HMD Praxis der Wirtschaftsinformatik
https://doi.org/10.1365/s40702-023-00948-2

SCHWERPUNKT

Auf der Suche nach ökonomisch tragfähigen Identitäts-Ökosystemen: Gibt es einen Markt für digitale IDs?

Michael Kubach · Heiko Roßnagel

Eingegangen: 25. September 2022 / Angenommen: 31. Januar 2023
© Der/die Autor(en) 2023

Zusammenfassung Die Unzufriedenheit mit bestehenden digitalen Identitätslösungen ist groß. Insbesondere Politik und Wirtschaft drängen auf die Entwicklung neuer Identitäts-Ökosysteme. Anstatt auf Defizite in Usability, Security und Datenschutz bestehender Lösungen zu fokussieren, nimmt diese Arbeit die für die Verbreitung von digitalen Identitätsmanagementlösungen ebenso bedeutsamen ökonomischen Aspekte in den Blick. Es wird analysiert, wie ID-Ökosysteme ökonomisch tragfähig aufgebaut und betrieben werden könnten, was entsprechend eine Zahlungs- oder Investitionsbereitschaft von irgendeiner Seite erfordert. Die Analyse wird über eine Betrachtung der Endnutzer-Anreize zur Adoption hinaus über die weiteren Ökosystemteilnehmer insbesondere auf die Serviceprovider erweitert, da bei diesen am Ehesten eine Zahlungsbereitschaft für ID-Services erwartbar ist. Somit stellt sich die Frage, ob und unter welchen Rahmenbedingungen ein Markt für digitale Identitäten entstehen kann und welche Einführungsstrategien – unter Beteiligung der öffentlichen Hand – bestehen.

Schlüsselwörter Digitale Identitäten · EID · Geschäftsmodelle · Digitale Ökosysteme · SSI · Adoption

✉ Michael Kubach · Heiko Roßnagel
Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, Nobelstraße 12, 70569 Stuttgart, Deutschland
E-Mail: michael.kubach@iao.fraunhofer.de

Heiko Roßnagel
E-Mail: heiko.rossnagel@iao.fraunhofer.de

Published online: 27 February 2023

In Search of Economically Viable Identity Ecosystems: Is there a Market for Digital IDs?

Abstract There is great dissatisfaction with existing digital identity solutions. Politics and business in particular are pushing for the development of new identity ecosystems. Instead of focusing on deficits in usability, security and data protection of existing solutions, this paper takes a look at the economic aspects that are just as important for the spread of digital identity management solutions. It analyzes how ID ecosystems could be set up and operated in an economically viable manner, which accordingly requires a willingness to pay or invest from some side. The analysis is extended beyond a consideration of end-user incentives for adoption to include the other ecosystem participants and, in particular, service providers, since these are the ones most likely to be willing to pay for ID services. This raises the question of whether and under what conditions a market for digital identities can emerge and what introduction strategies exist—with the involvement of the public sector.

Keywords Digital identities · EID · Business models · Digital ecosystems · SSI · Adoption

1 Einleitung

Technisch leistungsfähige und privatsphärenfreundliche Lösungen für digitale Identitäten (IDs) existieren bereits seit geraumer Zeit. Auf Public Key Infrastrukturen (PKIs) basierende Lösungen sind etabliert sowie leistungsfähig und mittels Attribute-based Credentials lassen sich höchste Ansprüche an den Privatsphärenschutz realisieren (Rannenberg et al. 2015). Der Personalausweis mit Online-Ausweisfunktion ist in der Bevölkerung inzwischen weit verbreitet und mit der NFC-Schnittstelle aktueller Smartphones nutzbar.[1] Die Entwicklung von privatsphärenfreundlichen Identitätsmanagementverfahren und Attribute-based Credentials wurden auch von großen IT-Konzernen wie Microsoft (Cardspace, U-Prove (Microsoft 2009, 2014)) und IBM (Camenisch and Herreweghen 2002) unterstützt. Mit der europäischen eIDAS Regulierung (Verordnung (EU) Nr. 910/2014, in Kraft seit 2014, geltend seit 2016) und dem Vertrauensdienstegesetz (VDG, in Kraft seit 2017) existiert ein etablierter rechtlicher Rahmen für privatsphärenfreundliche und sichere digitale Identitäten. Dennoch wird ein Mangel an weit verbreiteten, sicheren, interoperablen und einfach nutzbaren digitalen Identitäten erkannt. Dies gilt als große Hürde für die Digitalisierung öffentlicher und privatwirtschaftlicher organisatorischer Prozesse in Deutschland wie Europa (BMWi 2021; European Commission 2022), und mit der Entwicklung entsprechender Lösungen wird ein großes Entwicklungspotenzial

[1] Der „neue Personalausweis“ wurde 2010 eingeführt. Personalausweise ohne technische Fähigkeit zur Online-Ausweisfunktion sind seit Ende 2020 ungültig. Bei seit 2017 ausgegebenen Ausweisen ist sie standardmäßig aktiviert, seit 2022 lässt sie sich online nachträglich aktivieren. Jedoch haben sie bislang nur 9 % aller Personalausweisinhaber genutzt (Initiative D21 e. V. 2021).

für gesamte Volkswirtschaften (White et al. 2019) und ein entsprechend bedeutendes Wachstumspotenzial für den Identitätsmanagement-Markt (MarketsandMarkets 2021) verbunden.

Tatsächlich werden digitale Identitäten aber bereits tagtäglich vom Großteil der Bevölkerung genutzt, beispielsweise für Onlineshopping und Onlinebanking (Tenner und Mietke 2021). In der breiten praktischen Nutzung dominieren jedoch derzeit ID-Silos und föderierte IDs amerikanischer IT-Konzerne (Facebook-Login, Google-Login, Apple-ID, Amazon Account). Trotz oder auch gerade wegen ihrer weiten Verbreitung bei Endnutzern und Serviceprovidern stehen diese Plattform-IDs allerdings in der Kritik. Einerseits ergibt sich diese Kritik aus einer Privatsphärenschutz und IT-Sicherheitsperspektive. Diese Identitätsprovider verfügen über die Möglichkeit das Anmeldeverhalten ihrer Nutzer zu tracken und die Daten für ihre Zwecke weiterzuverwenden. Diese anfallenden Informationen sind darüber hinaus auch für potenzielle Angreifer interessant (Toth und Anderson-Priddy 2019; Schardong und Custódio 2022). Andererseits werden sie angesichts ihres breiten Erfolgs bei den Nutzern wie auch Serviceprovidern, also ihrer Marktmacht, und zentralen Position in der digitalen Wertschöpfungskette auch zunehmend als Bedrohung der digitalen Souveränität Deutschlands bzw. Europas angesehen (Ehrlich et al. 2021). Bei höheren Sicherheitsanforderungen kommen verbreitet Verfahren wie Video-Ident zum Einsatz, deren Sicherheit jedoch umstritten und Nutzerfreundlichkeit eingeschränkt ist (Tschirsich 2022; Pohlmann 2022).

