Anke, Jürgen; Richter, Daniel

Digitale Identitäten

HMD Praxis der Wirtschaftsinformatik

Provided in Cooperation with:
Springer Nature

Suggested Citation: Anke, Jürgen; Richter, Daniel (2023) : Digitale Identitäten, HMD Praxis der Wirtschaftsinformatik, ISSN 2198-2775, Springer Fachmedien Wiesbaden GmbH, Wiesbaden, Vol. 60, Iss. 2, pp. 261-282, https://doi.org/10.1365/s40702-023-00965-1

HMD Praxis der Wirtschaftsinformatik (2023) 60:261–282
https://doi.org/10.1365/s40702-023-00965-1

EINFÜHRUNG

Digitale Identitäten

Status Quo und Perspektiven

Jürgen Anke · Daniel Richter

Eingegangen: 3. Februar 2023 / Angenommen: 26. Februar 2023 / Online publiziert: 20. März 2023

Zusammenfassung Die digitale Transformation überführt Geschäfts- und Verwaltungsabläufe in den digitalen Raum. Zu deren sicherer und rechtskonformer Durchführung ist es oft notwendig, sich von den notwendigen Eigenschaften der Beteiligten zu überzeugen. Dafür werden digitale Identitäten eingesetzt, die Personen und andere Entitäten mittels Sammlungen von Attributen repräsentieren. Allerdings führt die große Vielfalt von Verfahren und Methoden für das Identitätsmanagement zu hoher Komplexität und Kosten. Als ein vielversprechender Ansatz zur Überwindung dieser Hürden erscheint das Paradigma der selbstbestimmten Identität. Es soll eine durchgängige sichere Identifizierung und Authentifizierung von Personen, Organisationen und Objekten ermöglichen. Dafür werden digitale Nachweise (Verifiable Credentials) über beliebige Sachverhalte von Herausgebern in einer kryptografisch gesicherten Form bereitgestellt. Die Inhaber dieser Nachweise verwalten diese selbst in digitalen Wallets und können sie bei Bedarf an Dritte zum Nachweis von diversen Merkmalen übermitteln. Der vorliegende Beitrag gibt einen Überblick zum aktuellen Stand digitaler Identitäten, den ihnen zugrundeliegenden Verfahren sowie den damit verbundenen praktischen Problemen. Darauf aufbauend werden laufende Aktivitäten zur Entwicklung einheitlich nutzbarer digitaler Nachweise gegeben, die eine Grundlage für künftige digitale Ökosysteme bilden. Zudem wird eine Einordnung in die aktuelle Forschung der Wirtschaftsinformatik zu diesem Thema gegeben.

Schlüsselwörter Digitale Identität · Selbstbestimmte Identität · Authentifizierung · Identifizierung · Nachweise · Vertrauen

✉ Jürgen Anke · Daniel Richter
Arbeitsgruppe Digitale Dienstleistungssysteme, Hochschule für Technik und Wirtschaft Dresden, Dresden, Deutschland
E-Mail: juergen.anke@htw-dresden.de

Daniel Richter
E-Mail: daniel.richter@htw-dresden.de

Digital Identity
Status Quo and Perspectives

Abstract Digital transformation is transferring business and administrative processes into the digital space. To carry them out securely and in compliance with the law, it is often necessary to verify the required attributes the involved parties. Digital identities are used for this purpose, representing persons and other entities through sets of attributes. However, the large variety of procedures and methods for identity management leads to high complexity and costs. The paradigm of self-determined identity appears to be a promising approach to address these challenges. It aims to enable secure end-to-end identification and authentication of persons, organizations and objects. To this end, verifiable credentials are provided by issuers in a cryptographically secured form. The holders of these credentials manage them in digital wallets and can present them to third parties as needed to prove various characteristics. This paper provides an overview of the current state of digital identities, their underlying processes, and the practical problems associated with them. Based on this, ongoing activities for the development of interoperable digital credentials are given, which form the basis for future digital ecosystems. In addition, a classification of related research topics in the field of information systems is given.

Keywords Digital identity · Self-sovereign identity · Authentication · Identification · Credentials · Trust

1 Einführung

Social Media, Videokonferenzen, Onlinebanking, digitale Verwaltung oder Onlinespiele – in verschiedenen Kontexten müssen Systeme feststellen können, wer die jeweilige Person ist und welche Rechte für sie eingeräumt werden sollen. Dies ist eine große Herausforderung, da die dem Internet zugrundeliegenden Protokolle zwar eine Identifizierung von Rechnern erlauben, jedoch nicht die Identifizierung von Personen, Organisationen oder Objekten, die den Rechner benutzen. Mit anderen Worten: „The Internet was built without a way to know who and what you are connecting to." (Cameron 2005, S. 1). Um dieses Problem zu lösen, werden Personen und andere Entitäten mit Hilfe von Attributen beschrieben, die als digitale Identitäten dienen.

In der Praxis verwenden Menschen zahlreiche digitale Identitäten, die für unterschiedliche Zwecke eingesetzt werden. Diese Vielfalt ist nicht nur verschiedenen technischen Ansätzen und den damit verbundenen Kosten geschuldet, sondern auch auf unterschiedliche Anforderungen an die Belastbarkeit und den Umfang der festzustellenden Eigenschaften zurückzuführen. So erfordern gesetzliche Vorschriften für die Eröffnung eines Bankkontos oder Verwaltungsvorgänge die Feststellung der legalen Identität, die durch hoheitliche Dokumente bescheinigt wird. Zudem setzen Anbieter verschiedene Mechanismen ein, um die mit digitalen Interaktionen verbundenen Risiken zu begrenzen. Die bisherigen Ansätze für das Identitätsmanagement führen zu einer großen Anzahl von Identitäten, die jeweils nur sehr begrenzt ein-

setzbar sind und unterschiedliche Qualitäten besitzen (Skierka 2020). Dies führt zu hoher Komplexität, Kosten und Risiken in Wirtschaft und Verwaltung.

So besteht zwar ein großer Bedarf nach digitalisierten Verwaltungsleistungen, allerdings ist die Nutzung der dafür verwendeten Identifikationsverfahren oft umständlich. Zum Beispiel wird die staatliche elektronische Identität des Personalausweises (eID) nur von 10 % der Befragten tatsächlich eingesetzt (Initiative D21 e. V. und TU München 2022). Der eGovernment-Monitor beziffert die Differenz zwischen der Nachfrage einer Leistung und deren digitaler Nutzung („Nutzungslücke") über alle betrachteten Leistungen in Deutschland mit 57 % (Initiative D21 e. V. und TU München 2022). Die geringe Zugänglichkeit digitaler Verwaltungsleistungen verhindert so die Erschließung der mit Digitalisierung einhergehenden Effizienzpotenziale und sorgt für unnötigen Wartezeiten.

Im Gegensatz zur Verwaltung wird in der Wirtschaft reger Gebrauch von digitalen Identitäten gemacht, insbesondere im E-Commerce. Der bei Onlinehändlern angestrebte hohe Komfort führt jedoch oft zu unzureichenden Schutzmaßnahmen wie dem Verzicht auf Zweifaktor-Authentifizierung. So können Händler nicht erkennen, ob die behauptete Identität tatsächlich vom rechtmäßigen Besitzer verwendet wird. Mit gestohlenen Identitätsdaten können unberechtigte Dritte Verträge abschließen, Waren bestellen und Prämienpunkte einlösen (Verbraucherzentrale 2021). Dadurch entstehen jährlich rund 1,4 Mrd. € Schaden (Kolf 2021). Weitere Schäden drohen durch die zunehmende Zahl von schwer zu erkennenden „Fakeshops", die keine oder falsche Produkte liefern (Akinci 2023).

Die Entwicklungen in Wirtschaft und Verwaltung zeigen, dass sich die Mechanismen für die Herstellung von Vertrauen in der digitalen und physischen Welt unterscheiden. Während im Internet mit großem Aufwand und vielfältigen Methoden die erforderlichen Eigenschaften von Akteuren geprüft werden, nutzt man in physischen Interaktionen häufig Urkunden und Ausweise und andere Dokumente. Um diesen Mechanismus digital nutzen zu können, müssen die Herausgeber der in diesen Dokumenten enthaltenen Daten überprüfbar sein. Weiterhin müssen die derart bereitgestellten Nachweise die gleiche rechtliche Wirkung besitzen, wie ihre physischen Pendants.

Der derzeit diskutierte Ansatz „Self-Sovereign Identity" (SSI) bzw. selbstbestimmte Identität könnte hierfür eine Lösung darstellen. SSI basiert auf dem Konzept der nutzerzentrierten dezentralen Identität (Allen 2016). Dabei werden digital signierte Nachweise in einer digitalen Brieftasche (Wallet) unter der Kontrolle der Nutzenden verwaltet und auf Anfrage über einen direkten, verschlüsselten Kanal an Dritte bereitgestellt. Während Privatpersonen von SSI durch höheren Komfort und besseren Schutz der Privatsphäre profitieren, erlaubt dieser Ansatz Dienstanbietern vertrauenswürdige Informationen automatisiert zu empfangen, zu prüfen sowie eigene Nachweise auszustellen (Preukschat und Reed 2021).

