Interoperable Selbstsouveräne Identitäten: Ein Digital Markets Act für Endnutzer?

HMD Praxis der Wirtschaftsinformatik (2023) 60:405–421
https://doi.org/10.1365/s40702-023-00947-3

SCHWERPUNKT

Interoperable Selbstsouveräne Identitäten: Ein Digital Markets Act für Endnutzer?

Hakan Yildiz · Artur Philipp · Aljoscha Schulte · Axel Küpper · Sebastian Göndor · Sandro Rodriguez Garzon

Eingegangen: 24. September 2022 / Angenommen: 30. Januar 2023 / Online publiziert: 28. Februar 2023

Zusammenfassung Der Digital Markets Act zielt darauf ab, den unilateralen Markteinfluss der Betreiber (sogenannte Gatekeeper) zentraler Plattformdienste, wie z. B. App-Stores, zu regulieren. In vielen Fällen zwingen Gatekeeper ihren Geschäftskunden (den Dienstanbietern) die Integration eigener Plattform-Identitätsdienste in ihren Diensten und Anwendungen auf. So benötigen die Endnutzer der Dienstanbieter digitale Identitäten, die durch Plattform-Identitätsdienste bereitgestellt und verwaltet werden müssen, um auf die angebotenen Anwendungen der Dienstanbieter zugreifen zu können. Der Digital Market Act sieht vor, dass Plattformanbieter ihre Geschäftskunden nicht dazu zwingen dürfen, plattformspezifische Identitätsdienste in die Anwendungen und Dienste der Geschäftskunden zu integrieren. Zwar können nach dem Digital Markets Act Dienstanbieter die Identitätsdienste frei wählen, aber die Endnutzer sind weiterhin dazu gezwungen, die von den

In diesem Beitrag wird „Endnutzer" geschlechtsneutral verwendet. Der Begriff umfasst dabei immer die Anrede für Mann, Frau und Divers.

✉ Hakan Yildiz · Artur Philipp · Aljoscha Schulte · Axel Küpper · Sebastian Göndor · Sandro Rodriguez Garzon
Service-centric Networking, TU Berlin, Berlin, Deutschland
E-Mail: hakan.yildiz@tu-berlin.de

Artur Philipp
E-Mail: a.philipp@tu-berlin.de

Aljoscha Schulte
E-Mail: a.schulte@tu-berlin.de

Axel Küpper
E-Mail: axel.kuepper@tu-berlin.de

Sebastian Göndor
E-Mail: Sebastian.goendoer@tu-berlin.de

Sandro Rodriguez Garzon
E-Mail: Sandro.rodriguezgarzon@tu-berlin.de

Dienstanbietern angebotenen Identitätsdienste zu verwenden. Das neue Paradigma der selbstsouveränen Identitäten (Self-sovereign identity, SSI) verspricht Endnutzern unabhängig von Identitätsdiensten Kontrolle und Hoheit über ihre digitalen Identitäten. Die Zahl der Dienste und Anwendungen, welche das SSI-Paradigma umsetzen, nimmt rapide zu. Zugrundeliegende Standards und Protokolle unterscheiden sich jedoch teils signifikant. Aufgrund dieser Divergenz ist das Sicherstellen der Interoperabilität unterschiedlicher Dienste und Anwendungen, die das SSI-Paradigma umsetzen, einer der größten Herausforderungen, um eine breite Nutzerakzeptanz zu erreichen. In diesem Artikel diskutieren wir die Herausforderungen der Interoperabilität im Detail, bieten einen systematischen Ansatz zu ihrer Beseitigung und zeigen ein praktisches Beispiel auf nationaler Ebene in Deutschland.

Schlüsselwörter Digitale Identitäten · Selbstsouveräne Identitäten · SSI · Interoperabilität · Digital Markets Act

Interoperable Self-sovereign Identities: Digital Markets Acts for End Users

Abstract The Digital Markets Act aims to regulate the unilateral market influence of operators (so-called gatekeepers) of central platform services, such as app stores. In many cases, gatekeepers force their business customers (service providers) to integrate their platform identity services into the services and applications of the business customers. Thus, the end users of service providers require digital identities to be provisioned and managed by platform identity services to access the service providers' applications and services. The Digital Markets Act provides that platform providers may not require their business customers to integrate platform-specific identity services with the applications and services of the business customers. While the Digital Markets Act allows service providers to choose identity services freely, end users are still forced to use the identity services offered by the service providers. The new paradigm of self-sovereign identity (SSI) promises end users control and sovereignty over their digital identities independent of identity services. The number of services and applications implementing the SSI paradigm is proliferating. However, underlying standards and protocols differ, sometimes significantly. Due to this divergence, ensuring the interoperability of different services and applications that implement the SSI paradigm is one of the biggest challenges to achieving broad user adoption. In this article, we discuss the interoperability issues in detail, provide a systematic approach to address them, and show a practical example at the national level in Germany.

Keywords Digital Identity · Self-sovereign Identity · SSI · Interoperability · Digital Markets Act

1 Einleitung

Die hoheitliche Identität einer Person im digitalen Raum abzubilden ist seit jeher eine Herausforderung. Identitäten sind ein essenzieller Bestandteil unseres digitalen Alltags, da sie authentifizierte, und zusammen mit kryptografischen Verfahren, sichere Kommunikation ermöglichen. Diese wiederum ist die Voraussetzung für Handel und Zahlungen im digitalen Raum. Wer die Identität einer Person verwaltet oder kontrolliert (z. B. ein zentralisierter Identitätsdienst), hat zu einem gewissen Grad Einblick und Einfluss auf ihre Kommunikation und Aktivitäten im digitalen Raum. Ein Beispiel für die Herausforderungen, die mit der Identität einer Person im digitalen Raum verbunden sind, ist die Verwaltung von Online-Konten. Wenn beispielsweise ein zentralisierter Identitätsdienst zur Anmeldung bei einem Onlineshop genutzt wird, können die Metadaten aus diesem Informationsfluss einen Einblick in die Aktivitäten des Endnutzers geben.

Unternehmen, die eine marktbeherrschende Stellung haben und solche Identitätsdienste anbieten, können diese Kontrolle ausnutzen, um Macht über Einzelpersonen und den Markt auszuüben.

Um dem entgegenzuwirken hat die Europäische Kommission eine Verordnung „über bestreitbare und faire Märkte im digitalen Sektor" (Digital Markets Act, DMA) in das Europäische Parlament eingebracht, welches diese 2022 verabschiedete (European Commission 2020).

Der DMA reguliert den Einfluss von *Gatekeepern* auf Digitale Märkte. Gatekeeper sind als „Betreiber Zentraler Plattformdienste" (European Commission 2020) definiert, womit implizit die großen nordamerikanischen Digitalkonzerne gemeint sind. *Zentrale Plattformdienste* sind u. a. Suchmaschinen, App Stores, soziale Netzwerke, Betriebssysteme, aber auch Identifizierungsdienste. Dienstanbieter nutzen die von Gatekeepern angebotenen zentralen Plattformdienste, um beispielsweise den Zugriff auf eigene Anwendungen zu ermöglichen.

