Fraunhofer FIT

Fraunhofer-Institut für Angewandte Informationstechnik FIT

Mythbusting Self-Sovereign Identity (SSI)

Diskussionspapier zu selbstbestimmten digitalen Identitäten

Projektgruppe Wirtschaftsinformatik

Mythbusting Self-Sovereign Identity (SSI)

Diskussionspapier zu selbstbestimmten digitalen Identitäten

Autoren

Benjamin Schellinger, Johannes Sedlmeir, Lukas Willburger, Prof. Dr. Jens Strüker und Prof. Dr. Nils Urbach

Die Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT vereint die Forschungsbereiche Digital Disruption, Digital Business und Digital Transformation in Augsburg und Bayreuth. Die interdisziplinäre Expertise in fachlichen und technischen Themen der Wirtschaftsinformatik und des Informationsmanagements sowie die Fähigkeit, methodisches Know-how auf höchstem wissenschaftlichem 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 Mitarbeitenden Tobias Guggenberger und Fabiane Völter für ihre tatkräftige Unterstützung bei der Erstellung dieses Diskussionspapiers. Dieses Diskussionspapier ist in Zusammenarbeit mit IBM im Kontext des Projektes „Ökosystem Digitaler Identitäten" entstanden.

Disclaimer

Empfohlene Zitierweise

Schellinger, B., Sedlmeir, J., Willburger, L., Strüker J. und Urbach, N. (2022): Mythbusting Self-Sovereign Identity (SSI). Diskussionspapier zu selbstbestimmten digitalen Identitäten. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Bayreuth.

Bildquellen


Selbstbestimmte digitale Identitäten ermöglichen Nutzer*innen ein hohes Maß an Sicherheit und Komfort bei gleichzeitiger Verbesserung der Kontrolle über die Freigabe ihrer Daten.

Vorwort

Im vergangenen Jahr wurden von der EU-Kommission Rahmenbedingungen für die Einführung einer europäischen digitalen Identität vorgelegt. Mit dem Vorschlag sollen Bürger*innen und Unternehmen digitale Identitätsnachweise erlangen, verifizierbare Dokumente in elektronischer Form austauschen und sich bei Internetdiensten in ganz Europa authentifizieren können. Für die Verwaltung und Verwendung dieser Nachweise möchte die EU Nutzer*innen mit digitalen Brieftaschen ausstatten, sogenannten Wallet-Apps oder digitalen Wallets.

Mit der Einführung eines solchen selbstbestimmten digitalen Identitätsmanagements (engl. Self-Sovereign Identity – SSI) soll Nutzer*innen ein hohes Maß an Sicherheit und Komfort bei gleichzeitiger Verbesserung der Kontrolle über die Freigabe ihrer Daten ermöglicht werden. Die bequeme, datenschützende und effiziente Verwaltung von anbieterübergreifenden digitalen Identitätsdokumenten und sonstigen Nachweisen erfolgt über digitale Wallets. Damit gehen zahlreiche Anwendungsmöglichkeiten digitaler Nachweise einher, etwa ein passwortloser Login auf Webseiten oder die effizientere Interaktion mit Online-Services von Unternehmen und Behörden. Darüber hinaus ergeben sich mit SSI neue Möglichkeiten wie die selektive Freigabe von Identitätsattributen oder die automatische Überprüfbarkeit digitaler Identitätsnachweise durch Serviceanbieter. Neben digitalen Identitäten für Personen ermöglicht SSI auch Identitätsnachweise für Maschinen und Unternehmen und erweitert so bestehende analoge und digitale Identitätsmanagementsysteme. Die vielschichtigen Anwendungsfelder von SSI versprechen damit großes ökonomisches Potenzial.

Ein europäisches Ökosystem SSI-basierter digitaler Identitäten zielt auch darauf ab, die Risiken großflächiger Datenlecks bei Identitätsprovidern zu verringern und die Unabhängigkeit von Identitätsprovidern aus dem US-amerikanischen und chinesischen Raum zu stärken. Damit soll SSI dazu beitragen, die digitale Souveränität Deutschlands und Europas zu verbessern und fairen Wettbewerb im digitalen Raum zu ermöglichen. Vor diesem Hintergrund werden von der Bundesregierung zahlreiche SSI-Projekte mit Nachdruck verfolgt, wie beispielsweise die vier Schaufensterprojekte Sichere Digitale Identitäten des Bundeswirtschaftsministeriums oder die Pilotierungsprojekte des Bundeskanzleramts.

Wir wollen in diesem Diskussionspapier aktuelle Debatten über den Mehrwert und die Herausforderungen von SSI, digitalen Wallets und der Verwendung von Blockchain-Technologie aufklären. In diesem Kontext greifen wir gegenwärtige Meinungen in der Öffentlichkeit auf und versuchen, Missverständnisse aufzulösen. Im Anschluss fassen wir die Ergebnisse dieses Diskussionspapiers zusammen und wagen einen Blick in die Zukunft. Für einen Einstieg in die Thematik möchten wir auf unser SSI-Grundlagenpapier verweisen, in welchem wir die technischen Bausteine, Anwendungsmöglichkeiten und Potenziale von SSI erklären. Wir wünschen viel Freude beim Lesen und möchten alle Leser*innen einladen, mit uns in einen Dialog zu treten.

Prof. Dr. Jens Strüker

Professor für Wirtschaftsinformatik und Digitales Energiemanagement

Universität Bayreuth

Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT, Leiter des Fraunhofer Blockchain Labors

©Hochschule Fresenius/ John M. John

Prof. Dr. Nils Urbach

Professor für Wirtschaftsinformatik, Digital Business und Mobilität

Frankfurt University of Applied Sciences

Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT, Leiter des Fraunhofer Blockchain Labors

©Björn Seitz – kontender.Fotografie

Inhaltsverzeichnis

1 Motivation und Relevanz

1 Motivation und Relevanz

Die EU hat sich zum Ziel gesetzt, ein Ökosystem digitaler Identitäten aufzubauen und auf europäischer Ebene miteinander zu verbinden, um insbesondere die grenzüberschreitende Anerkennung staatlicher elektronischer Identitäten (eID) zu fördern. Das entsprechende Fundament wird aktuell bereits mit der Überarbeitung des Vorschlags für elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen (eIDAS) gelegt[1]. Ein zentraler Aspekt der eIDAS-Verordnung ist der Zugang zu öffentlichen Diensten – unabhängig vom Mitgliedsstaat, in dem die eID ausgestellt wurde. Allerdings fehlt es hierbei noch an einer europäischen Harmonisierung, da EU-Mitgliedstaaten ihre Identitäts-Schemas im Rahmen eines Notifizierungsverfahrens den Expert*innen der Mitgliedstaaten zur Begutachtung vorlegen müssen, um die gegenseitige Anerkennung des eID-Systems in der gesamten EU zu gewährleisten (European Commission, 2021).

Demzufolge erstellt und implementiert jedes Mitgliedsland unter eIDAS sein eigenes Schema. Dabei fällt auf, dass die eIDAS-Verordnung insbesondere auf Governance-Aspekte abzielt, jedoch bislang keine Anforderungen an die technische Implementierung stellt[2]. Daneben ist der Umfang der aktuell verfügbaren Identitätsdokumente auf Basisinformationen, wie beispielsweise Daten aus dem Personalausweis, beschränkt. Diese Identitätsdokumente beinhalten damit nicht den Führerschein, die Gesundheitskarte oder Ausbildungsdokumente. Eine der Ursachen der geringen Bekanntheit und Nutzung der eID sowie die fehlende Ausweitung auf weitere Identitätsdokumente dürfte die für die Integration weiterer Organisationen notwendige, aber aufwändige Zertifizierung sein. Der Einbezug der Privatwirtschaft war daher bislang äußerst zurückhaltend. Zudem ist in der ersten eIDAS-Verordnung die Ausstattung aller Bürger*innen mit einer eID nicht als verpflichtender Bestandteil aufgenommen worden.

Im Zuge der Evaluierung der Funktionsweise von eIDAS 1.0 und der damit einhergehenden Schwachstellen (European Commission, 2021) sowie in Anbetracht des Ziels einer Ausweitung auf eine Vielzahl von Anwendungsfällen wurde die Initiative zum European Digital Identity Framework (eIDAS 2.0) von der Europäischen Kommission ins Leben gerufen. Der Vorschlag soll insbesondere die Nutzung digitaler Identitäten für natürliche und juristische Personen innerhalb der EU fördern und erwähnt auch den Einsatz einer digitalen Wallet. Mit der geplanten Einführung von eIDAS 2.0 sollen im Gegensatz zur aktuellen eIDAS 1.0-Verordnung neue Services zur Verfügung gestellt werden, die jegliche Art von Nachweisen abbilden können und somit weit über die Speicherung von Stammdaten ähnlich denen eines physischen Personalausweises hinausgehen. Im Gegensatz zur vorherigen Verordnung sollen werden die Mitgliedstaaten dabei zur Umsetzung verpflichtet werden.

Langfristiges Ziel ist dabei die Bereitstellung einer europäischen Identität mittels von den Mitgliedsländern und Unternehmen bereitgestellter, interoperabler digitaler Wallets (Bundeskanzleramt (AT), 2021). Die unterschiedlichen SSI-Projekte der Bundesregierung und des privaten Sektors bereiten sich auf eine solche neue Verordnung bereits intensiv vor und entwickeln dafür gemeinsam eine Lösung, die europaweit umgesetzt werden könnte. Über die Bestrebungen der Europäischen Union hinaus, ein Ökosystem digitaler Identitätsdokumente zu fördern, wurden in anderen Ländern wie in der Schweiz (Digital Identity and Data Sovereignty Association (DIDAS), 2021) oder in Kanada (Boysen, 2021) bereits SSI-basierte Lösungen für eine eID auf den Weg gebracht.

Neben der Erweiterung der bisherigen technischen Umsetzung von eIDAS wird SSI als vielversprechendes Konzept gesehen, um basierend auf interoperablen Standards eine Verbindung zwischen bislang fragmentierten Ökosystemen zu erreichen und so

[1] Siehe Stellungnahme zur Verordnung zu Vertrauensdiensten (VDV) des Bundesministeriums für Wirtschaft und Klimaschutz.

[2] Für technische Anforderungen gelten die Standards und Spezifikationen des Europäischen Instituts für Telekommunikationsnormen (ETSI).

eine Vielzahl weiterer identitätsbezogener Dokumente für die elektronische Nutzung verfügbar zu machen. Technisch baut SSI auf bekannten und in der eID genutzten kryptographischen Techniken wie digitalen Signaturen auf und nutzt zudem unter anderem Zero-Knowledge Proofs (ZKPs) für die besonders privatsphäreschützende Weitergabe verifizierbarer Nachweise von Eigenschaften und Berechtigungen einer bestimmten Identität. Dabei verwendet SSI etablierte Mechanismen für die Identifikation von Organisationen in Form einer Public-Key-Infrastruktur (PKI). Im Vergleich zur eID ist der SSI-Ansatz jedoch durch eine dezentralere Datenhaltung der Nachweise bei den Nutzer*innen selbst sowie eine dezentralere Governance der PKI in Form eines verteilten Systems charakterisiert. Ziel der dezentraleren Datenhaltung ist, Nutzer*innen ein höheres Maß an Kontrolle und Privatsphäre zu ermöglichen. Dies wird unter anderem über die selektive Freigabe von Daten ohne die Notwendigkeit der Kommunikation mit einer zertifizierten Drittpartei erreicht. Eine aktuelle Studie belegt, dass Nutzer*innen ein höheres Maß an Selbstbestimmung über die Datenverwendung als eine der wichtigsten Eigenschaften einer digitalen Wallet beimessen (PwC, 2021).

Darüber hinaus kann das Risiko für Datenpannen, welche eine große Anzahl an Nutzer*innen betreffen, durch SSI-basierte Lösungen reduziert werden. Auf der anderen Seite sollen neue Governance-Mechanismen für vertrauenswürdige Institutionen und Unternehmen auch bei einer großen Zahl neuer Organisationen im Identitätsökosystem eine ausreichend hohe Flexibilität für Zertifizierung und Partizipation bereitstellen. Für die dabei nötige Speicherung der Zuordnung von Signaturschlüsseln zu Organisationen wie Unternehmen oder staatlichen Behörden, die im Internet heute in der Regel über Zertifizierungsstellen erfolgt, werden dabei neben etablierten zentralen Systemen auch dezentrale Alternativen, wie beispielsweise Blockchains, in Betracht gezogen und derzeit erprobt.

