Privacy Management mit Self-Sovereign Identity: Potenziale zur Erhöhung der informationellen Selbstbestimmung

Gunnar Hempel und Jürgen Anke

Zusammenfassung

Dieser Beitrag zeigt einen Ausblick für ein Privacy Management auf Basis von Self-Sovereign Identity (SSI). Dafür genutzte digitale Brieftaschen (SSI-Wallets) bieten konzeptionelle Eigenschaften, die die Privatheit der Nutzer besser als bisherige Ansätze schützen können und die Selbstbestimmtheit der Nutzer über ihre Daten erhöhen. Diese Verbesserungen entstehen jedoch nicht automatisch. Vielmehr sind ein wertegeleiteter Umgang mit der Technologie und zusätzliche Werkzeuge erforderlich, um diese Potenziale zu nutzen. Die mit dem Ansatz mögliche Neugestaltung der Beziehungen zwischen Nutzer und Serviceanbieter hat einen disruptiven Charakter. Mit Verfahren und Werkzeugen für digitale Interaktionen wie Selective Disclosure, Verifiable Presentations, Zero-Knowledge Proofs, nicht-korrelierbaren Identifikatoren und Filterfunktionen eröffnen SSI-Wallets vollkommen neue Möglichkeiten für die Organisation des Datenmanagements.

1. Einführung

Die Kommerzialisierung von Internet-Diensten und die Verlagerung behördlicher Dienstleistungen schaffen zunehmend eine Verknüpfung von realer und virtueller Identität. Bei so gut wie jedem Online-Angebot wird eine digitale Identität erzeugt und mit Nutzerdaten verknüpft. Der Identitätsnachweis ist für natürliche Personen oft erforderlich, wenn es um Interaktionen mit Staat und Verwaltung geht oder wenn Finanz- und Zahlungsdienstleistungen involviert werden. Für zahlreiche weitere privatwirtschaftliche Dienste werden gleichfalls Identitätsnachweise verlangt. Auf den Identitätsnachweis folgt in den meisten Fällen eine Verarbeitung von Nutzerdaten und Nachweisen. Serviceanbieter haben oftmals ein berechtigtes Interesse daran zu wissen, wer ihre Nutzer sind, und Informationen über ihre Nutzer in möglichst guter Qualität zu verarbeiten, sei es für das Kun-

denbeziehungsmanagement und um Services zu verbessern, um Marketing zu betreiben oder um zusätzliche Wertschöpfung und Mehrwertdienste anzubieten. Nutzer digitaler Dienstleistungen hingegen haben das Recht, die wesentlichen Informationen über die beabsichtigte Verarbeitung zu erfahren, grundsätzlich selbstbestimmt über die Verarbeitung ihrer personenbezogenen Daten zu entscheiden, und müssen prinzipiell nur solche Daten preisgeben die für die Nutzung des Dienstes erforderlich sind.

In der Umsetzung entstehen für die Akteure oftmals rechtlich komplizierte und nicht sauber lösbare Situationen sowie ein unbefriedigendes Handling der technischen und organisatorischen Prozesse. Die Verwendung digitaler Ausweise gibt oft mehr Daten preis als erforderlich. Zudem schafft das Ausfüllen von Onlineformularen und das Erstellen von immer wieder neuen Passwörtern überflüssige Aufwände. Halbdigitale Verfahren, bei denen Dokumente eingescannt oder in Video-Anrufen vorgezeigt werden, sind lästige Zwischenschritte, welche die Customer Journey beeinträchtigen und die Sicherheit der Verarbeitung oftmals herabsetzen. Zahlreiche weitere Szenarien lassen sich hier aufreihen. Die Digitalisierung von Services stellt die beteiligten Akteure immer wieder vor interdisziplinäre Herausforderungen. Dedizierte Ansätze und neue Werkzeuge sind erforderlich, um interessengerechte Lösungen zu schaffen.

Zu beobachten ist indes auf verschiedenen Gebieten, dass sich sowohl die Art und Weise verändert, wie Identitäten verwaltet werden als auch wie der Zugang zu Daten vermittelt wird. Ansätze wie Self-Sovereign Identity ermöglichen eine Transformation von einem isolierten oder föderierten Identitätsmanagement hin zu einem selbstbestimmten Identitätsmanagement. Technische Entwicklungen wie digitale SSI-Wallets können die Speicherung von Nutzerdaten in „Datensilos“ zunehmend ersetzen und in ein „On Demand“-Modell überführen.

Damit öffnen sich neue Gestaltungsräume, wie Identitätsnachweise und Authentifizierung, aber auch der Austausch von Daten und die Legitimierung von Datenverarbeitung für Services zukünftig ausgestaltet werden können.

Rückenwind bekommt der SSI-Wallet-Ansatz indes durch die EU-Gesetzgebung und nationale Gesetzgebung, sowie durch gesellschaftliche Entwicklungen. Es ist davon auszugehen, dass Wallets für Nutzer und Dienstanbieter im öffentlichen und privaten Bereich eine zunehmende Rolle spielen werden.

Mit dem vorliegenden Beitrag soll skizziert werden, wie ein durch ein SSI-Wallet unterstütztes Privacy Management aussehen kann und welche

Potentiale dieser Ansatz im Sinne einer Data Governance bietet. Ziel dieser Arbeit ist es überdies aufzuzeigen, welche Themenfelder noch tiefgreifender zu untersuchen sind und an welchen Stellen konkreter Forschungs- und Entwicklungsbedarf besteht. Hierfür wird der Ansatz elaboriert und potentielle Herausforderungen identifiziert.

2. Ansatz und Thesen für ein SSI-Privacy Management

Für die Konzeption eines SSI-gestützten Privacy-Managements wurden drei initiale Fragen vorangestellt: Welche Bestandteile von SSI können zu einem fortschrittlichen Privacy-Management beitragen? Welche potentiellen Auswirkungen und Verbesserungen bietet ein SSI-Privacy-Management für die Selbstbestimmtheit und für eine interessengerechte Datenverarbeitung? Welche Werkzeuge und Maßnahmen sind für die Umsetzung erforderlich?

2.1 Self-Sovereign Identity

Self-Sovereign Identity, bzw. selbstbestimmte Identität, ist ein Ansatz, der es einer Person, einer Organisation oder einer Maschine erlaubt, eine digitale Identität zu erzeugen und selbst, also ohne einen Vermittler oder eine zentrale Partei, zu kontrollieren.[1] Die Identitätsverwaltung mittels SSI-Wallets funktioniert, wie der Name es schon sagt, ähnlich wie eine Brieftasche mit verschiedenen Ausweisen und Dokumenten darin. Je nach Anwendungsfall stellt der Nutzer Identitätsdaten oder auch nur Nachweise über bestimmte Eigenschaften seiner Person über einen verschlüsselten Kanal für einen anfragenden Akteur bzw. Dienstanbieter bereit (s. Abb. 1).[2]

1 *Allen*, The path to self-sovereign identity, 2016.
2 *Anke / Richter*, HMD 2023, S. 261ff.