Ohne eine Regulierung können Gatekeeper ihre Marktmacht nutzen, um gezielt Einfluss auf den Markt, aber auch auf Endnutzer zu nehmen. Der DMA soll den Einfluss von Gatekeepern auf Dienstanbieter eingrenzen. Es ist Gatekeepern untersagt, vom Dienstanbieter „zu verlangen, im Zusammenhang mit Dienstleistungen, die sie [die Dienstanbieter] über die zentralen Plattformdienste dieses Gatekeepers anbieten, einen Identifizierungsdienst des Gatekeepers zu nutzen, anzubieten oder mit ihm zu interoperieren" (European Commission 2020). *Identifizierungsdienste* sind „Nebendienstleistungen, die unabhängig von der verwendeten Technologie jegliche Art von Überprüfung der Identität von Endnutzern oder gewerblichen Nutzern ermöglichen" (European Commission 2020).

Für Dienstanbieter bedeutet das, dass sie den oder die Dienste zur Identifizierung ihrer Endnutzer frei wählen können. Neben einem eigenen zentralen Identifizierungsverfahren, wie z. B. E-Mail und Passwort, können sie also freiwillig ein oder mehrere externe Identitätsdienste anbieten. Diese Wahlfreiheit wirkt einer weiteren Zentralisierung digitaler Märkte entgegen.

Da der DMA auf Unternehmen ausgerichtet ist, hat das Regelwerk jedoch nur mittelbare Auswirkungen auf Endnutzer. Diese sind bei der Nutzung von Onlinedienstleistungen weiterhin auf die Identifizierungsdienste angewiesen, die der Dienstan-

bieter zur Verfügung stellt. Endnutzer haben somit keinen direkten Einfluss darauf, wo und wie ihre Identitätsdaten gespeichert und verarbeitet werden. Endnutzer sind immer von der Vorauswahl der Dienstanbieter anhängig, da diese auf externe Dienste oder spezifische Implementierungen zurückgreifen.

Mit dem aufkommenden Identitätsparadigma der *selbstsouveränen Identitäten* (Self-sovereign Identity, SSI) können Endnutzer selbst über Verwaltung und Offenlegung ihrer Identitätsdaten entscheiden, statt diese einem Identitätsdienst zu überlassen. SSI kann dabei helfen, den Gedanken der Datensouveränität des DMA auf die Endnutzer auszuweiten. Damit möglichst viele Endnutzer von dieser Datensouveränität profitieren können, sind interoperable SSI-Implementierungen unabdingbar.

Im Rahmen eines Innovationswettbewerbs gibt es bereits mehrere von der Bundesregierung geförderte *Schaufensterprojekte* für Sichere Digitale Identitäten[1]. Diese setzen jedoch zum Teil auf Tech-Stacks mit unterschiedlichen Standards und Protokollen. Das Ergebnis sind *SSI-Stacks*, die nicht miteinander kompatibel sind.

In diesem Artikel zeigen wir auf, welche Schritte notwendig sind, um eine interoperable SSI-Landschaft mit geringen Einstiegs- bzw. Nutzungshürden zu schaffen.

2 Selbstsouveräne Identitäten

Die SSI-Grundprinzipien wurden erstmals 2016 von Christoper Allen (2016) skizziert. Die von Identitätsanbietern ausgestellten Identitätsdaten der Endnutzer werden nicht mehr zentral bei einem Identitätsanbieter gespeichert müssen. Endnutzer sind nun in der Lage, ihre Daten selbst zu verwalten. Sie können souverän darüber entscheiden, an welchem Speichertort diese abgelegt und mit welchen Dienstanbietern diese bei Bedarf geteilt werden. Das Verwalten der Identitätsdaten in einer Cloudumgebung eines Fremdanbieters bleibt dabei prinzipiell möglich. Aufgrund der Sensibilität der Identitätsdaten ist jedoch das Speichern in einer sogenannten digitalen *Wallet* auf einem privaten Endgerät der Endnutzer zu bevorzugen. Somit haben Endnutzer die vollständige Kontrolle über ihre Daten.

Mit dem SSI-Paradigma wird die Rolle eines Identitätsanbieters auf die eines *Ausstellers* reduziert, da die Identitätsdaten der Endnutzer von den Identitätsanbietern getrennt werden. Um die Authentizität und Integrität eigens verwalteter, aber auch gleichzeitig von Ausstellern kryptografisch signierter Identitätsdaten für Dritte prüfbar zu machen, muss der Zugang zum öffentlichen kryptografischen Schlüsselmaterial des Ausstellers gewährleistet sein. Darüber hinaus kann das Schlüsselmaterial vom Aussteller eigenständig in einer *Verifiable Data Registry* (VDR) gespeichert werden, welche die Zuordnung des Schlüsselmaterials zum Aussteller ermöglicht. VDRs können mittels unterschiedlicher Technologien umgesetzt werden, z. B. *Distributed-Ledger-Technologien* (DLT), Peer-to-Peer Systemen aber auch klassischen Webservern, und bieten jeweils unterschiedliche Eigenschaften wie Manipulations- und Ausfallsicherheit.

[1] Schaufenster Digitale Identitäten: https://www.digitale-technologien.de/DT/Navigation/DE/Programme Projekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/projekte_umsetzungsphase.html.

3 Herausforderungen der Interoperabilität

Zwar sind bereits verschiedene Standards von mehreren Organisationen wie der *Decentralized Identity Foundation* (DIF)[2] und das *World Wide Web Consortium* (W3C)[3] in der Entwicklung, jedoch ist SSI derzeit noch keine vollständig standardisierte Technologie auf allen Ebenen.

Das W3C hat 2022 eine Spezifikation für persistente dezentrale Identifikatoren (*Decentralized Identifiers* DIDs) verabschiedet (Sporny et al. 2022b). DIDs sind global eindeutige Uniform Resource Identifiers (URIs). Organisationen, Dinge und natürliche Personen können durch DIDs repräsentiert werden. Darüber hinaus wurde das Containerformat *Verifiable Credentials* (VC) definiert (Sporny et al. 2022a).

Beide Spezifikationen bieten jedoch Freiraum für unterschiedliche Umsetzungen und technische Implementierungen. Dies hat zur Folge, dass mittlerweile über 130 Implementierungsvarianten (sogenannte *DID-Methoden*[4]) für VDRs und DIDs existieren und es mehrere unterschiedliche Umsetzungen des VC-Containerformates gibt (Young 2022). DID-Methoden sind konkrete technische Spezifikationen, welche beschreiben, wie man die zu einer DID gehörenden Informationen (beispielsweise kryptografisches Schlüsselmaterial) laden, speichern, aktualisieren, löschen oder deaktivieren kann. Neben der Vielzahl an DID-Methoden und VC-Containerformaten kann man sich verschiedener Protokolle für das Ausstellen, Transferieren und Präsentieren von VCs bedienen.