Aktuell werden mehrere prototypische Anwendungsfälle insbesondere für digitale Personenidentitäten, etwa für einen Hotel-Checkin, einen digitalen Nachweis der Fahrerlaubnis oder die Eröffnung eines Online-Bankkontos, durch die Bundesregierung mit kooperierenden Organisationen auf SSI-Basis entwickelt und getestet[3]. Zum Teil befinden sich diese Lösungen bereits im Pilotbetrieb. Darüber hinaus werden selbstbestimmte digitale Identitäten für Unternehmen etwa beim Bayerischen Landesamt für Steuern (LfSt) im Kontext der Steuerverwaltung von Händlern, aber auch für Maschinen-Identitäten, beispielsweise im Rahmen des Projekts zum Blockchain Machine Identity Ledger der Deutschen Energie-Agentur, auf ihre Machbarkeit und ihren Mehrwert erprobt (Guggenberger et al., 2021). Allgemein konzipieren und erproben Unternehmen und öffentliche Institutionen gemeinsam in vier großen Konsortien (ID-Ideal, IDunion, ONCE und SDIKA)[4] übergreifend unterschiedliche Anwendungsfälle im Rahmen der Schaufensterprojekte Sichere Digitale Identitäten. Neben der Vorbereitung zur eIDAS 2.0-Verordnung, die darauf abzielt, Bürger*innen mehr Sicherheit geben und schnellere Prozesse zu ermöglichen, soll durch die zahlreichen Projekte die Wettbewerbsfähigkeit von Unternehmen im digitalen Wandel sichergestellt werden. Insbesondere kleine und mittelständische Unternehmen erlangen durch SSI die Möglichkeit, besser mit Nutzer*innen und anderen Organisationen interagieren zu können.

Mit diesen Projekten wurde damit der Startschuss eines übergreifenden Ökosystems digitaler Identitäten für Bürger*innen, Unternehmen, Behörden und Maschinen gelegt. Die Entwicklung und Inbetriebnahme dieser Anwendungsfälle auf Basis der SSI-Technologie hat dabei sowohl positive als auch negative Reaktionen in der breiten Öffentlichkeit und in Kreisen von Expert*innen für IT-Sicherheit hervorgerufen. Insbesondere erntete der verfrühte Start des digitalen Führerscheins in der ID-Wallet App kurz vor der Bundestagswahl im September 2021 von IT-Spezialist*innen, Politiker*innen, Unternehmensvertreter*innen, Medien und Nutzer*innen viel Kritik (Heeger, 2021; Wittmann, 2021; Chaos-

[3] Siehe Pilotprojekte der Bundesregierung.
[4] Siehe Auswahl der Use Cases des Bundesministeriums für Wirtschaft und Klimaschutz.

radio, 2021). Die mediale Berichterstattung hat dabei oft den Eindruck erweckt, dass die SSI-Projekte der Bundesregierung und der Privatwirtschaft insgesamt unnötig, konzeptionell wenig durchdacht und nicht ausreichend mit anderen Identitätsprojekten koordiniert seien und daher keinen nachhaltigen Mehrwert für den Wirtschaftsstandort Deutschland liefern könnten.

Insgesamt mangelt es jedoch bislang an einer umfassenden Einordnung, um die Vor- und Nachteile eines SSI-basierten Identitätsmanagements im Gesamtkontext beurteilen sowie zwischen dem aktuellen Status quo der Umsetzung und den konzeptionellen Stärken und Herausforderungen des SSI-Ansatzes differenzieren zu können. Darüber hinaus scheinen viele Hintergründe und Vorteile der SSI-Projekte in Deutschland sowie die technologischen Grundlagen noch nicht ausreichend bekannt zu sein. Folglich wollen wir in diesem Diskussionspapier zum allgemeinen Verständnis von SSI-basierten digitalen Identitäten und Nachweisen beitragen, aktuelle Diskussionen in der Öffentlichkeit aufgreifen und kritisch reflektieren sowie bestehende Vorurteile aufklären. Die nachfolgende Diskussion von sieben Mythen, die wir in einer Vielzahl von Beiträgen und Diskussionen im Kontext von SSI identifiziert haben, soll dazu dienen, Missverständnisse aufzulösen und die Grundlage dafür schaffen, über den Mehrwert der eingesetzten Technologien informiert diskutieren zu können. Im Anschluss fassen wir die Ergebnisse dieses Diskussionspapiers zusammen und wagen einen Blick in die Zukunft.

2 Sieben Mythen zu SSI-basierten digitalen Identitäten

2 Sieben Mythen zu SSI-basierten digitalen Identitäten

SSI verspricht, das bestehende digitale Identitätsmanagement in hohem Maße zu verbessern, geht jedoch noch mit einigen Herausforderungen einher, weshalb der öffentliche Diskurs zu diesem Thema derzeit kritisch geführt wird. Für die Förderung eines auf SSI-basierenden Ökosystems digitaler Identitäten in Europa ist es unabdingbar, deren Vor- und Nachteile – insbesondere im Vergleich mit etablierten und alternativen technischen Umsetzungen digitalen Identitätsmanagements – sowie ihre Bedeutung für Gesellschaft, Wirtschaft und Politik kritisch zu beleuchten und besser zu verstehen. Mittels sieben ausgewählter Mythen zu unterschiedlichen Themen rund um SSI-basierte digitale Identitäten sollen deshalb gegenwärtige Meinungen diskutiert und der Mehrwert der eingesetzten Technologien aus einer wissenschaftlichen Perspektive beleuchtet werden. Im Folgenden stellen wir diese Mythen vor und analysieren sie. Tabelle 1 fasst die einzelnen Mythen zusammen.

#	**Mythen**
1.	Aktuelle digitale Identitätsmanagement-Lösungen sind ausreichend.
2.	Eine digitale Wallet adressiert nicht die Bedürfnisse der Nutzer*innen.
3.	Regulatorische Anforderungen sind bei einer SSI-basierten Lösung nicht erfüllt.
4.	Das SSI-Konzept weist technische Sicherheitslücken auf.
5.	SSI kann nur mithilfe der Blockchain-Technologie umgesetzt werden.
6.	Bei SSI werden personenbezogene Daten auf der Blockchain gespeichert.
7.	Eine SSI-basierte Lösung ist ineffizient und verbraucht viel Energie.

Tabelle 1: Übersicht der sieben Mythen zu SSI-basierten digitalen Identitäten.

Mythos 1

Aktuelle digitale Identitätsmanagement-Lösungen sind ausreichend.

Mythos 1: Aktuelle digitale Identitätsmanagement-Lösungen sind ausreichend.

Im Zeitalter des Internets nutzen Bürger*innen zahlreiche unterschiedliche Konten und Passwörter für den Zugang zu digitalen Dienstleistungen, Marktplätzen und Plattformen. Häufig wird für den Zugang zu Online-Dienstleistungen noch immer eine Kombination aus Nutzername und Passwort verwendet. Neben der Notwendigkeit, wiederholt Identitätsinformationen in Accounts zu hinterlegen, deren Verifizierung in der Regel sowohl für Serviceanbietende als auch für Nutzer*innen aufwändig ist, stellt die Vielzahl an Passwörtern Nutzer*innen vor große Herausforderungen. Im Durchschnitt haben Nutzer*innen mittlerweile über 100 unterschiedliche digitale Accounts und passen ihre bekannten Passwörter nur selten an. Dies führt häufig zu weitreichenden Sicherheitsproblemen.

Um die Verwaltung der Vielzahl an digitalen Identitäten bequemer zu gestalten, bieten insbesondere US-amerikanische Technologiekonzerne ihren Kund*innen einen Zugang über Single Sign-On (SSO) an. Dabei wird für jeden Identitäts- oder Berechtigungsnachweis mit dem Identitätsanbieter interagiert. Die Erfahrung zeigt, dass Big-Tech-Unternehmen nicht nur Wettbewerbsvorteile erzielen, sondern auch die ihnen zur Verfügung stehenden Daten analysieren und monetarisieren (Lapienytė, 2021). Allgemein ist die Abhängigkeit europäischer Organisationen und Unternehmen von SSO, das von Konzernen bereitgestellt wird, um Mitarbeitenden und Kund*innen effiziente und sichere Interaktionen zu ermöglichen, kritisch zu betrachten. Darüber hinaus sind zentralisierte Systeme anfällig bei Netzwerkausfällen, da sie einen Single-Point-of-Failure darstellen. Der zurückliegende Fall des Facebook-Konzerns zeigt, dass ein Ausfall der Infrastruktur erhebliche Auswirkungen auf die Anmeldemöglichkeiten in anderen Systemen hat und damit auch indirekt zu Verlusten für andere Firmen führen kann (Zivadinovic, 2021).

Zudem stellen zentrale Datenbanken hohe Anreize für Cyber-Kriminelle dar, da hier der Aufwand, eine große Datenmenge zu entwenden, pro Datensatz gerechnet verhältnismäßig gering ist. Auch das Ausstellen gefälschter Zertifikate mit einer validen Signatur stellt ein hohes Risiko für einen potenziellen Datendiebstahl dar. Beispielsweise kam es während der Corona-Pandemie hierbei zu Problemen, als gefälschte digitale Covid-19 Impfzertifikate von einzelnen Apotheken-Mitarbeitenden ausgestellt wurden (Frank Jordan, 2021). Solche Zertifikate sind kryptographisch korrekt erstellt, aber nicht ohne weiteres als Fälschungen erkennbar. Das Fehlen einer möglichen Rückrufbarkeit gefälschter Zertifikate war unter anderem bei Covid-Impfpässen ein großes Problem (Wolf und Nabben, 2021).

Des Weiteren können zentrale Lösungen Staaten ermöglichen, ihre Bürger*innen und Unternehmen stärker zu kontrollieren. In China wird durch das Social Credit System beispielsweise mithilfe von Big Data das Verhalten von Bürger*innen und Unternehmen erfasst und ausgewertet (Liang et al., 2018). Die gezielte Überwachung der Gesellschaft und Organisationen durch den Staat steht im Widerspruch zu den Grundwerten der Europäischen Union, die Kontrolle und Souveränität über die eigene (digitale) Identität den Nutzer*innen zu überlassen. Obwohl SSO in der Wahrnehmung von Nutzer*innen komfortabel erscheint und der Schutz der Privatsphäre für viele keine übergeordnete Rolle spielt, sind die aufgeführten Nachteile nicht zu vernachlässigen.

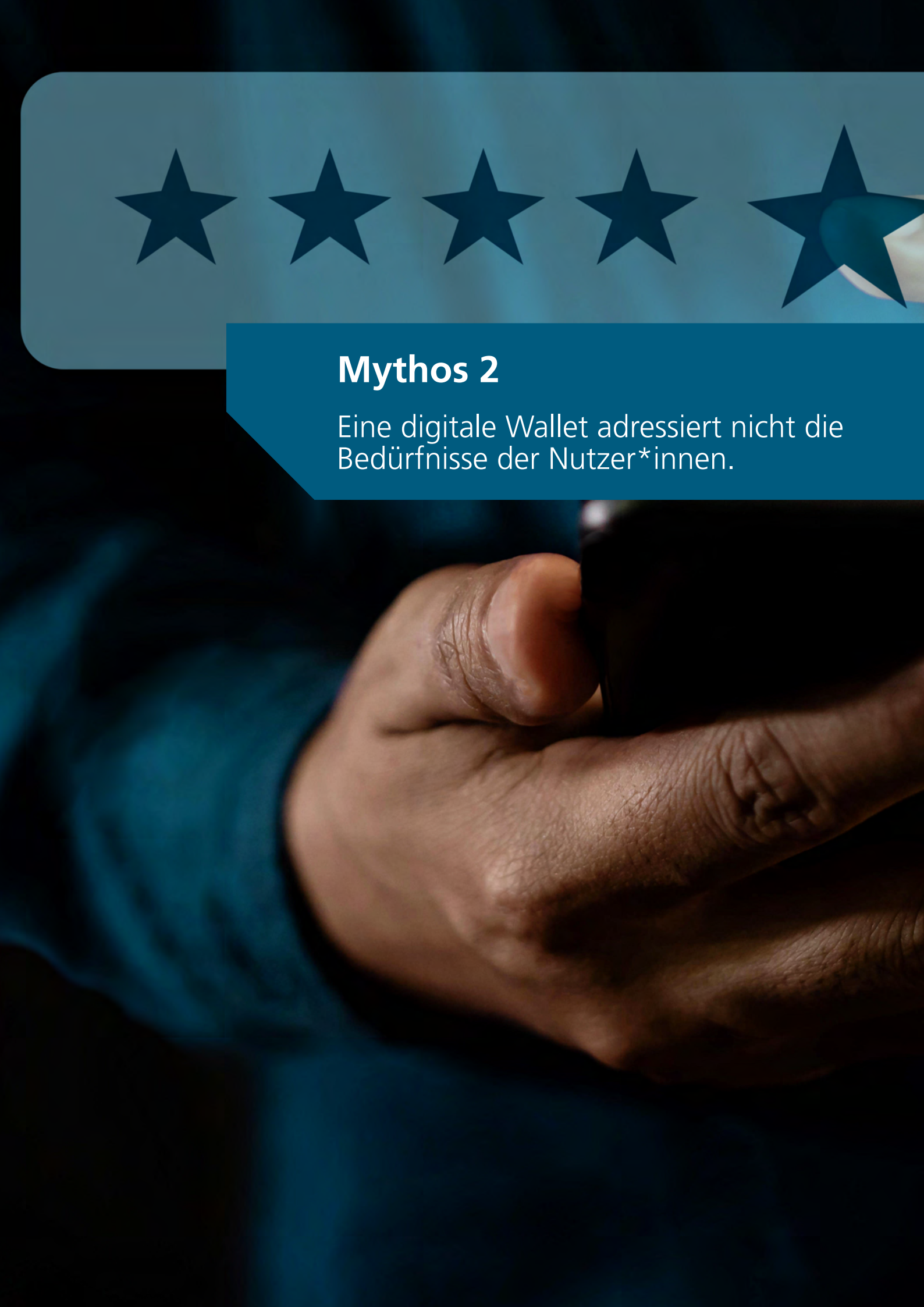
Wie oben aufgeführt, rühren die Überlegungen und Entwicklungen zu SSI aus den Problemen zentralisierter Lösungen für digitale Identitäten, wie z. B. staatlicher Überwachung, aggregierter Datensilos, digitalem Identitätsdiebstahl oder kompromittierter Zertifizierungsstellen (Sedlmeir, Smethurst et al., 2021). Im Gegensatz zu den genannten zentralisierten Identitätslösungen großer Unternehmen kann die Kontrolle bei dezentralen Konzepten in die Hände der Nutzer*innen zurückgegeben werden. Vor diesem Hintergrund gibt die Bundesregierung bei der Entwicklung und Erprobung von SSI-basierten Identitätslösungen die Rahmenbedingungen vor: Das Ziel umschließt den Aufbau eines

übergreifenden Ökosystems digitaler Identitäten für Bürger*innen, Unternehmen und Maschinen. Damit soll mit der voranschreitenden Digitalisierung, die sich besonders durch das zunehmende Angebot an digitalen Produkt- und Dienstleistungen darstellt, Schritt gehalten werden[5].

