleich und Beweis eines biometrischen Datensatzes (Pocket Pattern) zwischen Holder und Verifier kann es also zu Korrelations- und somit Privatsphäre-Problemen kommen.
(2) Daher ergibt es in vielen Fällen Sinn, auf einen Anbieter zurückzugreifen, der die biometrische Übereinstimmung prüft (Biometric Service Provider Pattern). Der Verifier bekommt in diesem Modell keine Information über die biometrischen Daten des Holders, muss aber dem Biometric Service Provider Pattern trauen. Um das Vertrauen zu stärken, können auch mehrere Biometric Service Provider Pattern in den Prozess eingebunden werden.
(3) Eine dritte Möglichkeit ist die Identitätsprüfung anhand von vielen nicht eindeutig in Beziehung zueinanderstehenden, schwachen biometrischen Eigenschaften (Low-Fi Layers Pattern). So ist die Augenfarbe kein starkes Identitätsmerkmal. Die Kombination aus Augenfarbe, Größe, Alter und einem genetischen Fingerabdruck, der zu beispielsweise einem Prozent der Bevölkerung passt, kann aber dem Verifier als Identitätsnachweis genügen. Auf diese Weise kann der Verifier zudem selbst bestimmen, welche Anforderungen auf eindeutige Identifizierbarkeit in einem bestimmten Anwendungsfall nötig sind.

Biometrische Verfahren bieten noch großes Forschungs- und Implementierungspotenzial, sind aber ein essenzieller Faktor, um SSI-Lösungen in der Praxis noch sicherer zu machen und Betrug vorzubeugen.

4 SSI bietet eine Vielzahl praktischer Anwendungs-möglichkeiten

Anwendungsmöglichkeiten

Überblick über verschiedene Anwendungsmöglichkeiten von SSI

Neben der bereits ausführlich beschriebenen Anwendung von SSI für Privatnutzer*innen im Internet ergibt sich aus dem SSI-Paradigma eine Vielzahl neuer Möglichkeiten für Organisationen und individuelle Akteure. Im Folgenden werden beispielhaft drei Anwendungen näher beschrieben.

SSI für das Gesundheitswesen

Der geläufigste und bisher prominenteste Anwendungsfall von SSI findet sich, wie zuvor dargelegt, im Bereich personenbezogener Identitäten. Durch SSI lassen sich fälschungs- und manipulationssichere digitale Versionen von wichtigen persönlichen Dokumenten wie Personalausweis, Reisepass, Geburtsurkunde oder medizinischen Rezepten erstellen. Auch lässt sich durch diese digitalen Identitätsnachweise ein sicherer, passwortfreier Zugang zu Webservices realisieren. Der Einsatz von SSI ist auch für allgemeine Anwendungen denkbar, wie im Folgenden am Beispiel von E-Rezepten gezeigt wird, die Ärzt*innen für Patient*innen ausstellt:

1. Die Verbindungseinladung

Zunächst muss der Agent des Patienten (Holder) mit dem Agenten der Ärztin (Issuer), die das Rezept (VC) ausstellen soll, verbunden werden. Dabei wird ein sicherer Kommunikationskanal aufgebaut. Dazu ermittelt die Ärztin nach Patientenanfrage – auf Basis der (digitalen) Patientenakte – eine (SSI-)ungebundene Anlaufstelle, beispielsweise eine E-Mail-Adresse des Patienten. Über diese Anlaufstelle – oder etwa über ein Display oder Plakat in der Praxis – lässt die Ärztin dem Patienten einen QR-Code zukommen, der einen Einladungslink zur Verbindung beider Parteien enthält: ein „Out-of-Band-Mechanismus".[7]

2. Die Verbindungsanfrage

Der Patient kann den QR-Code nun scannen, um mittels des darin verlinkten öffentlichen Schlüssels und des Dienstendpunktes der Ärztin eine sichere Nachricht an sie zurückzuschicken. Falls der Patient die Verbindungseinladung annehmen möchte, erstellt dieser einen neuen DID mit zugehörigem DID-Dokument für die entstehende Verbindungsbeziehung zwischen Patient und Ärztin. Diesen verpackt die Wallet-App des Patienten im Sinne einer Verbindungsanforderung und schickt sie an die Ärztin zurück.

3. Die Verbindungsantwort

Der Agent bzw. die digitale Wallet der einladenden Ärztin empfängt am anderen Ende die Verbindungsanfrage des Patienten und entschlüsselt sie, um die entsprechende Nachricht mit der Verbindungsanforderung zu finden. Der Identifier in der Nachricht informiert die Ärztin darüber, mit welcher Einladung er diese Nachricht verknüpfen soll. Daraufhin speichert der Arzt diese erhaltenen Informationen im Verbindungsdatensatz des Patienten. Dabei erstellt auch die Ärztin einen DID und ein DID-Dokument, verpackt diese in eine Antwortnachricht und schickt diese Nachricht dann an den Patienten zurück.

4. Der finale Verbindungsaufbau

Der Patient wiederholt diesen Vorgang ebenfalls und speichert den erhaltenen Ärztin-DID und das DID-Dokument im entsprechenden Verbindungsdatensatz. Damit sind Patient und Ärztin mittels eines sicheren, privaten und Ende-zu-Ende-verschlüsselten Nachrichtenkanals verbunden.[8]

5. Ausstellen des Rezeptes

Nach der ärztlichen Untersuchung und der erfolgreichen Verbindung des Patientenagenten und des Agenten der Ärztin stellt sie – mit allen nötigen Informationen auf Basis der ärztlichen Untersuchung und der Patientenakte – dem Patienten über diese Verbindung ein entsprechendes Rezept zur medizinischen Behandlung aus. Der Patient erhält das VC und speichert dieses in seiner digitalen Wallet. Gegebenenfalls wird im Zuge der Ausstellung sofort oder etwa kumuliert am Abend das zu dem VC gehörige Revocation Register von der Ärztin aktualisiert.

6. Initialisierung der Medikamentenvergabe durch die Apotheke (Verifier)

Im nächsten Schritt beginnt die eigentliche Ausgabe des Medikaments. Mittels der digitalen Wallet fragt der Patient die Apotheke nach

[7] Die Einladung ist ein JSON-Datenpaket, das einen eindeutigen Identifier und dieselbe Art von Informationen wie das DID-Doc enthält – insbesondere befinden sich darin auch ein öffentlicher Schlüssel und ein Dienstendpunkt.

[8] Der Prozess des Verbindungsaufbaus (Punkt 1–4) erfolgt in der realweltlichen Anwendung von einigen Bestätigungsaufforderungen bis hin zu voll automatisiert ab.

einem bestimmten Medikament – entsprechend dem ausgestellten Rezept – an. Daraufhin möchte die Apotheke spezifische Daten des Patienten erhalten, die in dem Sinne überprüfbar sind, dass die Herkunft der nachgefragten Attribute auf einen Vertrauensanker, in diesem Fall die Ärztin, zurückgeführt werden kann.[9] Die Abfrage erfolgt in einem standardisierten Schema, einem sogenannten Proof Request. Dies umfasst etwa die vorzuzeigenden Attribute (Name des Patienten, Name der Ärztin, Medikament, Gültigkeitsdatum), die akzeptierten Aussteller (Public Keys vertrauenswürdiger Ärzt*innen) und gegebenenfalls einen Beweis, dass das VC nicht bereits vor Ablaufdatum zurückgerufen wurde.

7. Der digitale Nachweis (Proof)

Die digitale Wallet des Patienten kann dieser Anfrage nachkommen, indem es auf Basis eines darin gespeicherten VCs, das die im Proof Request formulierten Anforderungen erfüllt, die vorzuzeigenden Attribute übermittelt – inklusive eines Nachweises, dass diese genau so von der Ärztin ausgestellt wurden.[10] Dieser Nachweis heißt auch Verifiable Presentation und kann von der Apotheke mittels des öffentlichen Schlüssels der Ärztin sowie – falls eine Prüfung auf Revocation erforderlich ist – des öffentlichen Standes des Revocation Registers (lokal, von einer Blockchain oder einer vertrauenswürdigen Datenbank) abgerufen werden.

8. Genehmigung der Medikamente

Nachdem die Apotheke die Gültigkeit der angegebenen Rezeptinformationen verifiziert hat, erfolgt nach der Prüfung und Verarbeitung letztlich die Genehmigung zur Ausgabe oder zum Versand des entsprechenden Medikaments. In der realen Anwendung des Beispiels der E-Rezepte muss zudem in der Regel eine Mehrfachverwendung von E-Rezepten verhindert werden. Zwar könnte das Einlösen der E-Rezepte durch eine eindeutige ID von E-Rezepten protokolliert werden, jedoch würde dies die Mehrfachverwendung nur in derselben Apotheke (bzw. den an dem System des Verifiers beteiligten Apotheken) verhindern. Zur apothekenübergreifenden Protokollierung sind weitere Double-Spend-Mechanismen notwendig. In diesem Fall kann etwa die Blockchain-Technologie dazu verhelfen, mit einem dezentralen System Mehrfachverwendung zu verhindern, etwa, indem man das VC mit einem Token, der keine sensitiven Daten beinhaltet und nur das Double-Spending verhindert, koppelt.