Aufgrund dieser technologischen Vielfalt existieren heute schon diverse SSI-Stacks auf dem Markt und es entwickeln sich fortlaufend neue. Diese unterscheiden sich in den jeweils angebotenen Merkmalen und Funktionsweisen. Als Beispiel dieser technologischen Fragmentierung sind die vier nationalen Schaufensterprojekte zu nennen: *ID-Ideal*[5]; *IDunion*[6] *ONCE*[7] und *SDIKA*[8]. So sind beispielsweise Wallets aus IDunion nicht mit dem SSI-Stack von ONCE kompatibel. Endnutzer sind durch die Wahl einer Wallet zum Speichern und Verwalten der eigenen Identitätsdaten an ein Schaufensterprojekt und damit implizit an einem SSI-Stack gebunden.

Aufgrund der Wahlfreiheit der Endnutzer hinsichtlich einer Wallet und dem damit verbundenen SSI-Stack, entstehen für Dienstanbieter als Konsumenten von Identitätsdaten technische Herausforderungen: Sie müssten mehrere SSI-Stacks auf der eigenen Infrastruktur implementieren, um alle Endnutzer mit Wallets aus diversen SSI-Stacks bedienen zu können. Wenn der Wallet nicht mehrere SSI-Stacks unterstützen, müssten die Endnutzer mehrere Wallets aus diversen SSI-Stacks nutzen, was den Verlust potenzieller Endnutzer für den Dienstanbieter und womöglich einen wirtschaftlichen Nachteil bedeuten könnte. Um die Einstiegshürden für Endnutzer niedrig zu halten, aber auch um das Spektrum potenzieller Endnutzer für Dienstan-

[2] DIF: https://identity.foundation.

[3] W3C: https://www.w3.org.

[4] DID Methods: https://www.w3.org/TR/did-spec-registries/#did-methods.

[5] ID-Ideal: https://id-ideal.de.

[6] IDunion: https://idunion.org.

[7] ONCE: https://once-identity.de.

[8] SDIKA: https://www.sdika.de.

bieter zu maximieren, ist es notwendig, Interoperabilität zwischen unterschiedlichen SSI-Stacks zu ermöglichen.

Eine weitreichende Interoperabilität zwischen unterschiedlichen SSI-Stacks kann nur erreicht werden, wenn Inkompatibilitäten erkannt und gezielt vermieden werden können. Im weitesten Sinne definieren Palfrey et al. Interoperabilität als die Fähigkeit, Daten und andere Informationen zwischen Systemen, Anwendungen oder Komponenten auszutauschen (Palfrey und Gasser 2012). Dazu ist ein gemeinsames Verständnis von Interoperabilität in Bezug auf SSI notwendig. Yildiz et al. verwenden ein Rahmenwerk zur Definition von SSI-Interoperabilität (Yildiz et al. 2022). Dieses Rahmenwerk wurde bereits für die Definition von Interoperabilität in anderen Technologien verwendet und wurde vom Europäischen Institut für Telekommunikationsnormen anerkannt (van der Veer und Wiles 2008). Interoperabilität wird hierbei in vier aufeinander aufbauenden Stufen eingeteilt. Im Kontext von SSI sind die vier Interoperabilitätsstufen folgende:

- *Technische Interoperabilität* ist die Fähigkeit, dass die teilnehmenden Parteien untereinander Daten austauschen können.
- *Syntaktische Interoperabilität* ist die Fähigkeit, dass die Struktur der Zusammensetzung ausgetauschter Daten grundlegend interpretiert werden kann. Datenaustauschformate sowie die Syntax der Daten sind jeweils Bestandteile der syntaktischen Interoperabilität.
- *Semantische Interoperabilität* ist die Fähigkeit, dass die ausgetauschten Daten eindeutig interpretiert werden können. So haben beispielsweise die Identitätsmerkmale eines VC für alle Parteien die gleiche Bedeutung. Dies kann durch die Nutzung von Ontologien und Vokabularen erreicht werden.
- *Organisatorische Interoperabilität* ist die Fähigkeit, Informationen zwischen verschiedenen Organisationen und Tech-Stacks auszutauschen und zu verwerten. Dies umfasst zusätzlich die *rechtliche Interoperabilität* (z. B. gegenseitige Erfüllung und Anerkennung von Compliance-Regeln) als auch die *wirtschaftliche Interoperabilität* (z. B. gegenseitige Anerkennung von VCs innerhalb einer gemeinsamen Wertschöpfungskette).

Die vier vorgestellten Interoperabilitätsstufen bauen aufeinander auf. So erfordert semantische Interoperabilität zunächst das Erreichen der technischen und syntaktischen Interoperabilität. Abb. 1 illustriert die Interoperabilitätsstufen und ihre Abhängigkeiten zueinander.

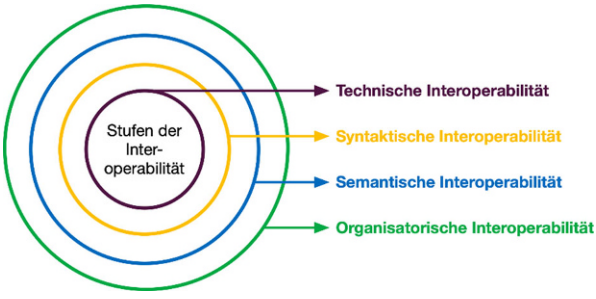

Abb. 1 Interoperabilitätsstufen adaptiert von (van der Veer und Wiles 2008)

Interoperabilitätsstufen ermöglichen ein gemeinsames Verständnis und Zielsetzung zwischen Parteien, die miteinander interoperabel sein wollen. Im folgenden Abschnitt betrachten wir inhaltlich die zuvor genannten Schaufensterprojekte Sichere Digitale Identitäten sowie den aktuellen Stand und deren gemeinsame Zielsetzung hinsichtlich Interoperabilität zueinander.

4 Schaufensterprojekte Sichere Digitale Identitäten

Im Jahr 2020 initiierte das deutsche Bundesministerium für Wirtschaft und Klimaschutz (BMWK) einen Innovationswettbewerb *Sichere Digitale Identitäten*. Der Innovationswettbewerb beschäftigt sich mit der Frage, wie neue Technologien für digitale Identitäten wirtschaftliche oder administrative Prozesse in Deutschland für Menschen und Objekte zugänglich machen können. Die vier ausgewählten Schaufensterprojekte erarbeiten verschiedene Konzepte und setzen diese mit zahlreichen Anwendungsfällen bis März 2024 um. Diese Projekte werden im Folgenden kurz vorgestellt.

IDunion[9] baut ein dezentrales Identitätsökosystem auf, das für Dinge sowie natürliche und juristische Personen geeignet ist. Kern dieses Ökosystems ist ein DLT-basiertes, verteiltes Identitätsnetzwerk, welches für das Ausstellen und Verifizieren von Credentials verwendet wird. Das darunterliegende Identitätsnetzwerk ist ein *public permissioned* DLT, d. h. jeder darf Daten aus dem Ledger lesen aber nur zugelassene Entitäten dürfen auf dem Ledger schreiben. Die Governance des Netzwerkes ist von einer europäischen Genossenschaft geregelt. Innerhalb von IDunion werden mehr als 35 Anwendungsfälle aus verschiedenen Anwendungsgebieten wie z. B. Banking, E-Governance und Bildung umgesetzt.