Dieser Beitrag soll einen Überblick über den aktuellen Stand und die Perspektiven auf dem Gebiet der digitalen Identitäten geben. Dazu wird nach der Definition wesentlicher Begriffe auf die Grundmodelle des Identitätsmanagements eingegangen. Dabei wird insbesondere das Paradigma der selbstbestimmten Identität herausgestellt, welches die Etablierung des Nachweisaustauschs als Mechanismus für den Aufbau von Vertrauen im digitalen Raum ermöglicht. Um eine praktische Nutzbar-

keit von digitalen Nachweisen zu erreichen, müssen rechtliche Rahmenbedingungen für den Umgang und die Anerkennung digitaler Nachweise geschaffen werden. Perspektivisch können so digitale Ökosysteme entstehen, die durch interoperable Nachweise für Anbieter einfacher zu etablieren und für Nutzende leichter zugänglich sind. Zur Realisierung dieser Potenziale ist noch Entwicklungsarbeit zu leisten, die derzeit in diversen Projekten und Initiativen adressiert werden. Zudem ergeben sich auf dem Gebiet der digitalen Identitäten zahlreiche Forschungsthemen für die Wirtschaftsinformatik, deren Übersicht diesen Beitrag abrundet.

2 Grundbegriffe im Umgang mit digitalen Identitäten

2.1 Definition und Aufbau

Der Zweck von digitalen Identitäten ist die Repräsentation von **Entitäten**. Entitäten sind alle Gegenstände, die den Regeln einer bestimmten Domäne unterliegen bzw. für deren Funktionieren relevant sind. In diesem Beitrag werden primär Personen als Entitäten betrachtet, jedoch umfassen Entitäten ebenfalls Organisationen und Objekte. Gemäß ISO/IEC 24760-1 ist eine Identität eine Menge von Attributen, die eine bestimmte Entität beschreiben (Pohlmann 2022, S. 170 f). Mithilfe eines **Identifikators** lässt sich eine digitale Identität von anderen gleichartigen Datensätzen im selben Gültigkeitsbereich unterscheiden. Solche Identifikatoren sind z. B. Kunden-, Pass- oder Matrikelnummern (Abb. 1).

Um sicherzustellen, dass lediglich berechtigte Nutzerinnen und Nutzer eine digitale Identität einsetzen können, wird diese digitale Identität über sogenannte **Credentials** an die zugeordnete Entität gebunden. Credentials werden von einer autorisierten Stelle in physischer Form (z. B. als Smartcards) oder in digitaler Form (z. B. als Zugangsdaten oder Zertifikate) ausgegeben. Credentials können neben dem Identifikator verschiedene Angaben zu Identität, Berechtigungen, Qualifikation o. ä. der Entität enthalten sowie eigene Attribute besitzen, z. B. ein Ausgabedatum oder eine Gültigkeitsdauer.

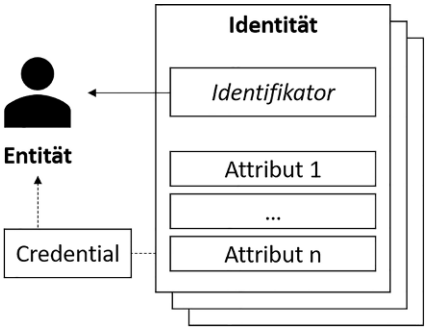

Abb. 1 Aufbau einer digitalen Identität. (Nach ISO und IEC 2019)

2.2 Registrierung und Identifikation

Die Erzeugung digitaler Identitäten ist ein Vorgang, der ausgewählte Merkmale einer Entität in eine digitale Repräsentation überführt. Wenn eine Person im Rahmen einer Registrierung die benötigen Angaben selbst macht, entsteht eine *ungeprüfte Identität*. Sie erlaubt die Wiedererkennung der Person, z. B. um deren Inhalte und Einstellungen korrekt zuordnen zu können. Ungeprüfte Identitäten sind für Anwendungen wie die Nutzung von sozialen Netzwerken (z. B. Twitter, Instagram) oder Kollaborationstools (z. B. Miro, GitHub) ausreichend oder im Sinne des Datenschutzes sogar erwünscht (UC Berkeley 2019).

Für viele gesetzlich regulierte Anwendungen muss die digitale Identität eine Verbindung zur legalen Identität besitzen. Dazu wird bei der Erzeugung der Identität mittels **Identifizierungsverfahren** eine überprüfbare Zuordnung zur realen Person hergestellt. Beispiele für solche Verfahren sind *PostIdent, VideoIdent* sowie das Ausweisen mit Hilfe der eID des Personalausweises (Pohlmann 2022, S. 174ff.). Sie stellen sicher, dass die in der Identität angegebenen Attribute mit den Merkmalen der Entität übereinstimmen. Dafür wird die legale Identität durch hoheitliche Dokumente sowie persönliche Identifikation festgestellt. Standardisierte Identifizierungsverfahren werden häufig durch spezialisierte Dienstleister erbracht, die eine dafür erforderliche Zertifizierung besitzen und somit von Dritten als vertrauenswürdige Quelle eingestuft werden können.

Je nach geplantem Einsatzgebiet einer digitalen Identität sind zusätzliche Daten zur Charakterisierung relevant, z. B. Telefonnummern, Emailadressen, Postanschriften sowie Zahlungsdaten. Solche Angaben können verifiziert werden, indem z. B. ein Code („Aktivierungscode“) per Post, E-Mail oder SMS an die jeweilige Adresse versendet wird. Der Empfänger beweist durch die Eingabe des übermittelten Codes, dass er tatsächlich Kontrolle über die angegebenen Geräte, Postfächer bzw. Konten hat (Pohlmann 2022, S. 171). Damit wird auch dem Missbrauch von Daten Dritter zum Anlegen von Nutzerkonten vorgebeugt. Weiterführende Attribute zur Charakterisierung wie Angaben zu Qualifikationen, Versicherungen, Mitgliedschaften, Befugnissen und Vollmachten werden in der Regel über gescannte Dokumente, Urkunden oder Ausweise übermittelt und manuell geprüft. Dies ist nicht nur aufwändig, sondern macht Fälschungen und Manipulationen der Nachweisdokumente schwer erkennbar.

2.3 Authentifizierung

Um die Bindung zwischen digitaler Identität und ihrer zugeordneten Entität herzustellen, werden sogenannte **Authentifizierungsfaktoren** verwendet. Diese lassen sich in die Kategorien *Wissen* (geheimes Wissen der Entität, z. B. Passwort, PIN), *Besitz* (der Entität zugeordnetes Gerät, z. B. Mobiltelefon, Token, privater Schlüssel oder Smartcard) oder *Inhärenz* (physische Merkmale der Entität, z. B. Fingerabdrücke) einordnen (Pohlmann 2022, S. 173 f). Beim Erzeugen der digitalen Identität wird dem Benutzer das entsprechende Credential ausgestellt. Dies kann die Festlegung eines Passworts, die Registrierung einer Authenticator-App auf einem Smartphone, die Erzeugung von digitalen Zertifikaten (z. B. für die elektronische

Steuererklärung ELSTER) oder die Ausgabe von Smartcards (z. B. Bankkarte, Personalausweis) sein.

Mit Credentials kann eine Person die rechtmäßige Nutzung einer digitalen Identität gegenüber einem System nachweisen. Die Überprüfung der behaupteten Identität wird während der **Authentifizierung** durch das System geprüft. Abhängig von den verwendeten Authentifizierungsfaktoren erfolgt dies durch Eingabe von Passwörtern, Versenden von Einmal-Passwörtern an registrierte Geräte, biometrische Erfassung oder kryptografische Challenge-Response-Verfahren (Pohlmann 2022, S. 187ff.).

Je nach gewünschtem Komfort, Sicherheitsbedürfnis und gesetzlichen Regelungen sind in konkreten Anwendungen mehrere Authentifizierungsfaktoren – idealerweise aus verschiedenen Kategorien – notwendig. Diese Zweifaktor- bzw. Multifaktor-Authentifizierung (2FA/MFA) soll den Missbrauch von Identitäten durch Dritte („Impersonation“) reduzieren, der beispielsweise durch den Diebstahl von Passwörtern möglich wird (Pohlmann 2022, S. 216). So erfordert die eID-Funktion des Personalausweises den physischen Personalausweis als Token (Besitz) sowie eine PIN (Wissen). Allerdings hat diese zusätzliche Sicherheit den Preis einer komplexeren Interaktion, die potenziell das Nutzungserlebnis beeinträchtigt und zudem einen höheren Umsetzungsaufwand beim Anbieter des Dienstes verursacht (Kostic et al. 2016; Sinell und Beckmann 2022).

2.4 Vertrauensniveaus

In konkreten Interaktionen ist es entscheidend, dass die Anforderungen des Empfängers an den Umfang und die Qualität der Daten sowie an die Stärke der Authentifizierung erfüllt werden. Dies wird durch **Vertrauensniveaus** beschrieben. Sie geben an, in welchem Maß sich eine dritte Partei auf die bereitgestellten Daten verlassen kann. Zur Einstufung des Vertrauensniveaus werden die Identifikationssicherheit und die Authentifikationssicherheit herangezogen (Temoshok et al. 2022).