Angesichts dieser Herausforderungen erhielten in den letzten 3–5 Jahren neue Ansätze, zunächst basierend auf Blockchain und Distributed-Ledger-Technologien (DLT), im Laufe der Zeit dann stärker unter dem Begriff Self-sovereign Identities (SSI), viel Aufmerksamkeit. Sie versprechen ein neues Paradigma für digitale Identitäten und die dargelegte „identity crisis“ (Toth und Anderson-Priddy 2019, S. 19) zu lösen, indem sie die Nutzer und den Schutz ihrer Daten in den Mittelpunkt stellen. Entsprechend erarbeitet die Europäische Kommission derzeit die eIDAS 2.0 Verordnung mit EU Digital Identity Wallets[2] und die Bundesregierung fördert mehrere Projekte zu selbstsouveränen Identitäten (SSI; im Rahmen des Schaufenster Sichere digitale Identitäten und des Ökosystems Digitale Identitäten[3]) sowie zur Speicherung und Nutzung von Personalausweisdaten auf dem Smartphone (Smart-eID)[4]. Zudem sind zahllose weitere Startups, Projekte und Initiativen, wie auch IT-Großkonzerne, in diesem Feld aktiv – ein Überblick findet sich etwa bei Kubach und Sellung (2021) sowie Soltani et al. (2021). Aber auch diese Ansätze stehen vor der Herausforderung sich am Markt etablieren zu müssen. Das bedeutet, sie müssen sich gegenüber den bereits etablierten Technologien durchsetzen und ökonomisch tragfähige Ökosysteme[5] aufbauen. Dies ist bisher noch nicht geschehen.

[2] https://digital-strategy.ec.europa.eu/en/funding/european-digital-identity-wallet.

[3] https://digitale-identitaeten.de/.

[4] https://www.personalausweisportal.de/.

[5] Das Werteversprechen eines ID-System kann nicht von einem einzigen Unternehmen erreicht werden, sondern ergibt sich erst im Zusammenspiel mehrerer Organisationen sowie Nutzer in einem Ökosystem und entspricht damit etwa der Charakterisierung eines *innovation ecosystem* bei Talmar et al. (2020).

Anstatt nun weiter auf potenzielle Defizite in Benutzbarkeit, Sicherheit und Datenschutz bestehender Lösungen zu fokussieren und potenzielle technische Lösungsarchitekturen zu diskutieren, nimmt diese Arbeit daher im Folgenden die für die Verbreitung von digitalen Identitätsmanagementlösungen ebenso bedeutsamen ökonomischen Aspekte in den Blick. Hierzu werden zunächst in Kapitel zwei die wesentlichen Grundlagen zu Adoption von ID-Lösungen und für den Betrieb eines ID-Ökosystems betrachtet. In Kapitel drei werden dann Wertschöpfungsketten für ID-Lösungen analysiert. Hierzu greift die vorliegende Arbeit auch auf die Ergebnisse einer qualitativen Befragung von 23 Serviceprovidern zurück. Auf diese Elemente aufbauend werden im vierten Kapitel Strategien zum Aufbau ökonomisch tragfähiger ID-Ökosysteme diskutiert.

Der vorliegende Beitrag erweitert damit den Blick auf digitale Identitäten von einer funktional-technischen Perspektive mit starker Betonung auf Sicherheit und Privatsphäre um Betrachtung der ökonomischen Erfolgsfaktoren. Hierbei wird der Begriff der digitalen Identitäten, im Folgenden digitale IDs, bewusst weit gefasst und schließt Identitätsdaten und sonstige geprüfte und ungeprüfte Nachweise und Attributzertifikate ein. Der Beitrag versucht die Frage zu beantworten, wie ein ökonomisch tragfähiges Identitäts-Ökosystem entstehen kann und ob dieses derzeit oder in absehbarer Zeit auf einem Markt für digitale IDs aufbauen kann. Der Beitrag basiert auf etablierten theoretischen Konzepten wie die Diffusions- und Adoptionstheorie und empirischen Ergebnissen einer qualitativen Befragung. Entwickler von Identitätsmanagementlösungen, wie auch (potenzielle) Anwender und politische Entscheidungsträger, erhalten somit eine ganzheitlichere, theoretisch wie empirisch gestützte Basis für ihre Investitions- und Gestaltungsentscheidungen hinsichtlich digitaler Identitäten als grundlegender Digitalisierungstechnologie.

2 Grundsätzliche Marktstruktur für digitale IDs

Damit die derzeit in Entwicklung befindlichen ID-Technologien ihre in der Einleitung skizzierten Versprechungen einlösen und die digitale Souveränität von Bürgern und europäischer Wirtschaft tatsächlich sichern können, müssen Sie eine signifikante Verbreitung in der Anwendung erreichen. Wenn diese Verbreitung nicht staatlich verordnet, sondern über Marktmechanismen erreicht werden soll, sind die spezifische Struktur und Dynamiken des Marktes für digitale IDs zu betrachten.

Wie bereits für föderiertes Identitäten (Zibuschka und Roßnagel 2012) und SSI (Kubach und Sellung 2021) gezeigt wurde, entsteht eine besondere Herausforderung beim Markteintritt von ID-Lösungen daraus, dass es sich hierbei um einen mehrseitigen Markt mit Netzwerkeffekten handelt. Ein solcher Markt bedient mindestens zwei verschiedene Arten von Kunden, die in wesentlicher Weise voneinander abhängig sind (Evans 2003). So besteht ein ID-Ökosystem zumindest aus Nutzern und Serviceprovidern. Als Serviceprovider werden in diesem Kontext Organisationen bezeichnet, die digitale IDs zur Erbringung ihrer Dienstleistungen voraussetzen. Nutzer übermitteln den Serviceprovidern digitale IDs, um die Dienstleistungen in Anspruch nehmen zu können. Hierzu kommen weitere Ökosystemteilnehmer und Stakeholder (ID-Provider, Credential Issuer, Vertrauensdiensteanbieter, Technologie-

anbieter, Standardisierungsgremien, staatliche Akteure, ...), die sich gegebenenfalls je nach ID-Lösung und Rahmenbedingungen unterscheiden. Dass der Nutzen für die eine Gruppe der Teilnehmer des ID-Ökosystems von der Nutzung durch die andere Gruppe abhängt (die jeweils andere Seite des mehrseitigen Marktes), führt zu Netzeffekten mit positiver Rückkopplung: Wenn mehr Serviceprovider eine ID-Lösung einführen, steigt dessen Attraktivität für Nutzer und umgekehrt.