ID-Ideal[10] konzipiert einen rechtssicheren digitalen Raum namens *TrustNet*. In TrustNet sind die Entitäten eindeutig identifizierbar, die ausgetauschten Informationen überprüfbar und die Transaktionen rechtssicher. Gleichzeitig kann die Datenhoheit für alle Beteiligten gewährleistet werden. Um dieses Konzept umzusetzen, konzentriert sich ID-Ideal auf die Definition eines Vertrauensrahmens. Dieses Regelwerk hilft bei der Harmonisierung zur Erreichung von Interoperabilität verschiedener Identitätsdienste und bietet Anreize für ihre Nutzung.

Im Mittelpunkt des ONCE-Projekts[11] steht die Entwicklung digitaler Identitäten mit einem hohen technischen Sicherheitsniveau. Vertrauenswürdige Unternehmen, Institutionen und Verwaltungen sollen bei der Digitalisierung ihrer Dienstleistungen mit digitalen Ausweisen und Online-Dokumenten zum Zwecke des Zugriffs auf die entsprechenden digitalen Identitäten unterstützt werden.

[9] vgl. https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/IDunion/IDunion.html.

[10] vgl. https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/IDideal/IDideal.html.

[11] vgl. https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/Once/Once.html.

SDIKA[12] entwickelt eine Identitätslösung, die in zahlreichen Anwendungsfällen in Karlsruhe und der Metropolregion Rhein-Neckar getestet wird. Hierbei wird sowohl die Nutzung von zentral verwalteten Identitäten als auch von selbst verwalteten Identitäten (SSI) berücksichtigt. Das Projekt richtet sich nicht nur an Endnutzer, sondern auch an Organisationen wie Unternehmen, öffentliche Körperschaften und Verbände, die ihre organisatorischen Identitäten mit SDIKA nutzen möchten.

Die vier vorgestellten Schaufensterprojekte bauen zum Teil auf unterschiedlichen Tech-Stacks auf, die miteinander nicht interoperabel sind. Jedoch ist die gemeinsame Zielsetzung aller Projekte das Erreichen der organisatorischen Interoperabilität untereinander. Dies soll durch die Verwendung einer gemeinsam getroffenen Auswahl von Standards und Protokollen erreicht werden. Darum arbeiten verschiedene Stakeholder aus allen Schaufensterprojekten zusammen daran, sich nach einem gemeinsamen Interoperabilitätsprofil auszurichten und dadurch ihre Interoperabilitätsziele zu erreichen.

5 Referenzmodell

Durch das Modellieren eines Referenzmodells können spezifische Herausforderungen komplexer Systeme besser verstanden und bewaltigt werden (Vernadat 2010). So präsentierte die Trust over IP (ToIP) Foundation im Jahr 2019 ein Modell vor, um die Hürden zum Aufbau von Vertrauen zwischen Parteien zu bewältigen. Dabei wurde ein SSI-Stack in zwei Perspektiven aufgeteilt: Technologie und Governance. Der Technologiestack befasst sich mit den notwendigen technischen Bausteinen für den Aufbau von Vertrauen. Der ToIP-Ansatz geht davon aus, dass Vertrauen nicht nur technologisch aufgebaut werden kann, sondern durch Governance unterstützt werden muss (Matthew et al. 2019). Dementsprechend wird zusätzlich ein Governance-Stack modelliert, der die notwendigen Governance-Rahmenbedingungen für z. B. Netzwerk, Emittent und SSI darstellt.

Für die Bewältigung der Herausforderungen um Interoperabilität zwischen verschiedenen SSI-Implementierungen kann ein ähnlicher Ansatz verwendet werden. Der erste Schritt für das Schaffen eines projektübergreifenden Interoperabilitätsprofils und dadurch das Erreichen der vereinbarten Zielsetzung, ist das Erarbeiten eines gemeinsamen technischen Verständnisses zwischen den einzelnen Projekten. Hierzu ist die besondere Betrachtung aller innerhalb der Schaufensterprojekte verwendeten SSI-Stacks notwendig. Ein SSI-Stack besteht aus mehreren aufeinander aufbauenden Schichten, welche jeweils unterschiedlichen Zwecken dienen. Basierend darauf haben Yildiz et al. ein Referenzmodell[13] vorgeschlagen, das für die Abbildung und Ausrichtung verschiedener SSI-Stacks verwendet werden kann, um die nach Abb. 1 definierten Interopearbilitätsziele zu erreichen (Yildiz et al. 2022). Das Referenzmodell nach Yildiz et al. basiert auf einer ähnlichen Struktur und Schichten des

[12] vgl. https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/SDIKA/SDIKA.html.

[13] siehe https://identity.foundation/faq/#how-is-this-faq-structured.

ToIP-Modells. Allerdings liegt der Fokus stark auf den technischen Bausteinen und thematisch mehr auf Interoperabilität statt auf Vertrauensaufbau.

Im Folgenden werden das Referenzmodell und seine Schichten in einer konsolidierten Form erläutert.

5.1 Technische Vertrauensschicht

Die Ausstellung und Validierung von SSIs setzt Vertrauen zwischen interagierenden Ausstellern, Identitätsinhabern und Verifizierern voraus. Obwohl jede Rolle von jeder Partei wahrgenommen werden kann, sind Aussteller und Verifizierer i. d. R. Organisationen, und Identitätsinhaber sind natürliche Personen und Dinge. Jede dieser Parteien kann über eine DID repräsentiert werden. Die Verwaltung einer DID wird von der jeweiligen DID-Methode beschrieben. Eine DID-Methode ist eine technische Beschreibung wie eine DID erstellt, in ein *DID-Dokument* aufgelöst, aktualisiert oder gelöscht bzw. deaktiviert werden kann (Sporny et al. 2022b). DIDs und dazugehörige DID-Dokumente können bei Bedarf in einer VDR gespeichert werden. In diesem Fall spricht man von *Public DIDs*. DID-Dokumente der Public DIDs enthalten öffentlich zugängliches Schlüsselmaterial sowie Kommunikationsendpunkte (Wittek et al. 2020). Im Gegensatz dazu werden *Pairwise-DIDs* nicht in einer VDR gespeichert. Stattdessen tauschen miteinander kommunizierenden Parteien ihre Pairwise-DIDs und DID-Dokumente direkt untereinander aus (Wittek et al. 2020). Damit können DIDs für die kryptografisch gesicherte Interaktion zwischen zwei Parteien verwendet werden, ähnlich wie es auf X.509-Zertifikaten basierende TLS und HTTPs der Fall ist, und schaffen somit technisches Vertrauen. Einen Sonderfall stellt die *did:key* DID-Methode dar, da sich das zur DID zugehörige DID-Dokument aus der DID selbst ableiten lässt und nicht separat verwaltet werden muss (Sporny et al. 2022c). Eine did:key DID kann bei Bedarf, beispielsweise für eine öffentliche Organisation, zusätzlich in einer VDR gespeichert werden.