- *Identifikationssicherheit* beschreibt, wie hoch das Vertrauen in die Übereinstimmung der behaupteten mit der tatsächlichen legalen Identität ist. Eine niedrige Identifikationssicherheit besteht bei Selbstauskünften, während die aufwändige Verifikation aller relevanten Attribute durch standardisierte Identifikationsverfahren zu einer hohen Sicherheit führt.
- *Authentifikationssicherheit* bezeichnet die Wahrscheinlichkeit, dass eine Person die Verfügungsgewalt über die von ihr genutzten Credentials hat und diese gültig sind. Es wird geprüft, ob eine behauptete Identität von der zugeordneten Person eingesetzt wird. Hier kann mit Kombination verschiedener Authentifikationsfaktoren eine höhere Vertrauenswürdigkeit erreicht werden.

3 Grundmodelle des Identitätsmanagements

3.1 Isolierte und föderierte Identitäten

Die Verwaltung digitaler Identitäten lässt sich in die drei Grundmodelle isoliert, föderiert und selbstbestimmt einteilen (Ehrlich et al. 2021). Sie unterscheiden sich vor

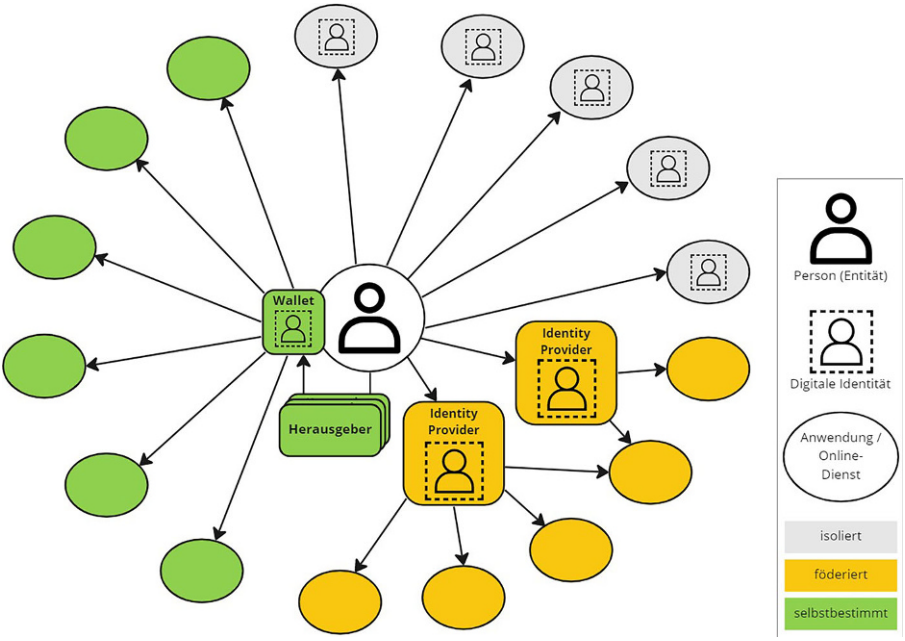

Abb. 2 Grundmodelle des Identitätsmanagements

allem hinsichtlich des Speicherorts, des Gültigkeitsbereichs, des Schutzes der Privatsphäre sowie der Verfügungsmacht über die Daten durch die Nutzenden (Abb. 2).

Beim **isolierten Identitätsmanagement** legen neue Nutzende bei einem Dienst eine digitale Identität in Form eines *Nutzerkontos* an. Dieser Prozess wird als Registrierung bezeichnet und kann im einfachsten Fall mit der Angabe einer Emailadresse als Identifikator sowie der Festlegung eines Passworts zur Authentifizierung erfolgen. Weitere Attribute wie Name, Adresse, Telefonnummer können ebenfalls erfasst und bei Bedarf verifiziert werden. Nach der Registrierung können Nutzende den Dienst verwenden, indem sie sich bei diesem unter Verwendung ihres Passworts authentisiert. Nutzerkonten im isolierten Modell sind nur für den jeweiligen Dienst einsetzbar. Daher führt dieser Ansatz zu einer schnell steigenden Anzahl von digitalen Identitäten. Diese sind für den Nutzenden aufwändig zu verwalten, da nicht nur eine große Anzahl von Passwörtern sicher verwahrt werden müssen, sondern auch die Daten in den Nutzerkonten an vielen Stellen im Internet verteilt sind. Zudem ist oft unbekannt, wie gut der Dienst seine Daten schützt. Immer wieder schaffen es Cyberkriminelle, Kundendaten von Unternehmen zu erbeuten[1].

Eine Verbesserung der Situation bietet das **föderierte Identitätsmanagement**. Dabei übernimmt ein dedizierter *Identity Provider* (IdP) die Aufgabe, Nutzende zu registrieren, zu identifizieren und zu authentifizieren. Ein Dienst, der diese Funktionen von einem IdP verwendet, wird in diesem Kontext als *Relying Party* bezeichnet.

[1] Ob man selbst davon betroffen ist, lässt sich zum Beispiel mit dem Identity Leak Checker des Hasso-Plattner-Instituts überprüfen: https://sec.hpi.de/ilc/.

Alle Dienste, die den gleichen IdP benutzen, bilden die namensgebende Föderation. Dieser Ansatz kommt u. a. in Unternehmen als *Single-Sign On (SSO)* zum Einsatz, damit alle Mitarbeitenden nach einmaliger Authentifizierung die ihnen zugewiesenen internen Anwendungen nutzen können. Privatpersonen wird dieser Mechanismus im Internet als *Social Login* von Internetkonzernen wie Google, Microsoft, Apple, Facebook und Twitter bereitgestellt. Andere Onlinedienste können diese IdPs integrieren. Sie reduzieren damit ihre Einstiegshürde, da bereits angelegte Identitäten verwendet werden können. Bei der Authentifizierung mittels einer föderierten Identität werden die Nutzenden zum IdP umgeleitet. Dies erzeugt bei den IdPs ein umfassendes digitales Abbild über deren Verhalten (Cyphers und Gebhart 2019), die teilweise für Werbezwecke verwendet werden. Zudem begeben sich Nutzende und Onlineanbieter in eine große Abhängigkeit zum IdP, der die Nutzungsbedingungen diktieren oder im Extremfall Teilnehmende sperren kann.

3.2 Selbstbestimmte Identitäten

Die Überwindung dieser Nachteile soll durch das Modell der **selbstbestimmten Identität** gelingen (Ehrlich et al. 2021; Preukschat und Reed 2021). Die Motivation hinter der Entwicklung von SSI ist es, Menschen die Hoheit und Kontrolle über ihre Identitätsdaten zurückzugeben. Konkretisiert wird diese Forderung durch 10 Prinzipien, die 2016 von Christopher Allen in seinem Beitrag „The Path to Self-Sovereign Identity“ formuliert wurden (Allen 2016). Demnach sollen Identitätsdaten möglichst langlebig, breit einsetzbar und übertragbar sein. Die Bereitstellung von Daten an Dritte soll im minimalen Umfang und nur nach Zustimmung der Nutzenden erfolgen (Cucko et al. 2022). Folgende Bestandteile sind für ein SSI-basiertes Identitätssystem erforderlich (Mühle et al. 2018; Preukschat und Reed 2021, S. 21 ff.):

- *Decentralized Identifier (DID)* identifizieren eine Entität und verweisen u. a. auf einen öffentlichen Schlüssel zur Durchführung kryptografischer Vorgänge,
- *Verifiable Credentials (VC)* dienen als signierte Datenstrukturen zur strukturierten Beschreibung von Aussagen über ein Subjekt („Claims“),
- *Wallets* sind benutzerverwaltete Speicher für Schlüssel, Verbindungen, VCs und andere sensible Daten,
- *Agents* sind Softwarekomponenten zum Aufbau von Beziehungen sowie dem Austausch von Daten mit anderen Akteuren unter Nutzung von Wallets sowie
- *vertrauenswürdige Register* sind gemeinsam genutzte Speicher für öffentliche DIDs, Schemata sowie Widerrufe.

Das Modell der selbstbestimmten Identität arbeitet nicht mit Nutzerkonten. Stattdessen werden direkte Verbindungen zwischen Interaktionspartnern aufgebaut. Die Grundlage dafür ist asymmetrische Kryptografie, die Paare aus privatem und öffentlichem Schlüssel einsetzt. Der private Schlüssel wird in der Wallet gespeichert, während der öffentliche Schlüssel über die Auflösung der DID durch Kommunikationspartner ermittelt werden kann. So lassen sich sowohl die Schutzziele Vertraulichkeit (durch Verschlüsselung der Daten mit dem öffentlichen Schlüssel des Empfängers) als auch Authentizität und Zurechenbarkeit (durch Signieren von Daten mit dem pri-

vaten Schlüssel des Versenders) erreichen. Die Kommunikation zwischen Partnern findet über direkte Peer-to-Peer-Verbindungen statt (Mühle et al. 2018; Preukschat und Reed 2021). Dies erfolgt über den Austausch von öffentlichen Schlüsseln der beiden Partner, die sich über dezentrale Identifikatoren (DIDs) adressieren. Damit hat keine der beiden Parteien die alleinige Kontrolle über die Verbindung.