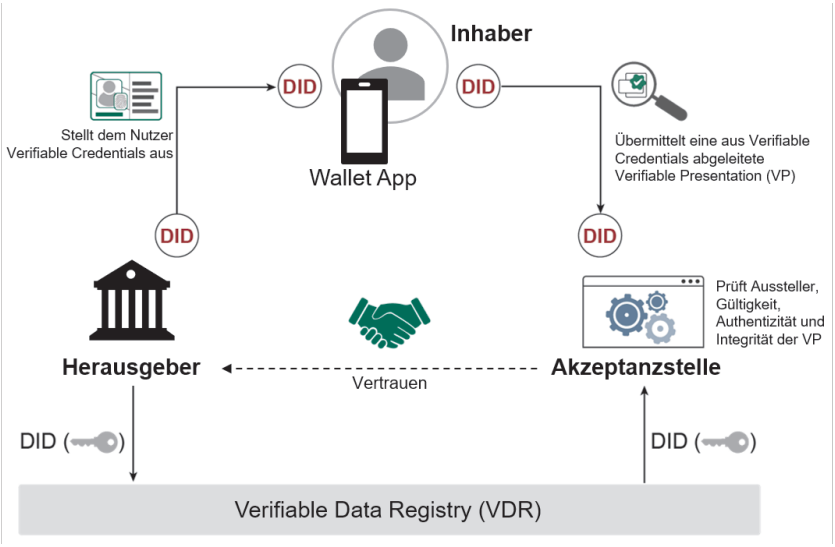

Abb. 1: Architektur von Self-Sovereign Identity Systemen (Quelle: Anke / Richter, HMD 2023, S. 269)

Während die Nutzer durch SSI von einer besseren Transparenz und Selbstbestimmtheit über ihre Daten profitieren, erhalten Dienstanbieter automatisch prüfbare Nachweise zum Nutzer und für die Verarbeitung nachweisbar autorisierte Daten.[3] In Zukunft können so, durch interoperable Nachweise, digitale Ökosysteme entstehen, in denen Kommunikation, Informationsaustausch und Datenverarbeitung einfacher und interessengerechter im Sinne eines Privacy-Managements umgesetzt werden können.

2.2 SSI als Basis für ein wirksames Privacy Management

Die folgende Darstellung zeigt einen Ausblick, wie ein SSI-Privacy-Management und eine Data Governance in einem digitalen Ökosystem neugestaltet werden könnte:

Ein Nutzer wird über eine Sammlung digitaler Nachweise in Form einer digitalen Identität repräsentiert. Die Nachweise werden von vertrauenswürdigen Stellen herausgegeben und vom Nutzer in der Wallet verwaltet. Die Wallet wird in eine technische und organisatorische Infrastruktur einge-

3 *Preukschat / Reed*, Self-sovereign identity, 2021, S. 248f.

bunden, der Nutzer kann darüber digitale Nachweise empfangen, speichern und präsentieren. Bereitgestellt wird die Wallet beispielsweise als Smartphone-App. Die Speicherung der Daten kann auf dem Gerät selbst oder über eine Cloud-Anbindung erfolgen.

Will der Nutzer einen digitalen Service verwenden, wird eine Peer-to-Peer-Verbindung zwischen der SSI-Wallet und dem Service aufgebaut. Dies erfolgt beispielsweise durch das Aufrufen eines Webservices oder Scannen eines QR-Codes. Über die Verbindung können Nutzer und Serviceanbieter Nachweise, Anforderungen und Datensätze empfangen und präsentieren. Beispielsweise können sich Dienstanbieter und Nutzer gegenseitig über Verifiable Credentials (VC) identifizieren, die Nutzungsbedingungen für die Inanspruchnahme des Services sowie für die Verarbeitung der Nutzerdaten (Terms of Use), als auch die Daten selbst durch Verifiable Presentations (VP) austauschen.

Anstatt seine Daten beim Aufrufen eines Services in Webformularen einzugeben oder Nachweise hochzuladen, gibt der Nutzer auf Anfrage die Daten aus seiner Wallet frei und legitimiert die Datenverarbeitung für den angefragten Anwendungsfall. Dabei kann über ein feingranulares Rechtemanagement bestimmt werden, welche Daten im Rahmen der Nutzungsbedingungen verarbeitet werden dürfen.

Diese Neugestaltung erfordert jedoch noch technische Weiterentwicklungen der Wallets und geeigneter Privacy-Werkzeuge, sowie organisatorische Anpassungen der Datenhaltung und Bereitstellung. Wenn solche Mechanismen praktisch einsetzbar sind, besitzen alle Nutzer eine Historie aller Empfänger ihrer Daten, sowie den damit verbundenen Nutzungsbedingungen. Dies ist die Grundlage, um Wallets mit einem mit PIMS (Personal-Information-Management-Service[4], an anderer Stelle auch „Personal Information Management-Systeme“[5]) vergleichbaren Ansatz für das Einwilligungs-Management zu erweitern. Konkret könnten Wallets auf diese Weise die Rechte auf Auskunft, Korrektur und Löschung von Daten nicht nur praktisch nutzbar machen, sondern teilweise automatisieren. Für Dienstanbieter, die Daten empfangen und verarbeiten, entsteht gleichzeitig der Effekt, dass die Herkunft und berechtigte Nutzung von Daten (durch die Signatur des Betroffenen) jederzeit nachgewiesen werden kann. Perspektivisch ist die technische Abbildung von Regelwerken als „Machine-Readable

4 *Stiftung Datenschutz*, Neue Wege bei der Einwilligung im Datenschutz, 2017.
5 *European Data Protection Supervisor*, Personal Information Management-System, 2021.

Governance“ ein Weg, um allen Beteiligten in einer Vertrauensdomäne den Umgang mit Nachweisen automatisiert zu gewährleisten.[6]

Der Leitgedanke ist, dass verlässliche Informationen über einen Nutzer mit dem Voranschreiten digitaler Geschäfts- und Servicemodelle für eine datenorientierte Wertschöpfung zunehmend an Bedeutung gewinnen. Die Bereitstellung, Legitimierung und Beweisbarkeit der Informationen muss rechtlichen Anforderungen entsprechen und sollte möglichst interessengerecht und schwer korrumpierbar sein.

Die Reorganisation der Datenhaltung und Bereitstellung hin zu einem „On-Demand“-Modell könnte gewichtige Vorteile für eine interessengerechte Verarbeitung personenbezogener Daten in digitalen Ökosystemen schaffen. In erster Linie betrifft dies datenschutzrechtliche Aspekte wie Transparenz und Selbstbestimmtheit der Verarbeitung, ökonomische Fragen bezüglich der Datenqualität, Kosten für die Datenhaltung und Pflege sowie Aspekte der Accountability und Compliance. Gleichfalls ist denkbar, dass sich durch den Ansatz zum SSI-Privacy-Management auch datenschutzfreundliche Angebote und ökonomische Marktprozesse besser unterstützten lassen.

2.3 Eigenschaften von Technik und Organisation

Die Wirkweise des SSI-Privacy-Managements ist in zwei Perspektiven zu betrachten. Zum einen die technisch-inhärenten Fähigkeiten von SSI für den Schutz der Privatsphäre und zum anderen die daraus abgeleitete Handhabung von personenbezogenen Daten durch Dienstanbieter.

Technische Fähigkeiten von SSI für den Schutz der Privatsphäre

SSI enthält konzeptionelle Merkmale, die Privatsphäre der Nutzer besser als bisherige Ansätze schützen können und die Selbstbestimmung über Daten erhöhen. Für den grundlegenden Umgang mit digitalen Nachweisen sind folgende Mechanismen für den Schutz der Privatsphäre relevant:

- *Vermeidung von Korrelation:* Voraussetzung für den Austausch von Nachweisen ist der Aufbau einer verschlüsselten Peer-to-Peer-Verbindung. Die dabei verwendeten Decentralized Identifiers (DIDs) können für jede Verbindung neu erzeugt werden. Somit ist eine Zusammenfüh-

6 *Hardmann*, Aries RFC 0430, 2020.

rung (Korrelation) von Datensätzen über eine Person aus verschiedenen Organisationen erschwert. Ausgeschlossen ist sie jedoch nicht, da bei Vorliegen ausreichend spezifischer anderer Attribute, eine Korrelation über diese stattfinden kann.