SSI-basierte Identitäten innerhalb der EU erfordern dabei offene Standards, Interoperabilität und Skalierbarkeit. Deshalb ist es wichtig, SSI im Gesamtkontext zu verstehen und eine europaweite, kompatible, skalierbare Lösung für digitale Identitäten jeglicher Art und unterschiedliche Zielgruppen zu entwickeln. Durch das Bekenntnis der Bundesregierung, digitale Identitäten mittels des SSI-Ansatzes zu entwickeln, soll insbesondere der deutsche und europäische Wettbewerb durch den Aufbau der Infrastruktur des Ökosystems gefördert werden (Bundeskanzleramt (DE), 2021).

Mit diesem Vorgehen wird die europäische Wirtschaft unterstützt und die Abhängigkeit gegenüber großen Technologie-Unternehmen aus dem außereuropäischen Ausland vermindert. In diesem Kontext soll eine mögliche Einführung von eIDAS 2.0 digitale Identitäten für natürliche und juristische Personen innerhalb der EU fördern. Zusätzlich können jegliche Art von Nachweisen abgebildet werden, die beispielsweise mithilfe einer SSI-Lösung umgesetzt werden können. Nutzer*innen können dabei sicherstellen, dass Interaktionen nicht von einer zentralen Stelle nachverfolgt werden, sofern sie einer (staatlich zertifizierten und/oder Open Source) Wallet vertrauen.

[5] Siehe Beitrag der Bundesregierung.



Mythos 2

Eine digitale Wallet adressiert nicht die Bedürfnisse der Nutzer*innen.

Mythos 2: Eine digitale Wallet adressiert nicht die Bedürfnisse der Nutzer*innen.

In der analogen Welt enthalten Identitätsdokumente sowie andere Bescheinigungen und Nachweise stets personenbezogene Daten und Attribute einer Identität, die für gewöhnlich auf Plastikkärtchen oder in Form von Papierdokumenten ausgestellt werden. Beim Vorzeigen dieser Nachweise, beispielsweise im Rahmen einer Polizeikontrolle, bei der Kreditbeantragung oder beim Nachweis über den Impfstatus, ist es oft nicht möglich, nur die für den Anwendungsfall erforderlichen Daten preiszugeben und die nicht relevanten Informationen zu verbergen. Darüber hinaus besteht für Bürger*innen keine Möglichkeit, Teile einer Identität privatsphäreschützend vorzuzeigen. Allerdings steigt im Zuge der voranschreitenden Digitalisierung der Bedarf an digitalen Versionen von Nachweisen, wie beispielsweise eines Personalausweises oder Führerscheins sowie die Möglichkeit Identitätsattribute selektiv offenzulegen (Bundesregierung, 2021).

Auch gängige Zertifikatssysteme wie der digitale Impfpass haben diese Schwächen bislang nicht beseitigt, da hier ein Personalausweis zum Abgleich benötigt wird. Generell werden bei der Prüfung von Zertifikaten stets alle Information von Inhaber*innen offengelegt. Eine selektive Freigabe von Attributen ist über Vertrauensdienste möglich, wie beispielsweise beim deutschen elektronischen Personalausweis (nPA) (Tsakalakis, Stalla-Bourdillon und O'Hara, 2016). Allerdings erfordert dieser Ansatz die Einbindung einer dritten Partei, die alle Attribute des jeweiligen Identitätsnachweises einliest und für die gewünschte Teilmenge eine entsprechende Bestätigung erstellt und weiterleitet (Slamanig, Stranacher und Zwattendorfer, 2014). Bei einer SSI-Lösung erfolgt die selektive Freigabe dagegen durch Nutzer*innen selbst: Ähnlich wie bei physischen Ausweisdokumenten und Bescheinigungen können Personen ihre verifizierbaren Nachweise in einer digitalen Wallet auf dem Smartphone, in der Cloud oder auf einem anderen vertrauenswürdigen System speichern, verwalten und bei Bedarf datenminimierend vorzeigen, ohne dazu die Berechtigung einer dritten Partei einholen zu müssen. Die lokale und damit dezentrale Speicherung personenbezogener Informationen bei einer SSI-Lösung gewährleistet die Sicherheit und den Schutz der Daten. Nutzer*innen können somit überprüfbare Berechtigungsnachweise zur Identifizierung, Authentifizierung und Autorisierung eigenständig verwenden (Sporny, Longley und Chadwick, 2019).

Bei der Verifizierung von Nachweisen werden darüber hinaus nur die Daten übermittelt, die von der verifizierenden Partei über einen sogenannten Proof Request angefordert und von Anwender*innen durch eine Verifiable Presentation, also der zu übermittelnden Daten an die Prüfstelle, explizit freigegeben. Darüber hinaus ermöglicht Selective Disclosure, dass einzelner Attribute einer Identität beim Vorzeigen selektiv freigegeben werden können. Damit geht ein Vorteil gegenüber bestehenden Zertifikatsstrukturen und dem analogen Identitätsmanagement einher, bei denen Zertifikate und kryptographische Identifikatoren vollständig und wiedererkennbar übermittelt werden müssen (Sporny, Longley und Chadwick, 2019). Im Gegensatz zu gängigen Zertifikaten auf Basis von JSON-Web Tokens oder X.509 kann bei SSI-basierten Zertifikaten bewiesen werden, dass die angegebenen Werte in der Verifiable Presentation von einer vertrauenswürdigen ausstellenden Entität signiert wurden, ohne dabei das Verifiable Credential selbst zu übermitteln.

Ermöglicht wird dies durch sogenannte Zero-Knowledge Proofs (ZKPs), die nachweisbar das Minimum an Informationen offenbaren, die für die Interaktion erforderlich sind. ZKPs sind kryptografische Protokolle, die eine prüfende Partei davon überzeugen, dass eine (mathematische) Aussage über Daten korrekt ist, ohne die Informationen selbst offenzulegen (Goldwasser, Micali und Rackoff, 1989). Es ist zu betonen, dass ZKPs in den wenigsten Fällen aus Anonymitätsgründen genutzt werden, da häufig relativ eindeutige Iden-

titätsmerkmale übermittelt werden müssen. Sie ermöglichen jedoch, mathematisch garantiert nicht mehr Informationen als unbedingt notwendig zu übertragen. Damit wird sichergestellt, dass bei der Überprüfung eindeutige Identifikatoren und nicht erforderliche Attribute nicht weitergegeben werden. Im Allgemeinen verlässt das Verifiable Credential zu keiner Zeit die Wallets der Anwender*innen. Außerdem besteht bei SSI die Möglichkeit, mittels Range Proofs numerische Werte wie das Geburtsdatum, Ausstellungsdatum oder andere Attribute datenminimierend nachzuweisen, ohne dabei die Informationen selber preiszugeben (Camenisch, Chaabouni et al., 2008; Dingle, 2020).

Generell ist zu betonen, dass SSI der Wahrung der Vertraulichkeit von sensiblen Informationen größte Bedeutung beimisst und regulatorische Vorgaben deutlich übertrifft. Dies zeigt sich sowohl bei der Vermeidung von domänenübergreifenden Datentöpfen mit besonders weitreichenden Folgen bei Sicherheitslücken und bei der selektiven Freigabe von Identitätsinformationen. Allerdings befindet sich die Entwicklung verifizierbarer Nachweise noch in einem frühen Stadium und repräsentiert somit kein rechtsverbindliches Endprodukt. Beispielsweise stellt in diesem Zusammenhang die Basis-ID des SSI-Piloten des Bundeskanzleramts aufgrund ihres prototypischen Status noch kein offizielles Ausweisdokument dar. Die Basis-ID ist demzufolge zunächst nur dort einsetzbar, wo der Gesetzgeber keinen elektronischen Personalausweis (E-Perso) beziehungsweise keine Smart-eID verlangt, wie etwa beim Carsharing oder bei Mietwagenanbietern (Wölbert, 2021). Langfristig sollen Bürger*innen ihre verifizierbaren Nachweise, wie beispielsweise Führerschein, Geburtsurkunde oder Zeugnisse, in der Wallet-App auf dem Smartphone selbstbestimmend speichern, verwalten und vorzeigen können. Mit dem Entwurf zu eIDAS 2.0 soll die Anerkennung solcher Nachweise erheblich vorangetrieben werden.

Für die technische Implementierung digitaler Wallets gibt es bereits vielversprechende Open-Source-Lösungen, wie z. B. im Rahmen des Software Development Kits (SDK) von Hyperledger Indy[6]. Aus der Sicht der Nutzer*innen sollten wegen der bislang begrenzten Erfahrungen mit Wallet-Apps für Identitätsdokumente vor einem großflächigen Einsatz jedoch auch noch weitere Verbesserungen bei der Bedienbarkeit auf Basis von großflächig angelegten Studien zur Nutzungsfreundlichkeit angestrebt werden.

Die Bundesregierung fördert in diesem Zusammenhang bereits den inländischen Wettbewerb für die Entwicklung digitaler Wallets. Obwohl die Implementierung digitaler Wallets viele technologische Komponenten umfasst, sind die Arbeiten, die bei Unternehmen, Konsortien und Forschungsinstituten für die Integration von SSI-Lösungen erforderlich sind, vor allem prozessualer Natur. Für die Integration einer digitalen Wallet sind somit nur wenige Schnittstellen anzupassen. Hierbei geht es insbesondere um das Testen dieser Lösungen, Erfahrungen zu sammeln und Technologie-Wissen aufzubauen. Darüber hinaus wären die EU-Mitgliedsländer unter dem aktuellen Vorschlag zu eIDAS 2.0. dazu verpflichtet, ihren Bürger*innen innerhalb eines Jahres eine digitale Wallet-Lösung zur Verfügung zu stellen beziehungsweise diese zu fördern.

Zusammenfassend stellt die digitale Wallet eine wesentliche Komponente im SSI-Gesamtökosystem dar und besitzt viele Eigenschaften, die nicht nur in rein digitalen Interaktionen aus Sicht der Nutzer*innen erhebliche Vorteile und Effizienzgewinne bringen können.

[6] Siehe technische Dokumentation zur Indy-SDK Default Wallet Implementation.

Mythos 3

Regulatorische Anforderungen sind bei einer SSI-basierten Lösung nicht erfüllt.

Mythos 3: Regulatorische Anforderungen sind bei einer SSI-basierten Lösung nicht erfüllt.

Die meisten Identitätsdokumente und insbesondere hoheitliche Dokumente, wie beispielsweise die Basis-ID oder der mobile digitale Führerschein, enthalten personenbezogene Daten natürlicher Personen, die unter Art. 1 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) fallen. Beim SSI-Ansatz werden Daten allerdings nach der initialen Ausstellung von kryptographisch signierten Verifiable Credentias nur bilateral zwischen Nutzer*innen und verifizierenden Parteien ausgetauscht. Die Ausstellung der Nachweise findet hierbei über einen sicheren, bilateralen Kommunikationskanal der Nutzer*innen und ausstellenden Institutionen statt, sodass Dritte keinen Einblick in die Datenflüsse erhalten. Mit diesem „Privacy by Design"-Ansatz können insbesondere die strengen Vorgaben der DS-GVO für natürliche Personen in der EU eingehalten werden: Die Beschränkung des Austauschs persönlicher Informationen direkt zwischen den beteiligten Parteien sowie nur auf die benötigten Informationen adressiert etwa das Prinzip der „Datenminimierung" (vgl. Artikel 5 Satz 1 (c) DS-GVO). Zudem ermöglicht die Speicherung von Verifiable Credentials in der digitalen Wallet Portabilität (vgl. Artikel 20 DS-GVO) sowie die selbstständige Löschung von Identitätsinformationen durch Nutzer*innen („Recht auf Vergessenwerden", vgl. Artikel 17 DS-GVO).