5.2 Agentenschicht

Im SSI-Paradigma werden Parteien durch Agenten repräsentiert. Agenten sind Software, die mit anderen Agenten über sichere *Kommunikationskanäle* Nachrichten und Daten austauschen und ebenfalls durch eine eigene DID repräsentiert werden können. Mit Informationen aus dem assoziierten DID-Dokument kann ein SSI-Agent eigene Nachrichten signieren und empfangene Nachrichten entschlüsseln. Gleichzeitig kann ein SSI-Agent die zu sendenden Nachrichten mit der Schlüsselinformation aus dem DID-Dokument des Empfängers verschlüsseln, sodass sie nur vom Empfänger entschlüsselt werden können. Agenten können in zwei Typen unterschieden werden. *Edge-Agenten* laufen in der Domäne der Partei, beispielsweise auf einem Smartphone oder Tablet. *Cloud-Agenten* können innerhalb oder außerhalb der eigenen Domäne betrieben werden (Nitin und Paul 2021). Beispiele hierfür sind die auf Servern laufende Agenten, die Nachrichten von und zu einem Edge-Agenten weiterleiten (sogenannte *Mediators (Hardman* 2019*a)*) oder den Organisationen zur Ausstellung und Validierung von SSIs dienen.

5.3 Credential-Schicht

Aufbauend zum technischen Vertrauen und den sicheren Kommunikationskanälen können Agenten Verifiable Credentials ausstellen oder verifizieren. Es gibt eine Vielzahl von Credential-Formaten, von denen VCs nach W3C Standard am meisten verbreitet sind. Ein VC ist ein fälschungssicherer Datencontainer, der Identitätsdaten über einen Identitätsinhaber enthält (Sporny et al. 2022a). Er wird von einem Aussteller erstellt, mit entsprechenden Identitätsdaten befüllt und digital signiert. Wenn Identitätsinhaber sich mit Hilfe von VCs authentifizieren wollen, tun sie dies mit einer *Verifiable Presentation* (VP). Eine VP ist ein anderer vom VC abgeleiteter Datencontainer, der Identitätsdaten aus dem VC und zusätzlich einen Inhabernachweis enthält (Sporny et al. 2022a).

Es existieren mehrere unterschiedliche Protokolle für die Ausstellung, Austausch und die Verifizierung von VCs. Ebenso existieren unterschiedliche Widerrufsmechanismen für VCs durch den ursprünglichen Aussteller (Yildiz et al. 2022). Alle hier genannten Datencontainer, Protokolle und Mechanismen werden in der Credential-Schicht verortet.

5.4 Anwendungsschicht

Als höchste Schicht im Referenzmodell baut die Anwendungsschicht auf der Vertrauensschicht, Agentenschicht und Credentialschicht auf und beinhaltet die anwendungsspezifische Geschäftslogik. So benötigt zum Beispiel die auf einem Edge-Agenten basierte Wallet-Anwendung einen Mediator, um Nachrichten zu empfangen und kann Authentifizierung mittels PIN oder biometrischen Daten für den Zugriff verwenden. Eine Unternehmensanwendung hingegen kann ohne einen Mediator betrieben werden und Nutzerauthentifizierung mit anderen Methoden gewähren. So können sich die Geschäftslogik zwischen Unternehmensanwendungen und Endnutzer-Wallets unterscheiden. Darüber hinaus wird die Semantik in der Anwendungsschicht definiert und ist damit Grundlage für semantische Interoperabilität. Sie enthält branchen- und anwendungsspezifische Datenmodelle.

6 Ausgangsituation

Die von den Schaufensterprojekten verwendeten Bausteine wurden nach dem in oben beschriebenen Referenzmodell den jeweiligen Schichten zugeordnet. Dies hilft bei der Erkennung von Inkompatibilitäten und ermöglicht die Erstellung eines gemeinsamen Interoperabilitätsprofils. Im Folgenden betrachten wir zwei SSI-Stacks: zum einen den von IDunion verwendeten SSI-Stack mit Hyperledger Indy & Aries, zum anderen den Jolocom-Stack, welcher von ID-Ideal, Once und SDIKA eingesetzt wird. Basierend auf dem jeweiligen SSI-Stack eines Schaufensterprojekts werden verschiedene Unternehmensanwendungen und Wallets angeboten.

6.1 SSI-Stack mit Hyperledger Indy & Aries

Hyperledger Indy ist ein DLT-basiertes VDR, welches die did:sov-Methode verwendet. Hyperledger Aries bietet Protokolle für die Kommunikation zwischen Agenten an.

Der Indy-Ledger erfüllt Kriterien wie Verfügbarkeit und Manipulationssicherheit. Daher können Public DIDs, die im Ledger speichert werden, zum Aufbau von Vertrauen verwendet werden. So kann eine Entität das Schlüsselmaterial und den Endpunkt aus dem assoziierten DID-Dokument extrahieren und sich auf deren Authentizität und Integrität verlassen. Um die Privatsphäre von Endnutzern zu schützen, unterstützt Hyperledger Aries zusätzlich als Pairwise-DID die did:peer-Methode, die keine VDRs erfordert. Stattdessen wird technisches Vertrauen dadurch hergestellt, dass nur die Entität, die den privaten Schlüssel besitzt, die entsprechende Pairwise-DID aus dem Schlüsselpaar erzeugen kann (Deventer et al. 2021).

Die Agentenschicht basiert auf zwei Aries-Frameworks: *Aries Cloud Agent Python* für Cloud-Agenten und *Aries.NET* für Edge-Agenten. Beide Frameworks basieren auf dem *DIDComm V1 Envelope* für den sicheren Austausch von Informationen. DIDComm V1 ist ein nachrichtenbasiertes und transportagnostisches Simplex-Protokoll, das sich auf DIDs und Public-Key-Kryptografie stützt (Hardman 2018). Die initiale Übertragung von Schlüsselinformation kann bei Bedarf unverschlüsselt über das Aries-Out-of-Band-Protokoll (West et al. 2019) erfolgen. Diese Schlüsselinformation wird anschließend zur Erstellung eines sicheren Kommunikationskanals verwendet, welcher Authentizität, Integrität und Vertraulichkeit gewährleistet. Beide Aries-Frameworks unterstützen derzeit HTTP(s) und Websockets als Transportprotokolle.

Auf der Credential-Schicht nutzt Hyperledger Indy das *AnonCreds-1.0-Credential-Format*. AnonCreds bieten datenschutzorientierte Offenlegung von Identitätsdaten und Widerrufsmechanismen (Curran et al. 2022). Für das Ausstellen eines AnonCreds-Credentials wird das *Issue-Credential-V1-Protokoll* (Khateev 2019a) verwendet, während für die Präsentation *Present Proof V1* (Khateev 2019b) genutzt wird. Beide bauen auf DIDComm V1 auf und sind zustandsbasiert.