Hinsichtlich der Adoption ergibt sich somit ein *Henne-Ei-Problem*: Ein ID-Ökosystem mit wenigen Serviceprovidern ist für Nutzer nicht attraktiv, auch wenn sie über die grundsätzlichen Möglichkeiten zur Nutzung verfügen. Sie gehen keine (immateriellen) Investitionen ein: lernen keine neuen Interaktionsmuster, laden keine besondere Software herunter oder beschaffen gar neue Hardware.[6]

Wenn umgekehrt eine bestimmte ID-Lösung über kaum Nutzer verfügt, ist der Anreiz für Serviceprovider die Investitionsrisiken zu ihrer Implementierung einzugehen sehr gering. Schließlich erreichen sie über diese ID-Lösung kaum Nutzer, was eine Amortisation der erforderlichen Investitionen für Einrichtung und Betrieb unwahrscheinlich macht. Ein tragfähiges ID-Ökosystem erfordert also eine bei Nutzern weit verbreitete ID-Lösung, die von einer Vielzahl von Dienstanbietern unterstützt wird. Aufgrund der Netzwerkeffekte ist die initiale Hürde zur Schaffung eines solchen Ökosystems jedoch hoch. Verschiedene Strategien sind grundsätzlich anwendbar, um die Hürde zu überwinden und schließlich über positive Rückkopplungseffekte ein rasches Wachstum des Ökosystems zu erreichen.

Wie bereits oben dargestellt, besteht ein ID-Ökosystem jedoch auch nicht nur aus Nutzern und Serviceprovidern. Entsprechend ist nicht lediglich die Nutzenbeziehung zwischen diesen beiden Akteuren zu betrachten, sondern darüber hinaus zu erweitern. Die ID-Technologie/-Komponenten und zugehörige Services werden von weiteren Ökosystemteilnehmern entwickelt und bereitgestellt. Im Falle eines klassischen „zentralisierten" ID-Ökosystems mit einem einzelnen ID-Provider, der auch die notwendigen Komponenten für Nutzer und Serviceprovider bereitstellt, ergibt sich somit eine Dreiecksbeziehung (Nutzer – Serviceprovider – ID-Provider), wie von Zibuschka und Roßnagel (2012) dargestellt. In dezentralisierten ID-Ökosystemen entwickeln dagegen verschiedene Akteure Komponenten (z. B. Wallets, Agents), stellen diese zur Verfügung und übernehmen bestimmte operative Funktionen (etwa Vertrauensdienste). Ein durchschnittlich interessierter Nutzer oder auch ein kleiner Serviceprovider mit geringen IT-Ressourcen wird jedoch vermutlich auch hier annehmen, es mit einem für ihn monolithischen ID-System zu tun zu haben (z. B. einer bestimmten SSI Wallet von Hersteller X, die stellvertretend für das ganze System sichtbar ist) – auch wenn dieses System an sich aus verschiedenen Akteuren besteht. Die vereinfachte Betrachtung einer Dreiecksbeziehung (Nutzer – Serviceprovider – ID-System) erscheint darum an dieser Stelle für vertretbar.

Die Beziehungen zwischen Nutzern und ID-System sowie zwischen Serviceprovidern und ID-System sind wesentlich von Vertrauen abhängig. Nutzer sind möglicherweise eher nicht bereit, den Umgang mit ihren persönlichen Identitätsdaten an ein ID-System zu delegieren, wenn sie diesem (bzw. der dahinterliegenden Tech-

[6] Ein prägnantes Beispiel hierfür stellt der Personalausweis mit Online-Ausweisfunktion dar. Er ist weit verbreitet, jedoch kaum praktisch nutzbar.

nologie und den einzelnen Akteuren) nicht zutrauen diese Daten in ihrem Sinne zu verwalten bzw. zu schützen. Ein Serviceprovider muss darauf vertrauen können, dass ein ID-System zuverlässig Daten in benötigter Qualität liefert,[7] wobei regulierte Vertrauensniveaus, etwa nach eIDAS, nur für manche Anwendungsfälle von Relevanz sind. Dementsprechend fokussieren Forschung und Entwicklung zu digitalen Identitäten stark auf Sicherheit und Datenschutz entsprechender Lösungen.[8] Dennoch sind hier ebenso ökonomische Aspekte zu betrachten. Die verschiedenen Akteure des ID-Systems erwarten selbstverständlich eine Entlohnung für ihre erbrachten Dienstleistungen von irgendeiner Seite – sie haben schließlich Kosten zu decken. Eine entsprechende Entlohnung könnte über eine Zahlungsbereitschaft bestimmter Marktteilnehmer realisiert werden. So könnten prinzipiell sowohl Nutzer als auch Serviceprovider kommerzielle ID-Dienstleistungen in Anspruch nehmen und auch bezahlen. Serviceprovider bezahlen zum Beispiel für die aktuell gängigen Video-Ident-Verfahren. Auch Nutzer sind unter Umständen bereit für bestimmte Formen von Identitäten (wie z. B. Kreditkarten) eine Gebühr zu entrichten. Allerdings müssten diese Dienstleistungen dann auch einen entsprechenden Mehrwert gegenüber den bisher am Markt etablierten Systemen liefern, die zu großen Teilen kostenlos angeboten werden. Inwieweit das gelingen kann, wird im nächsten Kapitel näher betrachtet.

3 Analyse der Wertschöpfungsketten von ID-Ökosystemen

Nachdem der Markt für digitale IDs im vorangegangenen Kapitel auf theoretischer und konzeptioneller Basis analysiert wurden, soll im Folgenden konkret untersucht werden, wie ID-Ökosysteme Werte generieren um auf diesen Überlegungen aufbauend schließlich im nachfolgenden Kapitel Strategien für den Aufbau ökonomisch tragfähiger ID-Ökosysteme entwickeln zu können.

3.1 Konzeptioneller Rahmen der Analyse

Für die Analyse der Wertschöpfungskette erfolgt eine Orientierung an Talmar et al. (2020). Mit dem Ecosystem Pie Model (EPM) liefern sie ein Tool, das unter anderem zur Analyse der Werterfassung und der Beziehungen in Innovationsökosystemen genutzt werden kann. Ein Innovationsökosystem zeichnet sich nach Talmar et al. (2020) dadurch aus, dass ein einzelnes Unternehmen nicht über die Ressourcen verfügt, um ein komplexes Nutzenversprechen von Anfang bis Ende zu entwickeln und zu vermarkten. Unternehmen stützen sich darum auf andere Akteure in ihrem Innovationsökosystem, um ein gemeinsames Nutzenversprechen für das Ökosystem aufzubauen. Da dies, wie oben in den Ausführungen zum mehrseitigen Markt dargestellt, offensichtlich auch auf ID-Ökosysteme zutrifft, erscheint das EPM als

[7] Nutzer und Serviceprovider müssen darüber hinaus darauf vertrauen können, dass das ID-System zuverlässig dann funktioniert, wenn sie es benötigen.