Nach Aufbau der Verbindung werden Verifiable Credentials ausgetauscht, die von verschiedenen Herausgebern stammen können. Nutzende speichern und verwalten diese Nachweise eigenständig in einer Wallet, die in der Regel als Smartphone App umgesetzt ist. Wenn sie im Rahmen einer Interaktion Eigenschaften nachweisen sollen, können sie eine Verbindung zum Agent der Akzeptanzstelle aufbauen, z. B. durch Scannen eines QR-Codes. Die Akzeptanzstelle stellt anschließend eine Anfrage nach den benötigten Daten, die in der Wallet angezeigt wird. Die Nutzenden entscheiden selbst, ob sie diese Daten freigeben möchten. Durch Mechanismen zur selektiven Freigabe von Attributen sowie Beweisen ohne Offenlegung der Daten („Zero-Knowledge Proof“) wird eine Datenminimierung erreicht und damit der Datenschutz verbessert. Die Akzeptanzstelle kann die erhaltenen Daten automatisch auf Gültigkeit, Unverfälschtheit sowie Herkunft prüfen, ohne dass sie den Herausgeber kontaktieren muss (Sedlmeir et al. 2021). Dafür kann mittels der Verifiable Data Registry eine DID zu einem DID-Dokument aufgelöst werden, in dem u. a. der öffentliche Schlüssel des Herausgebers sowie ggf. Verweise auf ein Widerrufsregister abgelegt sind (Abb. 3).

SSI weist gegenüber den anderen beiden Modellen zahlreiche Verbesserungen auf. So werden Identifikation, Authentifikation und Bereitstellung von Nachweisen in einem einheitlichen System ermöglicht, das sowohl für digitale Dienste im Internet als auch für Interaktionen in der physischen Welt einsetzbar ist. VCs besitzen eine sehr

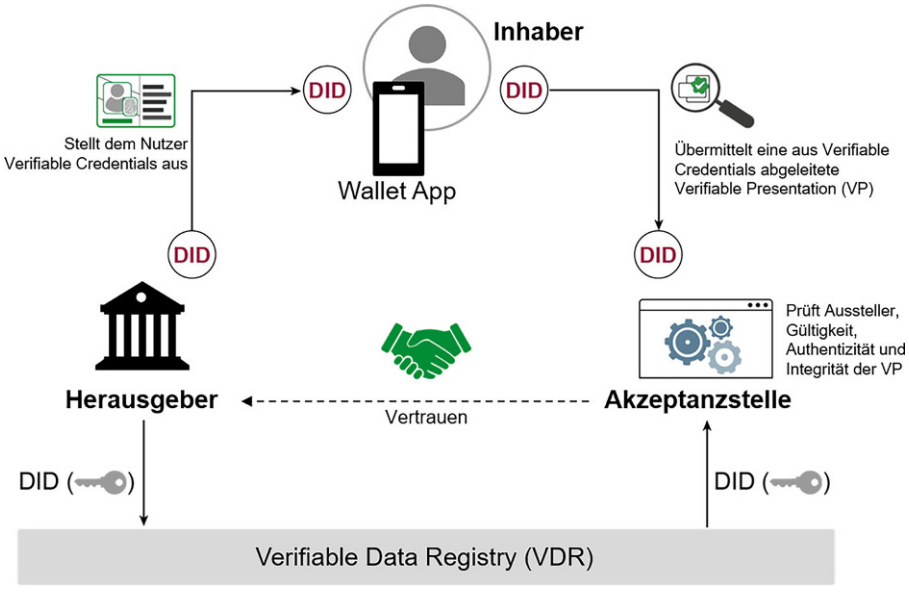

Abb. 3 Architektur von Self-Sovereign Identity. (Modifiziert nach Pohlmann 2022, S. 649)

hohe Flexibilität hinsichtlich der Struktur der ausgetauschten Daten, so dass nahezu jedes bisher auf Papier genutztes Dokument in einem digitalen Nachweis repräsentiert werden kann. Damit können nicht nur Personen, sondern auch Organisationen und Gegenstände mit ihren Eigenschaften repräsentiert werden. Die datensparsame Weitergabe von Informationen an Dritte unter expliziter Freigabe verbessert zudem den Datenschutz und erfüllt damit eine zentrale Forderung von Nutzenden (eco – Verband der Internetwirtschaft e. V. und echConsult GmbH 2022). Nicht zuletzt erlaubt die automatisierbare Prüfung der erhaltenen Dokumente bei Akzeptanzstellen einen bisher kaum erreichbaren Automatisierungsgrad und damit verbundene Effizienzgewinne (Jürgenssen et al. 2022; Laatikainen et al. 2021a). So kann der Nachweisaustausch als Vertrauensmechanismus digital abgebildet werden. Dieser wird aufgrund seiner zentralen Bedeutung nachfolgend detailliert beschrieben.

4 Einsatz digitaler Identitäten zur Schaffung von Vertrauen

4.1 Digitaler Nachweisaustausch

Vertrauen in ein Gegenüber gründet auf Überzeugungen über dieses (McKnight und Chervany 1996). Dazu gehören Kompetenz, Wohlwollen und Integrität im Falle von Personen (McKnight et al. 2002) oder Funktionalität, Verlässlichkeit und Nützlichkeit im Falle von Systemen (Lankton et al. 2015). Um zu diesen Überzeugungen zu gelangen, ist es notwendig, dieses Gegenüber beispielsweise anhand des Auftretens oder vergangener Erfahrungen einzuschätzen (Sztompka 2003, S. 70). In digitalen Interaktionen ist die Bildung von Vertrauen somit erschwert, da solche häufig unmittelbaren Einschätzungen nicht ohne weiteres durchgeführt werden können (Beldad et al. 2010). Darüber hinaus lässt sich ein Großteil der Charakteristiken von Personen nicht wie biometrische Merkmale in diesen selbst finden, sondern existiert lediglich „auf dem Papier“. Der *Nachweis* solcher sozialen Fakten lässt sich in der Regel nur mithilfe von Dokumenten führen, welche von vertrauenswürdigen Herausgebern ausgestellt werden (Smith et al. 2020). Daher ist im digitalen Raum der Austausch von Nachweisen als Mechanismus zum Aufbau von Vertrauen von besonderer Bedeutung.

Dieser Mechanismus lässt sich wie folgt beschreiben: Eine vertrauenswürdige Stelle dokumentiert bestimmte Aussagen in Form eines Nachweises eines bestimmten Typs und gibt diesen anschließend an den jeweiligen Inhaber aus. Der Inhaber kann die Korrektheit seiner Angaben mithilfe des Nachweises bei einer dritten Stelle bescheinigen. Diese Akzeptanzstelle muss ihr Vertrauen somit nicht in die Glaubwürdigkeit der potenziell großen Anzahl an Nachweisinhabern setzen, sondern lediglich in die des zugehörigen Herausgebers. Nachweise erlauben es daher, die Vertrauenswürdigkeit von Herausgebern bezüglich der im Nachweis getroffenen Sachverhalte auf die Inhaber zu übertragen (Milliman und Fugate 1988). Das so entstehende Vertrauen wiederum begünstigt Interaktionen unter Unsicherheit und hat damit einen koordinierenden Effekt (Kautonen 2006).

SSI bedient sich dieses Mechanismus' für die Bereitstellung vertrauenswürdiger Informationen in Form von VCs (Preukschat und Reed 2021, S. 132 f). Um die

Eigenschaften von Entitäten zu überprüfen, können VCs durch Akzeptanzstellen hinsichtlich verschiedener formaler Aspekte geprüft werden, die sich an den Zielen der Informationssicherheit orientieren (Petrlic et al. 2022, S. 10; Preukschat und Reed 2021, S. 23):

- *Integrität:* Nachweise dürfen nicht verfälscht bzw. manipuliert worden sein
- *Gültigkeit:* Nachweise dürfen nicht widerrufen oder abgelaufen sein
- *Authentizität:* der Herausgeber des Nachweises muss korrekt sein
- *Verbindlichkeit:* der Nachweis ist auf den Inhaber ausgestellt bzw. darf von ihm eingesetzt werden

Nach der formalen Prüfung muss der Nachweis inhaltlich verarbeitet werden. Durch standardisierte Datenformate wird die Abfrage von Informationen ermöglicht, die sonst nur mit geringer Qualität (z. B. als Selbstauskunft) oder hohem Aufwand (z. B. als Scan) digital bereitgestellt werden konnten. Dies wird durch **Schemata** auf Basis standardisierter Vokabulare erreicht. Sie beschreiben die in einem Nachweis vorhandenen Aussagen als Menge von Attributen mit Namen, Datentyp sowie ggf. Wertebereich. Nachweisdokumente sind Instanzen dieser Schemata und enthalten Referenzen auf die Schemadefinition. Die vereinbarten Schemata bilden die „gemeinsame Sprache" der Beteiligten. Analog zu Schemata für die öffentliche Verwaltung (XÖV)[2] oder Geschäftsnachrichten (UN/EDIFACT)[3] wird so die semantische Interoperabilität im Nachweisaustausch erreicht.