In erster Linie gelten für SSI-basierte Lösungen dieselben regulatorischen Anforderungen, wie es beispielsweise bei anderen elektronischen Identitätsnachweisen der Fall ist. Jedoch ist zwischen den Anwendungsfällen zu differenzieren, um die jeweils gültigen, anwendbaren regulatorischen Vorgaben zu erfüllen. Diese Differenzierung greift unter anderem bei den SSI-Projekten des Bundeskanzleramts, z. B. bei der Basis-ID (Personalausweisgesetz) oder dem Bayerischen Landesamt für Steuern, wie z. B. bei Umsatzsteuerbescheinigungen (Geldwäsche- und Know-Your-Customer-Vorgaben). Hierbei liegen aufgrund des Anwendungszwecks dieser Identitäten unterschiedliche gesetzliche und regulatorische Anforderungen vor. In Bezug auf datenschutzrechtliche Vorgaben, wie in der DS-GVO, könnte SSI die strengen Anforderungen durch Privacy by Design in hohem Maße erfüllen (siehe Mythos 2).

Für die Schaffung von einheitlichen Rahmenbedingungen in der grenzüberschreitenden Verwendung elektronischer Identifizierungsmittel und Vertrauensdienste gibt die eIDAS-Verordnung die regulatorischen Leitplanken vor (siehe Abschnitt 1 Motivation und Relevanz). Um eIDAS 1.0 als Vertrauensanker im europäischen SSI-Ökosystem verfügbar zu machen, konzipierte die Europäische Kommission die eIDAS-Bridge, die den ausstellenden Institutionen beim Signieren des Verifiable Credentials unterstützt (Joinup, 2021). Darüber hinaus hilft sie bei der Identifizierung der ausstellenden Partei (eine juristische Person im Rahmen dieses Projekts) anhand ihres öffentlichen Schlüssels. Demzufolge könnte mittels der eIDAS-Bridge ein Verifiable Credential potenziell als vertrauenswürdig und rechtssicher verwendbar eingestuft werden (Joinup, 2021).

Eine abschließende Einschätzung, ob die aktuellen SSI-Projekte zutreffende regulatorische Vorgaben erfüllen, ist zum gegenwärtigen Zeitpunkt nicht möglich. Unter anderem müssten SSI-basierte Identitätslösungen unter einer möglichen, einzuführenden eIDAS 2.0 Verordnung anerkannt werden. Außerdem muss Interoperabilität zu bestehenden Zertifikatssystemen aufgebaut werden, was durch eine Verbindung bestehender PKI mit den in den Pilotprojekten des Bundeskanzleramts verwendeten Verifiable Credentials oder etwa mit der Verwendung von den bereits beschriebenen allgemeineren ZKPs in Verbindung mit X.509-Zertifikaten erzielt werden könnte (Delignat-Lavaud et al., 2016).

Bei den Anwendungsfällen, die im Rahmen der Schaufensterprojekte mit SSI umgesetzt werden, fällt auf, dass es etwa für einen digitalen Personalausweis (elektronischer Identitätsnachweis (eID)) und einen digitalen Führerschein (ISO/IEC 18013-5:2021) bereits entsprechende Ansätze mit anderen technologischen Standards gibt. Während letz-

tere sehr umfangreich auf spezifische Anwendungsfälle reagieren und im Fall der eID dafür sowohl Regulatorik als auch technische Umsetzung vorgeben, liefert SSI eine breitere, allgemeinere Basis, die für verschiedene Anwendungsfälle mit der zugehörigen fachlichen und rechtlichen Komponente geeignet ist.

Eine eID in ihrer momentanen technischen Implementierung unterstützt bisher nur Stammdaten und kann nicht wie mit einer SSI-basierten Lösung um zusätzliche Attribute erweitert werden, da sie ausschließlich auf der Repräsentation des Personalausweises beruht. Die eigentliche Abfrage der Daten erfolgt dabei nicht direkt vom Endgerät, sondern über einen Schlüssel, welcher den Zugriff auf die Daten von einem eID-Service zulässt, was im Gegensatz zum nutzerzentrierten SSI-Konzept steht. Deshalb sind auch sowohl für Endanwender*innen als auch für Unternehmen und Behörden die Einstiegshürden ungleich höher.

Da für hoheitliche Dokumente, wie einen digitalen Personalausweis oder perspektivisch einen digitalen Führerschein, das in der eIDAS-Verordnung festgelegte Level « HIGH » erforderlich ist, müssen für eine Anerkennung des Credentials hohe sicherheitstechnische Anforderungen erfüllt sein. So können für eine SSI-Lösung beispielsweise Implikationen aus den sicherheitstechnischen und Governance-Mechanismen anhand der eID-Architektur abgeleitet werden. Da laut Bundesamt für Sicherheit in der Informationstechnik (2021) SSI zum jetzigen Zeitpunkt nicht in der Lage ist, dieses Niveau alleine abbilden zu können, ist auch eine Verknüpfung beider Technologien sinnvoll, um sowohl für Credentials niedriger als auch höherer Stufen eine Lösung anbieten zu können.

Im Kontext regulatorischer Hürden sollte auch darauf hingewiesen werden, dass aus einer technologischen Perspektive noch Elemente wie die zugrundeliegende Kryptographie vorliegen, die zum jetzigen Zeitpunkt noch keine Zertifizierung durch Behörden wie das BSI durchlaufen haben (siehe Mythos 6). Auch wenn aktuell keine konkreten Sicherheitslücken bekannt sind, ist eine Ende-zu-Ende-Auditierung für ein hohes Maß an Sicherheit unabdingbar und ist entsprechend die Grundvoraussetzung für ein vollständiges regulatorisches Fazit. Da die Verwendung kryptographischer Methoden als Henne-Ei-Problem angesehen werden kann, ist für den weiteren Verlauf der Schaufensterprojekte Digitale Identitäten eine erste Überprüfung und Einschätzung der verwendeten kryptographischen Komponenten anzustreben. Werden diese Aspekte sukzessive adressiert, können die entsprechenden Hürden nach und nach abgebaut werden.

Grundsätzlich lässt sich festhalten, dass SSI als technologische Komponente durchaus in der Lage ist, mit den entsprechenden Vorkehrungen Standards und Governance-Thematiken vollumfänglich umzusetzen. Während viele Entwickler*innen und Unterstützer*innen von SSI plausibel argumentieren, dass eine dezentralere Governance für ein hoch skaliertes Ökosystem digitaler Identitäten notwendig oder hilfreich ist, kann eine Evaluation wohl nur durch eine praktische Umsetzung erfolgen. Entsprechend sind weitere Untersuchungen anzustreben, wie mit möglichst geringem Aufwand die Möglichkeit sowohl für zentrale als auch für dezentrale Ansätze offen gehalten werden kann.

Mythos 4

Das SSI-Konzept weist technische Sicherheitslücken auf.

Mythos 4: Das SSI-Konzept weist technische Sicherheitslücken auf.

Gerade die Einführung einer digitalen Repräsentation der Fahrerlaubnis hat mit ihrem vorzeitigen Stopp zu Kritik aus verschiedenen Reihen geführt (Wittmann, 2021; Muth, 2021). Im Rahmen technischer Analysen wurden berechtigte Fragen zur Implementierung sowie deren Sicherheitsmechanismen aufgeworfen. Wie bei jeder öffentlichen Softwarearchitektur muss auch bei einem SSI-basierten System jederzeit mit böswilligen Akteuren gerechnet werden. Somit müssen vor dem Start ausführliche Penetrationstests durchgeführt werden, um Angriffspunkte auszuschließen. Hier wurde insbesondere die Möglichkeit kritisiert, bei der Verifizierung eines Credentials im Rahmen eines Proof Requests, den Namen (und ggf. ein Bild) der anfragenden Partei frei wählen zu können. Daneben wurden auch die Sicherheit komplexer kryptographischer Verfahren für ZKPs und für Blockchains sowie die Eignung von Smartphones für die Speicherung sensibler Identitätsinformationen kontrovers diskutiert (Kahlo, 2021; Chaosradio, 2021)[7]. Auf diese Kritikpunkte soll im Folgenden eingegangen werden.

Zunächst entspricht es dem Kern einer selbstsouveränen Identität, darüber bestimmen zu können, in welcher Granularität Daten an wen herausgegeben werden. Vergleicht man dieses Szenario mit dem Aushändigen von Informationen einer physischen Identität an eine fremde Person in der realen Welt, ist die gleiche Sorgfaltspflicht zu erfüllen. Dieser Umstand kann in der digitalen Welt insofern bedenklich sein, als sich die Identität verifizierender Stellen für Endnutzer*innen bei digitalen Interaktionen zunächst nicht visuell überprüfen lässt. Dies ist problematisch, weil sensitive Informationen so in die falschen Hände geraten können.

Ein deutlich weitreichenderes Angriffsszenario, welches bei der Implementierung des digitalen Führerscheins nicht verhindert wurde, ist die sogenannte Man-in-the-Middle-Attacke (Wittmann, 2021; Lissi, 2021). Bei solch einem Angriff kann eine dritte Person unbemerkt die Kommunikation zwischen der verifizierenden Partei und Wallet-Nutzer*innen mitlesen, indem sie sich für Inhaber*in einer Wallet als verifizierende Partei und für die verifizierende Partei entsprechend als Inhaber*in einer Wallet ausgibt. Neben dem Mitlesen sensitiver Informationen können in der Interaktion neu ausgestellte Identitätsnachweise direkt für Angreifende nutzbar gemacht werden. Damit können Wallet-Nutzer*innen in späteren Interaktionen mit weiteren Organisationen unter Umständen inpersonifiziert werden. Die Folgen sind sowohl für Wallet-Inhaber*innen und verifizierende Parteien weitreichend, da sie sich auf die Authentizität verlassen.

Dieses Problem wurde bereits deutlich früher in der SSI-Community diskutiert und es wurden verschiedene Lösungsmöglichkeiten aufgezeigt. Eine Lösung, die insbesondere für hoheitliche Dokumente sinnvoll erscheint, ist, dass die ausstellende Institution nur bestimmte verifizierende Organisationen – oder von bestimmten Organisationen zertifizierte verifizierende Organisationen – als Empfänger angibt und die digitale Wallet die Weitergabe nur an diese verifizierende Organisation zulässt (Lissi, 2021). Somit können Endnutzer*innen bei hochsensiblen Daten oder weitreichenden Berechtigungen sicher sein, dass sie nur an autorisierte Organisationen weitergegeben werden und nicht an bösartig Handelnde. Diese Maßnahme kann beispielsweise über das Hinterlegen der öffentlichen Schlüssel einer verifizierenden Organisation in einem Vertrauensregister umgesetzt werden, das zentral oder dezentral verwaltet werden kann (siehe Mythos 5). Diese Vorkehrungen sind einfach zu implementieren, können bestehende Mechanismen zur Identifikation von Organisationen im Internet wie etwa SSL-Zertifikate und qualifizierte Webseitenzertifikate nutzen, und befinden sich etwa in der ID-Wallet bereits in der Umsetzung. Auf der anderen Seite stellt dieser Ansatz für viele Interaktionen auch eine möglicherweise zu starke Einschränkung von Nutzer*innen dar, etwa, wenn diese sich sicher sind, dass sie einer zwar nicht zertifizierten, aber vertrauenswürdigen Partei Infor-

[7] Zur Position des BSI gegenüber ZKPs allgemein siehe Studie des BSI zu sicheren Blockchains.

mationen übermitteln möchten. Besonders wenn die dabei involvierten Informationen wenig sensitiv oder mithilfe von ZKPs stark anonymisiert sind, sollten Nutzer*innen die Möglichkeit haben eine entsprechende Warnung der Wallet-App zu ignorieren. Das scheint etwa bei einem Nachweis über die Volljährigkeit oder über den Impfstatus ohne die Preisgabe des Namens sinnvoll. Weitere Diskussionen zu unterschiedliche Szenarien, unter welchen Bedingungen welche Herangehensweisen geeignet sind und wie feingranular diese Möglichkeiten unterschieden werden müssen, sind weiterhin nötig.