Die Anwendungsschicht enthält eine Vielzahl von Unternehmensanwendungen und Endnutzer-Wallets. Um Interoperabilität zwischen allen Anwendungen innerhalb des Konsortiums zu gewährleisten, hat IDunion sich 2020 auf das Aries Interoperability Profile 1.0 (AIP 1.0) geeinigt, welches die zu verwendenden Aries-Protokolle festlegt (Curran und Jordan 2019). AIP 1.0 kann nur von SSI-Implementierungen verwendet werden, die auf dem SSI-Stack von Hyperledger Indy basieren. Daher ist es als Interoperabilitätsprofil für die Schaufensterprojekte nicht geeignet.

6.2 Jolocom-Stack

Als eine der ersten SSI-Umsetzungen hat Jolocom seinen eigenen SSI-Stack *Jolocom SDK 1.0* entwickelt (Rusu 2021). Da es sich um eine der ersten Implementierungen handelt, basiert das SDK nicht auf bestehenden Frameworks und der Datenaustausch erfolgt nicht mit standardisierten Protokollen.

Zum Aufbau des technischen Vertrauens bietet das Jolocom SDK 1.0 zwei DID-Methoden an. Für Public DIDs wird die did:jolo-Methode eingesetzt. Sie gibt vor, die DID auf dem *Ethereum Rinkeby* Ledger und die entsprechenden DID-Dokumente im *InterPlanetary File System* (IPFS), einem verteilten Dateisystem, zu speichern (Cunningham 2020). Dieser Ansatz erfüllt ebenfalls Kriterien wie Verfügbarkeit und Manipulationssicherheit. Somit kann eine Entität das Schlüsselmaterial und den Endpunkt aus dem assoziierten DID-Dokument extrahieren und sich auf ihre Authentizität und Integrität verlassen. Darüber hinaus wird für mehr Schutz der Privatsphäre der Endnutzer zusätzlich die did:jun-Methode angeboten (Rusu 2022). Sie ist eine der ersten Implementierungen von *Key Event Receipt Infrastructure* (KERI). KERI bietet selbstzertifizierenden Identifikatoren an, die ähnlich wie did:peer-DIDs erstellt werden: Der Identifikator wird aus einem Schlüsselpaar abgeleitet. KERI ermöglicht anschließend eine sichere und überprüfbare Kette von Schlüsselrotationen für den erstellten Identifikator (Smith 2019). Zusätzlich bietet KERI die Zuordnung von Schlüsselmaterial an Aussteller, wobei die Identifikatoren sowie die überprüfbare Kette von Schlüsselrotationen in beliebigen VDRs gespeichert werden können.

Auf der Agentenschicht enthält das Jolocom SDK 1.0 einen *JSON Web Token* (JWT) Envelope. Der Token enthält u. a. den öffentlichen Schlüssel. Der zugehörige private Schlüssel wird zum Signieren des Tokens verwendet (Rusu 2022). Damit kann die Authentizität und Integrität der Nachrichten sichergestellt werden. Vertraulichkeit ist jedoch nicht Teil des JWT-Envelope. Um Nachrichten auf vertrauliche Weise auszutauschen, sind zusätzliche Sicherheitsmaßnahmen wie *Transport Layer Security* (TLS) erforderlich. Wie der SSI-Stack von Hyperledger Indy und Aries verwendet auch das Jolocom SDK 1.0 HTTP(s) und Websockets als Transportprotokolle. Auch für den initialen Austausch von Schlüsselinformation wird bei Bedarf ein Out-of-Band-Protokoll verwendet (Rusu 2022).

Auf der Credential-Schicht nutzt das Jolocom SDK 1.0 VC nach W3C Standard in JSON-Format und erweitert diese um JSON Linked Data (JSON-LD). Linked Data kann u. a. Ontologien mit einer JSON-Datei verknüpfen, die Integritätsnachweise enthalten können (Sporny et al. 2014). Im Bezug zu VC ermöglicht JSON-LD das Speichern eines Kontexts, beispielsweise aus einem Webserver. Damit können Identitätsdaten zu einer Ontologie zugeordnet werden. Diese Zuordnung ermöglicht semantische Eindeutigkeit und schließlich semantische Interoperabilität. Das Jolocom SDK 1.0 unterstützt keinen Widerrufsmechanismus und verwendet maßgeschneiderte Credential-Austauschprotokolle (Jolocom 2019). Diese Protokolle folgen keinem Standard aus Normungsinstitutionen und erschweren dadurch das Erreichen der technischen Interoperabilität.

Jolocom bietet Enterprise- und Wallet-Anwendungen auf der Anwendungsschicht an, die in der Lage sind, sich gegenseitig mittels JWT zu authentifizieren, VCs auszustellen sowie VPs zu validieren (Jolocom 2019). Darüber hinaus können semantische Datendefinitionen wie schema.org verwendet werden, um die semantische Eindeutigkeit der Identitätsdaten in einem VC herzustellen.

7 Interoperabilitätsprofil der Schaufensterprojekte

Zum Erreichen der Interoperabilitätsziele haben die Schaufensterprojekte in August 2021 damit begonnen, sich auf die gemeinsame Verwendung ausgewählter Standards und Protokolle zu einigen. Diese Standards und Protokolle bilden ein Interoperabilitätsprofil, an dem der jeweilige SSI-Stack der Schaufensterprojekte ausgerichtet werden kann. Das Interoperabilitätsprofil ist kein festes sondern ein lebendiges Profil, das noch nicht finalisiert ist. Anforderungen von Konsortien können dazu führen, dass weitere Standards und Protokolle in das Profil aufgenommen werden müssen.

Auf der technischen Vertrauensschicht die did:indy-Methode für Public DIDs unterstützt (Curran et al. 2021). Die did:indy-Methode ist eine weiterentwickelte Form der did:sov-Methode und kann DIDs aus beliebigen Indy VDRs auflösen. Außerdem werden für Pairwise-DIDs die did:keri- und did:peer-Methoden unterstützt. Die did:keri-Methode ist eine weiterentwickelte Version der did:jun-Methode, die mit der aktuellen KERI-Spezifikation (Smith et al. 2021) konform ist und vom Jolocom SDK 2.0 nativ unterstützt wird. Aries-Frameworks können die did:keri-Methode entweder durch native Implementierung oder über den DIF Universal Resolver unterstützen. Dieser kann für jede unterstützte DID-Methode DIDs auflösen (Sabadello 2017). Schließlich wird die Unterstützung der zuvor erwähnten did:key-Methode geprüft.

Im Rahmen des angestrebten Interoperabilitätsprofils werden die SSI-Stacks DIDComm V2 als Envelope unterstützen. DIDComm V2 ist eine von der DIF erarbeitete Spezifikation (Hardman 2019b), die signifikanten Änderungen zu V1 mit sich bringt. Diese Änderungen betreffen u. a. die Handhabung der Pairwise-DIDs sowie die zugrundeliegenden Verschlüsselungsalgorithmen als auch die Nachrichtenstrukturen (Hardman 2022). Ähnlich zur Ausgangssituation verwenden die Agenten zunächst ein Out-of-Band-Protokoll zum Austausch von initialen Schlüsselinformationen, um einen sicheren Kommunikationskanal aufzubauen. HTTP(s) und Websockets werden weiterhin als Transportprotokolle unterstützt.