[8] Das Schaufensterprogramm des BMWK ist nicht zufällig „Sichere digitale Identitäten“ benannt und nicht etwa „Einfach nutzbare digitale Identitäten“.

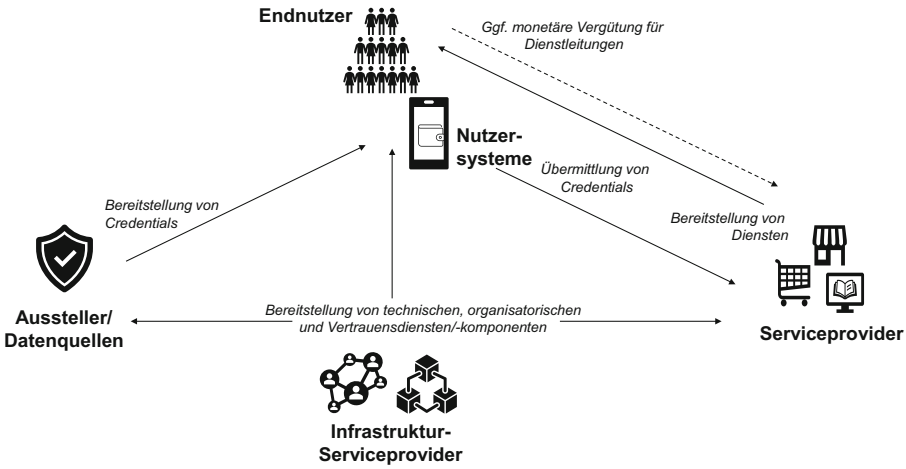

Abb. 1 Überblick über die Akteure in einem ID-Ökosystem

geeignet für die Analyse von Wertschöpfungsketten von ID-Lösungen. Anzumerken ist hierbei, dass Talmar et al. lediglich von Akteuren sprechen und keine Unterscheidung zwischen Akteuren als Organisationen und möglichen unterschiedlichen eingenommenen Rollen derselben Organisationen in einem Ökosystem vornehmen. Es ist darum klarzustellen, dass im Folgenden mit Talmar et al. von Akteuren gesprochen wird. Es wird hiermit jedoch auf die jeweiligen Rollen der Organisationen beziehungsweise Akteure im Ökosystem abgezielt.

Für das EPM identifizieren Talmar et al. (2020) drei Konstrukte auf Ökosystemlevel (1. Werteversprechen, 2. Nutzersegmente, 3. Akteure) und sechs auf Akteurslevel (1. Ressourcen, 2. Aktivitäten, 3. Wertschöpfung, 4. Werterfassung, 5. Risiko, 6. Abhängigkeiten). Für das den Rahmen dieser Untersuchung setzende Forschungsprojekt[9] wurden das ID-Ökosystem modelliert und die Konstrukte diesbezüglich analysiert.

Aufgrund des begrenzten Raumes muss an dieser Stelle eine Fokussierung auf das Konstrukt der Werterfassung auf dem Akteurslevel erfolgen. Während das Ökosystem durch Interaktionen Werte für die Endnutzer schafft, strebt jeder Ökosystemakteur nach individuellen Vorteilen und muss sich diese auch aneignen können (Teece 1986). Das Konstrukt Werterfassung stellt dar, wie, welche Art und wie viel vom Ökosystem geschaffener Wert von einem Akteur erfasst wird – eine der Hauptmotivationen zum Anschluss an ein Ökosystem. Darüber hinaus erwarten Akteure, dass sie einen fairen Anteil des geschaffenen Wertes erhalten. Der Wert muss dabei nicht zwingend monetärer Natur sein, wenn eine Ökosystem-externe Monetarisierung (z. B. von Reputation, Wachstum, Wissen) möglich ist (Talmar et al. 2020). Die Fokussierung auf das Konstrukt Werterfassung als eine der Hauptmotivationen für den Beitritt in ein Ökosystem erscheint damit an dieser Stelle als vertretbar.

[9] Das durch das Bundesministerium für Wirtschaft und Klimaschutz geförderte Projekt ONCE (www.once-identity.de).

Im Folgenden werden die Akteure[10] eines beispielhaften ID-Ökosystems hinsichtlich ihrer Möglichkeit zur Werterfassung betrachtet. Als relevante Akteure wurden identifiziert (siehe auch Abb. 1): (1) *Aussteller und Datenquellen* für digitale IDs, (2) *Serviceprovider*, die digitale IDs für ihre Diensteerbringung nutzen, (3) *Infrastruktur-Serviceprovider*, welche Infrastrukturdienste für das ID-Ökosystem entwickeln, bereitstellen und administrieren (z. B. technische Middlewares/Gateways in das ID-Ökosystem, Vertrauensinfrastrukturen, ID-Lifecycle Dienste), beziehungsweise das gesamte Ökosystem steuern und nach außen vertreten, (4) *Endnutzer* bzw. Bürger und zuletzt (5) *Nutzersysteme* (diese Arbeit fokussiert auf ID-Systeme, die vom Endnutzer mittels einer Smartphone Wallet Applikation genutzt werden), mit welchen die Endnutzer ihre Digitale IDs verwalten und nutzen um über das ID-Ökosystem Zugang zu gewünschten Diensten zu erhalten.

3.2 Empirische Grundlage der Analyse

Die folgenden Analysen basieren auf der Auswertung von qualitativen Interviews mit 23 Organisationen. Diese könnten als Aussteller und Datenquellen, Serviceprovider und in Teilaufgaben auch als Infrastruktur-Serviceprovider in ID-Ökosystemen auftreten. Das Sample besteht aus acht Städten, vier weiteren Organisationen aus der öffentlichen Verwaltung (z. B. auf Bundeslandebene), drei IT-Serviceprovidern mit Fokus auf die öffentliche Verwaltung, vier Organisationen aus dem Mobilitätssektor und vier Unternehmen aus dem Hotel- und Tourismussektor. Die Rekrutierung der Befragten erfolgte im Kontext eines Forschungsprojektes zu sicheren digitalen Identitäten und stellt somit keine Zufallsstichprobe dar. Ziel war die Bildung eines heterogenen Samples. Dieses sollte Organisationen in verschiedenen Sektoren mit zumindest ersten Erfahrungen mit digitalen Identitäten und unterschiedlichen Sicherheits- bzw. Vertrauensanforderungen umfassen, um einen umfassenden Einblick in die Thematik zu erhalten. Die qualitative Vorgehensweise wurde insbesondere auch gewählt, um die relativ neuen und sich dynamisch entwickelnden Konzepte ausführlich erläutern und gegebenenfalls Rückfragen stellen zu können.