Neben klassischen Zertifizierungsstellen (engl. Certificate Authorities, CA), die die PKI des heutigen Internets bilden, können Signaturschlüssel auch über dezentrale Register mithilfe der Distributed Ledger Technologie (DLT), wie beispielsweise der Blockchain-Technologie[8], zugeordnet und veröffentlicht werden. Im Rahmen der Schaufensterprojekte des Bundes wird die Hoheit mithilfe der Blockhain über mehrere vertrauenswürdige Parteien verteilt, die sogenannten Knotenbetreiber[9]. Die Knoten einer Blockchain, wie beispielsweise Hyperledger Indy, werden von Unternehmen oder Behörden in deren eigenen Infrastruktur betrieben. In Summe muss ein Netzwerk erreicht werden, dass in seinem Aufbau ausreichend gegen Ausfälle geschützt ist, da ein verteiltes System nur mit einer begrenzten Menge an wegfallenden oder kompromittierten Knoten bestehen kann, bevor der Konsens verloren wird.

Kompromittierte Knoten können auch mithilfe von Mehrheiten der übrigen Knoten aus dem Netzwerk entfernt werden. Solange nicht ein signifikanter Anteil (i.d.R. 1/3) der Knoten im Netzwerk kompromittiert ist, ist die Übernahme des Netzwerks durch diese Mechanismen nicht möglich. Um dieser Angriffsfläche proaktiv entgegenzuwirken, sollte das gesamte Netzwerk kontinuierlich überwacht werden, um solche Gefährdungen frühzeitig zu erkennen und im Fall einer Übernahme die betreffenden Knoten vom Konsens ausschließen zu können und ihnen die Rechte zu entziehen. Im Vergleich zu einer zentralen Softwarearchitektur ergibt sich der Vorteil, dass nicht sofort die gesamte Infrastruktur durch einen Angriff in Gefahr ist, sondern die Angriffsfläche auf mehrere Stakeholder verteilt wird und somit eine flexible Reaktion möglich wird. So genügt es nicht mehr, nur in eine Organisation einzudringen: Wegen der zugrundeliegenden Konsensfindung muss zumindest die Mehrheit der Knoten angegriffen werden oder ein beträchtlicher Anteil einer knappen Ressource wie Rechenleistung des Gesamtsystems erreicht werden. Insgesamt ergibt sich dadurch konzeptionell eine nachweisbar hohe Verfügbarkeit und Robustheit gegen Angreifer. Der im Zusammenhang mit der ID-Wallet verwendete Distributed Ledger nutzt einen Konsensmechanismus, der auf mathematisch seit mehr als 20 Jahren bekannten Konzepten aufbaut und nachweisbar sicher ist, solange weniger als 1/3 der Knoten angegriffen werden oder ausfallen (Castro, Liskov et al., 1999; Aublin, Mokhtar und Quéma, 2013; Naik und Jenkins, 2021). In der Praxis ist die Implementierung jedoch nach wie vor komplex und weder hinsichtlich ihrer Sicherheit noch hinsichtlich ihrer Performanz über lange Zeiträume erprobt (siehe Mythos 5).

In Bezug auf das Smartphone-Wallet sollte in einem IT-Sicherheitskontext die Frage gestellt werden, wie sichergestellt werden kann, dass kryptographische Schlüssel und Zertifikate nicht über Cyber-Angriffe oder physischen Zugang zum gesperrten Gerät extrahiert werden können. Untersuchungen legen nahe, dass Smartphones zwar ein hohes Sicherheitsniveau erreichen könnten, dass entsprechende Mechanismen jedoch oft nur unzureichend eingesetzt werden (Lovejoy, 2021; Zinkus, Jois und Green, 2021). Insgesamt sollte dieses Thema in der Diskussion noch stärkere Aufmerksamkeit erfahren, insbesondere da bekannt ist, dass beispielsweise Unternehmen wie die NSO Group im Falle der Pegasus-Spyware Smartphones gezielt und unbemerkt angreifen können (Munzinger, 2021). Dabei sollten auch die Abhängigkeit der Herstellerfirmen von Smartphones und deren Betriebssysteme sowie die Sicherstellung, dass diese

[8] Im Folgenden verwenden wir die Begriffe Blockchain und DLT als Synonyme.
[9] Siehe z. B. Governance bei IDunion.

Mythos 4: Das SSI-Konzept weist technische Sicherheitslücken auf.

Aktivitäten in der Wallet nicht nachverfolgen können, berücksichtigt werden. Perfekte Sicherheit ist nur sehr schwer zu erreichen, und ein Verzicht auf eine Smartphone-Anwendung würde wohl auch mit erheblicher Einschränkung der Nutzerfreundlichkeit einhergehen. Daher müssen hier fundiert Abwägungen zwischen den unterschiedlichen Realisierungsoptionen einer digitalen Identität getroffen werden. Außerdem ist bei der direkten Verknüpfung von Betriebssystem und digitalen Wallets fraglich, inwiefern Behörden der einzelnen Länder eine Möglichkeit zum Eingriff oder der Anpassung besitzen, da die Nachweise in der jeweiligen integrierten Walletlösung gespeichert werden. Hier ist die Abwägung zwischen einer Generalisierung über eine Norm und Abweichungen in bestimmten Fällen zu treffen. Dies gilt jedoch analog für alle mobilen digitalen Identitätslösungen.

Des Weiteren stellt sich bei der Verwendung einer digitalen Wallet-App die Frage, inwieweit die sicherheitstechnischen Anforderungen eines sicheren Zugangs für Nutzer*innen gegeben sind. In diesem Kontext nimmt die Zwei-Faktor-Authentifizierung eine hohe Bedeutung ein, um die Sicherheit der Nutzer*innen über die Verwaltung personenbezogener Informationen zu gewährleisten. Darüber hinaus ist es wichtig, den unbemerkten Diebstahl von Nachweisen zu verhindern, beispielsweise mithilfe der Anbindung an das mobile Endgerät.

Um den praktischen Nutzen einer digitalen Wallet-App zu erhöhen und sicherheitsrelevante Vorgaben zu erfüllen, ist es unabdingbar, die Wiederherstellung von Identitätsdokumenten und kryptographischen Schlüsseln, beispielsweise über Backups, zu ermöglichen. In diesem Zusammenhang sollten Nutzer*innen die Möglichkeit besitzen, ihre Daten regelmäßig abzusichern, um sie im Falle von Verlust oder Diebstahl wiederherzustellen. Auf dem Markt gibt es bereits einige digitale Wallets, die über eine integrierte Einrichtung automatisierter verschlüsselter Backups auf Cloud-Services verfügen. Bei der Installation der App wird initial ein Recovery Key generiert, der zur Entschlüsselung des Backups, beispielsweise über Cloud-Anbieter*innen oder Services der Wallet-Anbieter*innen, erforderlich ist. Die Aufbewahrung der Schlüssel kann dabei offline, über das Auslagern an eine Vertrauensperson oder verteilt über mehrere Geräte (Multi-Device Recovery) erfolgen (it-daily.net, 2021). Dabei ist zu beachten, dass Backups für Schlüssel in sicheren Schlüsselspeichern möglicherweise nicht umsetzbar sind. Es ist jedoch denkbar, dass etwa nur der digitale Personalausweis über eine Gerätebindung (Device Binding) verfügt. Im Falle von Diebstahl oder Verlust müssen dann – wie im analogen Fall – der alte (digitale) Personalausweis zurückgerufen und ein neuer erstellt werden. Die verbleibenden Identitätsdokumente können dagegen über Backups wiederhergestellt werden, gleichzeitig aber über Vorzeigen in Verbindung mit dem Personalausweis bei Bedarf dessen Gerätebindung „erben".

Neben der Speicherung kryptographischer Schlüssel in der Wallet-App kann eine besonders starke Gerätebindung verwendet werden, die im Gegensatz zum Schlüsselspeicher des Betriebssystems einen speziellen Chip – das sogenannte Secure Element – nutzt, dessen einziger Zweck die sichere Speicherung von kryptographischen Schlüsseln ist. Durch diesen Ansatz kann das Kopieren von verifizierbaren Nachweisen sowie zugehöriger Schlüssel auf ein anderes Smartphone praktisch komplett verhindert werden. Damit wird sichergestellt, dass die Nutzung nur auf einem mobilen Endgerät möglich ist und das Teilen von Berechtigungen erschwert. Dabei ist festzuhalten, dass die in aktuell genutzten SSI-Implementierungen verwendeten ZKPs noch nicht in der Lage sind, den Nachweis über die Kontrolle über Schlüssel im Secure Element zu erbringen, ohne eine eindeutige Spur zu hinterlassen. Die Machbarkeit der Vereinbarkeit von Sicherheit und Datenminimalität auch in diesem Fall wurde jedoch bereits anhand von X.509 Zertifikaten gezeigt (Delignat-Lavaud et al., 2016), und es ist wünschenswert, dies auch in den verwendeten SSI-Implementierungen zu ermöglichen.

Mythos 5

SSI kann nur mithilfe der Blockchain-Technologie umgesetzt werden.

Mythos 5: SSI kann nur mithilfe der Blockchain-Technologie umgesetzt werden.

In vielen SSI-Pilotprojekten wird für die Zuordnung und Veröffentlichung von Signaturschlüsseln der Einsatz der Blockchain-Technologie erprobt. Allerdings können für diesen Zweck auch zentrale Alternativen in Betracht gezogen werden. Generell sind für die Zuordnung von (öffentlichen) Signaturschlüsseln zu Organisationen, die verifizierenden Organisationen in der Regel als Grundlage dient, um die Vertrauenswürdigkeit von Identitätsdokumenten einzustufen, ein oder mehrere nachprüfbare und öffentlich verfügbare Datenregister notwendig.

Die verteilte und synchronisierte Datenhaltung in einer Blockchain-basierten Lösung ermöglicht breite Akzeptanz und das Referenzieren einer gemeinsamen Grundlage für die Verwendung von hoheitlichen und weiteren Nachweisen. In diesem Kontext können Organisationen ihre eigenen öffentliche Kennungen (engl. Public DID) generieren und darauf basierend Nachweise ausstellen. Nutzer*innen können digitale Identitätsnachweise zusammen mit anderen Nachweisen in einem Ökosystem SSI-basierter Identitäten verwalten und kombiniert in einem Vorgang verwenden. Personen und Organisationen sollten die Kontrolle über ihre digitale Identität besitzen, ohne von einer dritten Partei abhängig zu sein. Dies ist wichtig, weil DIDs die Basis für jedes Identitäts- und Kommunikationssystem bilden können, denn ohne diese gibt es keine Beziehungen, Transaktionen und Nachrichten zwischen Entitäten (Sabadello, 2017). Außerdem können neue Vorlagen (engl. Schema) für verifizierbare Identitäten leicht im Netzwerk registriert werden und somit neue Nachweisklassen für ausstellende Institutionen definieren und nutzbar machen.

Ein weiterer Vorteil geht mit der Möglichkeit der Ungültigerklärung (engl. Revocation) ausgestellter Nachweise einher, die eine Korrelation von Nutzer*innen durch die Verwendung von nicht änderbaren Listen (engl. Tails Files) und kryptographischen Akkumulatoren (engl. Accumulator) unterbinden und somit die Privatsphäre trotz öffentlicher Verfügbarkeit schützen kann[10]. Dadurch ermöglicht ein Blockchain-basiertes Revocation-Register nicht nur Verbesserungen in der Verfügbarkeit von Revozierungs-Informationen, sondern befähigt Nutzer*innen, die Gültigkeit ihrer Identitätsnachweise zu beweisen, ohne dafür die ausstellenden Parteien erneut kontaktieren zu müssen. Im Gegensatz dazu arbeiten PKI-basierte Identitätslösungen mit interaktiven Diensten, die die Gültigkeit der Zertifikate bei der Abfrage überprüfen und so eine Korrelation der Nutzer*innen ermöglichen. Für eine Blockchain-basierte SSI-Architektur spricht darüber hinaus die Unveränderbarkeit und Transparenz der Transaktionshistorie, die unter anderem die Hinzunahme von neuen Schemas, Credential Definitions oder Einträgen in das Revocation-Register, aber auch die Anpassung von Rechten und Rollen öffentlich einsehbar abspeichern. Ferner können bei Blockchains Angriffs- oder Ausfallpunkte verringert werden. Falls einzelne DIDs oder Server, die das Register speichern, kompromittiert werden sollten, betrifft das nur wenige Aussteller-Dienste, jedoch nicht das Gesamtsystem (siehe Mythos 4).

Jedoch erhöht sich bei Verwendung einer Blockchain die Komplexität und bietet somit Potenzial für Angriffe. Insbesondere bergen die Anwendbarkeit von Revozierungsmöglichkeiten über Blockchain-basierte Register eine hohe Komplexität, da in diesem Fall kryptographische Konzepte angewandt werden, die ein tiefgreifendes Verständnis und ausgeklügeltes Sicherheitssystem erfordern. Zugangsbeschränkte Blockchain-basierte Systeme wie Hyperledger Indy weisen zwar oft große Herausforderungen hinsichtlich der Performanz von Schreiboperationen auf (Sedlmeir, Ross et al., 2021). Allerdings stellen diese bei sinnvoller Verwendung der Blockchain – überwiegend für Lesezugriffe, für die horizontale Skalierung möglich ist – im Falle von SSI keine nennenswerten Probleme dar. Insbesondere waren die Performanzprobleme beim Start der mobilen, digitalen Fahrerlaubnis in

[10] Siehe Dokumentation zu Tails Files und Accumulator.

der ID-Wallet nicht der Blockchain-Komponente geschuldet[11].