SSI für den E-Commerce

Dieser Anwendungsfall birgt im Zuge der voranschreitenden Digitalisierung ein enormes Potenzial, da er sich auch auf weitere Beispiele des E-Commerce und andere Supply-Chain-Fallbeispiele ausweiten lässt. Weltweit steigt der jährliche Umsatz im E-Commerce um knapp 15 Prozent und liegt für das Jahr 2020 bei etwa zwei Billionen Euro (Statista 2020). Dies unterstreicht die enorme zukünftige Bedeutung des E-Commerce und die damit verbundenen Potenziale für den Einsatz von personenbezogener SSI, was im Folgenden ausgeführt wird.

Die rasante Verbreitung von sozialen Medien und E-Commerce-Anbietern hat das Bewusstsein vieler Nutzer*innen für Privatsphäre und Datenschutz erhöht. Da die Abwicklung der Bezahlung oder der Versand von Waren stets die Nutzung von Teilidentitäten erfordern, sind auch die Verifizierung und die Nutzung der Nutzeridentitäten eine Herausforderung (Schneier 2018). So kann beispielsweise bei alkoholhaltigen Getränken das Alter der bestellenden Person aktuell einzig durch den Paketdienst geprüft werden.

Durch eine personenbezogene SSI können im E-Commerce viele Prozesse vereinfacht und beschleunigt werden. Während bisher das finanzielle Transaktionsrisiko häufig durch spezialisierte Anbieter abgefangen wird, können Banken als VCs den sofortigen Nachweis von Finanztransaktionen erstellen, die Kund*innen beim Kauf vorzeigen. Dies verringert das operative Risiko für E-Commerce-Anbieter und macht diese unabhängiger von zentralisierten Zahlungsabwicklern. Auch können dadurch Nachweise gegenüber staatlichen Behörden, z. B. für die Entrichtung der Einkommenssteuer, erbracht werden. Zudem können Elemente von SSI im Bereich E-Commerce mit dezentralen digitalen Währungen, wie z. B. Kryptowährungen, kombiniert werden. So lässt sich neben einem sicheren Nachweis der Identität auch die Zahlung der Ware dezentral abwickeln. Außerdem können Nutzer*innen SSI

[9] In diesem Zusammenhang gehen wir davon aus, dass die benötigten Claims durch die Ärztin attestiert sind und die Apotheke zur Ausgabe der Medikamente den ärztlichen Informationen vertraut.

10 Dieser Nachweis kann auf mehrere Arten erfolgen – etwa durch herkömmliches Vorzeigen der digitalen Signatur des Issuers oder ZKPs.

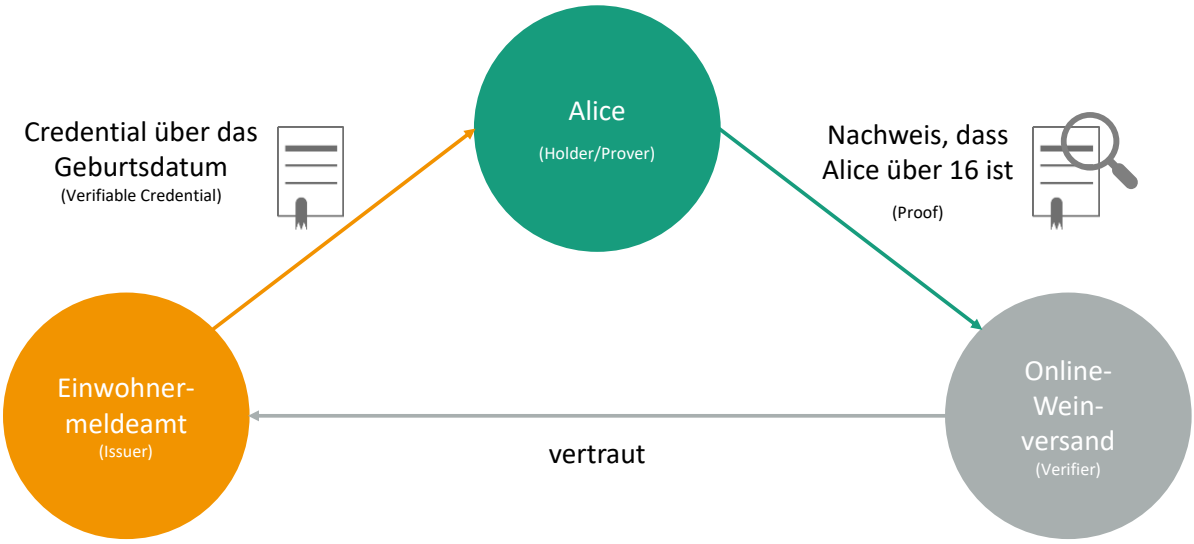


Abbildung 10: Beispielhafte Anwendung einer SSI im E-Commerce

einsetzen, um ihr Alter nachzuweisen, etwa beim Erwerb alkoholhaltiger Getränke (siehe Abbildung 10).

SSI für das Internet der Dinge

Neben personenbezogener SSI ist das potenzielle Anwendungsgebiet noch wesentlich größer. So lassen sich digitale Identitäten nicht nur für Personen, sondern auch für Maschinen, Geräte und andere physische Dinge erstellen. Das aufkommende Internet der Dinge (IoT) sieht die Integration von technologiegestützten physischen Objekten in eine vernetzte Gesellschaft vor (Rosemann 2013) und ermöglicht dabei eine Vielzahl von verschiedenen Interaktionen zwischen Menschen und Maschinen (Oberländer et al. 2018). Beweisbare digitale Identitäten sind entsprechend eine wesentliche Voraussetzung für das Zusammenspiel dieser Vielzahl an Akteuren.

Ein Anwendungsfall an der Schnittstelle von IoT und SSI ist die Nutzung einer SSI für Kraftfahrzeuge. In den letzten Jahren wurden immer mehr digitale Technologien in Autos integriert. Damit interagieren Fahrzeuge mit einer Vielzahl unterschiedlicher Instanzen wie beispielsweise Behörden, Mautstellen, Tankstellen oder Werkstätten. Informationen über das Kraftfahrzeug werden bisher über den Fahrzeugbrief sowie das Serviceheft übermittelt. Somit lassen sich wichtige Informationen der Identität des Fahrzeugs leicht manipulieren und anderen Instanzen vortäuschen. Auch die schnell voranschreitende Entwicklung des autonomen Fahrens unterstreicht die Notwendigkeit für digitale Fahrzeugidentitäten. So lässt sich bereits in absehbarer Zeit ein Anwendungsszenario vorstellen, in dem Taxis als autonom fahrende und ökonomisch unabhängig agierende Einheit im Straßenverkehr auftreten.

Durch VCs kann ein Fahrzeug seine „Geburt", also den Beginn des Fahrzeuglebenszyklus, analog zu einer Geburtsurkunde für Menschen nachweisen. Die Verknüpfung zwischen dem digitalen Abbild des Fahrzeugs, der Vehicle Identity (VID), und dem physischen Objekt wird dabei durch die Fahrzeugidentifikationsnummer (VIN) sichergestellt, die jedem Auto durch den Hersteller zugewiesen wird (Mobility Open Blockchain Initiative 2019). Dies stellt einen kritischen Aspekt in der Verknüpfung von digitaler Identität mit dem physischen Objekt dar, da sich das Objekt – im Gegensatz zu einem Menschen mit in der Regel persistenten biometrischen Eigenschaften – nicht durch eindeutige und schwer auswechselbare Merkmale identifizieren lässt. Die Verbindung mit der VIN ist dabei auch ein Risiko, da diese insbesondere an älteren Fahrzeugen physisch manipuliert werden kann. Sichere Hardwareelemente in zentralen Steuerungskomponenten des Fahrzeugs könnten eine noch höhere Verbindungsstärke auf kryptographische Weise erreichen. Nichtsdestotrotz ist die Kopplung der VID mit der VIN eine verhältnismäßig starke Verbindung für ein physisches Objekt.