Die leitfadengestützten Gespräche wurden von September bis November 2021 als Videocalls durchgeführt und aufgezeichnet (nach Einholung der Zustimmung der befragten Personen). Anschließend wurden sie transkribiert und mit MAXQDA codiert sowie ausgewertet. Der umfangreiche Leitfaden umfasste Abschnitte zum aktuellen Stand der Nutzung digitaler Identitäten bei den Organisationen, Treibern und Hürden für den Einsatz digitaler Identitäten sowie zu Eckdaten der Organisationen und Interviewten. Der vorliegende Artikel fokussiert insofern nur auf einen Aspekt dieser Befragung – eine umfassende Darstellung der gesamten Ergebnisse erfolgt in einer separaten Publikation. Die Gespräche dauerten zwischen 30 und 90 min. Die Befragten haben in den jeweiligen Organisationen unterschiedliche Positionen inne, vom Geschäftsführer bis zum Experten für Identitätsmanagement. Entscheidend ist nicht die konkrete Position der jeweiligen Person, sondern dass die Befragten ihre Organisationen und die relevanten Tätigkeitbereiche ausreichend gut kennen, was

[10] Wie oben dargestellt kann eine einzelne Organisation im Ökosystem gleichzeitig unterschiedliche Akteure darstellen.

Tab. 1 Befragte und Organisationen

#	Position der Befragten	Organisation
1	Berater/in	Entwickler/Betreiber Mobilitätsplattform
2	Product Owner Dezentrale Services	Entwickler/Hersteller von Hard- und Software im Mobilitätskontext
3	IT-Projekt Manager/in	Stadt
4	Leiter/in operative IT	Regionales Verkehrsunternehmen
5	Inhaber/in und Geschäftsführer/in	Hotel
6	Strategische/r Projektmanager/in zum CEO	IT-Serviceanbieter Mobilitätskontext
7	Projektleitung/Strategische Entwicklung Verwaltung der Zukunft	Stadt
8	Projektleitung Digitalisierung in der Stabstelle des Chief Digital Officer	Landkreis
9	Stabsstelle Innovation und Technologietransfer	IT-Serviceanbieter für die öffentliche Verwaltung
10	Stellvertretende/r Geschäftsführer/in	Regionaler Tourismusverband
11	Gruppen-Manager/in	Hotelgruppe
12	Geschäftsführer/in	Regionaler Tourismusverband
13	Stellvertretende/r Abteilungsleiter/in; Projekt Digitalisierung	Stadt
14	Leitung IT-Abteilung	Stadt
15	Verantwortliche/r Digitalisierung	Stadt
16	Zentrales Prozess- und Projektmanagement: Transformation	Stadt
17	Abteilungsleitung eGovernment	Stadt
18	Leitende Verantwortung Digitalisierung und eGovernment	Metropolregion
19	Stabstelle des Vorstandes	IT-Serviceanbieter für die öffentliche Verwaltung
20	Beauftragte/r für eGovernment	Stadt
21	Prokurist/in	IT-Serviceanbieter für die öffentliche Verwaltung
22	Referent Referat OZG-Umsetzung	Ministerium für Infrastruktur und Digitales Bundesland
23	Referent eGovernment, Open Government und Verwaltungsmodernisierung	Innenministerium Bundesland

sie zu Experten für ihre Organisation (Key Informants) macht (Homburg et al. 2012). Tab. 1 gibt einen Überblick über die Befragten und die Organisationen.

3.3 Ergebnisse der Analyse

(1) Bei *Ausstellern und Datenquellen* für digitale IDs ist zwischen staatlichen Einrichtungen, beispielsweise kommunalen Verwaltungen, und privatwirtschaftlichen Ausstellern zu unterscheiden. Das Handeln der öffentlichen Verwaltung und somit ob und an wen diese bestimmte digitale IDs ausstellen, richtet sich grundsätzlichen nach den Vorgaben des Gesetzgebers. Die Möglichkeit zur Werterfassung tritt inso-

fern als Grund zum Beitritt in das ID-Ökosystem in den Hintergrund. Eine politische Entscheidung bzw. gesetzliche Grundlagen könnten also dazu führen, dass staatliche Aussteller dazu verpflichtet werden, Digitale IDs für ein bestimmtes ID-Ökosystem auszugeben, um etwa Digitalisierungsprozesse zu fördern. Für privatwirtschaftliche Aussteller und Datenquellen muss sich dagegen ein direkter Mehrwert aus dem Beitritt zum Ökosystem ergeben. Dieser muss die Kosten für den Beitritt (Investitionen etwa für Prozessänderungen, neue Software beziehungsweise -anpassungen) und die Ausstellung der digitalen IDs, gegebenenfalls auch für Gewährleistung für Korrektheit der ID-Daten aufwiegen. Ein Mechanismus der Werterfassung für die Ausstellung von digitalen IDs ist jedoch nicht ersichtlich. Eine Zahlungsbereitschaft von Endkunden für sichere IDs ist nicht absehbar (Roßnagel et al. 2014). Die Vergütung der ursprünglichen Aussteller für den Einsatz von digitalen IDs bei dritten Serviceprovidern würde eine Erfassung jeder Verwendung dieser digitalen IDs erfordern. Dies würde die die Privatsphäre des Nutzers verletzen und somit auch einen wesentlichen Grundgedanken von SSI. In einem SSI Ökosystem wäre dies somit nicht möglich.[11] Darüber hinaus scheint nur eine sehr begrenzte Zahlungsbereitschaft bei Serviceprovidern vorhanden zu sein. Daher erscheint diese Monetarisierungsoption nicht geeignet. Entsprechend ergibt sich für Aussteller und Datenquellen nur eine mögliche Erfassung immaterieller Werte. Einen solchen Wert könnte die Möglichkeit zur Nutzung der ID-Daten für eigenen Dienste darstellen, über welche schließlich eine Werterfassung (dann in der Rolle als Serviceprovider, siehe nächster Punkt) möglich ist.