Neben der Implementierung eines Revocation-Registers, entstehen grundsätzliche Fragen hinsichtlich der Governance. Es bedarf einer sorgfältigen Evaluierung, welche Entitäten als vertrauenswürdig einzustufen sind, die die einzelnen Knoten im Netzwerk betreiben dürfen. Wenn Knotenbetreiber böswillige Absichten hegen, könnten diese potenziell das Netzwerk angreifen und das Gesamtsystem übernehmen. Folglich würde dies zu einem Vertrauensverlust in die Technologie sowie involvierte Organisationen führen. Darüber hinaus ist es essenziell, vorab ein übergreifendes Governance-System hinsichtlich des Rollen- und Rechtemanagements zu definieren, um beispielsweise erforderliche Zugrifss- und Schreibrechte für Veränderungen auf dem Blockchain-Ledger den entsprechenden Organisationen zuzuteilen. Die Blockchain-Technologie befindet sich im Vergleich zu etablierten CA- und PKI-Strukturen noch in einem jungen Stadium und muss sich über längere Zeit in der Praxis erst noch als alternativer, dezentraler Vertrauensanker beweisen und für alle Anwendungen eine Authentisierung auf angemessenem Niveau gewährleisten (Bundesamt für Sicherheit in der Informationstechnik, 2021).

Wie bereits erwähnt, könnte auch eine zentralisierte Lösung mittels CAs und PKI öffentliche Schlüssel einer Person oder Organisation im Internet zuordnen, verwalten und beglaubigen. Insbesondere wenn Anwendungen ein erhöhtes Sicherheitsniveau erzielen sollen, die beispielsweise eine eIDAS-konforme Authentisierung verlangen, sollten PKI-basierte Lösungen in Betracht gezogen werden (Bundesamt für Sicherheit in der Informationstechnik, 2021). Zudem bietet sich die Möglichkeit mittels PKI an, wenn bereits ein hohes Maß an Vertrauen in zentralisierte Entitäten vorherrscht. Jedoch stellt sich die Frage, wer diese vertrauenswürdige Entität bei einer zentralisierten Variante sein soll. In Deutschland gelten gesetzlich festgelegte Anforderungen für digitale Zertifikate und qualifizierte elektronische Signaturen nach dem Vertrauensdienstegesetz[12]. Die CAs unterliegen dabei der Aufsicht der Bundesnetzagentur, die die Integrität der Zertifikate im Rechtsverkehr gewährleistet.

Auf der anderen Seite können sich Prüfstellen aus mehreren Entitäten zusammensetzen, insbesondere wenn die Governance in der europäischen Gesamtbetrachtung erfolgt. In einem ähnlichen Kontext wie bei der internationalen Zivilluftfahrtorganisation (International Civil Aviation Organization, ICAO) gibt es bereits übergreifende Standards bei der Ausstellung und Überprüfung elektronischer Reisepässe. Hierbei richtet jedes Land als Vertrauensstelle eine nationale Wurzelzertifizierungsstelle für das Signieren (Country Signing Certification Authority, CSCA[13]) ein. Die nationale CSCA erstellt die Wurzelzertifikate (CSCA-Zertifikate) und signiert Zertifikate, die für das Signieren von Daten auf (Ausweis-)Dokumenten, sogenannte Document Signer Zertifikate, des Passherstellers erforderlich sind. Anschließend muss der Document Signer mit der CSCA abgeglichen werden, um die digitale Signatur zu validieren.[14]. Damit stünde trotz nationaler Zertifizierungsstelle eine dezentrale, standardisierte Alternative auf europäischer Ebene zu einer Blockchain-Infrastruktur zur Verfügung.

Die Blockchain-Technologie erfährt in Industrie und anderen Ländern sowie in unterschiedlichen SSI-Projekten (z. B. Hyperledger Indy) ein großes Momentum, das zu einem grenzüberschreitenden Ökosystem kompatibler digitaler Wallets, innovativer privatsphäreschützender Funktionen und gut gelösten Revozierungsmöglichkeiten beitragen kann. In der Zukunft kann es allerdings auch SSI-basierte Ökosysteme geben, die mehrere unterschiedliche Register auf zentraler und dezentraler Basis für die Zuordnung und Validierung von Schlüsselmaterial erlauben.

[11] Zur Performance der genutzten Hyperledger Indy Blockchain siehe Sedlmeir, Ross et al. (2021).

[12] Siehe Gesetzestext.

[13] Siehe Beispiel zur Country Signing Certification Authority (CSCA).

[14] Siehe Erläuterung des BSI.

Mythos 6

Bei SSI werden personenbezogene Daten auf der Blockchain gespeichert.

Mythos 6: Bei SSI werden personenbezogene Daten auf der Blockchain gespeichert.

Bei einer Blockchain-basierten SSI-Lösung sind wie bei der Verwendung zentraler Alternativen (bspw. CAs) Vorgaben hinsichtlich des Datenschutzes einzuhalten. Der große Unterschied zur zentralen Verwaltung besteht bei Blockchain-basierten Systemen in der Unveränderbarkeit der Transaktionshistorie sowie im Replizieren der Daten auf mehreren Knoten. Dies erfordert somit weitaus umfassendere Maßnahmen, um bestehende Datenschutzvorgaben einzuhalten. Aufgrund der Eigenschaften von Blockchain hinsichtlich transparenter und unveränderbarer Dateneinträge, die auf vielen Knoten gespeichert sind, verstoßen diese potenziell gegen datenschutzrechtliche Vorgaben, wie beispielsweise der DS-GVO bei natürlichen Personen.

Bei der Verarbeitung personenbezogener Daten auf einer Blockchain in anderen Anwendungsfällen werden die Daten in der Regel pseudonymisiert, um den Personenbezug zu brechen. Die Pseudonymisierung kann jedoch mit vertretbarem Aufwand sowie unter der Verwendung technischer Hilfsmittel aufgehoben werden und einen Personenbezug damit nicht verhindern[15]. Daneben ist zu beachten, dass Nutzer*innen eine vorher getätigte Einwilligung zur Datenverarbeitung jederzeit widerrufen können[16]. Aufgrund der praktischen Unveränderbarkeit können Daten auf Blockchain-basierten Systemen in der Regel im Nachhinein nicht mehr verändert werden. In diesem Zusammenhang ist das Ausüben des Rechts auf Anpassungen inkorrekter Daten[17] oder der Löschung[18] von Daten durch Nutzer*innen bei Blockchains nur sehr erschwert möglich (Schellinger et al., 2022).

Demzufolge muss bei der Nutzung einer Blockchain-Infrastruktur darauf geachtet werden, den Personenbezug von Daten sowie die Offenlegung von betriebsinternen Unternehmens- und Maschinendaten grundsätzlich zu vermeiden (Schlatt et al., 2021). Wichtig ist hierbei die Feststellung, ob es sich bei den Daten um personenbezogene Daten handelt. Beispielsweise zeigt die rechtliche Evaluierung des SSI-Prototyps des bayerischen LfSt, der auf Basis der Blockchain-Technologie umgesetzt wurde, dass eine rechtskonforme Gestaltung grundsätzlich möglich erscheint. Allerdings können in diesem Projekt nicht alle datenschutzrechtlichen Risiken beim Einsatz der Blockchain-Technologie evaluiert werden, da es diesbezüglich derzeit noch an einer klaren Gesetzgebung und Rechtsprechung mangelt (Guggenberger et al., 2021).

Im Rahmen der SSI-Piloten des Bundeskanzleramts werden datenschutzrechtliche Vorgaben bei der Ausstellung und Verifizierung der Credentials in der digitalen Wallet eingehalten (siehe Mythos 3). Die Verwendung der Blockchain Hyperledger Indy dient in diesem Pilotierungsprojekt nur für die Speicherung öffentlichen Schlüsselmaterials (öffentliche Schlüssel und DIDs) ausstellender Parteien sowie als dezentrale Prüfinfrastruktur. Personenbezogene Daten werden weder bei der Ausstellung noch bei der Verifizierung von Nachweisen auf den Blockchain-Ledger geschrieben. Insbesondere werden nicht nur Identitätsattribute, sondern auch von Personen verwendete öffentliche Schlüssel zu keinem Zeitpunkt auf eine Blockchain geschrieben, sondern lediglich in der digitalen Wallet der Nutzer*innen gespeichert und bilateral mit verifizierenden Parteien geteilt. Zudem können – wie bereits in Mythos 5 diskutiert – durch die Verwendung von ZKPs bei der Verwendung eines Blockchain-basierten Revocation-Registers keine Rückschlüsse auf Personen durch Korrelation erfolgen. Es ist zu beachten, dass ausstellende Institutionen von Credentials ein natürliches Interesse an relevanten Daten haben, die aufgrund des Anwendungsfalls zwingend erforderlich sind und mit rechtlichen Folgen einhergehen, wie beispielsweise Informationen über das Ablaufdatum des Personalausweises oder einer entzogenen Fahrerlaubnis. Somit verarbeiten, speichern und kontrollieren ausstellende Entitäten immer personenbezogene Daten in ihren eigenen

[15] Vgl. Artikel 4 Satz 5 DSG-VO.
[16] Vgl. Artikel 7 Satz 3 DSG-VO. Mit Ausnahme von Artikel 6 Satz 1b) bis f).
[17] Vgl. Artikel 16 DSG-VO.
[18] Vgl. Artikel 17 DSG-VO.

Datenbanken – unabhängig davon, ob eine Blockchain verwendet wird oder nicht.

Das Revocation-Register auf dem Ledger bezieht sich stets auf eine vorhandene Credential-Definition und enthält Informationen über den aktuellen Akkumulator, den URI der Tails Files sowie dessen Hashwert. Nutzer*innen erhalten bei der Ausgabe eines Credentials zusätzlich den Index-Wert sowie eine Kennzahl (das Produkt aller anderen Akkumulator-Werte in den Tails Files), den sogenannten Witness. Auf dem Ledger wird der neue Akkumulator-Wert der ausstellenden Entität regelmäßig und global im Revocation-Register aktualisiert. Ein entsprechendes Delta zwischen dem bisherigen und dem neuen Witness wird über den aktualisierten Akkumulator-Wert beim Vorzeigen des Credentials abgeleitet. Dabei verändert sich der Index-Wert in den Tails Files nicht. Nutzer*innen beweisen während des Verifikationsprozesses, dass sie gültige Credentials besitzen, indem sie kryptographisch nachweisen, dass sie mithilfe des öffentlichen auf der Blockchain gespeicherten Akkumulator-Werts einen bestimmten Eintrag in den Tails Files kennen. Für die verifizierenden Parteien entfällt die Notwendigkeit, sich mit ausstellenden Institutionen in Verbindung zu setzen oder eine Sperrliste zu prüfen. Mit diesem Vorgehen können Nutzer*innen die Gültigkeit ihrer Credentials auf innovative und datenschutzkonforme Weise vorzeigen.

Mythos 7

Eine SSI-basierte Lösung ist ineffizient und verbraucht viel Energie.

Mythos 7: Eine SSI-basierte Lösung ist ineffizient und verbraucht viel Energie.

Generell sollen mit der Entwicklung von SSI die Schwächen bisheriger Systeme für digitale Identitäten adressiert werden. Dabei ist es wichtig, dass die Grundsätze der Kontrollierbarkeit, Portabilität und Sicherheit selbstbestimmter digitaler Identitäten berücksichtigt werden, um das Potenzial eines übergreifenden SSI-Ökosystems freizusetzen (Allen, 2016). Insgesamt soll eine SSI-basierte Lösung digitale Identitäten bequem, privatsphäreschützend und anbieterübergreifend in einer digitalen Wallet verwaltbar machen. Nutzer*innen steht es frei, eine digitale Wallet-App eines bestimmten Anbieters, die durch den offenen Wettbewerb von der Bundesregierung gefördert wird, auszuwählen. Damit wird ein klassischer Lock-In-Effekt wie bei SSO-Diensten vermieden.