4.2 Rechtsrahmen und Governance als Basis für Vertrauensentscheidungen

Die Bereitstellung von Nachweisen geht über eine bloße Informationsübertragung hinaus: Die in Nachweisen dokumentierten Aussagen vermitteln auch den Status ihrer Inhaber innerhalb eines bestimmten Rechtsrahmens. Da dieser Status nicht in der Person selbst zu verorten ist, sondern ein soziales Phänomen darstellt (Searle 2006), ermöglicht häufig erst der Einsatz von Nachweisen deren Inhabern die Ausübung bestimmter Rechte (Smith et al. 2020). Der erwähnte Rechtsrahmen stützt sich dabei nicht nur auf Gesetzesnormen, sondern wird darüber hinaus durch organisationsspezifische Regelungen und private Präferenzen geformt (van Kersbergen und van Waarden 2004). Neben den im vorhergehenden Abschnitt genannten Überzeugungen, stellt auch die Verlässlichkeit dieses Rechtsrahmens eine wichtige Grundlage für die Bildung von Vertrauen dar (McKnight et al. 2002).

Beispielsweise bestimmt ein Carsharing-Anbieter selbst, welche Kriterien zur Feststellung der Bonität seiner Kundschaft zugrunde liegen sollen, welche Nachweise hierfür akzeptabel sind und welche Personen damit zur Anmietung von Fahrzeugen berechtigt sind. Auf der anderen Seite ist der Anbieter aufgrund gesetzlicher Regelungen verpflichtet, Informationen über die Gültigkeit der Fahrerlaubnis seiner Kundinnen und Kunden anzufordern. Diesen wiederum obliegt es zu entscheiden, welchen Dienstleistern sie diese Informationen bereitstellen möchten. Es ergibt sich also eine abgeleitete Vertrauensentscheidung bezogen auf die Handhabung der be-

[2] https://www.xrepository.de/.

[3] https://unece.org/trade/uncefact/introducing-unedifact.

reitgestellten Nachweise (Povey 1999). Auch diese könnte durch die Präsentation von Nachweisen zur Untermauerung der Datenschutzpraktiken des Unternehmens unterstützt werden (Luo 2002). Der Nachweisaustausch ermöglicht es daher, Unsicherheiten beider Akteure auszuräumen und wechselseitiges Vertrauen aufzubauen.

Anhand dieses Beispiels lässt sich erkennen, dass die Wirkung von Nachweisen – zum Aufbau von Vertrauen und zur Gewährung bestimmter Rechte – sowohl mit deren inhaltlichen Gestaltung als auch mit den Regeln im Umgang mit diesen zusammenhängt. Um Nachweise erfolgreich zum Vertrauensaufbau in digitalen Interaktionen zu verwenden, ist neben einem bewussten Einsatz von Methoden des Vertrauensmanagements auch eine transparente, elektronisch dokumentierte **Governance** zur Handhabung von Nachweisen nötig. Die Governance von Nachweisdokumenten ist bislang weder durch die Praxis noch durch die Wissenschaft ausreichend detailliert beschrieben worden (Laatikainen et al. 2021b). Dies lässt sich damit begründen, dass Nachweise selbst – obgleich sie in einer Vielzahl von Typen und Formaten vorkommen – unzureichend als eigenständiges Phänomen erforscht worden sind (z. B. Smith et al. 2020).

Als einen ersten Schritt in Richtung einer standardisierten Governance des Nachweisaustauschs werden, in Anlehnung an die Konzepte prozeduraler Data Governance (Abraham et al. 2019), die Rollen der an diesem Mechanismus beteiligten Akteure und deren Aufgaben beschrieben (Ehrlich et al. 2021; Sporny et al. 2022). Dabei kann ein Akteur auch mehrere Rollen wahrnehmen (Abb. 4).

- Ein **Kontrollorgan** erarbeitet und veröffentlicht ein Rahmenwerk mit Regeln zur Handhabung von Nachweisen eines bestimmten Typs. Diese Regeln beschreiben mindestens die Ausstellung und Verifizierung der Nachweise und legen einen primären Anwendungszweck für Nachweise des zu regelnden Typs fest, auf den sich das Rahmenwerk bezieht (Davie et al. 2019).
- Als **Subjekt** wird diejenige Entität bezeichnet, auf welche sich die Inhalte eines Nachweises beziehen. Dies kann ein Gegenstand, eine natürliche oder juristische Person sein.
- Der **Inhaber** verwahrt Nachweise nach der Ausstellung in seinem persönlichen Verfügungsbereich und kann diese zur Überprüfung vorweisen (Smith et al. 2020).

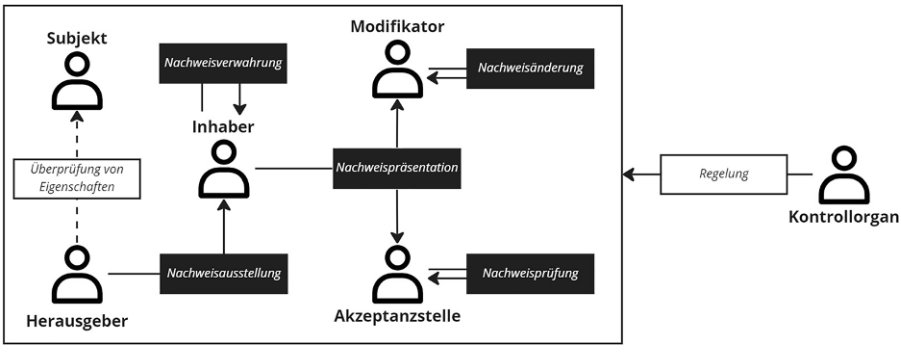

Abb. 4 Nachweisoperationen und beteiligte Rollen

Mittels Transfers kann ein Nachweis einem Dritten übertragen werden, welcher damit zum neuen Inhaber wird.
- Ein durch die Governance berechtigter **Herausgeber** prüft die Eigenschaften des Subjekts und belegt diese durch die Ausstellung eines Nachweises (Mühle et al. 2018).
- Eine **Akzeptanzstelle** verlangt zum Aufbau von Vertrauen und zur Gewährung bestimmter Rechte von Inhabern Nachweise bestimmter Herausgeber (Liu et al. 2020b).
- Ein **Modifikator** ist in der Lage, die Inhalte und den Status eines Nachweises zu verändern, d. h. ihn zu entziehen oder zu entwerten.

4.3 Entstehung digitaler Ökosysteme durch interoperable Nachweise

Das Zusammenspiel von Technologie und Governance wird im *Trust over IP Framework* der gleichnamigen Stiftung systematisiert (Huitema et al. 2021). Dieses Framework beschreibt auf vier Ebenen ein Modell zur Schaffung von Vertrauen im Internet. Der Nachweisaustausch ist auf Ebene 3 angesiedelt und setzt auf die technischen Grundlagen von Kommunikation zwischen Agents und Wallets auf. Dabei wird deutlich, dass es auf jeder Ebene geeigneter Regelwerke bedarf, die den Technologieeinsatz nachvollziehbar und damit vertrauenswürdig machen (Abb. 5).

Wie erläutert, unterliegen Nachweise jeweils einer eigenen Governance. Diese bildet durch die Definition von zulässigen Akteuren sowie Regeln zu Art, Umfang und Handhabung von Daten und Nachweisen eine **Vertrauensdomäne**. Akteure

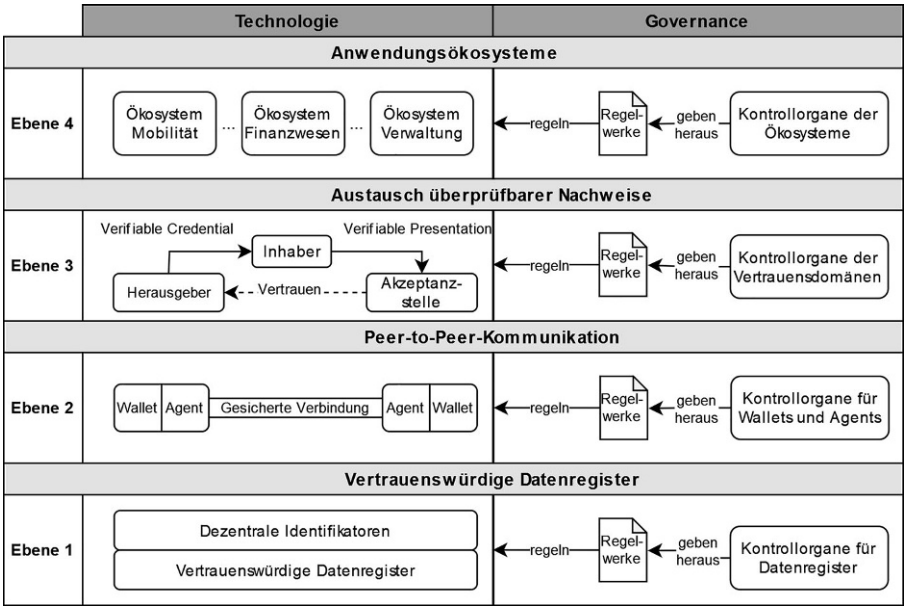

Abb. 5 Das „Trust over IP"-Modell als Rahmenwerk für digitales Vertrauen. (Modifiziert nach Huitema et al. 2021)

werden durch ihre Rolle als Herausgeber, Inhaber, Akzeptanzstelle und Modifikator von Nachweisen Teil verschiedener Vertrauensdomänen. Durch die Verschränkung von Vertrauensdomänen entstehen **Ökosysteme**, in denen digitale und digital-unterstützte Dienstleistungen erbracht werden.