(2) Wie zuvor ist bei *Serviceprovidern* grundsätzlich zwischen staatlichen und privatwirtschaftlichen Akteuren zu unterscheiden. Staatliche Serviceprovider folgen den politischen beziehungsweise rechtlichen Vorgaben. Für diese sind potenzielle Effizienzgewinne durch die Digitalisierung von Verwaltungsprozessen, welche durch ein funktionierendes ID-Ökosystem ermöglicht werden können, als Mechanismus der Werterfassung relevant. In den Interviews geben jedoch einige Kommunen an, dass sie sich angesichts der angespannten Haushaltslage nicht in der Lage sehen, hierfür zu bezahlen. Auch für privatwirtschaftliche Serviceprovider sind Effizienzsteigerungen durch die Digitalisierung von Prozessen attraktiv. Darüber hinaus bietet sich die Chance auf Umsatzsteigerungen durch die Möglichkeit zum Angebot neuer digitaler Produkte und Services, die Senkung von Kosten im Gegensatz zu alternativen Identifizierungsverfahren (PostIdent, VideoIdent – sofern ein entsprechendes Vertrauensniveau erforderlich ist), die Senkung von Prozesskosten durch Vermeidung von Betrug und fehlerhaften Angaben und zuletzt Umsatzsteigerung durch ein schnelleres Onboarding von Kunden und eine höhere Conversion-Rate. In der Befragung geben dann auch einige Serviceprovider an, dass, abhängig vom Anwendungsfall, eine grundsätzliche Zahlungsbereitschaft für diesen immateriellen Mehrwert besteht. Gleichzeitig lassen aber auch sie eine sehr hohe Preissensibilität erkennen. Plattformbasierte Identitäten (etwa Log-In mit Google oder Facebook) können kostenlos genutzt werden und erlauben die Erhebung von Nutzerdaten für

[11] Und wie im Artikel eingangs dargestellt wird, versprechen zahleiche aktuelle Projekte und Initiativen die sogenannte identity crisis mittels SSI zu lösen.

die Optimierung der Dienste. Auch wird in den Interviews ein Vergleich mit Gebühren für Kreditkartentransaktionen oder PayPal gezogen, welche nur sehr zähneknirschend akzeptiert werden. Bis heute halten sie zahlreiche Unternehmen davon ab, diese Zahlungsform zu akzeptieren. In zahlreichen Anwendungsfällen reicht es zudem aus, wenn das Geld ankommt – eine darüber hinaus verifizierte Identität ist nicht notwendig und würde damit auch nicht vergütet. Können bereits aktuell genutzte, kostenpflichte ID-Verfahren (z. B. VideoIdent) abgelöst werden, besteht eine entsprechende Zahlungsbereitschaft, da die Kosten offensichtlich sind.

(3) Je nach konkreter Ausgestaltung eines Ökosystems ergeben sich unterschiedliche *Infrastruktur-Serviceprovider* (ISSP). Vereinfachend werden im Folgenden ein rein technischer ISSP und ein Ökosystem-Orchestrator unterschieden. Der technische ISSP entwickelt Middleware, Konnektoren oder andere Komponenten für die technische Teilnahme am Ökosystem. Gegebenenfalls kann er diese auch für Ökosystemteilnehmer betreiben. In einem Ökosystem können aber auch mehrere technische ISSP agieren, im Sinne einer Coopetition konkurrieren oder sich auf unterschiedliche Aufgaben fokussieren (z. B. Entwicklung von Konnektoren für staatliche eIDs, Entwicklung von SSI-Komponenten, Betrieb von Komponenten wie Web-Agents etc.). Der Ökosystem-Orchestrator (Lingens et al. 2022) übernimmt dagegen die übergeordnete Steuerung des Ökosystems und verantwortet das Regelwerk (Trust Framework: gemeinsame Normen und Standards, Verfahren, Regeln, Grundsätze) des Ökosystem. Er ist insofern besonders für die Herstellung von Vertrauen in das Ökosystem verantwortlich. Hiermit verbunden ist auch das Management der wirtschaftlichen Basis des Ökosystems. Der Orchestrator kann des Weiteren auch bestimmte Infrastrukturdienste (z. B. Verzeichnisdienste) technisch bereitstellen und das Ökosystem nach außen vertreten, etwa als zentraler Ansprechpartner für die Politik oder für potenzielle neue Ökosystemteilnehmer.

Zur Werterfassung ergibt sich für technische ISSP durch die Teilnahme am Ökosystem die Chance auf Lizenzeinnahmen für die entwickelten Komponenten, mögliche Vergütungen für die Integration der Komponenten in die Systeme anderer Ökosystemteilnehmer und für den Betrieb von Komponenten (z. B. Web-Agents), wobei unterschiedliche Preisgestaltungsmodelle (Grundgebühr, transaktionsbasierte Gebühren, Anzahl der Nutzer etc.) denkbar sind. Für den Ökosystem-Orchestrator bestehen Möglichkeiten zur Werterfassung über Zertifizierungsgebühren[12] (z. B. für Komponentenhersteller, möglicherweise auch für Serviceprovider die ID-Daten aus dem Ökosystem auf einem bestimmten, höheren Sicherheitsniveau erhalten möchten) für den Beitritt zum Ökosystem und laufende Mitgliedschaftsgebühren. Werden Infrastrukturdienste technisch bereitgestellt, könnten auch hierfür Nutzungsgebühren erhoben werden. Generell ist jedoch zu berücksichtigen, dass Gebühren für den Beitritt in das beziehungsweise die Nutzung des Ökosystems eine Hürde zur Adoption darstellen. Insofern ist fraglich, ob – zumindest zu Beginn während des Aufbaus des Ökosystems – diese Werterfassungsstrategien zielführend sind.

[12] Zertifizierungen können auch von externen Zertifizierungsstellen bzw. Auditoren durchgeführt werden.

Tab. 2 Akteure im ID-Ökosystem: Werterfassung und Zahlungsbereitschaft

Akteur	Werterfassung	Zahlungsbereitschaft
Aussteller	Nur als SP	Keine
Serviceprovider	Mittel	Gering–mittel
Infrastruktur-Serviceprovider	Unklar	Keine
Endnutzer	Gering–mittel	Gering
Nutzersysteme	Unklar	Keine

(4) *Endnutzer bzw. Bürger* fragen digitale Angebote nach und nutzen dafür das ID-Ökosystem, wenn sie der Meinung sind, dass dies für sie vorteilhaft ist. Breite Anwendbarkeit, hohes Vertrauen, ein gesteigerter Komfort oder die bessere Kontrolle der eigenen Daten könnten beispielsweise als entsprechende Vorteile angesehen werden und eine immaterielle Werterfassung darstellen. Eine Notwendigkeit zur Erfassung direkter monetärer Werte durch Endnutzer ergibt sich nicht. Umgekehrt ist auch eine Zahlungsbereitschaft von Endnutzern für ID-Systeme und damit die Finanzierung eines ID-Ökosystems über die Endnutzer äußerst unwahrscheinlich (Roßnagel et al. 2014). Auch die befragten Organisationen erwarten mittelfristig keine entsprechende Zahlungsbereitschaft der Endnutzer.