Der VID können anschließend weitere Zertifikate, wie z. B. der aktuelle Tachostand oder die Besitzurkunde, zugewiesen werden, die dann in

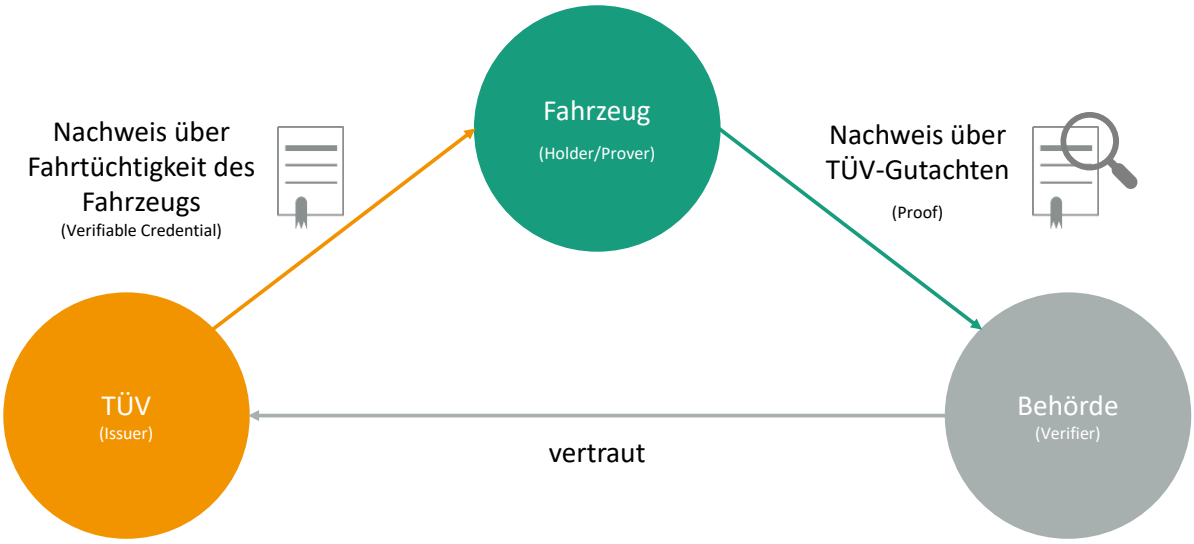


Abbildung 11: Beispielhafte Anwendung einer VID

der Wallet des Fahrzeugs hinterlegt sind. Relevante Instanzen, wie z. B. Behörden, Hersteller, Banken und Fahrzeugbesitzer*innen, können als Issuer auftreten und gewisse Attribute dem Fahrzeug als VCs zuschreiben. Ein Beispiel hierfür ist die erfolgreiche Hauptuntersuchung, die durch den TÜV als VC hinterlegt werden kann und z. B. in einer Verkehrskontrolle benötigt wird (siehe Abbildung 11).

Laut ADAC entsteht aufgrund der „beliebten" Tachomanipulationen bei Gebrauchtwagen allein in Deutschland ein jährlicher Schaden in Höhe von sechs Milliarden Euro (ADAC 2019). Ein Fahrzeug würde darüber hinaus über seine VID auch gegenüber Dienstleistern wie Tankstellen, Mautstellen oder auch Werkstätten wirtschaftlich autark agieren können. Dies senkt die Transaktionskosten für Besitzer*innen und Nutzer*innen von Fahrzeugen, aber auch für die beteiligten Dienstleister.

SSI für öffentliche Institutionen

Auch im Bereich öffentlicher Institutionen lassen sich diverse Anwendungsbeispiele finden, in denen SSI einen Vorteil gegenüber existierenden Lösungen haben. Ein Beispiel hierfür sind Zertifikate, Zeugnisse und Urkunden, die von öffentlichen Institutionen, wie z. B. Universitäten, ausgestellt werden. Diese werden heute in Papierform gedruckt und denjenigen, die sie erworben haben, physisch zur Verfügung gestellt. Diese Dokumente dienen danach in vielfältiger Art und Weise zum Nachweis gewisser Qualifikationen, die z. B. im Rahmen des Studiums erworben wurden. Bisher gibt es bis auf die Erstellung beglaubigter Kopien durch ein Notariat keinerlei Möglichkeiten, die Übereinstimmung des Dokuments mit einem Original nachzuweisen. Insbesondere durch die fortschreitende Digitalisierung von Bewerbungsprozessen in Unternehmen werden bei Bewerbungen häufig nur eingescannte – und damit leicht manipulierbare – Dokumente gefordert. Schätzungen zufolge werden jährlich mit gefälschten Zeugnissen ca. 500 Milliarden US-Dollar umgesetzt (Goldfarb 2019). Daher greifen Unternehmen vermehrt auf professionelle Anbieter*innen zurück, die Echtheitsprüfungen der von Bewerber*innen eingereichten Dokumente durchführen. Diese kostspielige Lösung könnte durch den Einsatz von VCs durch öffentliche Institutionen abgelöst werden.

Eine Universität könnte beispielsweise allen Studierenden ein Zertifikat über ihre aktuellen Leistungen ausstellen. Mit Beendigung erhalten die Studierenden dann ein VC, das ihre Abschlussnote nachweist. Dieses VC können Absolvent*innen in vielfältiger Art und Weise nutzen. Zum einen können bei einem Wechsel der Universität bestehende Leistungen nachgewiesen werden, zum anderen können diese Leistungen auch gegenüber nicht staatlichen Organisationen wie Unternehmen im Rahmen eines Bewerbungsprozesses verifiziert werden (siehe Abbildung 12).

Da Unternehmen durch den Einsatz von VCs einen Großteil ihrer Compliance- und Background-Checks ersetzen können, birgt dieser

Anwendungsmöglichkeiten

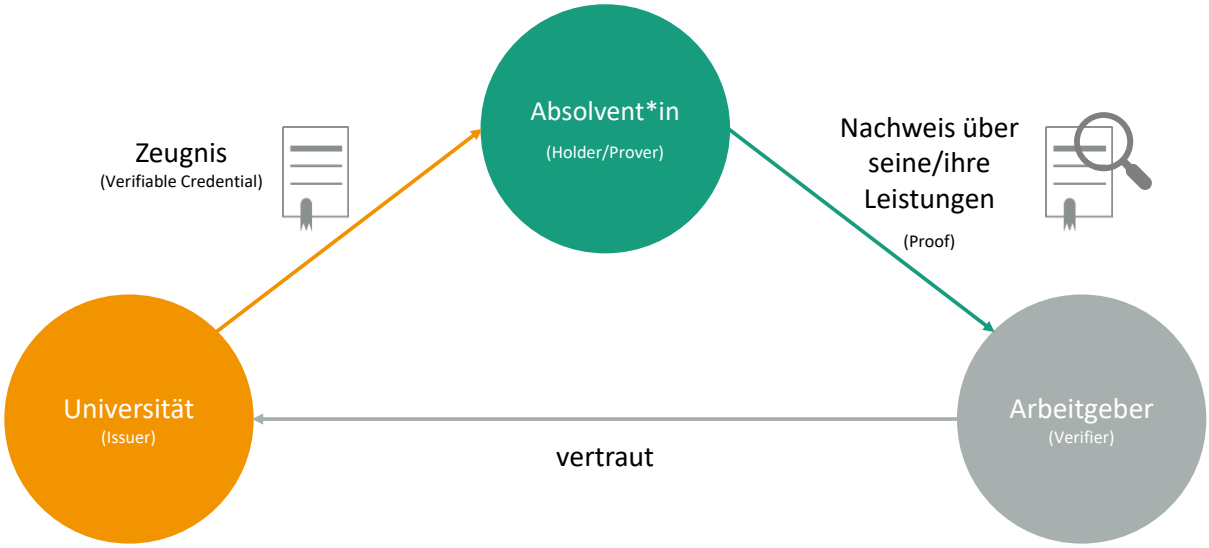


Abbildung 12: Beispielhafte Anwendung von VCs durch Universitäten

Anwendungsfall auch ein hohes ökonomisches Potenzial (World Economic Forum 2020). So ließe sich ein Pilotprojekt in diesem Bereich auch als Anstoß einer weiteren Digitalisierung von Verwaltungsprozessen in öffentlichen Institutionen verstehen. Tabelle 3 fasst abschließend die relevantesten Aspekte der vorgestellten SSI-Anwendungsfälle zusammen.

SSI birgt ein großes ökonomisches Potenzial

Bei einer zunehmenden Nutzung des Internets sowohl von Privatpersonen als auch von physischen Objekten im Kontext des IoT (Rosemann 2013) ist die Notwendigkeit einer sicheren und interoperablen technischen Lösung für digitale Identitäten größer denn je. Mit schätzungsweise 4,2 Milliarden Internetnutzer*innen kann personenbezogene SSI weltweit flächendeckend Anwendung finden (McKinsey & Company 2019; World Economic Forum 2020).

In der Luftfahrtindustrie könnte laut einer Studie des Weltwirtschaftsforums die Einführung von SSI-Lösungen im internationalen Luftverkehr die Abwicklung des Identitätsmanagements effizienter gestalten und somit zu massiven Kosteneinsparungen führen, wobei gleichzeitig mittels verbesserter KYC-Prozesse zusätzlich Kosten eingespart werden könnten (World Economic Forum 2020). In diesem Zusammenhang kann durch den Einsatz einer SSI-Lösung ein erheblicher Teil der Know-Your-Customer (KYC)-Prozesse von Banken vereinfacht werden (World Economic Forum 2020). Für den gesamten Markt für SSI-Lösungen wird bis zum Jahr 2023 ein Marktvolumen von bis zu zwei Milliarden US-Dollar erwartet (MarketsandMarkets 2018). Darüber hinaus sorgt das SSI-Paradigma für fälschungssichere Zertifikate im Bereich der öffentlichen Institutionen. Das Ausstellen fiktiver Zeugnisse von z. B. gefälschten akademischen Abschlüssen täuscht die Öffentlichkeit und betrügt damit Arbeitgeber sowie Kund*innen und richtet darüber hinaus erhebliche Reputationsschäden an. Dementsprechend sind im Bereich der öffentlichen Institutionen mittels des Einsatzes von SSI erhebliche Kosteneinsparungen möglich