In konkreten Anwendungen werden oft verschiedene Nachweise benötigt, um den gewünschten Geschäfts- oder Verwaltungsprozess durchzuführen. So erfordert beispielsweise Carsharing (Ökosystem Mobilität) den Führerschein (Ökosystem Verwaltung) und einen Bonitätsnachweis (Ökosystem Finanzwesen), um den Status „Kunde“ zu erlangen. Dieser Status-Nachweis wird vom Carsharing-Anbieter selbst ausgestellt, und eventuell um einen Nachweis über eine Haftpflichtversicherung ergänzt. Für die Buchung der Fahrzeuge können Kunden und Kundinnen ggf. Ermäßigungen geltend machen, z. B. durch Coupons, die von Partnerorganisationen ausgegeben werden. Nicht zuletzt ist für Elektrofahrzeuge auch die Berechtigung zur Nutzung von Ladesäulen durch Ladekarten des entsprechenden Betreibers erforderlich (Ökosystem Energiewirtschaft).

Die technische, semantische und rechtliche Standardisierung von Nachweisen macht sie interoperabel, d. h. in verschiedenen Kontexten unter Verwendung einer einheitlichen Infrastruktur einsetzbar. Dies verbessert die Zugänglichkeit der Dienste für Nutzende und reduziert Kosten sowie Komplexität für Dienstanbieter. Da diese Interoperabilität derzeit fehlt, sind Akzeptanzstellen gezwungen, verschiedene Formate, Protokolle und Systeme zu unterstützen, um die benötigen Nachweise digital zu verarbeiten. Dies zieht sehr hohe Kosten nach sich, weshalb derzeit oft auf papier-basierte Nachweise ausgewichen wird. In der Standardisierung des digitalen Nachweisaustauschs durch selbstbestimmte Identitäten steckt daher ein enormes Potenzial.

5 Perspektiven für Forschung und Entwicklung

5.1 Aktuelle Initiativen und Projekte

Der Bildung digitaler Ökosysteme stehen noch diverse Herausforderungen gegenüber, die von Laatikainen et al. (2021a) systematisiert wurden: Sie nennen unter anderem ungenügende Reife der Technologie, unklare Skalierbarkeit, mangelhafte Nutzbarkeit, fehlende Standardisierung, unzureichende Entwicklung der Governance sowie fehlende Interoperabilität mit bestehenden Systemen. Zudem werden rechtliche und regulatorische Unsicherheit, unklare Geschäftsmodelle sowie hohe Kosten für die Anpassung von Systemen und Prozessen als Hürden aufgeführt.

An der Beseitigung dieser Hürden zur Entwicklung einer neuen Generation digitaler Identitäten auf Basis des SSI-Paradigmas wird weltweit gearbeitet. In Deutschland sind vor allem die vier Projekte ID-Ideal, IDunion, ONCE und SDIKA des Schaufensterprogramms „Sichere Digitale Identitäten“[4] des BMWK zu nennen. Ziel des Programms ist es insbesondere, neue Ansätze für interoperable Identitäten in Modellregionen praktisch zu erproben und damit wertvolle Erkenntnisse für die

[4] http://www.schaufenster-sdi.de/.

technische und rechtliche Weiterentwicklung auf nationaler und europäischer Ebene zu liefern.

Parallel dazu wird die seit 2014 gültige europäische Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS) novelliert. Sie regelt die Eigenschaften und gegenseitige Anerkennung staatlicher elektronischer Identitäten und Dienste für die Ausgabe von elektronischen Signaturen, Siegeln, Zeitstempeln und Website-Zertifikaten. Die neue Fassung sieht gemäß aktuellem Entwurf (Council of the EU 2022) vor, dass jeder Mitgliedsstaat seinen Bürgerinnen und Bürgern mindestens eine „EU Digital Identity Wallet" (EUDIW) bereitstellt. Diese Wallet soll eine hoheitliche Identität der jeweiligen Mitgliedsstaaten sowie weiterführende Merkmale der Person aufnehmen. Die Entwicklung der EUDIW wird durch folgende Pilotprojekte begleitet:

- Das *POTENTIAL-Konsortium*[5] arbeitet am Einsatz der EUDIW für regulierte Anwendungen, u. a. Bankkonto eröffnen, SIM-Karte registrieren sowie Führerschein und e-Rezept nutzen.
- Das *EU Digital Identity Wallet Konsortium*[6] fokussiert sich auf den internationalen Reiseverkehr, Hotelbuchung sowie dem Kauf und Bezahlung von Waren und Dienstleistungen.
- Das von Banken besetzte *NOBID-Konsortium*[7] entwickelt grenzüberschreitend einsetzbare wallet-basierten Zahlungsmitteln und deren Akzeptanz im Einzelhandel.
- Das *Digital Credentials for Europe-Konsortium*[8] erarbeitet Anwendungsfälle in den Bereichen Bildung und Sozialversicherung in mehreren europäischen Ländern auf Basis der EUDIW.

Für die weltweite Verbreitung sind insbesondere folgende Aktivitäten zur Standardisierung relevant:

- Das *World Wide Web Consortium* hat die Spezifikationen für „Decentralized Identifier" und dem „Verifiable Credential Data Model" bis zur höchsten Stufe (Recommendation) vorangetrieben.
- Die *Decentralized Identity Foundation* arbeitet u. a. an der Standardisierung von Protokollen für den Nachrichtenaustausch auf Basis einer einheitlichen Methodik namens „DIDcomm".
- Ziel der *Open Wallet Foundation* ist die Entwicklung einer einheitlichen Open Source Engine für sichere Wallets, die zur Interoperabilität der darauf basierenden Wallet-Lösungen sowie zur Senkung der Entwicklungskosten beitragen soll. Vorbilder sind Browser Engines wie Webkit.
- Die *OpenID-Foundation* entwickelt ein Protokoll zur Erzeugung und Überprüfung von Verifiable Credentials (OpenID4VC) sowie der Nutzung von Wallets als (Self-Issued) Identity Provider.

[5] https://www.digital-identity-wallet.eu/.

[6] https://eudiwalletconsortium.org/.

[7] https://www.nobidconsortium.com/.

[8] https://www.dc4eu.eu/.

Die große Vielfalt zeigt einerseits das breite Interesse verschiedener Akteure am Thema SSI und illustriert das Potenzial dieses Konzepts. Gleichzeitig bestehen sowohl technisch als auch regulatorisch noch Defizite, so dass es für die praktikable Umsetzung noch einiger Entwicklung bedarf.

5.2 Herausforderungen für die Wirtschaftsinformatik

Wie gezeigt wurde, ist die Etablierung von zukunftsweisenden Identitätssystemen eine sehr herausfordernde Aufgabe. Die Wirtschaftsinformatik ist mit der soziotechnischen Perspektive der Informationssysteme und ihrem vielfältigem Methodenvorrat dafür prädestiniert, hierfür maßgebliche Beiträge zu leisten. Aus den vorangegangenen Ausführungen lassen sich dabei vier zentrale Perspektiven ableiten (Abb. 6), die nachfolgend kurz erläutert werden. Zu jeder Perspektive werden Forschungsfelder und ausgewählte Forschungsergebnisse der Wirtschaftsinformatik genannt.

Aus Sicht von **Organisationen** stellt sich die Frage, unter welchen Bedingungen sich die Nutzung digitaler Nachweise lohnt und wie bestehende Systeme dafür angepasst werden können. Gleichzeitig eröffnen sich Chancen für neue Geschäftsmodelle. Forschungsfelder für diese Perspektive sind:

- *Datenökonomie:* Der standardisierte Austausch digitaler Nachweise schafft Innovationspotenziale für neue Wertschöpfung in der Datenökonomie (Kölbel et al. 2022), z. B. Echtheitsnachweise für Produkte oder plattform-übergreifendes Reputationsmanagement (Hesse und Teubner 2020).
- *Service System Transformation:* Dienstleistungen in Wirtschaft und Verwaltung müssen angepasst werden, um von den Vorteilen digitaler Nachweise zu profitieren. Für diese Transformation sind Methoden und Werkzeugen erforderlich. Grundlage für deren Entwicklung können Beispiele für SSI-basierte Anwendungsszenarien sein (Feulner et al. 2022; Richter und Anke 2021). Auch die Bewertung von Auswirkungen dieser Veränderungen im Hinblick auf Ziele der Betroffenen ist bislang kaum systematisch untersucht (Jürgenssen et al. 2022).

Abb. 6 Perspektiven und Forschungsfelder der Wirtschaftsinformatik im Kontext digitaler Identitäten

- *Business Process Management:* Die Koordination der Leistungserbringung durch mehrere Akteure wird mit Hilfe von Geschäftsprozessen beschrieben, die sich ebenfalls durch den Einsatz digitaler Nachweise verändern. Hier wären u. a. Aspekte geeigneter Werkzeuge und Modellierungssprachen sowie die Rolle von Vertrauen und Unsicherheit in Prozessen zu betrachten (Müller et al. 2020).