(5) Hinsichtlich der *Nutzersysteme* werden Walletapplikationen betrachtet, die auf Smartphones genutzt werden. Smartphones, Smartphone-Betriebssysteme und spezielle sichere Hardwarekomponenten werden nicht spezifisch für die in diesem Artikel analysierten ID-Ökosysteme angepasst und hergestellt. Wir fokussieren darum auf die Hersteller der Wallets, die diese explizit für ein bestimmtes ID-Ökosystem entwickeln und bereitstellen. Vom Endnutzer erhobene Gebühren für die Nutzung der Wallet besitzen aufgrund der niedrigen Zahlungsbereitschaft und resultierenden Adoptionshürden kaum Werterfassungspotenzial. Ein für diesen Artikel befragter Wallethersteller gibt hierzu passend an, dass seine Wallet den Endkunden kostenlos zur Verfügung gestellt wird. Demensprechend müssen andere Wege zur Werterfassung gefunden werden. Wallethersteller könnten gegebenenfalls ein Branding der Wallet oder spezifische funktionale Anpassungen für bestimmte Aussteller und Datenquellen sowie Serviceprovider anbieten und sich von diesen vergüten lassen. Dies könnte um kostenpflichtige Beratungsleistungen rund um die Technologie und das Ökosystem ergänzt werden. Dennoch ist fraglich, ob sich eine Wallet Applikation für den Hersteller alleine trägt oder dieser nicht gleichzeitig als technischer ISSP weitere technische Komponenten anbieten müsste, für welche die Werterfassung einfacher möglich sein könnte.

Die Analyse der Wertschöpfungskette mit Fokus auf die Werterfassung (Überblick in Tab. 2) zeigt, dass diese für ID-Ökosysteme eine große Herausforderung darstellt. Die besten Möglichkeiten zur Werterfassung haben Serviceprovider – es handelt sich jedoch vor allem um immaterielle Mehrwerte. Auch Endnutzer können eindeutig von einem funktionierenden ID-Ökosystem profitieren. Wenn Aussteller und Datenquellen auch gleichzeitig als Serviceprovider vom Ökosystem profitieren, ergibt sich für sie das gleiche Potenzial zur Werterfassung. Ansonsten stellt sich für sie die Frage, warum sie die Investitionen für den Eintritt in das Ökosystem

eingehen und womöglich noch Haftungsrisiken für die Korrektheit der von ihnen ausgestellten digitalen IDs übernehmen sollten. Für die anderen Ökosystemteilnehmer ist weitgehend unklar, wie die angerissenen Möglichkeiten zur Werterfassung über verschiedene Gebühren realisiert werden können, ohne damit, angesichts begrenzter Zahlungsbereitschaft, zu hohe Adoptionshürden zu schaffen. Im nächsten Kapitel sollen darum aufbauend auf dieser Analyse mögliche Strategien für den Aufbau ökonomisch tragfähiger ID-Ökosysteme diskutiert werden.

4 Strategien für den Aufbau ökonomisch tragfähiger ID-Ökosysteme

Wie im letzten Kapitel dargestellt, sind sowohl die Möglichkeiten der Werterfassung als auch mögliche Zahlungsbereitschaften der Ökosystemteilnehmer stark limitiert. Eine Werterfassung ist am ehesten bei Serviceprovidern und Nutzern zu erwarten. Für alle anderen Ökosystemteilnehmer – sofern sie nicht selbst als Serviceprovider auftreten – ist eine finanzielle Kompensation erforderlich. Dies wiederum erfordert entweder eine Zahlungsbereitschaft der anderen Teilnehmer, die aber in einem nur sehr geringen Umfang vorhanden ist (siehe Kap. 3). Daher ist es in der aktuellen Situation kaum vorstellbar, dass ein funktionierender Markt für SSI Identitäten von allein nur durch Angebot und Nachfrage entstehen wird. Da aber, wie in der Einleitung dargestellt, von mehreren Seiten auf den Aufbau eines solchen Ökosystems gedrängt wird, erscheint es sinnvoll, verschiedene Möglichkeiten zum Aufbau und zur Unterstützung auch unter Beteiligung der öffentlichen Hand zu diskutieren. Aufbauend auf (Ozment und Schechter 2006) kommen dafür unterschiedliche Strategien in Frage, die im Folgenden diskutiert werden.

Ein möglich wenig invasiver Ansatz wäre, mit Hilfe einer Informationskampagne zu den Vorteilen sicherer digitaler Identitäten deren Nachfrage bei Endnutzern zu steigern, wenn diese Vorteile von den Nutzern auch als erkennbarer Mehrwert wahrgenommen werden. Allerdings ist der Effekt solcher Informationskampagnen erfahrungsgemäß sehr limitiert.[13]

Am anderen Ende des Spektrums steht mit der Zwangsadoption die massivste Form eines Markteingriffes zur Verfügung. Eine Zwangsadoption könnte entweder allgemein erfolgen und einen Einsatz sicherer Identitäten – bis hin zu Bußgeldern bei Nichteinhaltung – vorschreiben, oder auf einzelne Branchen oder Anwendungsgebiete beschränkt werden und mit Hilfe von Regulierungsmaßnahmen umgesetzt werden, die z. B. ein bestimmtes Vertrauensniveau vorschreiben. In stark regulierten Branchen wie Glücksspiel und Finanzdienstleistungen ist eine solche Regulierung bereits erfolgt und hat zu einer flächendeckenden Adoption von Video-ident Verfahren geführt. Sollten diese nicht mehr als ausreichend sicher eingestuft werden oder alternative Verfahren günstiger angeboten werden können, könnte dies zu einer entsprechenden Nachfrage nach anderen sicheren Identitäten führen.

Zwischen diesen beiden extremen Ansätzen sind auch weitere Vorgehensweise wie die Bündelung mit Komplementärgüter oder Subventionierungen denkbar. Ersteres erfordert jedoch eine enge Bindung an die Angebote und Dienstleistungen

[13] Siehe z. B. auch die Covid19-Impfkampagne.

der Serviceprovider. Letzteres erfordert eine Bereitschaft der öffentlichen Hand, die Kosten für den Betrieb des Ökosystems zumindest so lange zu subventionieren, bis sich ein tragfähiger Markt für sichere digitale IDs entwickelt. Wie lange dies dauern wird, bzw. ob dies überhaupt zu Stande kommt, ist aktuell nur schwer zu beantworten. In Anbetracht der dargestellten Schwierigkeiten der Werterfassung erscheint es gut möglich, dass skizzierte ID-Ökosysteme rein über Marktmechanismen nicht ökonomisch tragfähig werden.