Wie in den technischen Grundlagen ausgeführt, werden innerhalb eines SSI-Netzwerks von Teilnehmenden verschiedene Rollen eingenommen. Daraus ergeben sich wiederum auch in einer potenziellen Monetarisierung verschiedene Interessen und potenzielle Möglichkeiten, z. B. die Bereitstellung von Cloud Agents oder Digital Wallets. Dazu werden ebenfalls Betreiber für die technische Infrastruktur wie z. B. Blockchain-Knotenpunkte benötigt. Beispielsweise können auch Issuer ein intrinsisches Interesse an der Ausstellung von Credentials aufweisen. Durch die Auslagerung der Datensouveränität an die Nutzer*innen könnten Issuer die regulatorischen Anforderungen im Transfer von Daten zwischen verschiedenen Ländern per Design umsetzen. Außerdem können durch das regelmäßige Anfordern von VPs der Nutzer*innen im Finanzsektor Anforderungen im Bereich Anti-Money-

Anwendungsmöglichkeiten

Ausprägung	Anwendungsszenario	Vorteile des SSI-Paradigmas
Privatpersonen und Organisationen	Gesundheitswesen und E-Commerce	• Fälschungs- und manipulationssichere digitale Nachweise von wichtigen persönlichen Dokumenten wie Personalausweis, Reisepass, Geburtsurkunde oder medizinischen Dokumenten • Sicherer Zugang zu Webservices • Verbesserte Vertrauensbeziehung zu sensibleren Kund*innen (erhöhte IT-Sicherheitssensibilisierung der Kund*innen) • Prozessverbesserung (z. B. einfacherer Nachweis von Zahlungs- und Adressinformationen)
Physische Gegenstände	IoT-Geräte	• Selbstsouveränes Identitätsmanagement verschiedener IoT-Geräte (z. B. Verwaltung der digitalen Identitäten von Kraftfahrzeugen über den Fahrzeuglebenszyklus) • Essenzielle Rolle digitaler Identitäten im Bereich des autonomen Fahrens (Verwaltung der digitalen Identitäten autonom fahrender Fahrzeuge)
Öffentliche Institutionen	Universität	• Selbstsouveräne und manipulationssichere Verwaltung von Zertifikaten, Zeugnissen oder Urkunden • Optimierung von Verwaltungsprozessen (Background- Compliance-Checks) • Recruiting (Vereinfachung von Recruiting-Maßnahmen und operativer Durchführung)

Tabelle 3: Vorteile von SSI in verschiedenen Anwendungsszenarien

Laundering (AML) und KYC-Prozesse adressiert werden. Ebenfalls sind Unternehmen, beispielsweise in der Finanzbranche, entgegen geläufigen Meinungen nicht unbedingt immer daran interessiert, sensible Kundendaten auf ihren Infrastrukturen zu speichern, da die Verwaltung dieser sensiblen Kundendaten, unter Einhaltung der regulatorischen Anforderungen, umfangreiche Ressourcen bindet. Die Einführung von SSI könnte an dieser Stelle Unternehmen entlasten und damit ebenfalls Kosten einsparen.

Vorteile für Unternehmen durch SSI

Neben dem ökonomischen Potenzial von SSI ergeben sich für Unternehmen weitere Vorteile. So lässt sich durch die Anwendung von SSI die Kontrolle der Zugänge zu den IT-Systemen eines Unternehmens verbessern. Die umfassende Digitalisierung in Unternehmen hat die Anzahl an bestehenden IT-Systemen stark ansteigen lassen. So existiert neben Enterprise-Resource-Planning-, Customer-Relationship-Management, E-Mail- und Projektmanagement-Tools eine Vielzahl an weiteren Systemen. Diese IT-Systeme sind häufig separiert voneinander implementiert worden und lassen damit Datensilos entstehen, die wiederum separiert verwaltet werden müssen. So müssen individuell für alle Mitarbeiter*innen Zugänge erstellt oder gelöscht werden. Dies erfordert eine aufwendige Überwachung und Verwaltung der einzelnen Systeme und führt damit zu einer Vielzahl an redundanten Prozessen zur Erteilung und Verwaltung von Zugriffsrechten, die teilweise noch analog (papierbasiert) durchgeführt werden.

Eine schnelle und sichere Identifizierung und Authentifizierung von Mitarbeiter*innen durch SSI-Lösungen über verschiedene Systeme hinweg könne Kosten durch redundante Verwaltung, Datenspeicherung und Prozesse einsparen. Insbesondere werden im Sinne der „Single Source of Truth“ Redundanzen veralteter Dateiversionen innerhalb der Datenspeicherung reduziert. Konkret bedeutet das eine Verbesserung der Datenqualität. Zudem wird auch ein Schutz vor z. B. Phishing-Attacken, Identitätsdiebstahl (Identity Theft) oder anderen Formen des Betrugs mittels eines konsequent genutzten

asymmetrischen Verschlüsselungsverfahrens (Ende-zu-Ende-Verschlüsselung) gewährleistet. Dies gilt ebenfalls für die Autorisierung, also die Erteilung von z. B. Schreib- und Zugriffsrechten innerhalb von Systemen. Die individuelle Erteilung dieser Rechte im Rahmen einer benutzerbestimmbaren Zugriffskontrolle könnte daher wegfallen, wenn der Zugriff über entsprechende Credentials erfolgt. Außerdem wird durch den Wegfall von individuellen Log-in-Passwörtern und Nutzernamen sowie durch die Kombination mit Multi-Faktor-Authentifikationsverfahren die Anfälligkeit gegenüber individuellen Angriffsvektoren innerhalb der Unternehmen verbessert. In vielen Unternehmen werden von Mitarbeiter*innen aus Bequemlichkeit immer noch einfach zu erratende Passwörter verwendet, um individuelle Zugänge zu sichern. Die Verwendung von SSI für Mitarbeiter*innen in Unternehmen könnte diese Zugänge bei ähnlicher Nutzererfahrung besser absichern. Gleichzeitig würde für neue Mitarbeiter*innen die häufig mühsame Erstellung von individuellen Zugangskombinationen für verschiedene Softwaretools wegfallen.

Auch über Unternehmens- und Organisationsgrenzen hinweg lässt sich SSI einsetzen. Durch diesen Einsatz kann der Zugriff auf IT-Systeme unkompliziert über organisationale und technische Begrenzungen hinweg gesteuert werden und ermöglicht so eine entsprechende Interoperabilität. In diesem Fall lassen sich beispielsweise für einzelne Projekte neue Zugangsberechtigungen für externe Mitarbeiter*innen erstellen, die nach Ablauf des Projekts durch ein Revocation Register einfach widerrufen werden können. Dies verringert die Komplexität im Identitätsmanagement für Unternehmen und kann damit zur Kosteneinsparung beitragen. Gleichzeitig kann damit zu einem gewissen Grad die Gefahr der unberechtigten Weitergabe von Zugriffsdaten umgangen werden.

Zentralisierte Plattformen als Identitätsanbieter, wie z. B. Google, bringen stets die Gefahr einer Monopolstellung. Innerhalb der letzten Jahre wurde daher der Fokus auf die Etablierung dezentraler Plattformen auf Basis von Blockchain-Technologien gesetzt. Diese stehen jedoch häufig in Konflikt mit bestehender Regulierung im Bereich Datenschutz, wie z. B. der DSGVO (European Parliamentary Research Service 2019). SSI könnte daher die Nachteile beider Ansätze umgehen und ein dezentrales Ökosystem im Identitätsmanagement ermöglichen. So können mittels offener Standards und Spezifikationen eine innovative Umgebung geschaffen werden, die weder durch eine Herstellerbindung (Vendor-Lock-in) noch durch Patent-Restriktionen beeinflusst ist (Wagner et al. 2020).

Zudem lässt sich durch die Integration von öffentlichen SSI-Netzwerken die Kundenerfahrung im Zuge verschiedenster Unternehmensservices verbessern. Anstelle der manuellen Erstellung eines Nutzeraccounts mit einer Nutzername-Passwort-Kombination und Berechtigungsnachweisen können neue Kund*innen eine bestehende digitale Identität verwenden, um ihren Account zu erstellen. SSI erstellt dabei eine tragbare Identität, die von Einzelpersonen für etwaige Onlineprozesse verwendet werden kann – von einfachen Authentifizierungsanfragen mit einem einzigen Berechtigungsnachweis (z. B. Serviceanmeldung) bis hin zu komplexen Prozessen wie die gemeinsame Nutzung kuratierter Identitätsdaten für das automatisierte, digitale Ausfüllen von Formularen. In diesem Zusammenhang leistet SSI mittels der Bereitstellung wiederverwendbarer Identitätsattribute einen erheblichen Beitrag dazu, entsprechende Prozesse zu digitalisieren und damit die fortschreitende Automatisierung von Prozessen zu realisieren (Wagner et al. 2020). Letztlich verbessert dies die Benutzerfreundlichkeit der Website, die Service- und Produktverfügbarkeit, die Datenqualität und Datenverarbeitung von Unternehmen und hat damit potenziell eine Erhöhung der Nutzerzahlen und eine Verbesserung der Prozesseffizienz zur Folge.