Für **Individuen** ist es wichtig, gut nutzbare Technik zu erhalten, die den einfachen und nachvollziehbaren Umgang mit digitalen Identitäten erlaubt und vor dem Missbrauch der eigenen Daten schützt. Zudem sollen digitale Nachweise aber auch dazu dienen, die Vertrauenswürdigkeit von Dritten festzustellen, z. B. um Fake Shops zu erkennen. Mögliche Forschungsfelder dafür sind:

- *Usability:* Der Umgang mit digitalen Identitäten in einer Wallet ist für die meisten Menschen noch sehr ungewohnt. Daher müssen solche Systeme mit einer hohen Gebrauchstauglichkeit gestaltet werden, die bislang noch nicht ausreichend gegeben ist (Sartor et al. 2022). Zudem sind Sicherheitskonzepte erforderlich, die vor unbedachtem Übermitteln von Daten an Dritte ohne klar erkennbare Notwendigkeit und Zweck warnen. Mechanismen der *Usable Security* bzw. *Usable Privacy* können dabei unterstützen, derartige Risiken besser zu erkennen.
- *Technologieakzeptanz:* Die von digitalen Identitäten gewünschten Effekte treten nur dann ein, wenn die damit verbundene Technik auch eingesetzt wird. Dafür sind Fragen des Mehrwerts, einfachen Nutzbarkeit und Nutzungsabsicht relevant, die in Technologieakzeptanzmodellen systematisiert werden (Guggenberger et al. 2022).
- *Privacy:* Aus Sicht der Nutzenden ist die Offenlegung ihrer Identität und die damit verbundene Bereitstellung von Daten oft nicht gewünscht. Die Sammlung und Auswertung von personenbezogenen Daten von großen Unternehmen für die eigene Wertschöpfung, z. B. im zielgerichteten Marketing wird von vielen Menschen skeptisch gesehen (Beduschi 2021).

Der Einsatz digitaler Identitäten findet in einem Rechtsrahmen statt, der von **Gesellschaft und Politik** ausgehandelt wird. Dabei sind Ziele wie der Schutz des Individuums, Sicherstellung gesellschaftlicher Teilhabe[9], wettbewerbsfähige Wirtschaft sowie eine effiziente Verwaltung relevant. Durch die Rahmenbedingungen wird festgelegt, welche Akteure unter welchen Bedingungen wie mit digitalen Identitäten umgehen dürfen. Dies kann u. a. durch folgende Forschungsfelder untersucht werden:

- *Service Ecosystems:* Sowohl an der Entwicklung als auch an der Leistungserbringung von Dienstleistungen im Zusammenhang mit digitalen Identitäten sind zahlreiche Akteure beteiligt. Service Ecosystems erlauben die Analyse solcher Strukturen und die Gestaltung einer geeigneten Governance (Laatikainen et al. 2021a).
- *Digitale Ethik:* Beim Entwurf von Identitätssystemen sind nicht nur menschzentrierte Prinzipien zur formulieren, sondern auch die Technik zu verwenden, die de-

[9] Siehe dazu auch die Europäische Erklärung zu digitalen Rechten und Prinzipien: https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.

ren Erfüllung bestmöglich erreichen lässt (Ishmaev 2020). Dies umfasst z. B. die Berücksichtigung von technischen Fähigkeiten und Möglichkeiten aller Nutzenden. Damit wird eine wichtige Voraussetzung für die Akzeptanz solcher Systeme geschaffen. Grundlage dafür ist eine entsprechende Orientierung an geeigneten Werten, die wiederum Ausdruck einer bestimmten Weltanschauung sind (Whitley und Schoemaker 2022).

Die Entwicklung von **Technologie** sollte schließlich daran ausgerichtet werden, die Ziele aller Interessensgruppen bestmöglich zu erreichen. Dabei ist auch der sichere und ökonomisch nachhaltige Betrieb von Infrastrukturen zu berücksichtigen, welcher in folgenden Forschungsfeldern untersucht wird:

- *Dezentrales Vertrauen:* Eine Herausforderung im Umgang mit dezentralen Identitäten ist die Schaffung von technischem Vertrauen und dessen Verbindung mit geeigneter Governance. Es gilt zu klären, mit welchen technischen Mitteln Akzeptanzstellen die Vertrauenswürdigkeit von Herausgebern prüfen können. Dafür wurden bereits Blockchains (Liu et al. 2020a), Trustlists oder der Domain Name Service (Jeyakumar et al. 2022) vorgeschlagen.
- *Geschäftsmodelle:* Dienste und Komponenten für den Umgang mit digitalen Identitäten umfassen Identity Provider, Wallet-Anbieter, Betreiber von Registern sowie Dienste für das Ausstellen von elektronischen Signaturen und Siegeln sowie für die Bestätigung von Attributen. Diese müssen für Anwendungen in Wirtschaft und Verwaltung attraktiv sein und gleichermaßen sicher bereitgestellt werden. Dafür sind nachhaltige Betriebskonzepte und Geschäftsmodelle erforderlich (Kubach und Sellung 2021).

6 Fazit

Bislang werden digitale Identitäten vor allem im Kontext von Cybersecurity untersucht. Allerdings ist der Umgang mit digitalen Identitäten ein komplexes Thema, das weit über technische Fragestellungen hinausgeht. Zum einen ist für die Schaffung von Vertrauen zwischen Akteuren neben der eingesetzten Technik auch ein organisatorischer und rechtlicher Rahmen erforderlich. Zum anderen beeinflusst der Umgang mit digitalen Identitäten Interaktionen zwischen Akteuren in allen gesellschaftlichen Bereichen. Für die Akzeptanz und Verbreitung solcher Lösungen ist die Diskussion um Anwendungen und der daraus entstehende Nutzen, aber auch die Gefahren und Risiken für die Gesellschaft insgesamt mindestens genauso wichtig.

Für eine nachhaltige digitale Transformation müssen Systeme für digitale Identitäten so gestaltet werden, dass sie den gesellschaftlichen Nutzen maximieren. Dabei ist die Wirtschaftsinformatik mit ihrem soziotechnischen Fokus auf den Einsatz von IT in Wirtschaft und Verwaltung sowie der Wechselwirkung zwischen Mensch und Technik sehr gut geeignet, hierfür wesentliche Beiträge zu leisten. Daneben sind weitere Disziplinen gefragt, um diese Entwicklung vorzutreiben und zu lenken. Stellvertretend seien hier Politik- und Verwaltungswissenschaften, Soziologie sowie Rechts-, Arbeits- und Kognitionswissenschaften genannt. Nicht zuletzt geht mit dem Einsatz von digitalen Identitäten auch die Frage von Werten einher, die diese Ent-

wicklung leiten müssen. Diese leitenden Werte zu definieren und die Entwicklung daran auszurichten, ist Gegenstand der digitalen Ethik.

Zusammenfassend lässt sich feststellen, dass die Etablierung von digitalen Identitätssystemen nach dem Paradigma der selbstbestimmten Identität die Chance zu einer grundsätzlichen Transformation für die Herstellung vertrauenswürdiger digitaler Interaktionen eröffnet. Gleichzeitig kann die Privatsphäre aller Beteiligten damit besser geschützt werden. Die große Herausforderung besteht dabei darin, die Bedarfe verschiedener Anspruchsgruppen zu ermitteln und bestmöglich auszubalancieren. Alle Beteiligten sind aufgefordert, an diesem Prozess konstruktiv und verantwortungsvoll mitzuwirken, um den größtmöglichen gesellschaftlichen Nutzen aus künftigen digitalen Identitätssystemen zu ziehen.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Abraham R, Schneider J, Vom Brocke J (2019) Data governance: A conceptual framework, structured review, and research agenda. Int J Inf Manage 49:424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Akinci N Digital einkaufen: Fake-Shops erkennen und Schäden vermeiden. heise Online. https://www.heise.de/hintergrund/Digital-einkaufen-Fake-Shops-erkennen-und-Schaeden-vermeiden-7450348.html (Erstellt: 10. Jan. 2023). Zugegriffen: 27.02.2023

Allen C (2016) The path to self-sovereign identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html. Zugegriffen: 27.02.2023

Beduschi A (2021) Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. Data Policy. https://doi.org/10.1017/dap.2021.15

Beldad A, de Jong M, Steehouder M (2010) How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. Comput Human Behav 26(5):857–869. https://doi.org/10.1016/j.chb.2010.03.013

Cameron K (2005) The laws of identity. https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf. Zugegriffen: 27.02.2023

Council of the EU (2022) European digital identity (eID): Council makes headway towards EU digital wallet, a paradigm shift for digital identity in Europe. https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/. Zugegriffen: 27.02.2023

Cucko S, Becirovic S, Kamisalic A, Mrdovic S, Turkanovic M (2022) Towards the classification of self-sovereign identity properties. IEEE Access 10:88306–88329. https://doi.org/10.1109/ACCESS.2022.3199414

Cyphers B, Gebhart G (2019) Behind the one-way mirror: A deep dive into the technology of corporate surveillance. https://www.eff.org/wp/behind-the-one-way-mirror. Zugegriffen: 27.02.2023