Auf der Credentialschicht werden die Issue Credential (Khateev et al. 2021a) und Present Proof (Khateev et al. 2021b) V3 Protocols als Credential-Austauschprotokolle unterstützt. Die V3-Protokolle unterstützen DIDComm V2 als Envelope und beliebige Credentials als Anhang. Daher bieten die V3-Protokolle die Möglichkeit, mehrere Credential-Formate, wie z. B. VC und AnonCreds, zu unterstützen.

Auf der Anwendungsschicht muss aus technischer Sicht keine Ausrichtung erfolgen, da alle Anwendungen innerhalb der Schaufensterprojekte bereits die obengenannten Standards und Protokolle unterstützen werden. Zur Erreichung von semantischer Interoperabilität müssen die Credentials auf der Grundlage festgelegter Datendefinitionen ausgestellt werden. Die Datendefinitionen sind derzeit mit Zusammenarbeit aller Schaufensterprojekte erstellt.

Abb. 2 fasst die Ausrichtung der verschiedenen SSI-Stacks entsprechend den Schichten des SSI-Referenzmodells zusammen. Die Aufnahme der in Klammern genannten Bausteine in das Interoperabilitätsprofil ist derzeit in Prüfung.

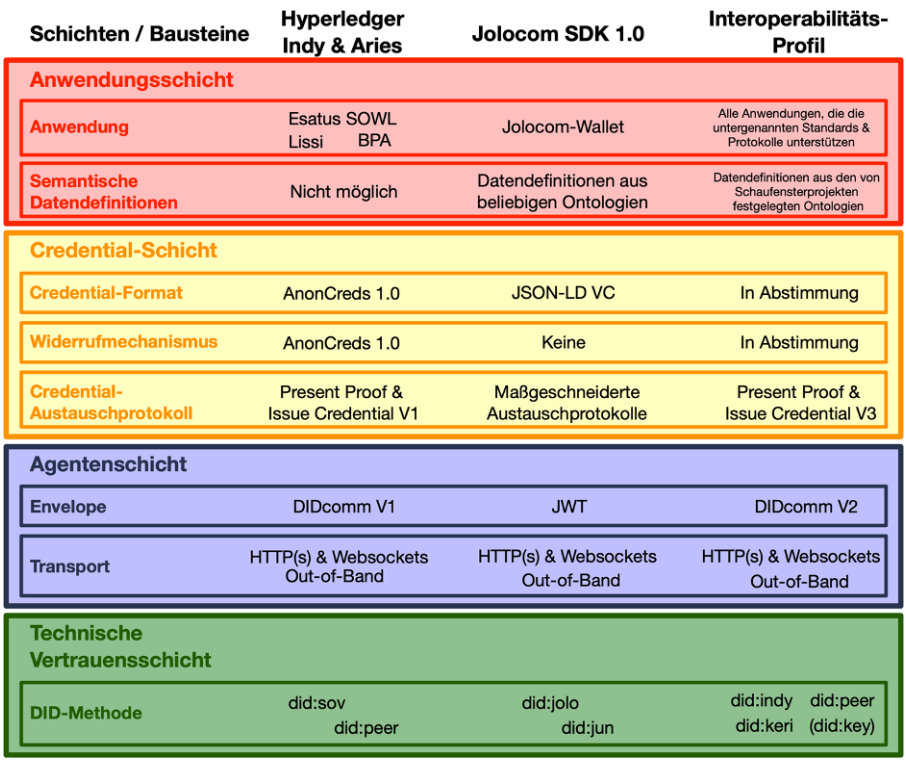

Abb. 2 Die Ausgangsituation und Ausrichtung nach dem SSI-Referenzmodell

8 Hürden der Interoperabilität

Die bedeutendste Hürde zum Erreichen der Interoperabilität ist die fehlende Ausrichtung von Credential-Formaten und deren Nachweisen. Der SSI-Stack von Hyperledger Indy und Aries unterstützt AnonCreds 1.0. Jeder andere Stack innerhalb der Schaufensterprojekte folgt dem VC nach W3C Standard. Die syntaktischen Unterschiede von AnonCreds zu VCs sind jedoch ein großes Hindernis für das Erreichen syntaktischer Interoperabilität. Sofern es zukünftig keine Kompatibilität zwischen AnonCreds und VCs geben sollte, können die Schaufensterprojekte ihre Interoperabilitätsziele nur erreichen, indem sie entweder beide Credential-Formate unterstützen oder sich auf ein einziges Format einigen.

Darüber hinaus sind die Schaufensterprojekte nicht auf einen gemeinsamen Widerrufsmechanismus abgestimmt. AnonCreds bieten einen datenschutzfreundlichen, aber nicht skalierbaren Widerrufsmechanismus. Die Schaufensterprojekte zielen darauf ab, sich auf einen einzigen Widerrufsmechanismus zu einigen, der die Privatsphäre schützt und gleichzeitig skalierbar ist. In der DIF Applied Crypto Working Group[14], in welcher auch Mitglieder der Schaufensterprojekte vertreten sind, wird aktuell an der Beseitigung dieser Hürde gearbeitet.

[14] DIF Applied Crypto Working Group: https://identity.foundation/working-groups/crypto.html.

9 Fazit

Der Digital Markets Act verlagert im geschäftlichen Kontext die Entscheidungsgewalt über digitale Identitäten von den Gatekeepern zu den Dienstanbietern. Jedoch kann echte Datensouveränität in Bezug auf digitale Identitäten nur erreicht werden, wenn die Endnutzer die Kontrolle über Ihre Identitätsdaten zurückbekommen. SSI ist der nächste naheliegende Schritt zur Verlagerung dieser Entscheidungsgewalt weg von den Dienstanbietern hin zu den Endnutzern. Für die breite Nutzung und Akzeptanz seitens Dienstanbieter und Endnutzer sind interoperable SSIs unumgänglich.

Als Ausgangsituation war Interoperabilität aufgrund der unterschiedlichen SSI-Stacks und diverser Standards und Protokolle eine Herausforderung, die national und international gelöst werden musste. Auf nationaler Ebene arbeiten die Schaufensterprojekte gemeinsam an ihren Interoperabilitätszielen, indem sie ihre jeweiligen SSI-Stacks entsprechend einem abgestimmten Interoperabilitätsprofil ausrichten. Dieses Interoperabilitätsprofil der Schaufensterprojekte bietet eine fundierte und projektübergreifende Grundlage für das Schaffen von Vertrauen zwischen den Parteien, die Kommunikation über sichere und authentifizierte Protokolle und den Austausch von Credentials. Es bestehen weiterhin Hürden der Interoperabilität aufgrund der nicht abgestimmten Credential-Formate und Widerrufsmechanismen. Positiv zu vermerken ist, dass die Credentials in den über die Austauschprotokolle gesendeten Nachrichten angehängt sind und der Widerruf unabhängig überprüft werden kann. D. h. sobald eine Abstimmung mit dem Credential-Format und Widerrufsmechanismus erfolgt, sollten die Interoperabilitätsziele der Schaufensterprojekte erreichbar sein.