Auch lässt sich die Compliance mit bestehenden Regulierungen im Bereich Datenschutz und Privatsphäre durch SSI besser als bisher umsetzen. Mit der Freigabe von Credentials durch die Kund*innen haben Unternehmen die Möglichkeit, jederzeit diese Freigabe nachzuweisen und damit „Privacy und Compliance by Design“ ohne zusätzlichen Aufwand im Identitätsmanagement umzusetzen. Gleichzeitig legen auch die Nutzer*innen immer mehr Wert auf ihren (persönlichen) Datenschutz. SSI-Lösungen erhöhen dabei die Sensibilität und die Aufmerksamkeit (IT Security Awareness) der Nutzer*innen zum Thema Datenschutz und Datennutzung.

5 Kritische Betrachtung von SSI

Kritische Betrachtung

Governance-Herausforderungen

Die Standardisierung und Interoperabilität von SSI-spezifischen Protokollen sind die relevantesten Herausforderungen im Bereich Governance. Während eine zunehmende Anzahl von Initiativen versuchen, SSI oder SSI-ähnliche Lösungen zu implementieren, wird ein gewisser Grad an Standardisierung und Interoperabilität, ähnlich zu Übertragungs- und Netzwerkprotokollen im Internet (z. B. TCP/IP-Protokolle), nötig sein, um eine flächendeckende Adoption zu erreichen. An dieser Stelle wurden beispielsweise durch das internationale W3C-Konsortium bereits erste Bemühungen für Standards wie z. B. DIDs und VCs gestartet, die eine Vereinheitlichung der SSI-Protokolle bezwecken. Diese Bemühungen werden von der Trust over IP Foundation[11] unterstützt, die es sich zum Ziel gesetzt hat, eine ganzheitliche Architektur für digitales Vertrauen im Internet aufzubauen. Insbesondere für eine flächendeckende Adoption von personenbezogener SSI wird die Möglichkeit der Portabilität von VCs zwischen verschiedenen Netzwerken entscheidend sein. Ebenfalls wird zunächst die Anzahl an Anbietern maßgebend sein, um eine breite Masse an Nutzern zu erreichen. Die damit einhergehende Skalierung der SSI-Netzwerke könnte durch erfolgreiche technische Standardisierung der Protokolle vereinfacht werden.

Sozioökonomische Herausforderungen

Im Bereich der sozioökonomischen Herausforderungen ergibt sich insbesondere die Frage nach der Akzeptanz von SSI-Lösungen durch die Verbraucher*innen und Unternehmen. Auch wenn durch bestehende Initiativen ein hohes Maß an Benutzerfreundlichkeit ermöglicht wird, erfordert eine sichere Nutzung von SSI stets die Einbindung eines zweiten Geräts – also eines zweiten Kommunikators –, was die Benutzerfreundlichkeit mindert. Insbesondere in Hinsicht auf die mangelnde Nutzung von ähnlich aufwendigen Verfahren, wie z. B. der Multi-Faktor-Authentifizierung bei zentralisierten Systemen, ist eine ganzheitliche Adoption fraglich. Ferner ist an dieser Stelle der Kostenaspekt nicht zu vernachlässigen. Die Nutzung einer SSI wird zwangsläufig für Konsument*innen mit Kosten verbunden sein. Mögliche Betreiber einer SSI-Lösung müssen beispielsweise Cloud Agents und DLTs unterhalten. Falls nicht aufgrund der bereits beschriebenen Sicherheits- und Interoperabilitätsvorteile Einsparungen bei Prozessen direkt für diese Betreiber bestehen, könnten die mit SSI verbundenen Kosten und eine Gewinnmarge an die Konsument*innen weitergegeben, die sich dann zwischen einem kostenfreien Single Sign-on und einer kostenpflichtigen SSI entscheiden müssten. Auf der anderen Seite ist jedoch die technische Umsetzbarkeit einer Bezahlung im Rahmen einer VP unklar, da der Issuer in Verifizierungsprozesse nicht involviert ist.

SSI sollte auch nicht als Allheilmittel für die Privatsphäre von Nutzer*innen im Internet gesehen werden. Zwar kann durch den Einsatz von ZKPs sichergestellt werden, dass nur ein Minimum der benötigten Informationen geteilt wird, jedoch kann dies allein keine Privatsphäre garantieren. So können Verifier nach wie vor mehr Daten abfragen, als sie eigentlich benötigen, oder aufgrund des geringen Aufwands in Prozessen personenbezogene Daten verlangt werden, in denen dies bislang nicht der Fall war, etwa beim Eintritt in ein Gebäude. Falls der Holder diese Daten mit dem Verifier bereitwillig teilt, ist der Zugewinn an Privatsphäre durch den Einsatz von SSI teilweise aufgehoben. Auch ist es fraglich, inwieweit Nutzer*innen dazu bereit sind, ein neuartiges Identitätsmanagement zu verwenden.

Rechtliche Herausforderungen

Darüber hinaus sind insbesondere Aspekte der Regulierung noch weitestgehend ungeklärt. Viele der positiven Ergebnisse von SSI können nur erreicht werden, wenn die Wiederverwendung von Berechtigungsnachweisen über Sektoren hinweg realisiert wird (Credential Roaming). Die Wiederverwendung von Berechtigungsnachweisen ist technisch möglich, aber das Credential Roaming hat aufgrund mangelnder regulatorischer Klarheit noch keine weite Verbreitung gefunden (Wagner et al. 2020). So können durch SSI und ihre technologischen Lösungen zwar eindeutige Vorteile z. B. im Bereich der Privatsphäre erzielt werden, jedoch müssen die gesetzlichen Grundlagen dafür geschaffen werden. Ein solcher Regulierungsansatz sollte im besten Fall in einem supranationalen Rahmen erfolgen.

[11] Siehe dazu: https://trustoverip.org/

Kritische Betrachtung

Ein weiterer wichtiger Aspekt ist die Akzeptanz von elektronischen Signaturen. Eine wichtige Initiative wurde dabei durch die EU mit der eIDAS-Verordnung gestartet (Europäisches Parlament 23.07.2014). eIDAS schafft seit der Verabschiedung im Jahr 2016 die rechtlichen Rahmenbedingungen für die Verwendung elektronischer Signaturen. Damit wird einer elektronischen Transaktion die gleiche rechtliche Stellung wie einer papierbasierten Transaktion ermöglicht. Auch andere regulatorische Initiativen wie das European Self-Sovereign Identity Framework (ESSIF) könnten durch eine Vereinheitlichung und Kooperation mit internationalen Organisationen wie Trust over IP oder dem W3C der EU eine Vorreiterrolle in der Verwendung von SSI verschaffen.

Neben den Rahmenbedingungen der eIDAS steht die Nutzung des SSI-Paradigmas vor der Herausforderung, den Anforderungen der DSGVO gerecht zu werden. Konkret greift die DSGVO vor allem dann, wenn personenbezogene Daten übermittelt und verarbeitet werden. Das bedeutet, sobald personenbezogene Informationen einer natürlichen Person zugeordnet werden können, muss diese geschützt werden. Diesen Schutz stellt die DSGVO dar. Dies gilt jedoch nach Erwägungsgrund 14 der DSGVO nicht für juristische Personen (Europäisches Parlament 27.04.2016), sodass nicht alle Anwendungsfälle von SSI durch die DSGVO abgedeckt sind. Beispielsweise sind Anwendungsfälle wie das Erstellen und Übertragen von Vorlagen, Standardisierungen, öffentlicher Benachrichtigungen oder die öffentliche Anzeige von Informationen über juristische Personen nicht von der DSGVO betroffen. Betroffene und relevante Hindernisse zur Einhaltung der DSGVO-Richtlinien, die im Rahmen der Architektur und Funktionsweise von SSI beachtet werden müssen, sind folgende Themen:

(1) Anonymisierung und Pseudonymisierung
(2) Standardisierung und Verarbeitung der Transaktionen
(3) Einheitliches Rollenverständnis durch Begriffsdefinitionen
(4) Verarbeitung der personenbezogenen persönlichen Daten

In diesem Zusammenhang ist die Rolle der Blockchain-Technologie demnach nicht die, sensitive Daten direkt auf der Blockchain zu speichern, sondern lediglich die Möglichkeit zu bieten, sensitive Daten mittels bspw. Widerrufungsregistern (Revocation Registries) auf ihre Gültigkeit zu überprüfen. Zur Überwindung der genannten Einhaltungshindernisse sind SSI-Netzwerke bestrebt, Datenverarbeitungsvereinbarungen mit Regierungsbehörden sowie Interessengruppen der EU abzuschließen, um diese gleichzeitig auch über die Thematik der SSI aufzuklären. Im Zuge dessen befinden sich diese Regulierungsbehörden aufgrund der Anwendung der DSGVO auf DLTs in einem Wandel, sodass trennscharfe Datenverarbeitungsvereinbarungen dazu beitragen können, die Entwicklung der Gesetzgebung der Regulierungsbehörden zu unterstützen, um SSI-Ökosysteme möglichst DSGVO-konform zu regulieren.