- *Selektive Freigabe*: Zentral für den Datenschutz ist das Konzept der VP. Diese stellen die Antwort der Wallet des Inhabers auf die Anfrage einer Akzeptanzstelle dar. Durch die selektive Freigabe von Attributen entsteht eine Datenminimierung, die ein Privacy Pattern ist.[7] Hierbei ist durch die Anfrage kenntlich zu machen, welche Attribute für den betreffenden Vorgang nach dem Grundsatz der Erforderlichkeit verpflichtend und welche optional sind, damit der Inhaber eine entsprechende Entscheidung treffen kann.
- *Kontrolle*: Der Inhaber der Wallet bekommt nicht nur den Anfragenden angezeigt, sondern auch die Liste der gewünschten Daten in Form einer Liste von Attributen. Nur wenn der Inhaber die Freigabe erteilt, werden die Daten übertragen.
- *Zurechenbarkeit*: Jede VP wird spezifisch auf die jeweilige Anfrage ausgestellt. Damit kann zum einen vermieden werden, dass eine VP an anderer Stelle erneut verwendet wird. Zum anderen kann die Akzeptanzstelle auch kryptografisch beweisen, dass der Inhaber ihr diese Daten bereitgestellt hat.
- *Transparenz*: Die mit verschiedenen Akteuren ausgetauschten Daten werden in einigen Wallets bereits heute in Form einer Historie gespeichert. Damit ist im Gegensatz zum heutigen Umgang mit digitalen Identitäten jederzeit nachvollziehbar, wer wann welche Daten erhalten hat, was die Ausübung von Rechten zur informationellen Selbstbestimmung erleichtert. Dies erfüllt gleichermaßen eine zentrale Forderung des Bundesverfassungsgerichts an die Gesellschafts- und Rechtsordnung, wonach der Bürger mit dem Recht auf informationelle Selbstbestimmung in der Lage sein soll zu beurteilen, wer was wann und bei welcher Gelegenheit über ihn weiß.[8]

Derzeit sind weitere Teilaspekte für SSI in Entwicklung, die für den Schutz der Privatsphäre genutzt werden können. Ein wichtiges Mittel zur weiteren Datenminimierung sind Zero-Knowledge Proofs (ZKP), die kryptografisch überprüfbare Aussagen ohne Offenlegung der zugrundeliegenden Daten möglich machen. Ein häufig bemühtes Beispiel ist die Altersprüfung, die

7 https://privacypatterns.org/patterns/Support-Selective-Disclosure.
8 BVerfGE 65, 1 (43).

gegen einen bestimmten Schwellwert (z. B. 18 oder 21 Jahre) durchführbar ist, ohne das Geburtsdatum der Person offenzulegen. Andere Anwendungsmöglichkeiten wären eine bestimmte Mindestnote in Zeugnissen, Mindestwohndauer in einer Kommune oder schlicht die Existenz eines gültigen Nachweises (z. B. Wohngeldbescheid, Sozialpass, Ticket). Bislang ist noch nicht festgelegt, welche konkreten kryptografischen Verfahren für ZKP in der Praxis Anwendung finden. Allerdings stellen sowohl die eID-Funktion des Personalausweises als auch die geplante EU Digital Identity Wallet entsprechende Funktionen bereit.

Handhabung von personenbezogenen Daten durch Dienstanbieter

Für Dienstanbieter bietet die Nutzung von digitalen Nachweisen mittels SSI folgende Vorteile:

- Die vom Nutzer eingesetzte Technik kann Daten automatisiert bereitstellen, statt sie in ein Formular einzugeben. Damit ist die Erfassung deutlich effizienter und kann anlassbezogen erfolgen, statt eigene Datenbestände zu führen.
- Die gelieferten Daten haben eine hohe Qualität, d. h. sie sind unverfälscht, aktuell und geprüft. Aufwändige Verfahren zur Verifizierung von Daten durch externe Dienste können damit entfallen.
- Die bereitgestellten Daten enthalten kryptografisch prüfbare Einwilligungen für die Verarbeitung der Daten, die für den anfragenden Dienstanbieter ausgestellt wurden. Damit ist es gegenüber Aufsichtsbehörden leichter möglich, die korrekte Handhabung von personenbezogenen Daten zu beweisen.

Offen ist jedoch, ob und in welchem Maße Dienstanbieter SSI verwenden, um die Privatsphäre von Betroffenen zu schützen. Die oben aufgeführten Möglichkeiten stellen lediglich Potenziale dar, die durch die Anwendung des Paradigmas der selbstbestimmten Identitäten entstehen können. Damit diese Potenziale im Sinne der Privatsphäre wirksam werden, müssen Dienstanbieter diese technischen Möglichkeiten auch ausschöpfen. Dies bedeutet konkret:

- Für alle Interaktionen dürfen nur die Daten erfragt werden, die für den jeweiligen Zweck unbedingt erforderlich sind.
- Alle nicht erforderlichen Daten sollten deutlich als optional gekennzeichnet werden, so dass Nutzende frei entscheiden können, ob sie diese teilen

möchten. Hier ergeben sich u. U. Ansätze für Anreize und Kompensationen in Form einer selbstbestimmten Datenökonomie.
- Sobald praktisch einsetzbar, sollten Daten in Form von Zero-Knowledge Proofs abgefragt werden, so dass lediglich ja/nein Aussagen zu bestimmten Sachverhalten anstatt der zugrundeliegenden Daten offengelegt werden müssen.
- Die in den Anfragen vermerkten Nutzungsbedingungen (Terms of Use) sollten einfach verständlich und im Sinne des Nutzenden ausgestaltet sein. Dies betrifft insbesondere die Speicherdauer sowie eventuelle Maßnahmen zur Anonymisierung und Pseudonymisierung für weiterführende Auswertungen wie Marktforschung.
- Schnelle Beantwortung von Anfragen für die Ausübung von Datenschutzrechten, idealerweise automatisiert.
- Die Löschung der Daten nach abgelaufener Aufbewahrungsfrist sollte den Wallets der Nutzer mitgeteilt werden, damit diese ihre Historie aktualisieren können und keine unnötigen Löschanfragen stellen.

Die sich hierbei ergebenden Möglichkeiten und Potentiale sind zwar deutlich erkennbar, stehen jedoch im Widerspruch zur bisherigen Praxis des Umgangs mit Daten. Es stellt sich die Frage, warum Dienstanbieter die von SSI bereitgestellten Fähigkeiten nutzen sollten, um damit die Privatsphäre der Nutzer zu schützen und ihre Machtposition stärken. Hier kommt die Gesetzgebung der EU ins Spiel. Mit der Novellierung der eIDAS-VO sind Regulierungen zur Attributbestätigung über eine European Digital Identity Wallet (EUid-Wallet) in der Planung, die die Souveränität des Nutzers in den Vordergrund stellen soll (vgl. Abschn. 3.2).

Gegenstand der weiteren Forschung muss es sein, die tatsächlichen Anforderungen der Akteure als auch die rechtlichen und technischen Herausforderungen zu untersuchen:

3. Hausforderungen

Für Tragfähigkeit des Privacy-Management-Ansatzes sind sowohl verhaltensökonomische, rechtliche, als auch technische und organisatorische Fragestellungen zu berücksichtigen. Im Folgenden werden wichtige Herausforderungen aus diesen Bereichen benannt und andiskutiert.

3.1 Verhaltensökonomie

Die SSI-Wallet befähigt den Nutzer zur selbstorganisierten und selbstbestimmten Verwaltung der Daten und damit auch zu Transparenz und Steuerung über die Verarbeitungen.