Schließlich stellt das einmalige Festlegen auf ein gemeinsames Interoperabilitätsprofil jedoch keine langfristige Lösung dar. Die SSI-Landschaft verändert sich stetig und auf EU-Ebene gibt es regelmäßig neue technologische und rechtliche Entwicklungen. Es ist von entscheidender Bedeutung, an diesen Entwicklungen mitzuwirken und das Interoperabilitätsprofil regelmäßig anzupassen.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Allen C (2016) The path to self-sovereign identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. Zugegriffen: 13. Dez. 2022

Cunningham C (2020) Jolocom DID method specification. https://github.com/jolocom/jolo-did-method/blob/master/jolocom-did-method-specification.md (Erstellt: 13. Dez. 2022). Zugegriffen: 13. Dez. 2022

Curran S, Jordan J (2019) Aries interop profile. https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0302-aries-interop-profile/README.md. Zugegriffen: 13. Dez. 2022

Curran S, Bastian P, Hardman D, Howland C, Bormann C, Wörner D et al (2021) Indy DID method. https://hyperledger.github.io/indy-did-method/. Zugegriffen: 13. Dez. 2022

Curran S, Philipp A, Yildiz H, Curren S (2022) AnonCreds specification. https://hyperledger.github.io/anoncreds-spec/. Zugegriffen: 13. Dez. 2022

Davie M, Gisolfi D, Hardman D, John J, O'Donnell D, Drummond R (2019) The trust over IP stack. IEEE Commun Stand Mag 3(4):46–51. https://doi.org/10.1109/MCOMSTD.001.1900029

Deventer O, Lundkvist C, Csernai M, Hartog KD, Sabadello M, Curren S et al (2021) Peer DID method specification. https://identity.foundation/peer-did-method-spec/. Zugegriffen: 13. Dez. 2022

European Commission (2020) Regulation of the European parliament and of the council on contestable and fair markets in the digital sector (digital markets act). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:842:FIN. Zugegriffen: 13. Dez. 2022

Hardman D (2018) Aries RFC 0005: DID communication. https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0005-didcomm/README.md. Zugegriffen: 13. Dez. 2022

Hardman D (2019a) Aries RFC 0046: mediators and relays. https://github.com/hyperledger/aries-rfcs/tree/main/concepts/0046-mediators-and-relays. Zugegriffen: 13. Dez. 2022

Hardman D (2019b) DIDComm messaging. Decentralized identity foundation. https://identity.foundation/didcomm-messaging/spec/. Zugegriffen: 13. Dez. 2022

Hardman D (2022) DIDComm v2: What's new? https://github.com/decentralized-identity/didcomm.org/blob/main/site/content/book/v2/whatsnew.md. Zugegriffen: 13. Dez. 2022

Jolocom (2019) Jolocom (2019): a decentralized, open source solution for digital identity and access management, white paper. https://jolocom.io/wp-content/uploads/2019/12/Jolocom-Whitepaper-v2.1-A-Decentralized-Open-Source-Solution-for-Digital-Identity-and-Access-Management.pdf. Zugegriffen: 13. Dez. 2022

Khateev N (2019a) Aries RFC 0036: issue credential protocol 1.0. https://github.com/hyperledger/aries-rfcs/tree/main/features/0036-issue-credential. Zugegriffen: 13. Dez. 2022

Khateev N (2019b) Aries RFC 0037: present proof protocol 1.0. https://github.com/hyperledger/aries-rfcs/tree/main/features/0037-present-proof. Zugegriffen: 13. Dez. 2022

Khateev N, Curran S, Curren S, Quadras R (2021a) Issue credential protocol 3.0. https://github.com/decentralized-identity/waci-presentation-exchange/tree/main/issue_credential. Zugegriffen: 13. Dez. 2022

Khateev N, Curran S, Curren S (2021b) Present proof protocol 3.0. https://github.com/decentralized-identity/waci-presentation-exchange/blob/main/present_proof/present-proof-v3.md. Zugegriffen: 13. Dez. 2022

Nitin N, Jenkins P (2021) Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology. In: 2021 IEEE International Symposium on Systems Engineering (ISSE), S 1–7

Palfrey J, Gasser U (2012) Interop: the promise and perils of highly interconnected systems. Basic Books, New York

Rusu E (2021) Jolocom SDK. https://github.com/jolocom/jolocom-sdk. Zugegriffen: 13. Dez. 2022

Rusu E (2022) Jolocom SDK 1.0 Stack, 2022 an Hakan Yildiz. Eigenes Gesprächsprotokoll

Sabadello M (2017) A Universal Resolver for self-sovereign identifiers. In: Decentralized Identity Foundation, 2017. https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c. Zugegriffen: 13. Dez. 2022

Smith SM (2019) Key event receipt infrastructure (KERI) (arXiv preprint arXiv:1907.02143)

Smith S, Cunningham C, Feairheller P (2021) The did:keri method v0.1. https://identity.foundation/keri/did_methods/. Zugegriffen: 13. Dez. 2022

Sporny M, Longley D, Kellogg G, Lanthaler M, Lindström N (2014) JSON-LD 1.0. W3C recommendation, Bd. 16, S 41

Sporny M, Longley D, Davig C (2022a) Verifiable credentials data model v1.1. W3C recommendation. W3C. https://www.w3.org/TR/vc-data-model/. Zugegriffen: 13. Dez. 2022

Sporny M, Longley D, Reed D, Sabadello M, Steele O, Allen C (2022b) Decentralized identifiers (DIDs) v1.0. W3C recommendation. W3C. https://www.w3.org/TR/did-core/. Zugegriffen: 13. Dez. 2022

Sporny M, Zagidulin D, Longley D, Steele O (2022c) The did:key method v0.7. https://w3c-ccg.github.io/did-method-key/. Zugegriffen: 13. Dez. 2022

van der Veer H, Wiles A (2008) Achieving Technical Interoperability. European Telecommunications Standards Institute

Vernadat FB (2010) Technical, semantic and organizational issues of enterprise interoperability and networking. Annu Rev Control 34(1):139–144. https://doi.org/10.1016/j.arcontrol.2010.02.009

West R, Bluhm D, Hailstone M, Curran S, Curren S, Aristy G (2019) Aries RFC 0434: out-of-band protocol 1.1

Wittek K, Lazzati L, Bothe D, Sinnaeve A-J, Pohlmann N (2020) An SSI based system for Incentivized and selfdetermined customer-to-business data sharing in a local economy context. In: 2020 IEEE European Technology and Engineering Management Summit (E-TEMS), S 1–5

Yildiz H, Küpper A, Thatmann D, Göndör S, Herbke P (2022) A tutorial on the interoperability of self-sovereign identities (arXiv preprint arXiv:2208.04692)

Young K (2022) Verifiable credentials flavors explained. https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf. Zugegriffen: 13. Dez. 2022