In diesem Zusammenhang birgt die Verwendung von DLTs eine weitere rechtliche Herausforderung. Da die Daten unveränderlich gespeichert werden, können sie nur durch eine weitere Transaktion überschrieben werden. Dies widerspricht der DSGVO der EU, die explizit die Möglichkeit der Löschung von personenbezogenen Daten vorsieht. Beispielsweise kann eine solche Speicherung personenbezogener Daten im Zusammenhang mit dem Widerrufungsregister und dem dazugehörigen kryptografischen Akkumulator relevant werden, da das Widerrufungsregister als Verbindung zu personenbezogenen Daten einer identifizierten oder identifizierbaren Person verwendet werden könnte. Rieger et al. (2019) präsentieren allgemeine Designprinzipien, um Blockchain-Lösungen DSGVO-konform zu gestalten und die daher insbesondere bei SSI zu beachten sind.

Technische Herausforderungen

Auch wenn die Blockchain-Technologie im Rahmen von SSI verwendet wird, sollte der Einsatz dieser Technologie stets ausgiebig geprüft und hinterfragt werden. So sollten personenbezogene Daten für SSI niemals auf einem solchen dezentralen Register gespeichert werden, da sonst Rückschlüsse auf einzelne Identitäten innerhalb dieses öffentlichen Netzwerks möglich wären. Ebenfalls sind an dieser Stelle noch nicht alle Herausforderungen hinsichtlich der Skalierbarkeit von öffentlichen DLTs gelöst. Zum Beispiel besitzen die Tails-Files, die Einträge für jedes ausgegebene VC eines Typs beinhalten und benötigt werden, um Akkumulatoren nutzen zu können, bei vielen Einträgen eine nicht zu vernachlässigende Dateigröße. Somit sind sie

aktuell ungeeignet, um auf DLT-Infrastrukturen abgespeichert zu werden, und können für Engpässe sorgen, z. B., wenn sie über mobile Endgeräte oder im Umfeld des IoT heruntergeladen und verarbeitet werden müssen. Auf der anderen Seite wird bereits an Revocation-Mechanismen mit Hilfe von Akkumulatoren gearbeitet, die nicht auf Tails-Files angewiesen sind.

Die zur Authentifizierung angegebenen Link Secrets sind zudem keine sicheren identitätsbestimmenden Merkmale. So hat der Verifier im Gegensatz zu etwa biometrischen Eigenschaften keine Möglichkeit, nachzuprüfen, ob das Link Secret wirklich zu der jeweiligen Person gehört. Es besteht die Möglichkeit, dass das Link Secret anderen Nutzer*innen weitergegeben wird oder mehrere Nutzer*innen anfangs bewusst das gleiche Link Secret wählen. Damit dies nicht geschieht, gibt es verschiedene Ansätze, wie eine Weitergabe des Link Secrets verhindert werden kann, wie etwa die Verwendung des in modernen Smartphones bereits vorhandenen Sicherheitschips.

Ein anderer Ansatz ist es, die Hemmschwelle der Weitergabe des Link Secrets zu erhöhen. Dazu kann der Verifier weitaus mehr Informationen verlangen, als eigentlich notwendig sind. So könnte zusätzlich bewiesen werden müssen, dass eine Person im Besitz einer Kreditkarte oder eines Führerscheins desselben Namens ist. Daneben könnte zudem ein Beweis vorgelegt werden müssen, dass das gleiche Link Secret schon in früheren Interaktionen verwendet wurde. Eine andere Möglichkeit wäre die Verknüpfung des Link Secrets zu einem Zugang zu Geldanlagen des/der Besitzer*in. Eine Weitergabe des Link Secrets würde dann einer eventuellen Räumung des Kontos gleichkommen (Hardman und Harchandani 2019).

Ein anderer Ansatz ist es, das Link Secret stärker an die Identität und somit an einen DID zu binden. Die entsprechenden Keys des DID können dann z. B. von dem Link Secret abgeleitet werden. Diese Ableitung kann wiederum bewiesen werden, ohne das Link Secret preiszugeben. Gegen ein Auftreten unter falschem DID schützt dieses Verfahren jedoch nicht. Mit biometrischen Verfahren können VCs noch stärker an eine Person gebunden werden, bedürfen aber noch weiterer Implementierungsarbeit und sind zusätzlich meistens von spezifischer Hardware abhängig (Hardman und Harchandani 2019).

Auch die Verknüpfung von physischer und digitaler Objektidentität stellt eine Herausforderung für die Anwendung von SSI dar. Es können für physische Objekte eindeutig definierte Merkmale, wie z. B. die VIN eines Fahrzeugs für die VID, verwendet werden. Bei Objekten ist individuell darauf zu achten, dass die schon existierenden Identifier sinnvoll in eine SSI-Architektur eingebunden werden können.

Die Revocation von VCs kann bei jetzigen SSI-Lösungen nur vom Issuer selbst vorgenommen werden. Dies stellt jedoch in vielen Fällen ein Problem dar, wenn das VC von einer anderen Partei widerrufen werden soll, als es ausgestellt wurde. Ein Beispiel hierfür ist das Rezept einer Arztpraxis. Das Rezept darf nur einmal eingelöst werden und der Patient bzw. die Patientin kann sich die Apotheke nach Belieben aussuchen. Die Apotheke hat nun drei Möglichkeiten: Sie muss entweder die Praxis darauf hinweisen, dass das VC eingelöst wurde, und diese erklärt anschließend das VC als ungültig. Oder sie teilt allen anderen Apotheken mit, dass das VC schon eingelöst wurde, ohne dabei die Privatsphäre des VC-Subjekts zu diskreditieren. Oder alle Apotheken wurden dazu berechtigt, das VC selbst zu widerrufen, wodurch weder Kontakt zu der Praxis noch zu den anderen Apotheken aufgenommen werden muss. Diese Berechtigung für Nicht-Issuer, Revocations zu veranlassen, ist in heutigen SSI-Lösungen noch nicht oder nur unzureichend implementiert. Wie genau dieses Problem technisch gelöst werden wird, bleibt also abzuwarten. Auch in Szenarien, in denen nicht das wiederholte Verwenden eines VCs problematisch ist, wie etwa bei der Revocation eines Führerscheins durch die Polizei im Rahmens einer Alkoholkontrolle, ergeben sich derartige Fragestellungen.

6 Fazit

Fazit

Das SSI-Paradigma verspricht eine neue Entwicklungsstufe des digitalen Identitätsmanagements, aus der sich vielfältige Einsatzmöglichkeiten ableiten. Entsprechend wird das Konzept bereits in unterschiedlichen Initiativen auf regionalen, nationalen und internationalen Ebenen diskutiert, erprobt und umgesetzt.

Das vorliegende Papier analysiert die konzeptionellen Eigenschaften sowie die technischen Aspekte des SSI-Paradigmas und stellt darüber hinaus beispielhaft drei Anwendungsfälle vor. Dabei wird deutlich, dass SSI insbesondere Vorteile im Zuge der individuellen Kontrolle, Datensicherheit und vollen Portabilität der Identität zwischen verschiedenen Diensten mit sich bringt. Beispielsweise lassen sich fälschungs- und manipulationssichere digitale Versionen von wichtigen persönlichen Dokumenten wie Personalausweis, Reisepass, Geburtsurkunde oder medizinischen Bestätigungen erstellen. Die Anwendungsfälle sind jedoch nicht nur auf personenbezogene SSI beschränkt, sondern können z. B. auch digitale Identitäten physischer Objekte im Rahmen von IoT-Lösungen sein. Dies ist vor allem in Verbindung mit der umfassenden Digitalisierung von Unternehmen von großer Bedeutung.

In Anbetracht dessen wird SSI insbesondere durch die Kombination mit weiterführenden Technologien und Konzepten für die praktische Anwendung relevant. So könnte beispielsweise der Einsatz von DLT-Lösungen für die Protokollierung von Mehrfach-Verwendung von VCs, wie am Beispiel von E-Rezepten illustriert, relevant werden, welche durch den bloßen Einsatz von bilateralen Kommunikationswegen im Rahmen von SSI nicht adressiert werden kann. Darüber hinaus können mittels des Einsatzes von SSI sensitive Daten bilateral verifizierbar ausgetauscht und entsprechend von der Blockchain ferngehalten werden, sodass SSI dabei verhelfen kann die Vorteile der Blockchain-Technologie im Einklang mit den rechtlichen und regulatorischen Anforderungen zu bringen. Diese Funktionalitäten ermöglichen verschiedene Anwendungsszenarien in der Wirtschaft, etwa für Datentransaktionen von Privatpersonen, die Verwaltung digitaler Identitäten von physischen Objekten oder das Verwalten von Urkunden, Zeugnissen oder Beglaubigungen durch öffentliche Institutionen. Dabei lassen erste praktische Umsetzungen darauf schließen, dass SSI besonders den Bereich individueller Datentransaktionen von Privatpersonen bedeutend entwickeln und voranbringen kann.