Das selbstbestimmte Verwalten der Daten und der Datenverarbeitungen, sowie die Ausübung der Datenhoheit erfordern ein grundlegendes Verständnis und Fähigkeiten im Hinblick auf Informations- und Telekommunikationstechnologie (IKT). Das Bearbeiten der Interaktionen und das damit verbundene Verwalten von Informationen, von Anfragen und das Erteilen von Einwilligungen schafft Aufwände und stellt erhöhte Anforderungen an den Nutzer. Aus der Verhaltensforschung ist hinreichend bekannt,[9] dass ein Zuwachs an Informationen nicht gleichzeitig einer leichteren Entscheidungsfähigkeit oder zu besseren Entscheidungen beiträgt. Es kann davon ausgegangen werden, dass der Nutzer nach seinen individuellen Fähigkeiten und Interessen bereit ist, eine gewisse Informationsmenge zu erfassen, darüber hinaus jedoch die Informationsaufnahme abbricht. Für Nutzer ist es darüber hinaus eine große Herausforderung, die Sicherheitsaspekte der Technologie einzuschätzen und damit verbundene Risiken, wie durch Datendiebstahl und oder durch Profilbildung, zu bewerten.

Ziel der Technik muss es daher sein, eine Konfigurationsmöglichkeit anzubieten, die den Nutzer dort abholt, wo er sich mit seinen Fähigkeiten und seiner Bereitschaft befindet und ihn von dort aus bestmöglich unterstützt. Die Forschung zu Usable Security und Privacy untersucht und entwickelt auf diesem Gebiet bereits einschlägige Lösungsansätze. So könnte die Interaktions- und Informationsmenge beispielsweise über ein gestuftes Komplexitätsniveau auf die Bedürfnisse des Nutzers angepasst werden. Zu untersuchen wäre, welche Schemata und Methoden für eine solche Stufung geeignet wären, um für den Nutzer einen Mehrwert bei der Interaktion über SSI-Wallets zu bieten.

Grundlegend für die Akzeptanz der Technologie beim Anwender wird es sein, dass dieser einen möglichst unmittelbaren Nutzen aus der Anwendung ziehen kann. Generell bestehen in der Breite bei Anwendern Barrieren für das Anwenden von Neuerungen und das Anpassen an neue Prozesse. Diese Hürde lässt sich möglicherweise überwinden, wenn nicht nur ein positiver Anreiz zu einer theoretischen Verbesserung der Gesamtsituation besteht, sondern wenn möglichst zusätzlich auch ein unmittelbarer Nutzen

9 Weiterführend hierzu: *Roetzel*, Business Research 2019, 479.

für den Anwender entsteht, der als Treiber für die Reorganisation eines Prozesses dient.

Inwieweit Dienstanbieter bereit sind, eine Neuorganisation der Datenhaltung und Bereitstellung zu akzeptieren, dürfte zu einem großen Teil von ökonomischen Aspekten abhängen. Hier wird es darauf ankommen, ob sich Aufwände für die Datenhaltung und Datenpflege sowie Schutz- und Compliance-Maßnahmen reduzieren lassen und inwieweit Verbesserungen für die Datenqualität und für das Kundenbeziehungsmanagement umgesetzt werden können.

Im Hinblick darauf, dass die aktuelle EU-Gesetzgebung mit der Novellierung der eIDAS-VO vorsieht die Mitgliedsstaaten zu verpflichten, eine einheitliche Online- und Offline Identifizierung von Bürgern innerhalb der EU per EUid-Wallet bereitzustellen, lohnt es sich besonders zu analysieren, wie und welche Methoden geeignet sind, den Nutzer dahingehend zu befähigen, Privacy-Risiken einzuschätzen, Rechte wahrzunehmen und durchzusetzen, aber auch einen interessengerechten und wertstiftenden Austausch von Daten und eine Interaktion mit Dienstanbietern zu unterhalten.

3.2 Recht

SSI-Wallets sind ein Instrument, um die Verwaltung digitaler Identitäten in bestimmten Anwendungsszenarien durch Nutzer selbst zu steuern.

Welcher Rechtsnatur eine digitale Identität ist und inwieweit ein Recht auf und an einer solchen besteht, wird an zahlreichen Stellen diskutiert, es soll jedoch im Rahmen der vorliegenden Arbeit nicht vertieft untersucht werden. Zu betrachten sind in erster Linie die datenschutzrechtlichen Perspektiven für den Ansatz des SSI-Privacy-Managements und mögliche Spannungsfelder mit anderen Rechtsgebieten, insbesondere den Vorschriften zur elektronischen Identifizierung und Vertrauensdiensten, sowie den allgemeinen Vorschriften.

Die digitale Identität ist zunächst eine Repräsentation einer Person in der digitalen Informationstechnologie um diese auszuweisen.[10] Sie wird in Prozesse eingebettet und im Geschäftsalltag verwendet, wodurch ihr eine rechtliche Funktion und Geltung zukommt, die mehr und mehr an Bedeu-

10 Weiterführend hierzu *Hornung*, Die digitale Identität, 2005, S. 29f.

tung gewinnt. Soll ein Rechtsgeschäft z. B. im digitalen Raum[11] abgeschlossen werden, ist es in einer Vielzahl der Fälle[12] im Interesse mindestens einer beteiligten Partei, den Geschäftspartner zu identifizieren. Die zivilrechtlichen Vorschriften lassen ein rechtswirksames Handeln auf diesem Wege bis auf Ausnahmen zu. Rechtswirksames Handeln im Behördenverkehr richtet sich nach den einschlägigen Verfahrensvorschriften und ist unter den dortigen Bedingungen möglich. Bedeutung erlangen digitale Identitäten derzeit für die öffentliche Verwaltung besonders im Rahmen des Onlinezugangsgesetzes (OZG), wonach Bund, Länder und Kommunen verpflichtet werden, ihre Verwaltungsleistungen über Verwaltungsportale digital anzubieten.

Die Basis für die Möglichkeit einer vertrauenswürdigen elektronischen Identifizierung und die Nutzung von Vertrauensdiensten wurde durch die Verordnung „(EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ (eIDAS-VO) geschaffen. Die eIDAS-VO legt Bedingungen fest, unter denen die EU-Mitgliedsstaaten elektronische Identifizierungsmittel und notifizierte elektronische Identifizierungssysteme gegenseitig anerkennen. Nach dem aktuellen Kommissionsvorschlag zur Novellierung der eIDAS-VO[13] wird auch die Umsetzung einer EUid-Wallet geplant.[14] Jeder Mitgliedsstaat der EU soll nach Art. 6a Abs. 1 der Novellierung verpflichtet werden eine EUid-Wallet für natürliche und juristische Personen anzubieten. Die EUid-Wallets sollen dem Nutzer das sichere, transparente und nachvollziehbare Anfordern und Erhalten, Speichern, Auswählen, Kombinieren und Weitergeben der erforderlichen gesetzlichen Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen ermöglichen, um sich online und offline zur Nutzung öffentlicher und privater Online-Dienste zu authentifizieren (Art. 6a Abs. 3a). Sie muss zudem das Unterschreiben mit einer qualifizierten Signatur ermöglichen (Art. 6a Abs. 3b) und insbesondere Schnittstellen für Vertrau-

11 Digitaler Raum ist ein unscharfer Begriff, der sinngemäß für digitale Dienstleistungen und Internetanwendungen steht, vgl.: https://www.bmwk.de/Redaktion/DE/Schlaglichter-der-Wirtschaftspolitik/2021/11/05-im-fokus-digitale-identit%C3%A4ten.html.