5 Fazit

Die Entwicklung neuer ID-Lösungen fokussiert derzeit stark auf technische Aspekte rund um Datensicherheit, Privatsphärenschutz und Usability. Für die tatsächliche Realisierung dieser Vorteile, die sich aus einer breiten Adoption dieser Lösungen ergibt, sind jedoch auch der Markt für digitale IDs und die ihm zugrundeliegenden ökonomischen Wirkungszusammenhänge zu betrachten. Die Analysen in diesem Beitrag zeigen dann auch wie herausfordernd sich der mehrseitige Markt für digitale IDs hinsichtlich der Werterfassung durch die Akteure des ID-Ökosystems darstellt. Die Werterfassung im Ökosystem beschränkt sich auf wenige Teilnehmer und Gebühren für die Teilnahme am Ökosystem können angesichts geringer Zahlungsbereitschaft schnell zu hohe Adoptionshürden aufbauen. Die Analyse der Strategien für den Aufbau ökonomisch tragfähiger ID-Ökosysteme zeigt Optionen auf, allerdings bleiben Zweifel bestehen, dass ein ökonomisch tragfähiges ID-Ökosystem rein über Marktmechanismen ohne signifikante staatliche Eingriffe beziehungsweise Investitionen aufgebaut und betrieben werden kann. Wenn diese Analyse korrekt ist und akzeptiert wird, kann die Diskussion über die Konsequenzen geführt werden. Gesellschaftlich könnte das ID-Ökosystem schließlich auch als wichtige digitale Infrastrukturen betrachtet werden. Insofern unterläge es einer politischen Entscheidung, ob diese digitalen Infrastrukturen nicht dauerhaft staatlich zu subventionieren wären, wenn diese gesellschaftlich erwünscht sind. Es ist dementsprechend ein nüchterner Diskurs über die technische Ausgestaltung aber auch die ökonomischen Wirkbeziehungen und die Rolle des Staates beim Aufbau dieser Infrastruktur notwendig.

Funding Open Access funding enabled and organized by Projekt DEAL.

Open Access Dieser Artikel wird unter der Creative Commons Namensnennung 4.0 International Lizenz veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Artikel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.

Weitere Details zur Lizenz entnehmen Sie bitte der Lizenzinformation auf http://creativecommons.org/licenses/by/4.0/deed.de.

Literatur

BMWi (2021) Digitale Identitäten. Schlaglichter der Wirtschaftspolitik

Camenisch J, Herreweghen EV (2002) Design and implementation of the Idemix anonymous credential system. In: Atluri V (Hrsg) Proceedings of the 9th ACM conference on computer and communications security CCS 2002, Washington, DC, November 18–22, 2002 ACM, S 21–30

Ehrlich T, Richter D, Meisel M, Anke J (2021) Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. HMD 58:247–270. https://doi.org/10.1365/s40702-021-00711-5

European Commission (2022) European Digital Identity. In: Digital Identity for all Europeans. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en. Zugegriffen: 19. Aug. 2022

Evans DS (2003) Some empirical aspects of multi-sided platform industries. Rev Netw Econ 2:191–209

Homburg C, Klarmann M, Reimann M, Schilke O (2012) What drives key informant accuracy? J Mark Res 49:594–608

Initiative D21 e. V. (2021) eGovernment Monitor 2021

Kubach M, Sellung R (2021) On the market for self-sovereign identity: structure and stakeholders. In: Roßnagel H, Schunck CH, Mödersheim S (Hrsg) Open identity summit 2021. Gesellschaft für Informatik e. V, Bonn, S 143–154

Lingens B, Huber F, Gassmann O (2022) Loner or team player: how firms allocate orchestrator tasks amongst ecosystem actors. Eur Manag J 40:559–571. https://doi.org/10.1016/j.emj.2021.09.001

MarketsandMarkets (2021) Digital Identity Solutions Market Size, Share and Global Market Forecast to 2026 | Report Code TC 7537. https://www.marketsandmarkets.com/Market-Reports/digital-identity-solutions-market-247527694.html. Zugegriffen: 19. Aug. 2022

Microsoft (2009) Windows CardSpace. https://learn.microsoft.com/en-us/previous-versions/dotnet/netframework-3.5/ms733090(v=vs.90). Zugegriffen: 9. Jan. 2023

Microsoft (2014) U-Prove. In: Microsoft. https://www.microsoft.com/en-us/research/project/u-prove/?from=https%3A %2F%2 Fresearch.microsoft.com%2Fen-us%2Fprojects%2Fu-prove. Zugegriffen: 19. Aug. 2022

Ozment A, Schechter SE (2006) Bootstrapping the adoption of Internet security protocols Cambridge, S 1–19

Pohlmann N (2022) Nutzer-Identifizierung per Videoident: Mit wie viel Restrisiko können wir leben? In: heise online. https://www.heise.de/news/Videoident-Mit-wie-viel-Restrisiko-koennen-wir-beim-Verfahren-leben-7222518.html. Zugegriffen: 19. Aug. 2022

Rannenberg K, Camenisch J, Sabouri A (2015) Attribute-based credentials for trust. Identity in the Information Society. Springer, Berlin Heidelberg

Roßnagel H, Zibuschka J, Hinz O, Muntermann J (2014) Users' willingness to pay for web identity management systems. Eur J Inf Syst 23:36–50. https://doi.org/10.1057/ejis.2013.33

Schardong F, Custódio R (2022) Self-sovereign identity: a systematic review, mapping and taxonomy. Sensors 22:5641. https://doi.org/10.3390/s22155641

Soltani R, Nguyen UT, An A (2021) A survey of self-sovereign identity ecosystem. Secur Commun Netw 2021:1–26. https://doi.org/10.1155/2021/8873429

Talmar M, Walrave B, Podoynitsyna KS et al (2020) Mapping, analyzing and designing innovation ecosystems: the Ecosystem Pie Model. Long Range Plann 53:101850. https://doi.org/10.1016/j.lrp.2018.09.002

Teece DJ (1986) Profiting from technological innovation: implications for integration, collaboration, licensing and public policy. Res Policy 16:285–305

Tenner T, Mietke S (2021) Digitale Identitäten – Schritte auf dem Weg zu einem ID-Ökosystem. Bankenverband, Berlin

Toth KC, Anderson-Priddy A (2019) Self-sovereign digital identity: a paradigm shift for identity. IEEE Secur Privacy 17:17–27. https://doi.org/10.1109/MSEC.2018.2888782

Tschirsich M (2022) Praktischer Angriff auf Video-Ident, Version 1.2. Chaos Computer Club

White O, Madgavkar A, Manyika J et al (2019) Digital identification: a key to inclusive growth. McKinsey Global Institute

Zibuschka J, Roßnagel H (2012) Stakeholder economics of identity management infrastructures for the web. In: Proceedings of the 17th nordic workshop on secure IT systems (Nordsec 2012) Karlskrona