Dennoch bestehen Herausforderungen, die es vor einem flächendeckenden Einsatz des SSI-Paradigmas zu meistern gilt. Neben sozioökonomischen Herausforderungen müssen auch rechtliche und technische Hürden überwunden werden. Wir sind der Auffassung, dass vor allem die Themen Governance und Interoperabilität der SSI-Anwendungen einer tiefergehenden Betrachtung bedürfen. Kritische Fragestellungen, inwieweit eine Infrastruktur digitaler Identitäten aufgebaut werden kann und wie sich diese entwickeln sollte, müssen in diesem Zusammenhang definiert werden. Darüber hinaus müssen kulturelle Ausprägungen beachtet werden. Beispielsweise nutzt China ein System, das auf einer Single Identity basiert – einer einzigen Identität, die zur Authentifizierung für alle Onlineaktivitäten genutzt werden muss. Dementsprechend können staatliche Institutionen aus den digitalen Interaktionen dieser Single Identity grundsätzlich weitreichende Informationen über die Aktivitäten der Bürger*innen sammeln. Folglich muss definiert werden, in welchem Maße die Infrastruktur digitaler Identitäten gestaltet sein sollte, damit Cybersicherheit im Einklang mit der Privatsphäre der Onlinegesellschaft stehen kann. In Bezug auf die Interoperabilität führt dies zu einem Wettbewerb der proprietären und nicht proprietären Lösungen und zu der Frage, wie diese vereinheitlicht und interoperabel anwendbar adjustiert werden können.

Die einheitliche und individuelle Verwaltung von digitalen Identitäten gewinnt zunehmend an Aufmerksamkeit. Beispielsweise setzt die deutsche Bundesregierung auf eine „Europäische Digitale-Identitäten-Initiative“ zur Gewährleistung einheitlicher digitaler Identitäten für die breite Öffentlichkeit (Bundeskanzleramt 2021). Gleichzeitig nimmt die flächendeckende Integration von vernetzten Systemen in unser alltägliches Leben stetig zu. Dies birgt jedoch erhebliche Risiken für die Privatsphäre und das Recht auf informationelle Selbstbestimmung. Bisher konnte sich kein sicheres System zur selbstbestimmten Nutzung von digitalen Identitäten durchsetzen. Das SSI-Paradigma stellt im Zuge dessen einen vielversprechenden Lösungsansatz zur interoperablen Verwaltung digitaler Identitäten dar und ist somit ein interessanter Gegenstand für zukünftige Forschung und Anwendung in der Praxis.

Referenzen

Abramson, Will (2019): CL Signatures for Anonymous Credentials. Online verfügbar unter https://mister-wip.uk/cl-signatures, zuletzt aktualisiert am 15.06.2020, zuletzt geprüft am 15.11.2020.

ADAC (2019): Tacho-Manipulation. Online verfügbar unter https://www.adac.de/rund-ums-fahrzeug/auto-kaufen-verkaufen/gebrauchtwagenkauf/tacho-manipulation/, zuletzt aktualisiert am 13.05.2020, zuletzt geprüft am 13.11.2020.

Allen, Christopher (2016): The Path to Self-Sovereign Identity. Online verfügbar unter http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html, zuletzt aktualisiert am 01.07.2019, zuletzt geprüft am 19.11.2020.

Ben-Sasson, Ben; Bentov, Iddo; Horesh, Yinon; Riabzev, Michael (2018): Scalable, transparent, and post-quantum secure computational integrity. Online verfügbar unter https://eprint.iacr.org/2018/046.pdf, zuletzt geprüft am 02.12.2020.

Bundeskanzleramt (2021): Digitale Identität. Wie ein Ökosystem digitaler Identitäten zu einem selbstbestimmten und zugleich nutzerfreundlichen Umgang mit dem digitalen Ich beitragen kann. Online verfügbar unter https://www.bundesregierung.de/resource/blob/992814/1881838/296c9afc2ec79f8c939360f61135aadd/digitale-identitaet-download-bk-amt-data.pdf, zuletzt geprüft am 13.04.2021.

Callahan, John; Hardman, Daniel; Othman, Asem (2019): Aries RFC 0231: Biometric Service Provider. Online verfügbar unter https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0231-biometric-service-provider/README.md, zuletzt aktualisiert am 15.06.2020, zuletzt geprüft am 03.12.2020.

Camenisch, Jan; Lysyanskaya, Anna (2002): A Signature Scheme withv Efficient Protocols. Online verfügbar unter https://groups.csail.mit.edu/cis/pubs/lysyanskaya/cl02b.pdf, zuletzt geprüft am 25.11.2020.

Cameron, Kim (2005): The laws of identity. Microsoft Corp. Online verfügbar unter https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf, zuletzt geprüft am 02.12.2020.

Clauß, Sebastian; Köhntopp, Marit (2001): Identity management and its support of multilateral security. In: *Computer Networks* 37 (2), S. 205–219. DOI: 10.1016/S1389-1286(01)00217-1.

Datenschutz-Grundverordnung (2018): Art. 16 DSGVO – Recht auf Berichtigung. DSGVO. Online verfügbar unter https://dsgvo-gesetz.de/art-16-dsgvo/, zuletzt geprüft am 15.11.2020.

DID Communication Working Group (2019): Working Group Charter. Online verfügbar unter https://github.com/decentralized-identity/org/blob/master/Org%20documents/WG%20documents/DIF_DIDcomm_WG_Charter_v1.pdf, zuletzt geprüft am 02.12.2020.

Europäisches Parlament (23.07.2014): Verordnung (EU) über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt. Verordnung (EU) Nr. 910/2014. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910, zuletzt geprüft am 08.07.2020.

Europäisches Parlament (27.04.2016): Verordnung (EU) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Verordnung (EU) 2016/679.

European Parliamentary Research Service (2019): Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? Online verfügbar unter https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf, zuletzt geprüft am 27.10.2020.

Goldfarb, Seth (2019): Using digital identity to stamp out credential fraud and fake diplomas. Online verfügbar unter https://www.evernym.com/blog/credential-fraud-fake-diplomas/, zuletzt aktualisiert am 12.12.2019, zuletzt geprüft am 05.11.2020.

Goodell, Geoff; Aste, Tomaso (2019): A Decentralized Digital Identity Architecture. In: *Frontiers in Blockchain* 2, S. 69. DOI: 10.3389/fbloc.2019.00017.

Hardman, Daniel (2018): Credential Revocation. Online verfügbar unter https://github.com/hyperledger/indy-hipe/blob/master/text/0011-cred-revocation/README.md, zuletzt aktualisiert am 15.06.2020, zuletzt geprüft am 15.11.2020.

Hardman, Daniel (2019a): A Gentle Introduction to Verifiable Credentials. Online verfügbar unter https://www.evernym.com/blog/gentle-introduction-verifiable-credentials/, zuletzt aktualisiert am 14.02.2020, zuletzt geprüft am 02.12.2020.

Hardman, Daniel (2019b): Aries RFC 0004: Agents. Online verfügbar unter https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0004-agents/README.md, zuletzt aktualisiert am 15.06.2020, zuletzt geprüft am 15.11.2020.

Hardman, Daniel; Harchandani, Lovesh (2019): Preventing Transferrability with ZKP-based Credentials. Online verfügbar unter

Referenzen

https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/topics-and-advance-readings/zkp-safety.md#technique-2-prevent-link-secret-reuse, zuletzt geprüft am 02.12.2020.

Hardman, Daniel; Harchandani, Lovesh; Othman, Asem; Callahan, John (2019): Using Biometrics to Fight Credential Fraud. In: *IEEE Comm. Stand. Mag.* 3 (4), S. 39–45. DOI: 10.1109/MCOMSTD.001.1900033.

Lockl, Jannik; Schlatt, Vincent; Schweizer, Andre; Urbach, Nils; Harth, Natascha (2020): Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications. In: *IEEE Trans. Eng. Manage.*, S. 1–15. DOI: 10.1109/TEM.2020.2978014.

MarketsandMarkets (2018): Blockchain Identity Management Market Size, Share and Global Market Forecast to 2023. Online verfügbar unter https://www.marketsandmarkets.com/Market-Reports/blockchain-identity-management-market-241573621.html, zuletzt aktualisiert am 28.04.2020, zuletzt geprüft am 28.11.2020.

McKenna, Karla; Reed, Drummond; Schneider, Christoph; Tobin, Andrew (2020): Digital Identity for Commerce - An exploration of verifiable credentials and LEIs with GLEIF - YouTube. Online verfügbar unter https://youtu.be/ag5vW4OurKs, zuletzt aktualisiert am 15.06.2020, zuletzt geprüft am 15.06.2020.

McKinsey & Company (2019): Digital Identification. A key to inclusive growth. Online verfügbar unter https://www.mckinsey.com/~/media/mckinsey/featured%20insights/innovation/the%20value%20of%20digital%20id%20for%20the%20global%20economy%20and%20society/mgi-digital-identification-a-key-to-inclusive-growth.ashx, zuletzt geprüft am 28.11.2020.

Mobility Open Blockchain Initiative (2019): Vehicle Identity Standard. Online verfügbar unter https://dlt.mobi/wp-content/uploads/2019/09/MOBI-Vehicle-Identity-Standard-v1.0-Preview.pdf, zuletzt geprüft am 29.11.2020.

Mühle, Alexander; Grüner, Andreas; Gayvoronskaya, Tatiana; Meinel, Christoph (2018): A survey on essential components of a self-sovereign identity. In: *Computer Science Review* 30, S. 80–86. DOI: 10.1016/j.cosrev.2018.10.002.