12 Nicht betroffen sind z.B. Bargeschäfte des täglichen Lebens.

13 Europäische Kommission, COM (2021) 281 final.

14 Am 10.02.2023 hat die EU Kommission die erste EUID-Toolbox als Grundlage für die eID-Wallet veröffentlicht. URL: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework?utm_source=piano&utm_medium=email&utm_campaign=22038.

ensdiensteanbieter aufweisen, die Attributsbescheinigungen herausgeben (Art. 6a Abs. 4a). Die Attributsbescheinigungen können in verschiedenen technischen Formen, beispielsweise in Form von VC, ausgegeben werden. Neben der hoheitlichen, nationalen Identität sollen auch weitere Nachweise, wie der Führerschein, Hochschulzeugnisse und Bescheinigungen in die EUid-Wallet abgelegt werden können. Durch Art. 12b Abs. 2 werden Unternehmen und Behörden verpflichtet die Verwendung der EUid-Wallet zu akzeptieren, sofern diese auch Dienste erbringen, die eine Online-Identifizierung mit starker Nutzerauthentifizierung erfordern. Ausdrücklich betrifft dies die Anwendungsfelder Verkehr, Energie, Bank- und Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Trinkwasser, Postdienste, digitale Infrastrukturen, Bildung oder Telekommunikation. Darüber hinaus werden neue Anwendungsfelder auch dadurch erschlossen, dass die großen Online-Plattformanbieter dazu verpflichtet werden, für den Zugang zu ihren Online-Diensten die EUid-Wallet für die Nutzer-Authentifizierung zu akzeptieren, (Art. 12b Abs. 3).[15] Es ist daher davon auszugehen, dass Wallets mit digitalen Nachweisen für Bürger und Verwaltung bei der elektronischen Identifizierung in der digitalen Kommunikation eine zunehmende Rolle spielen.

Der elektronische Identitätsnachweis erfolgt durch die Verarbeitung personenbezogener Daten über eine (natürliche) Person, weshalb datenschutzrechtliche Vorschriften zu beachten sind. Die DSGVO schreibt in Art 5 Abs. 1 die Grundsätze der Verarbeitung personenbezogener Daten vor. Die Verarbeitung hat u. a. auf rechtmäßige Art und Weise, nach Treu und Glauben und für die betroffene Person in einer nachvollziehbaren Weise zu erfolgen und erfordert immer eine Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 DSGVO. Die Verarbeitung ist an festgelegte, eindeutige und legitime Zwecke gebunden, sie ist auf das notwendige Maß und die notwendige Dauer zu beschränken und bedarf angemessener Sicherheitsvorkehrungen, um die Integrität und Vertraulichkeit zu gewähren.

Dem SSI-Ansatz selbst ist immanent, dass er die Grundsätze der Transparenz und Selbstbestimmtheit unterstützt, was aus datenschutzrechtlicher Sicht positiv zu werten ist. ZKP adressieren zum einen den Grundsatz der Datenminimierung sowie durch die Pseudonymisierung auch die Grundsätze des „Data Protection by Design" und „Data Protection by Default".

15 Vgl. *Fiedler / Granc*, DuD 2022, S. 27f.

Die Möglichkeiten mittels SSI-Wallets über einen direkten Kanal Informationen auszutauschen, eröffnet zusätzliche Potentiale für Transparenz und Selbstbestimmtheit.

Rechtliche Fragestellungen ergeben hierbei insbesondere bezüglich der Legitimierung der Datenverarbeitung. Grundsätzlich legitimiert Art. 6 Abs. 1 UAbs. 1 lit b DSGVO die Verarbeitung der Daten, die für die Erfüllung des Vertrags oder die Vermittlung von Diensten erforderlich sind. Für eine weitergehende Verarbeitung von Daten, über das vertraglich vereinbarte, oder das für die Vertragserfüllung erforderliche Maß hinaus, kommt eine Einwilligung als Rechtsgrundlage in Betracht.

Nach Art. 6 Abs. 1 UAbs.1 lit. a DSGVO kann die betroffene Person in die Datenverarbeitung für einen bestimmten Zweck einwilligen. Die Erklärung der Einwilligung muss freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich erklärt werden (Art 4 Nr. 11 DSGVO). Freiwilligkeit liegt nur dann vor, wenn die betroffene Person eine echte und freie Wahl hat (Erwägungsgrund 42, Art. 7 Abs. 4) und nicht etwa an einen bestimmten Vorgang gekoppelt ist. Informiertheit liegt vor, wenn die betroffene Person vor der Abgabe der Einwilligungserklärung über den beabsichtigten Zweck der Verarbeitung ihrer personenbezogenen Daten im Einzelnen informiert werden (vgl. Art. 13, 14 DSGVO).

Weiter ist die betroffene Person vor Abgabe der Einwilligungserklärung über ihr Widerrufsrecht aufzuklären (Art. 7 Abs. 3; Art. 13 Abs. 2 lit. b, c; Art. 14 Abs. 2 lit. c, d DSGVO).

Für das SSI-Privacy-Management bedeutet dies, dass für jeden Verarbeitungszweck für den eine Einwilligung als Rechtsgrundlage erforderlich ist, eine Anfrage an den Nutzer zu senden ist, er sich über die Verarbeitungsbedingungen zu informieren hat und in diese freiwillig einwilligen muss.

Zu untersuchen ist, wie sich die Informiertheit in der Praxis umsetzen lässt. Vorauszuschicken ist, dass eine Generaleinwilligung in dem Sinne „Ich willige in alle Verarbeitungen ein, die der Serviceanbieter anfragt", nicht wirksam ist. Rechtsfolge einer fehlenden Informiertheit ist im Zweifel eine unwirksame Einwilligung und damit eine Datenverarbeitung ohne Rechtsgrund.

Die Herausforderung besteht darin, dass der Nutzer im Grunde für jeden „neuen" Verarbeitungszweck bezüglich einer Einwilligung angefragt wird und in diesen auch einwilligen muss. Je nach Anzahl der Touchpoints einer Customer Journey oder Anzahl der Interaktionspartner, die über die Wallet verwaltet werden, ist hier mit einer großen Zahl von Anfragen zu rechnen. Dieser Umstand würde die Usability des Ansatzes erheblich stören.

Die Problematik ist jedoch nicht neu. Bereits seit einigen Jahren stellt sich im Zusammenhang mit PIMS und Datentreuhändern die Frage, ob und wie eine Einwilligungsverwaltung rechtlich zulässig sein kann. Denkbar sind hier prinzipiell ein antizipiertes oder delegiertes Modell zur Einwilligungsverwaltung. Beim delegierten Modell ist die Frage, ob die Einwilligung z. B. an einen vertrauenswürdigen Dritten delegiert werden kann. Der Betroffene könnte dabei seine eigenen Datenschutzvorlieben benennen, damit Verarbeitungszwecke und Verarbeiter eingegrenzt und gefiltert werden können. Datenschutzrechtlich stellt dieser Teil im Grunde keine Hürde dar.

Weiter ist allerdings fraglich, inwieweit beispielsweise ein Datentreuhänder Empfehlungen für Einwilligungen aussprechen darf oder ob es sogar möglich ist, die Abgabe der Einwilligungserklärung nach definierten Parametern an eine solche Stelle zu delegieren.

Nach den gegenwärtigen Vorschriften ist eine solche Lösung für Einwilligungen allgemeingültig nicht wirksam umsetzbar. Es fehlt an der persönlichen und informierten Willensbildung, die immer an den bestimmten Zweck gekoppelt ist. Jenseits der DSGVO sind jedoch Entwicklungen zu beobachten, die in ausgewählten Bereichen und unter bestimmten Voraussetzungen eine Einwilligungsverwaltung oder Delegation zulassen können.

Mit dem TTDSG wurden in 2021 beispielsweise, in einem gewissen Rahmen, Verfahren zur Einwilligungsverwaltung in Verbindung mit unabhängigen Diensten zur Einwilligungsverwaltung anerkannt, §§ 26 Abs. 2, 25 TTDSG. Die Festlegung der technischen, organisatorischen und rechtlichen Anforderungen für diese unabhängigen Dienste ist gegenwärtig noch nicht erfolgt. Mit der Einwilligungsverwaltungsverordnung sollen diese Anforderungen für den Anwendungsbereich des TTDSG umrissen werden.[16] Der Ansatz zur Einwilligungsverwaltung ist jedoch nicht auf Konstellationen außerhalb des TTDSG anwendbar und somit nicht allgemeingültig auf die Einwilligungen in Datenverarbeitungen nach der DSGVO übertragbar. Ob und inwieweit zukünftig die EU-Privacy-Verordnung Neuerungen, z. B. im Hinblick auf privatsphärenfreundliche Modelle und Einstellungen in Browsern und Apps zulässt, ist bislang nicht klar ersichtlich und kann an dieser Stelle nicht eingeschätzt werden.