Trotz der komplexen und innovativen technischen Infrastruktur, können Nutzer*innen sehr bedienungsfreundlich, insofern diese in solch einem Maße ausgestaltet wurde, durch den Ausstellungs- und Verifizierungsprozess in ihrer Wallet-App geführt werden (siehe Mythos 2). Beispielsweise werden Anwender*innen aktiv von Prüfstellen darüber benachrichtigt, welche Daten für den Anwendungsfall erforderlich sind und können mittels weniger Clicks der Datenfreigabe zustimmen oder ablehnen. Angesichts potentieller Man-in-the-Middle-Angriffe durch nicht legitimierte verifizierende Organisationen sollten bei der Entwicklung jedoch etwaige Maßnahmen zur Risikobegrenzung berücksichtigt und umgesetzt werden (siehe Mythos 4). Letztlich verwalten die Nutzer*innen ihre Identitätsdokumente zusammen mit anderen Nachweisen in einer Hand – digital und dezentral auf dem Smartphone. Darüber hinaus können ausgestellte Credentials europaweit eingesetzt werden und ersparen wiederkehrende Behördengänge, wie beispielsweise beim Umzug im In- oder ins Ausland, oder Identifizierungsverfahren, wie z. B. bei der Eröffnung von (Bank-)Konten (Schlatt et al., 2021). Insofern stellt eine SSI-Lösung kein komplexes System für Endanwender*innen dar und kann im alltäglichen Gebrauch sehr praktikabel eingesetzt werden (siehe Mythos 2).

Für Softwareentwickler*innen können die verwendeten kryptographischen Primitive, das Zusammenspiel von innovativen, teilweise unausgereiften, von Communities zur Verfügung gestellten Open-Source Software-Komponenten sowie die Einhaltung der damit verbundenen technischen Standards hingegen zu Schwierigkeiten führen. In diesem Kontext sind beispielsweise ZKPs im Vergleich zur einfachen Überprüfung digitaler Signaturen wesentlich innovativer und komplexer und können aus diesem Grund größere Sicherheitsrisiken bergen (Kahlo, 2021). Allerdings sind die aktuell eingesetzten ZKPs seit 20 Jahren mathematisch bekannt und werden insbesondere bei Blockchain-Anwendungen in der Praxis verwendet, wodurch eine hohe Robustheit angenommen werden kann.

Die derzeit in den gängigen Implementierungen genutzten ZKP-Verfahren benötigen zusätzlich spezielle Signaturverfahren, wodurch sich nicht nur eine beschränkte Flexibilität bei zukünftigen Anpassungen, sondern auch eine mangelnde Kompatibilität mit sicheren Schlüsselspeichern ergibt. Auf der anderen Seite gibt es aktuell große Fortschritte bei deutlich allgemeineren ZKPs, die diese beiden Herausforderungen adressieren können. Für eine abschließende Bewertung bedarf es dabei noch weiterer Untersuchungen. Neben ZKPs kann zudem die Hinzunahme einer Blockchain als dezentrale Schlüsselzuordnungs- und Prüfstelle den Grad der Komplexität erhöhen (siehe Mythos 5). Hierbei entstehen weitere Fragestellungen, die die Governance sowie rechtliche und sicherheitstechnische Aspekte betreffen. Allerdings macht sich eine Blockchain bei Nutzer*innen nicht unmittelbar bemerkbar, da diese als Infrastruktur im Hintergrund fungiert.

Betrachtet man den Energiebedarf für die Herstellung von (Spezial-)Papier und Mobilität, so ist davon auszugehen, dass der Energieaufwand für das Ausstellen oder Verifizieren von Credentials gerin-

ger ausfallen wird als das bisherige, papierbasierte und oft Anwesenheit erfordernde Identitätsmanagement. Darüber hinaus ist durch die Portabilität der Credentials ein mehrfaches (und teilweise papierbasiertes) Ausstellen nicht erforderlich und spart zudem Energie ein. Die Abwicklung des Identitätsmanagements mittels einer SSI-Lösung über verschiedene Systeme hinweg könnte Kosten durch redundante Verwaltung, Datenspeicherung und (papierbasierte) Prozesse bei staatlichen und privatwirtschaftlichen Organisationen einsparen. Darüber hinaus wird durch die erhöhte Datenqualität und -verfügbarkeit die Effizienz in unterschiedlichen Anwendungsbereichen und -prozessen massiv gesteigert (Strüker et al., 2021).

Sollte eine Blockchain-basierte SSI-Lösung verwendet werden, so ist diese im Falle einer zugangsbeschränkten Blockchain hinsichtlich ihres Energieaufwands nicht mit offenen, Proof-of-Work-basierten Blockchain-Systemen wie Bitcoin oder Ethereum zu vergleichen. Grundsätzlich gilt es bei Blockchains zwischen den Designparametern und verwendeten Konsensmechanismen zu unterscheiden (siehe Mythos 4). Insbesondere zugangsbeschränkte Blockchain-basierte Ökosysteme, bei denen Knoten durch vertrauenswürdige Entitäten betrieben werden, weisen einen signifikant geringeren Energieaufwand als Blockchains, wie beispielsweise Bitcoin oder Ethereum, auf (Sedlmeir, Buhl et al., 2020).

Die zahlreichen öffentlich geförderten SSI-Projekte der Bundesregierung und privaten Wirtschaft in Deutschland nutzen Blockchains als hochverfügbaren und performanten Datenspeicher für die Bereitstellung vertrauensstiftender Daten, die einen hochgradig effizienten Synchronisationsmechanismus bereitstellen, z. B. Hyperledger Indy. Bei der Verwendung von 30 Knoten kann man den Energiebedarf auf das ca. 30-fache eines zentralen Servers schätzen, wobei in der Regel auch zentrale Systeme gewisse Ineffizienzen durch Backups aufweisen. Dadurch verbraucht eine solche Blockchain nicht wesentlich mehr Energie als herkömmliche, zentrale IT-Systeme (Sedlmeir, Buhl et al., 2020).

3 Fazit und Ausblick

3 Fazit und Ausblick

Dieses Diskussionspapier hat Meinungen aus dem kritisch geführten, öffentlichen Diskurs zum Thema SSI untersucht und vorgebrachte Argumente aufgegriffen, hinterfragt und diskutiert. Dabei haben wir den Mehrwert der eingesetzten Konzepte und Technologien aus einer wissenschaftlichen Perspektive beleuchtet und bestehende Herausforderungen aufgezeigt. Die in diesem Kontext untersuchten Mythen sollen in erster Linie Entscheidungsträger*innen in Wirtschaft und Politik sowie IT-Expert*innen und Bürger*innen dabei helfen, ein besseres Verständnis für SSI aufzubauen, um die daraus resultierenden Chancen und Risiken besser einordnen zu können. Dabei wird die Thematik aus einer multi-dimensionalen Perspektive hinsichtlich der komplexen Zusammenhänge zwischen datenschutzrechtlichen, sicherheitstechnischen, technologischen, Governance-bezogenen, forschungsnahen sowie allgemeinen Aspekten betrachtet.

Deutschland nimmt in der EU bei der Entwicklung eines SSI-basierenden Ökosystems digitaler Identitäten eine Vorreiterrolle ein, die sich durch die zahlreichen Projekte im öffentlichen und privaten Sektor auszeichnet. Insbesondere vor dem Hintergrund einer möglichen Einführung der eIDAS 2.0-Verordnung stellt Deutschland bereits frühzeitig die Weichen für eine interoperable SSI-Lösung, die europaweit umgesetzt werden könnte. Um diesen Prozess zu unterstützen und zu beschleunigen, tritt die Bundesregierung als Taktgeber für ein Ökosystem digitaler Identitäten auf, die durch vorgegebene Rahmenbedingungen, insbesondere der EU-Kommission, festgelegt werden. Dabei möchte die Bundesregierung fairen Wettbewerb im digitalen Raum ermöglichen. Die Anwendungsmöglichkeiten sind jedoch aktuell noch limitiert und befinden sich größtenteils im Test- und Pilot-Status. Darüber hinaus gilt es, in vielen Domänen die regulatorischen Vorgaben auf den neuen Standard anzupassen, um eine rechtswirksame und großflächige Verwendung digitaler Wallets zu ermöglichen. Spätestens mit Inkrafttreten der eIDAS 2.0-Verordnung könnte dieser Schritt auf nationaler wie europäischer Ebene zeitnah gelingen.

Insgesamt verspricht SSI großes ökonomisches Potenzial sowohl durch ein erhöhtes Maß an Sicherheit als auch an Effizienz und Flexibilität. Zudem können SSI-basierte digitale Identitäten für Unternehmen und Maschinen Potenziale beim Austausch von Stammdaten heben. Dies wird aktuell bereits in unterschiedlichen Pilotprojekten der Bundesregierung erprobt, die beispielsweise im Rahmen von Industrie 4.0 und CO_2-Nachweisen notwendig sind. Die Entwicklung und Adoption einer SSI-basierten Identitätslösung kann die Digitalisierung in Deutschland und Europa erheblich fördern und dazu beitragen, Ziele wie die des Online-Zuganggesetzes zu erreichen. Ein europäisches Ökosystem dezentraler digitaler Identitäten verringert außerdem die Risiken zentralisierter Systeme und stärkt die Unabhängigkeit. Damit kann SSI dazu beitragen, die digitale Souveränität Deutschlands und Europas zu stärken.

Um ein solches Ökosystem zu entwickeln und die Potenziale von SSI zu verwirklichen, müssen allerdings noch einige Herausforderungen und Abhängigkeiten gelöst werden. SSI ist sehr stark von einem florierendem Ökosystem mit vielen verschiedenen Anwendungsfällen abhängig, da der Mehrwert einer Identitätslösung erst mit der Anzahl der Anwendungsmöglichkeiten steigt. Insbesondere bei der Entwicklung weiterer Anwendungsfälle sollte die Basis-ID als grundlegendes digitales Ausweisdokument für Personenidentitäten betrachtet werden. Mithilfe einer eindeutigen, sicheren und digitalen Identität sind Nutzer*innen in der Lage, sich auf schnelle und effiziente Weise weitere Nachweise und Ausweisdokumente ausstellen zu lassen und diese im Alltag selbstbestimmend zu nutzen. Eine hohe Fragmentierung unterschiedlicher Lösungen für digitale Identitäten, wie bestehende konkurrierende PKI-Lösungen, können eine mögliche Adoption von SSI stark einschränken. Auf der anderen Seite ist auch das Zusammenspiel bestehender eID-Systeme für hoheitliche Dokumente mit SSI-basierten Nachweisen für alle anderen Fälle in einer

digitalen Wallet eine realistische Umsetzungsoption. Ein interoperables und skalierbares Ökosystem digitaler Identitäten bedarf dabei einer mindestens europaweiten Standardisierung technischer Komponenten, wie beispielsweise der technischen Gestaltung verifizierbare Nachweise und die entsprechenden grundlegenden Vertrauensstrukturen. Hier hat die Umsetzung von eIDAS in der Vergangenheit bereits eine sehr gute Basis geschaffen, die auch von SSI-basierten Ansätzen berücksichtigt werden sollte. Außerdem ist zu betonen, dass die beschriebenen Vorteile einer SSI-basierten Identitätslösung, insbesondere aus Perspektive der Nutzer*innen, nur mit einer Ende-zu-Ende Verschlüsselung ohne Backdoors vorstellbar ist. Die Politik in Deutschland und auf EU-Ebene soll auf diesem Wege ermutigt werden, die Rahmenbedingungen für eine solche Lösung vorzugeben.

Des Weiteren sollte eine SSI-basierte Lösung insbesondere aus regulatorischer, technischer und Governance-Perspektive den Anforderungen entsprechen. Viele Pilotierungsprojekte in Deutschland erproben die Machbarkeit von SSI in unterschiedlichen Anwendungsfällen und nutzen dabei agile Software-Engineering-Ansätze. Die schnelle und kontinuierliche Weiterentwicklung dieser SSI-Piloten darf jedoch nicht auf Kosten der Sicherheit erfolgen. Hierbei müssen zu jeder Zeit technische Standards und Anforderungen erfüllt bleiben. Dabei ist es wichtig, dass eine SSI-basierte Lösung und ihre Komponenten den Anforderungen einer Produktionsqualität standhalten. Zudem müssen bei der Systemeinführung Technikfolgenabschätzungen durchgeführt werden, um frühzeitig potenzielle Risiken zu identifizieren sowie die damit verbundenen Chancen von SSI gezielter nutzen zu können. In jedem Fall ist eine Open-Source Entwicklung der Komponenten sinnvoll, um einer breiten Gemeinschaft von Entwickler*innen und Expert*innen die Teilhabe, das Testen und das eingehende Prüfen zu ermöglichen.

Aus rechtlicher Sicht ist der regulatorische Rahmen mit dem Vorschlag zu eIDAS 2.0 bereits in die Wege geleitet worden. Ein SSI-basierter Ansatz kann die rechtlichen Anforderungen unter eIDAS 2.0 in unseren Augen sehr gut erfüllen oder eine sinnvolle Ergänzung zu bestehenden eID-Umsetzungen in weniger stark regulierten Bereichen sein. In diesem Kontext ist es auch der Auftrag der Bundesregierung, ihren Bürger*innen innerhalb eines Jahres eine digitale Wallet zur Verfügung zu stellen – ein weiterer positiver Indikator für eine SSI-basierte Lösung unter eIDAS 2.0.