Nauta, Jeele; Joosten, Rieks (2019): Self-Sovereign-Identity:-A-Comparison-of-IRMA-and-Sovrin. Online verfügbar unter https://www.researchgate.net/profile/Rieks_Joosten/publication/334458009_Self-Sovereign_Identity_A_Comparison_of_IRMA_and_Sovrin/links/5d359f1992851cd0467b96f3/Self-Sovereign-Identity-A-Comparison-of-IRMA-and-Sovrin.pdf, zuletzt geprüft am 23.07.2020.

Nelson, Clare (2018): Zero Knowledge Proofs (ZKP): Privacy Preserving Digital Identity with. Online verfügbar unter https://www.youtube.com/watch?v=D4iUeVbib_k, zuletzt aktualisiert am 15.06.2020, zuletzt geprüft am 15.11.2020.

Oberländer, Anna Maria; Röglinger, Maximilian; Rosemann, Michael; Kees, Alexandra (2018): Conceptualizing Business-to-Thing Interactions: A Sociomaterial Perspective on the Internet of Things. In: *European Journal of Information Systems* 27 (4), S. 486–502. Online verfügbar unter https://eref.uni-bayreuth.de/40060/.

Preukschat, Alex (2019): Peer DIDs: a secure and scalable method for DIDs that's entirely off. Online verfügbar unter https://www.youtube.com/watch?v=d-5MmLLd3xY, zuletzt aktualisiert am 15.06.2020, zuletzt geprüft am 15.11.2020.

Reed, Drummond; Law, Jason; Hardman, Daniel; Lodder, Mike (2019): DKMS (Decentralized Key Management System) Design and Architecture V4. Online verfügbar unter https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0051-dkms/dkms-v4.md, zuletzt aktualisiert am 15.06.2020, zuletzt geprüft am 15.06.2020.

Reed, Drummond; Sporny, Manu; Longley, Dave; Allen, Christopher; Grant, Ryan; Sabadello, Markus (2020): Decentralized Identifiers (DIDs) v1.0. Online verfügbar unter https://www.w3.org/TR/did-core/, zuletzt aktualisiert am 08.06.2020, zuletzt geprüft am 15.06.2020.

Rieger, Alexander; Guggenmos, Florian; Lockl, Jannik; Fridgen, Gilbert; Urbach, Nils (2019): Building a Blockchain Application that Complies with the EU General Data Protection Regulation. In: *MISQE* 18 (4), S. 263–279. DOI: 10.17705/2msqe.00020.

Rosemann, Michael (2013): The Internet of Things: new digital capital in the hands of customers. In: *Business Transformation Journal* 2013 (9), S. 6–15.

Schneier, Bruce (2018): Can Consumers' Online Data Be Protected? Schneier on Security. Online verfügbar unter https://www.schneier.com/blog/archives/2018/02/can_consumers_o.html, zuletzt aktualisiert am 25.07.2019, zuletzt geprüft am 17.11.2020.

Sovrin Foundation (2019): Innovation Meets Compliance - Data Privacy Regulation and Distributed Ledger Technology. Online verfügbar unter

Referenzen

https://sovrin.org/wp-content/uploads/GDPR-Paper_V1.pdf, zuletzt geprüft am 07.09.2020.

Sporny, Manu; Longley, Dave; Chadwick, David (2019): Verifiable Credentials Data Model 1.0. Expressing verifiable information on the Web. Online verfügbar unter https://github.com/decentralized-identity/org/blob/master/Org%20documents/WG%20documents/DIF_DIDcomm_WG_Charter_v1.pdf, zuletzt geprüft am 02.12.2020.

Statista (2020): eCommerce - weltweit, Marktprognose. Online verfügbar unter https://de.statista.com/outlook/243/100/ecommerce/weltweit, zuletzt aktualisiert am 14.05.2020, zuletzt geprüft am 14.11.2020.

Tobin, Andrew (2019): An Introduction to Self-Sovereign Identity - YouTube. Online verfügbar unter https://www.youtube.com/watch?v=HMrBP55xROc, zuletzt aktualisiert am 15.06.2020, zuletzt geprüft am 15.06.2020.

Tobin, Andrew; Reed, Drummond (2017): The Inevitable Rise of Self-Sovereign Identity. Online verfügbar unter https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf, zuletzt geprüft am 29.10.2020.

Tönsing, Friedrich (2015): Digitale Identitäten – Was braucht man zukünftig für eine vertrauenswürdige digitale Identität? In: Udo Bub, Viktor Deleski und Klaus-Dieter Wolfenstetter (Hg.): Sicherheit im Wandel von Technologien und Märkten. Wiesbaden: Springer Fachmedien Wiesbaden, S. 55–61.

Vescent, Heather; Young, Kaliya; Hamilton Duffy, Kim; Sabadello, Markus; Zagidulin, Dmitri; Caballero, Juan (2018): A Comprehensive Guide to Self Sovereign Identity.

Wagner, Kai; Pueyo, Xavier Vila; Vandy, Nathan; Bachenheimer, Daniel; Beron, Dominik (2020): Decentralized Identity: What's at Stake. A Position Paper by the INATBA Identity Working Grupd. Hg. v. International Association for Trusted Blockchain Applications. Online verfügbar unter https://inatba.org/wp-content/uploads/2020/11/2020-11-INATBA-Decentralised-Identity-001.pdf, zuletzt geprüft am 02.12.2020.

World Economic Forum (2020): Reimaging Digital Identity. A Strategic Imperative. Online verfügbar unter http://www3.weforum.org/docs/WEF_Digital_Identity_Strategic_Imperative.pdf, zuletzt geprüft am 28.11.2020.

Projektgruppe Wirtschaftsinformatik

Die Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT vereint die Forschungsbereiche Finanz- & Informationsmanagement in Augsburg und Bayreuth. Die Expertise an der Schnittstelle von Finanzmanagement, Informationsmanagement und Wirtschaftsinformatik sowie die Fähigkeit, methodisches Know-how auf höchstem wissenschaftlichen Niveau mit einer kunden-, ziel- und lösungsorientierten Arbeitsweise zu verbinden, sind ihre besonderen Merkmale. Aktuell besteht unser Team aus rund 80 wissenschaftlichen Mitarbeitenden und über 140 studentischen Mitarbeitenden.

Dabei sind unsere Forschungsaktivitäten in verschiedenen Forschungsbereichen thematisch gebündelt, wodurch wir über umfangreiche Kompetenzen in unterschiedlichen Bereichen der Wirtschaftsinformatik verfügen. Dadurch ist es uns möglich, in angewandten Forschungsprojekten mit zahlreichen Unternehmen aus verschiedenen Branchen aktuelle Forschungsergebnisse in praxistaugliche Lösungen zu transferieren und so langfristige „Win-Win-Situationen" zu schaffen. Darüber hinaus können wir das gewonnene Wissen in unsere zahlreichen Lehrveranstaltungen einfließen lassen, sodass wir unseren Studierenden theoretisch fundierte sowie praktisch relevante und aktuelle Inhalte näherbringen können. Unser Ziel ist es, auch zukünftig unser Themenspektrum um passende Forschungsbereiche synergetisch zu ergänzen.

Fraunhofer Blockchain-Labor

Fußend auf diesen Prinzipien wurde das Fraunhofer Blockchain-Labor gegründet, das sich durch die interdisziplinäre Kombination aus ökonomischen, rechtlichen und technischen Kompetenzen auszeichnet. Im Blockchain-Labor, welches mittlerweile weit über die nationalen Grenzen hinweg Bekanntheit erlangt hat, werden Blockchain-Lösungen konzeptioniert, entwickelt und evaluiert. Gemeinsam mit zahlreichen Partnern aus Wirtschaft und Wissenschaft wird intensiv daran gearbeitet, das Potenzial der Blockchain-Technologie umfänglich zu untersuchen und zugänglich zu machen.

Am Standort in Bayreuth begleiten seit unserer Gründung im Jahr 2016 Unternehmen und öffentliche Institutionen im Rahmen von angewandten Forschungsprojekten sowie bei der Entwicklung individueller und bedarfsgerechter Lösungen im Bereich der Blockchain-Technologie. Auch wenn Blockchain-Technologie über die erstmalige Anwendung als Basis der Kryptowährung Bitcoin bekannt geworden ist, zeigte sich schnell, dass das eigentliche Potential der Blockchain deutlich weiter greift. Beispielsweise können heute neben Geschäftslogiken, abgebildet durch sogenannte Smart Contracts, auch digitale und selbstverwaltete Identitäten mit Unterstützung der Blockchain umgesetzt werden.

Als eine der ersten Organisationen Deutschlands haben wir bereits im Jahr 2016 ein Whitepaper veröffentlicht, in welchem wir Grundlagen, Anwendungsmöglichkeiten und Potenziale der Blockchain-Technologie sowie die Rolle von Intermediären in verschiedenen Kontexten untersucht haben. Für unsere Arbeit wurden wir zudem mehrfach ausgezeichnet – unter anderem mit dem Innovationspreis Reallabore des Bundesministeriums für Wirtschaft und Energie sowie dem eGovernment-Preis für unser Projekt mit dem Bundesamt für Migration und Flüchtlinge.