16 Letzter Stand Referentenentwurf des Bundesministeriums für Digitales und Verkehr vom 08.07.2022. URL https://www.itm.nrw/wp-content/uploads/220708_BMDV_RefE_EinwVO.pdf.

Fraglich wird sein, ob solche Entwicklungen zukünftig ein Türöffner in das allgemeine Datenschutzrecht sein können. Aktuell ist eine Einwilligungsverwaltung durch technische Agentensysteme oder die Delegation an Dritte aber nicht möglich.

Zu untersuchen ist jedoch, ob eine mögliche Lösung ein gestufter Prozess sein kann, bei dem Anfragen an den Nutzer in einem ersten Schritt entsprechend seiner Vorlieben und Voreinstellungen in der Wallet gefiltert werden. In einem zweiten Schritt könnte der Nutzer Bedingungen definieren, unter denen eine Einwilligungserklärung erklärt und über die Wallet automatisch umgesetzt werden kann.

Ein Ansatz wäre es beispielsweise ein Modell mit geeigneten Kategorien zu entwickeln, in welchen die „Art personenbezogener Daten", die „Art und Weise der Verarbeitung" und der „Zweck der Verarbeitung" geclustert und standardisiert werden. Standardisierte Kategorien würden zum einen den Nutzer unterstützen die beabsichtige Datenverarbeitung leichter zu erfassen. Zudem könnte das Modell maschinenlesbare Automatisierungen unterstützen.

Zum Beispiel könnten personenbezogenen Daten unterteilt werden in Kategorien K1 bis Kx, wobei K1 - wenig sensible Daten (nutzerdefiniert), Kx - hochsensible Daten enthält. Die Arten von beabsichtigten Datenverarbeitungen wären gleichfalls in Kategorien mit mehr oder weniger kritischen (nutzerdefiniert) Verarbeitungstätigkeiten zu clustern. Die besonderen Anforderungen nach Art. 9 DSGVO für besondere Kategorien personenbezogener Daten müssten zusätzlich noch gesondert berücksichtigt werden.

Eine Hürde dieses Ansatzes besteht darin, dass eine Kategorie nicht die Wirklichkeit abbildet. Generell gibt es z. B. keine klare Festlegung für eine Kategorie zu „Verarbeitungen". Vielmehr sind die Bezeichnungen eine eigenmächtige Festlegung des Serviceanbieters. Welche konkreten Anforderungen in diesem Fall an die Informiertheit der Betroffenen zu stellen sind, muss umfassend untersucht werden. Ob und inwieweit ein solcher Ansatz funktionieren kann, bedarf daher weiterer Forschung.

3.3 Technik

Wenngleich die technische Entwicklung von SSI-Wallets und -Infrastrukturen mit großer Geschwindigkeit voranschreitet, befinden sich die notwendigen Komponenten derzeit in sehr unterschiedlichen Reifegraden. Diese lassen sich in die Kategorien (1) Wallet-Funktionalität, (2) Governance Frameworks und (3) Usability unterteilen.

Der *Funktionsumfang von Wallets* erlaubt heute vor allem das Entgegennehmen, Speichern und Präsentieren von Verifiable Credentials. Zudem werden oft Historien angeboten, die Austauschzeitpunkte von Daten mit unterschiedlichen Partnern nachvollziehbar machen. Allerdings werden empfangene Nachweise auch wieder präsentiert, so dass zwar eine Kontrolle und Freigabe für den Benutzer gegeben ist, eine Datenminimierung jedoch nicht. Die Verwendung von Verifiable Presentations für die selektive Freigabe und Unterstützung von ZKP ist nur in Prototypen vorhanden. Zudem existiert bislang noch kein Standard für die Datenportabilität, um Nutzern zu ermöglichen, ihre bestehenden Nachweise gesammelt in eine neue Wallet eines anderen Anbieters übertragen zu können. Schließlich ist auch der Umgang mit Nachweisen für Dritte, z. B. im Kontext von Sorgeberechtigungen, Vertretungsberechtigungen und Vollmachten in bestehenden Systemen kaum adressiert. Dies betrifft nicht nur Dienstanbieter wie Unternehmen, Vereine und Kommunen, sondern auf der Nutzerseite auch Familien.

Beim konkreten Einsatz digitaler Nachweise offenbart sich eine der größten Herausforderungen für die Nutzung von SSI: Einerseits soll damit eine technisch interoperable Lösung für die flexible Nutzung von digitalen Nachweisen in verschiedenen Szenarien erlaubt werden, andererseits ist der Umgang mit ihnen sehr stark von den Regeln des Nachweises und des Einsatzkontexts abhängig. Zur Verbindung der technischen Perspektive von SSI mit den Sphären von Wirtschaft, Recht und Gesellschaft werden Regelwerke genutzt, die auch als *Governance Frameworks* bezeichnet werden.[17] Diese Regelwerke sind zum einen erforderlich, um bestehende Gesetze abzubilden. Zum anderen können sie dem Benutzer eine Unterstützung in seinen Entscheidungen bei seinen Interaktionen in der SSI-Wallet zu geben. Damit soll vermieden werden, dass Credentials von unberechtigten Herausgebern in den Verkehr gebracht werden (Fälschungssicherheit) oder Nutzer ihre Daten arglos unberechtigten Akzeptanzstellen übermitteln (Schutz vor Identitätsdiebstahl). Konkret sind damit u. a. folgende Herausforderungen verbunden:

- *Vertrauenswürdige Akzeptanzstellen*: Die einfache Verfügbarkeit und Bereitstellung qualitativ hochwertiger Daten bergen das Risiko, dass Kriminelle über gefälschte Websites mittels Phishing-Daten von Nutzenden erbeuten. Daher sind Mechanismen erforderlich, die das Recht eines Ak-

17 *Preukschat / Reed*, Self-sovereign identity, 2021, S. 248f.

teurs zur Abfrage bestimmter Daten überprüfbar machen. Erste Ansätze dafür arbeiten mit SSL-Zertifikaten.[18] In Zukunft könnten dafür Trust Lists oder VCs genutzt werden.

- *Vertrauenswürdige Herausgeber:* Damit Vertrauen in Daten entsteht, muss nicht nur die Akzeptanzstelle, sondern auch der Inhaber sicher sein, dass nur autorisierte Herausgeber Nachweise erstellen.

Da Wallets ein zentrales Werkzeug für Interaktionen im digitalen Raum werden sollen, müssen sie ähnlich wie Web-Browser oder E-Mail-Programme für die breite Bevölkerung einfach nutzbar sein. Die Erweiterung von Wallets um Funktionen für die Wahrnehmung von datenschutzbezogenen Rechten sowie die differenzierte Nutzung von Nachweisen erfordert von Nutzern ein hohes Maß an Verständnis für die Interaktionen und ihrer Auswirkungen. Dafür ist eine hohe *Usability* erforderlich, die sich nicht nur auf die Wallet selbst, sondern auf die gesamte Interaktion z. B. mit einer Website, einer anderen Person oder einem öffentlichen Terminal erstreckt. Um einen Wechsel zwischen verschiedenen Wallets zu erleichtern, forderte Kim Cameron in seinen „Seven Laws of Identity" eine konsistente Nutzererfahrung in verschiedenen Einsatzkontexten.[19] Bislang hat die schnelle Entwicklung einer Vielfalt von Wallets nur sehr begrenzt zu übergreifenden Bedienkonzepten geführt.[20]

4. Forschungsbedarf und Realisierbarkeit

Zur Erschließung der Potenziale des SSI-Privacy-Managements ergeben sich Forschungs- und Entwicklungsbedarfe auf den Gebieten der Technologie, der Verhaltensökonomie und des Rechts. Die Technologie gibt dabei das Grundgerüst für den Ansatz vor, verhaltensökonomische und rechtlich Implikationen sind bei der Ausgestaltung des Ansatzes zu berücksichtigen. Nachfolgend werden die Forschungs- und Entwicklungsbedarfe kurz umrissen.