Abschließend gilt es festzuhalten, dass SSI die Möglichkeit für ein offenes technisches System mit einfachem Onboarding bietet, um ein europäisches Ökosystem selbstbestimmter, digitaler Identitäten zu ermöglichen und zu fördern, bei dem auch kleine und mittelständische Organisationen partizipieren können. Dabei müssen Regulatorik und Technik ineinandergreifen und integrativ betrachten werden.

Literatur

Allen, C. (2016). ***The Path to Self-Sovereign Identity***. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html (besucht am 28. 01. 2022).

Aublin, P.-L., Mokhtar, S. B. und Quéma, V. (2013). "RBFT: Redundant Byzantine Fault Tolerance". In: ***33rd International Conference on Distributed Computing Systems***. IEEE, S. 297–306.

Boysen, A. (2021). "Decentralized, Self-Sovereign, Consortium: The Future of Digital Identity in Canada". In: ***Frontiers in Blockchain*** 4, S. 11.

Bundesamt für Sicherheit in der Informationstechnik (2021). ***Eckpunktepapier für Self-sovereign Identities (SSI) unter besonderer Berücksichtigung der Distributed-Ledger-Technologie (DLT)***. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.pdf;jsessionid=0EE03D850260A455ECF294A830E0FB3E.internet462?__blob=publicationFile&v=2 (besucht am 28. 01. 2022).

Bundeskanzleramt (AT) (2021). ***Schaffung einer digitalen Identität für alle Europäerinnen und Europäer***. URL: https://www.bundeskanzleramt.gv.at/themen/europa-aktuell/schaffung-einer-digitalen-identitaet-fuer-alle-europaeerinnen-und-europaeer.html (besucht am 28. 01. 2022).

Bundeskanzleramt (DE) (2021). ***Digitale Identität – Wie ein Ökosystem digitaler Identitäten zu einem selbstbestimmten und zugleich nutzerfreundlichen Umgang mit dem digitalen Ich beitragen kann***. Bundeskanzleramt – Referat Digitaler Staat. März 2021. URL: https://www.bundesregierung.de/resource/blob/992814/1898280/d9819a40553a9543b9e8f3acb620b0c2/digitale-identitaet-neu-download-bundeskanzleramt-data.pdf (besucht am 28. 01. 2022).

Bundesregierung (2021). ***Ökosystem Digitale Identitäten: Nachweise für die digitale Brieftasche***. URL: https://www.bundesregierung.de/breg-de/suche/e-id-1962112 (besucht am 28. 01. 2022).

Camenisch, J., Chaabouni, R. et al. (2008). "Efficient Protocols for Set Membership and Range Proofs". In: ***International Conference on the Theory and Application of Cryptology and Information Security***. Springer, S. 234–252.

Castro, M., Liskov, B. et al. (1999). "Practical Byzantine Fault Tolerance". In: ***3rd Symposium on Operating Systems Design and Implementation***. Bd. 99. 1999, S. 173–186.

Chaosradio (2021). ***ID Wallet CR272 Wie die Union ihren Internetführerschein verlor***. URL: https://chaosradio.de/cr272-id-wallet (besucht am 28. 01. 2022).

it-daily.net (2021). ***Digitales Wallet: Was tun, wenn das Smartphone verloren geht?*** URL: https://www.it-daily.net/it-sicherheit/mobile-security/31150-digitales-wallet-was-tun-wenn-das-smartphone-verloren-geht (besucht am 28. 01. 2022).

Delignat-Lavaud, A., Fournet, C., Kohlweiss, M. und Parno, B. (2016). "Cinderella: Turning Shabby X.509 Certificates into Elegant Anonymous Credentials with the Magic of Verifiable Computation". In: ***2016 IEEE Symposium on Security and Privacy (SP)***, S. 235–254. DOI: https://doi.org/10.1109/SP.2016.22.

Digital Identity and Data Sovereignty Association (DIDAS) (2021). ***Eine E-ID auf Basis SSI – welche regulatorischen Voraussetzungen müssen geschaffen werden?*** URL: https://www.didas.swiss/de/2021/12/17/eine-e-id-auf-basis-ssi-welche-regulatorischen-voraussetzungen-muessen-geschaffen-werden/ (besucht am 28. 01. 2022).

Dingle, P. (2020). ***Advancing Privacy with Zero-Knowledge Proof Credentials***. URL: https://techcommunity.microsoft.com/t5/identity-standards-blog/advancing-privacy-with-zero-knowledge-proof-credentials/ba-p/1441554 (besucht am 28. 01. 2022).

European Commission (2021). ***Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) n° 910/2014 as Regards Establishing a Framework for a European Digital Identity***. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021SC0124&from=EN (besucht am 28. 01. 2022).

Frank Jordan, B. (2021). ***Hunderte digitale Impfpässe gefälscht – Festnahme in München***. URL: https://www.br.de/nachrichten/bayern/hunderte-digitale-impfpaesse-gefaelscht-festnahme-in-muenchen (besucht am 28. 01. 2022).

Goldwasser, S., Micali, S. und Rackoff, C. (1989). "The Knowledge Complexity of Interactive Proof Systems". In: ***SIAM Journal on Computing*** 18, S. 186–208.

Guggenberger, T. et al. (2021). ***SSI@LfSt: Einsatz der Blockchain-Technologie in der Steuerverwaltung***. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT. URL: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Whitepaper_SSI@LfSt.pdf (besucht am 28. 01. 2022).

Heeger, V. (2021). ***ID-Wallet: Ist das Projekt noch zu retten?*** URL: https://background.tagesspiegel.de/digitalisierung/id-wallet-ist-das-projekt-noch-zu-retten (besucht am 28. 01. 2022).

Joinup (2021). ***About SSI eIDAS Bridge***. URL: https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about (besucht am 28. 01. 2022).

Kahlo, C. (2021). ***Blockchain + SSI = ID?*** URL: https://medium.com/@ckahlo/blockchain-ssi-id-d7e51d98d050 (besucht am 28. 01. 2022).

Lapienytė, J. (2021). ***Tech Giants Endlessly Exploit our Data. Who Will Put an End to It?*** URL: https://cybernews.com/editorial/tech-giants-endlessly-exploit-our-data-who-will-put-an-end-to-it/ (besucht am 28. 01. 2022).

Liang, F., Das, V., Kostyuk, N. und Hussain, M. M. (2018). "Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure". In: ***Policy & Internet*** 10.4, S. 415–453. DOI: https://doi.org/10.1002/poi3.183.

Lissi (2021). ***Diskussion über die Sicherheit von Wallets für digitale Identitäten***. URL: https://lissi-id.medium.com/diskussion-%5C%C3%5C%BCber-die-sicherheit-von-wallets-f%5C%C3%5C%BCr-digitalen-identit%5C%C3%5C%A4ten-d1c6218fef66 (besucht am 28. 01. 2022).

Lovejoy, B. (2021). ***Johns Hopkins Security Researchers 'Shocked' at Android and iOS Vulnerabilities***. URL: https://9to5mac.com/2021/01/14/johns-hopkins-ios-vulnerabilities/ (besucht am 28. 01. 2022).

Munzinger, H. (2021). ***Pegasus auf die Schliche kommen***. URL: https://www.tagesschau.de/investigativ/report-muenchen/impfzertifikate-101.html (besucht am 28. 01. 2022).

Muth, M. (2021). ***Nutzlos, unsicher und schon wieder kaputt***. URL: https://www.sueddeutsche.de/wirtschaft/fuehrerschein-digital-id-wallet-1.5425432 (besucht am 28. 01. 2022).

Naik, N. und Jenkins, P. (2021). "Sovrin Network for Decentralized Digital identity: Analysing a Self-sovereign Identity System Based on Distributed Ledger Technology". In: ***International Symposium on Systems Engineering***. IEEE.

PwC (2021). ***Der Online-Ausweis auf dem Smartphone und die digitale Brieftasche. PwC-Studie 2021: Bevölkerungsbefragung zum Online-Ausweis (Smart eID) und Self Sovereign Identities (SSI)***. URL: https://www.pwc.de/de/branchen-und-markte/oeffentlicher-sektor/pwc-studie-der-online-ausweis-auf-dem-smartphone-und-die-digitale-brieftasche.pdf (besucht am 28. 01. 2022).

Sabadello, M. (2017). ***A Universal Resolver for self-sovereign identifiers. On any blockchain or other decentralized system***. URL: https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c (besucht am 28. 01. 2022).

Schellinger, B., Völter, F., Urbach, N. und Sedlmeir, J. (2022). "Yes, I Do: Marrying Blockchain Applications with GDPR". In: ***Proceedings of the 55th Hawaii International Conference on System Sciences***, S. 4631–4640. DOI: https://doi.org/10.24251/HICSS.2022.563.

Schlatt, V., Sedlmeir, J., Feulner, S. und Urbach, N. (2021). "Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity". In: ***Information & Management***, S. 103553. DOI: https://doi.org/10.1016/j.im.2021.103553.

Sedlmeir, J., Buhl, H. U., Fridgen, G. und Keller, R. (2020). "The Energy Consumption of Blockchain Technology: Beyond Myth". In: ***Business & Information Systems Engineering*** 62.6, S. 599–608. DOI: https://doi.org/10.1007/s12599-020-00656-x.

Sedlmeir, J., Ross, P., Luckow, A., Lockl, J., Miehle, D. und Fridgen, G. (2021). "The DLPS: A New Framework for Benchmarking Blockchains". In: ***Proceedings of the 54th Hawaii International Conference on System Sciences***. 54th Hawaii International Conference on System Sciences, S. 6855–6864. DOI: https://doi.org/10.24251/HICSS.2021.822.

Sedlmeir, J., Smethurst, R., Rieger, A. und Fridgen, G. (2021). "Digital Identities and Verifiable Credentials". In: ***Business & Information Systems Engineering*** 63.5, S. 603–613. DOI: https://doi.org/10.1007/s12599-021-00722-y.

Slamanig, D., Stranacher, K. und Zwattendorfer, B. (2014). "User-centric Identity as a Service-Architecture for eIDs with Selective Attribute Disclosure". In: ***Proceedings of the 19th ACM Symposium on Access Control Models and Technologies***, S. 153–164.

Sporny, M., Longley, D. und Chadwick, D. (2019). ***Verifiable Credentials Data Model 1.0: Expressing Verifiable Information on the Web***. URL: https://www.w3.org/TR/vc-data-model (besucht am 28. 01. 2022).

Strüker, J. et al. (2021). ***Self-Sovereign Identity – Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten***. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Bayreuth. URL: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Fraunhofer%5C%20FIT_SSI_Whitepaper.pdf (besucht am 28. 01. 2022).

Tsakalakis, N., Stalla-Bourdillon, S. und O'Hara, K. (2016). "What's in a Name: The Conflicting Views of Pseudonymisation under eIDAS and the General Data Protection Regulation". In: ***Open Identity Summit***. Gesellschaft für Informatik eV.

Wittmann, L. (2021). ***Mit der ID-Wallet kannst Du alles und jeder sein, außer Du musst Dich ausweisen.*** URL: https://lilithwittmann.medium.com/mit-der-id-wallet-kannst-du-alles-und-jeder-sein-au%5C%C3%5C%9Fer-du-musst-dich-ausweisen-829293739fa0 (besucht am 28. 01. 2022).

Wölbert, C. (2021). ***E-Perso: Der Personalausweis kommt in drei Varianten aufs Smartphone***. URL: https://www.heise.de/news/E-Perso-Der-Personalausweis-kommt-in-drei-Varianten-aufs-Smartphone-6194859.html (besucht am 28. 01. 2022).

Wolf, S. und Nabben, B. (2021). ***Handel mit falschen Nachweisen nimmt zu***. URL: https://www.tagesschau.de/investigativ/report-muenchen/impfzertifikate-101.html (besucht am 28. 01. 2022).

Zinkus, M., Jois, T. M. und Green, M. (2021). ***Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions***. URL: https://arxiv.org/abs/2105.12613 (besucht am 28. 01. 2022).

Zivadinovic, D. (2021). ***Der Facebook-Ausfall und die ungeahnten Folgen***. URL: https://www.heise.de/news/Der-Facebook-Ausfall-und-die-ungeahnten-Folgen-6221349.html (besucht am 28. 01. 2022).

Projektgruppe Wirtschaftsinformatik

Die Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT vereint die Forschungsbereiche Digital Disruption, Digital Business und Digital Transformation in Augsburg und Bayreuth. Die interdisziplinäre Expertise in fachlichen und technischen Themen der Wirtschaftsinformatik und des Informationsmanagements sowie die Fähigkeit, methodisches Know-how auf höchstem wissenschaftlichem Niveau mit einer kunden-, ziel- und lösungsorientierten Arbeitsweise zu verbinden, sind ihre besonderen Merkmale. Aktuell besteht unser Team aus rund 90 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. Im Jahr 2021 haben wir ein Grundlagenpapier zum Paradigma von SSI veröffentlicht.