18 https://docs.lissi.id/lissi-wallet/verification-of-contacts-within-the-lissi-wallet.
19 *Cameron*, The Laws of Identity 2005.
20 *Krauß* u.a., HMD 2023, S. 344f.

4.1 Technisch-organisatorisch

Für die Realisierung der in Abschn. 2.2 beschriebenen Vision eines SSI-Privacy-Managements ist Forschungs- und Entwicklungsarbeit im Hinblick auf die technisch-organisatorischen Aspekte, die Datenminimierung, die Governance und Usable Security zu leisten.

Für die *Datenminimierung* sind die Mechanismen für selektive Freigabe im Rahmen von Verifiable Presentations sowie Zero-Knowledge Proofs von großer Bedeutung. Beide sind konzeptionell beschrieben und prototypisch implementiert. Für eine praktische Nutzbarkeit bedarf es jedoch noch Abstimmungen hinsichtlich der verwendeten Datenformate und kryptografischen Verfahren. Die Anforderungen an kryptografische Verfahren betreffen dabei insbesondere die möglichst weite Verbreitung effizienter Implementierungen sowie Ausführbarkeit auch in ressourcen-beschränkten Umgebungen wie Hardware-Sicherheitsmodulen. Für die Repräsentation der zugrundeliegenden Datenstrukturen sind ebenfalls geeignete Festlegungen zu treffen, die auf offenen Standards beruhen und plattformunabhängig sind. Schließlich sind ebenfalls Protokolle zu vereinbaren, die eine selektive Abfrage von Daten überhaupt möglich machen.

Der Aufbau dezentraler Systeme für den Nachweisaustausch erfordert *übergreifende Verzeichnisse*, in denen gemeinsam genutzte Informationen öffentlich abgelegt werden. Dazu gehören z. B. öffentliche DIDs von Dienstanbietern, Schemata für Credentials sowie der Gültigkeitsstatus ausgegebener Nachweise. Die dafür notwendigen Mechanismen sind derzeit im Entstehen. Im Umfeld regulierter Vertrauensdienste nach der eIDAS-VO werden dafür Trust Lists[21] verwendet. Ähnliche Konzepte werden von der „Decentralized Identity Foundation" sogenannte Trust Registries[22] vorgeschlagen, um vertrauenswürdige Herausgeber, Akzeptanzstellen, verwendete Schemata und akzeptierte Wallets zu hinterlegen. Bislang bestehen hierfür nur erste Schnittstellen-Spezifikationen. Konkrete technische Implementierungen, deren Nutzung in SSI-Ökosystemen sowie die Bewertung ihrer rechtlichen Implikationen müssen Gegenstand künftiger Forschung sein.

Damit SSI einen transparenten und datenschutzkonformen Datenaustausch sowie eine Ermächtigung der Nutzer erlaubt, ist eine Automatisierung von Regeln für ein Governance Framework erforderlich. Es bestehen

21 https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home.
22 https://wiki.trustoverip.org/display/HOME/Trust+Registry+Task+Force.

zwar erste Ansätze zur Systematisierung von Governance für SSI,[23] jedoch ist deren technische Umsetzung und praktische Nutzung weitgehend unerforscht. Für das hier betrachtete Privacy-Management sind insbesondere Credential Governance und Ecosystem Governance relevant: Die *Credential Governance* beschreibt u. a. Inhalte, Anwendungsbereich und Gültigkeit von Nachweisen. Weiterhin kann festgelegt werden, welche Akteure berechtigt sind, bestimmte Nachweise auszustellen, zu prüfen oder zu verändern. Der Einsatz von Nachweisen ist Gegenstand der *Ecosystem Governance*. Sie organisiert das Zusammenspiel von Akteuren, die gemeinschaftlich Wertschöpfung betreiben. Dazu können Verweise auf Regeln zu Nachweisen, zulässiger Technik, Vertrauensniveaus, Vergütungsmodellen und Regeln zum Schutz der Privatsphäre etabliert werden. Sie legen beispielsweise fest, welche Akteure in einem definierten Kontext berechtigt sind, Nachweise eines bestimmten Typs auszustellen.

Diese Regelwerke müssen in maschinenlesbarer Form formuliert und innerhalb des Gültigkeitsbereichs für alle Akteure zugänglich gemacht werden. Zudem wird die Einhaltung von Regeln prüfbar, so dass bei Verstößen entsprechende Sanktionen verhängt werden können. Dafür müssen u. a. für folgende Aspekte konzeptionelle und technische Entwicklungen durchgeführt werden:

- *Angemessenheit von Anfragen:* Über die Prüfung der Akzeptanzstelle hinaus sollte Nutzern ein Hinweis gegeben werden, ob die für eine bestimmte Interaktion angefragte Datenmenge angemessen ist. Dieses Konzept gibt es bei der eID in Form des „Berechtigungszertifikats", das Akzeptanzstellen beim Bundesverwaltungsamt beantragen müssen. Für eine kostengünstigere und niederschwellige Prüfung wären andere Mechanismen wie die Bewertung von „Presentation Schemas" durch Zertifizierungen oder aggregierte Rückmeldungen („Crowd Intelligence") von Nutzern denkbar.
- *Nutzungsbedingungen von Daten*: Die Spezifikation des Verifiable Credentials Data Model enthält ein Attribut „termsOfUse", in dem die Nutzungsbedingungen (Policies) der Daten festgehalten werden können.[24] Dieses kann Pflichten, Verbote und Berechtigung im Umgang der betreffenden Daten durch die Akzeptanzstelle (Verifier) festlegen. Die Spezifikation sieht vor, dass damit Policies vom Herausgeber an den Inhaber (im VC) sowie vom Inhaber an die Akzeptanzstelle (in der VP)

23 *Anke / Richter*, HMD 2023, S. 270ff.
24 https://www.w3.org/TR/vc-data-model/#terms-of-use.

übermittelt werden können. Damit kann die Akzeptanzstelle gegenüber Dritten nachweisen, dass er die Daten rechtmäßig erhalten hat. Weicht die Akzeptanzstelle von den angegebenen Regeln ab, muss sie dafür die Verantwortung übernehmen.
- *Zweck von Abfragen:* Die im DIDcomm Protokoll „PresentationExchange" verwendeten Presentation Schemas besitzen ein Attribut „purpose", in dem der Zweck einer Anfrage angegeben werden kann. Wie auch bei termsOfUse ist derzeit noch nicht spezifiziert, wie dieses Attribut jenseits eines Freitext-Felds genutzt werden soll.

Zur Steigerung der *Usability* von Wallets sollten einheitliche Bedienkonzepte sowie eine einheitliche Terminologie etabliert werden. Dafür sind Forschungsarbeiten zur Verständlichkeit und Akzeptanz verschiedener Gestaltungen von Wallets für unterschiedliche Zielgruppen erforderlich. Für die Entscheidungen zum Teilen von Daten an Dritte sollten Nutzer geeignet unterstützt werden. Inhaltlich müssen dafür die vorliegenden Informationen aus den jeweilig geltenden Governance Frameworks genutzt werden. Diese Informationen müssen in geeigneter Art in die Benutzeroberfläche integriert werden, um die Benutzerinteraktion zu führen. Ein möglicher Weg dazu ist es, Konzepte zur Usable Security aus anderen sicherheitsrelevanten Interaktionen wie z. B. Onlinebanking und Web-Browser auf Wallets zu übertragen.

4.2 Verhaltensökonomisch

Für die Steigerung der Usability von Wallets und die Konzeption von Usable Security Maßnahmen ist zu eruieren, welche verhaltensökonomischen Faktoren Einfluss auf die Verständlichkeit und die Akzeptanz haben.

In einem ersten Schritt sind mögliche Barrieren und Treiber seitens der Nutzer in qualitativen und quantitativen Verfahren der empirischen Sozialforschung zu untersuchen, die für eine Inanspruchnahme der Transparenz und Selbstbestimmungsoptionen des SSI Privacy Managements bedeutend sind.

Basierend auf diesen Ergebnissen ist zu analysieren, welche Methoden geeignet sind, den Nutzer dahingehend zu befähigen, Privacy-Risiken einzuschätzen, Rechte wahrzunehmen und durchzusetzen, aber auch einen interessengerechten und wertstiftenden Austausch von Daten und eine Interaktion mit Dienstanbietern zu unterhalten.

Gewichtige Faktoren für die Akzeptanz werden vermutlich positive Nutzererlebnisse in Bezug auf Handhabung der Wallet, Reduzierung von zu administrierenden Aufwänden bei der Nutzung von Services, aber auch das Durchsetzen von Interessen und Rechten im Sinne der Selbstbestimmtheit sein.

4.3 Rechtlich

In rechtlicher Hinsicht sind regulatorische Implikation für die Prozesse und Funktionalitäten des SSI Privacy-Management zu untersuchen sowie geeignete Governance-Strategien und Maßnahmen zu entwickeln, die die Umsetzung und Durchsetzung von Rechen unterstützen.

Im Hinblick auf das Governance Framework sind die rechtlichen Rahmen und Anforderungen umfassend zu untersuchen und zu bewerten. Unter Berücksichtigung der Vorschriften aus der eIDAS-VO Novellierung sind regulatorische Anforderungen an Nachweise (Credentials Governance) sind zu evaluieren und daraus Ecosystem Governance-Strategien und Policies abzuleiten. Aus den Ergebnissen sind Mechanismen und Standards für automatisierbare und maschinenlesbare Prozesse zu definieren und Gestaltungsmuster zu entwickeln, die in ein Gesamtregelwerk überführt werden können.

Für die Implementierung der regulatorischen Vorgaben sind geeignete Methoden und verschiedene Gestaltungsmuster interdisziplinär zu evaluieren.

4.4 Gegenstand weiterer Forschung

Der Forschungsbedarf für das SSI Privacy-Management stellt sich als interdisziplinär, eng miteinander verzahnt und komplex dar. Gegenstand der weiteren Forschung muss es sein, die tatsächlichen Präferenzen von Akteuren und deren Auswirkungen zu untersuchen:

- Empfinden Benutzer die Verwendung von SSI als ein höheres Maß an Selbstbestimmung?
- Sind komplexere Mechanismen für das Aushandeln von Datenumfang und -Nutzungsbedingungen erforderlich?
- Sind Dienstanbieter bereit, einen Teil ihrer bislang selbstverwalteten Datenbestände auf die Wallets der Kunden zu verlagern und dort bei Bedarf abzufragen?

- Haben Dienstanbieter einen Wettbewerbsvorteil (z. B. durch höhere Akzeptanz von Diensten, höhere Zahlungsbereitschaft von Nachfragenden oder Kostensenkung im Umgang mit personenbezogenen Daten), wenn sie ihre Datennutzung transparent machen und die angefragte Datenmenge minimieren?
- Unter welchen Bedingungen sind Nutzer bereit, Daten zu teilen, die nicht der Erbringung von angefragten Leistungen dienen?

5. Zusammenfassung und Fazit

Self-Sovereign Identity und Wallets sind Werkzeuge, um digitale Identität von Personen, Organisationen oder Maschinen zu verwalten, Identitäts- und Berechtigungsnachweise zu erbringen und zu kontrollieren, aber auch um Daten auszutauschen und die Verarbeitung zu legitimieren. Für Nutzer digitaler Services bieten sie neue Möglichkeiten im Hinblick auf Selbstbestimmtheit und Transparenz. Für digitale Ökosysteme eröffnen sich neue Gestaltungsräume, um die Aufwände für die Datenhaltung zu minimieren, die Qualität von Daten zu verbessern und Daten interessengerechter verarbeiten zu können.

Das SSI-Privacy-Management setzt auf diese Werkzeuge und Möglichkeiten auf und zeigt einen Ausblick darauf, wie ein SSI-Wallet unterstütztes Privacy-Management aussehen kann und welche Potentiale dieser Ansatz im Sinne einer Data Governance bietet. Dabei ist erkennbar, dass SSI und Wallets, durch neuartige Mechanismen für Identitäts- und Berechtigungsnachweise sowie für Datenbereitstellungen, einen Paradigmenwechsel herbeiführen können, hin zu einer verbesserten Selbstbestimmtheit und zu interessengerechterer Data Governance.

Positive Nutzererlebnisse und die Akzeptanz aller Akteure im Ökosystem können, neben den technischen Weiterentwicklungen, der Schlüssel zu diesen Verbesserungen und damit der Treiber für das SSI Privacy-Management werden. Diese Potentiale zu heben, muss Gegenstand weiterer interdisziplinärer Forschung sein.

Literatur

Allen, C. (25. April 2016): The path to self-sovereign identity. URL: http://www.lifewithalacrity.com/previous/

Anke, J. und Richter, D. (2023): Digitale Identitäten. *HMD Praxis der Wirtschaftsinformatik* 60(2), S. 261–282. https://doi.org/10.1365/s40702-023-00965-1.

Cameron, K. (May 2005): The Laws of Identity. URL: https://www.identityblog.com/?p=352.

Europäische Kommission (03. Juni 2021): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität. COM(2021) 281 final. Brüssel. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52021PC0281

European Data Protection Supervisor (2021): Personal Information Management-System. Brussels. URL: https://edps.europa.eu/data-protection/our-work/subjects/systeme-de-gestion-des-informations-personnelles_de

Fiedler, A., Granc, F. (2022): Nationale und europäische Sicht auf eIDAS 2.0 – Aufwand und Nutzen. *Datenschutz und Datensicherheit (DuD),* 46, S. 27–31. https://doi.org/10.1007/s11623-022-1556-0

Hornung, G. (2005): *Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren*. Baden-Baden: Nomos.

Hardmann, D. (2020): Aries RFC 0430: Machine-Readable Governance Frameworks URL: https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0430-machine-readable-governance-frameworks/README.md.

Krauß, A.-M. Sellung, R.A. und Kostic, S. (2023): Ist das die Wallet der Zukunft?. *HMD Praxis der Wirtschaftsinformatik* 60(2), S. 34-365. https://doi.org/10.1365/s40702-023-00952-6.

Preukschat, A. und Reed, D. (2021): *Self-sovereign identity: Decentralized digital identity and verifiable credentials*. Shelter Island, NY : Manning Publications.

Roetzel, P.G. (2019): Information overload in the information age: a review of the literature from business administration, business psychology, and related disciplines with a bibliometric approach and framework development. *Business Research*, 12, S. 479-522. https://doi.org/10.1007/s40685-018-0069-z.

Stiftung Datenschutz (2017): Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. Leipzig: Stiftung Datenschutz. URL: https://stiftungdatenschutz.org/veroeffentlichungen.

Stand der Internetquellen in dieser Arbeit: 16.05.2023.