Davie M, Gisolfi D, Hardman D, Jordan J, O'Donnell D, Reed D, van Deventer O (2019) The trust over IP stack. The Linux Foundation. https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0289-toip-stack. Zugegriffen: 27.02.2023

eco – Verband der Internetwirtschaft e. V., echConsult GmbH (Hrsg) (2022) Security & digitale Identitäten in einer digitalisierten Welt

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

Feulner S, Sedlmeir J, Schlatt V, Urbach N (2022) Exploring the use of self-sovereign identity for event ticketing systems. Electron Markets 32(3):1759–1777. https://doi.org/10.1007/s12525-022-00573-9

Guggenberger T, Neubauer L, Stramm J, Völter F (2022) Accept me as I am or see me go: A qualitative analysis of user acceptance of self-sovereign identity applications. In: Bui T (Hrsg) Hawaii International Conference on System Sciences (HICSS)

Hesse M, Teubner T (2020) Takeaway Trust: A market data perspective on reputation portability in electronic commerce. In: Bui T (Hrsg) Proceedings of the Annual Hawaii International Conference on System Sciences, Proceedings of the 53rd Hawaii International Conference on System Sciences

Huitema C, Bachenheimer D, O'Donnell D, Reed D, Fleenor J, Young K, Hand K, Kneiss K, Jordan J, Bendixsen L, Subrahmanyam PA, Mukhopadhyay S, Perry S, Syntez V, Malhotra V, Chu W (2021) Introduction to trust over IP: Version 2.0. Trust Over IP Foundation. https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf. Zugegriffen: 27.02.2023

Initiative D21 e. V., TU München (2022) eGovernment MONITOR 2022: Nutzen und akzeptieren Bürger*innen die digitale Verwaltung? Die deutschen Bundesländer, Deutschland, Österreich und die Schweiz im Vergleich. https://initiatived21.de/app/uploads/2022/10/egovernment_monitor_2022.pdf. Zugegriffen: 27.02.2023

Ishmaev G (2020) Sovereignty, privacy, and ethics in blockchain-based identity management systems. Ethics Inf Technol. https://doi.org/10.1007/s10676-020-09563-x

ISO/IEC (2019) IT security and privacy—A framework for identity management: Part 1: Terminology and concepts ((24760-1:2019-05))

Jeyakumar IHJ, Chadwick DW, Kubach M (2022) A novel approach to establish trust in verifiable credential issuers in Self-sovereign identity ecosystems using TRAIN. In: Roßnagel H, Schunck CH, Mödersheim S (Hrsg) Open Identity Summit 2022. Gesellschaft für Informatik e. V., S 27–38 https://doi.org/10.18420/OID2022_02

Jürgenssen O, Richter D, Anke J (2022) Selbstbestimmte digitale Identitäten in der Smart City: Potenziale und Grenzen. In: Gemeinschaften in Neuen Medien: Digitalität und Diversität. TUDpress, Dresden

Kautonen T (2006) Trust as a governance mechanism in inter-firm relations—Conceptual considerations. Evolut Inst Econ Rev 3(1):89–108. https://doi.org/10.14441/eier.3.89

van Kersbergen K, van Waarden F (2004) 'Governance' as a bridge between disciplines: Cross-disciplinary inspiration regarding shifts in governance and problems of governability, accountability and legitimacy. Eur J Political Res 43:143–171

Kölbel T, Härdtner M-C, Weinhardt C (2022) Enterprise business models leveraging self-sovereign identity: Towards a user-empowering me2X economy. In: Bui T (Hrsg) Hawaii International Conference on System Sciences (HICSS)

Kolf F Onlinebetrug zerstört das Vertrauen zwischen Händler und Kunden. Handelsblatt. https://www.handelsblatt.com/unternehmen/handel-konsumgueter/e-commerce-jeder-vierte-wird-opfer-von-internetkriminalitaet-doch-viele-onlinehaendler-ignorieren-das-problem/27525176.html (Erstellt: 18. Aug. 2021). Zugegriffen: 27.02.2023

Kostic S, Heinemann A, Margraf M (2016in) Usability-Untersuchung eines Papierprototypen für eine mobile Online-Ausweisfunktion des Personalausweises. In: Mayr HC, Pinzger M (Hrsg) Informatik 2016: Tagung vom 26.–30. September 2016 in Klagenfurt. GI-Edition : Proceedings, Bd. 259. Gesellschaft für Informatik e. V., S 519–527

Kubach M, Sellung R (2021) On the market for self-sovereign identity: structure and stakeholders. In: Roßnagel A, Schunck CH, Mödersheim S (Hrsg) Open Identity Summit. Symposium im Rahmen der Tagung von Gesellschaft für Informatik, Bonn

Laatikainen G, Kolehmainen T, Abrahamsson P (2021a) Self-sovereign identity ecosystems: Benefits and challenges. In 12th Scandinavian Conference on Information Systems: Living in a digital world?. Association for Information Systems. https://aisel.aisnet.org/scis2021/10/

Laatikainen G, Kolehmainen T, Li M, Hautala M, Kettunen A (2021b) Towards a trustful digital world: exploring self-sovereign identity ecosystems. In: Twenty-fifth pacific asia conference on information systems. Association for Information Systems,
Lankton N, McKnight DH, Tripp J (2015) Technology, humanness, and trust: rethinking trust in technology. J Assoc Inf Syst 16(10):880–918. https://doi.org/10.17705/1jais.00411
Liu Y, He D, Obaidat MS, Kumar N, Khan MK, Raymond Choo K-K (2020a) Blockchain-based identity management systems: A review. J Netw Comput Appl 166:102731. https://doi.org/10.1016/j.jnca.2020.102731
Liu Y, Lu Q, Paik H-Y, Xu X, Chen S, Zhu L (2020b) Design pattern as a service for blockchain-based self-sovereign identity. IEEE Softw 37(5):30–36. https://doi.org/10.1109/MS.2020.2992783
Luo X (2002) Trust production and privacy concerns on the Internet. Ind Mark Manag 31(2):111–118. https://doi.org/10.1016/S0019-8501(01)00182-1
McKnight DH, Chervany NL (1996) The meanings of trust (MISRC 9604). University of Minnesota MIS Research Center
McKnight DH, Choudhury V, Kacmar C (2002) Developing and validating trust measures for e-commerce: an integrative typology. Inf Syst Res 13(3):334–359. https://doi.org/10.1287/isre.13.3.334.81
Milliman RE, Fugate DL (1988) Using trust-transference as a persuasion technique: an empirical field investigation. J Pers Sell Sales Manag 8(2):1–7
Mühle A, Grüner A, Gayvoronskaya T, Meinel C (2018) A survey on essential components of a self-sovereign identity. Comput Sci Rev 30:80–86
Müller M, Garzon SR, Rosemann M, Kupper A (2020) Towards trust-aware collaborative business processes: an approach to identify uncertainty. IEEE Internet Comput 24(6):17–25. https://doi.org/10.1109/MIC.2020.3023180
Petrlic R, Sorge C, Ziebarth W (Hrsg) (2022) Datenschutz. Springer, Wiesbaden https://doi.org/10.1007/978-3-658-39097-6
Pohlmann N (2022) Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung, 2. Aufl. Springer Vieweg, Wiesbaden https://doi.org/10.1007/978-3-658-36243-0
Povey D (1999) Developing electronic trust policies using a risk management model. In: Goos G, Hartmanis J, van Leeuwen J, Baumgart R (Hrsg) Secure Networking—CQRE [Secure] ' 99. Lecture notes in computer science, Bd. 1740. Springer, Berlin, Heidelberg, S 1–16 https://doi.org/10.1007/3-540-46701-7_1
Preukschat A, Reed D (2021) Self sovereign identity: Decentralized digital identity and verifiable credentials
Richter D, Anke J (2021) Exploring potential impacts of self-sovereign identity on smart service systems. Bus Inf Syst. https://doi.org/10.52825/bis.v1i.68
Sartor S, Sedlmeir J, Rieger A, Roth T (2022) Love at first sight? A user experience study of self-sovereign identity wallets. ECIS 2022 research papers. https://aisel.aisnet.org/ecis2022_rp/46
Searle JR (2006) Social ontology: Some basic principles. Anthropol Theory 6(1):12–29
Sedlmeir J, Smethurst R, Rieger A, Fridgen G (2021) Digital identities and verifiable credentials. Bus Inf Syst Eng 63:603–613. https://doi.org/10.1007/s12599-021-00722-y
Sinell A, Beckmann M (2022) Digitale Identitäten: der Online-Ausweisfunktion zum Durchbruch verhelfen. DigitalService GmbH des Bundes. https://digitalservice.bund.de/blog/projekt-digitale-identitaeten. Zugegriffen: 27.02.2023
Skierka I (2020) Digitale Identitäten. In: Klenk T, Nullmeier F, Wewer G (Hrsg) Handbuch Digitalisierung in Staat und Verwaltung. Springer, Wiesbaden, S 1–12 https://doi.org/10.1007/978-3-658-23669-4_66-1
Smith B, Loddo OG, Lorini G (2020) On credentials. J Soc Ontol 6(1):47–67. https://doi.org/10.1515/jso-2019-0034
Sporny M, Longley D, Chadwick DW (2022) Verifiable credentials data model v1.1: W3C recommendation. W3C. https://www.w3.org/TR/2022/REC-vc-data-model-20220303/. Zugegriffen: 27.02.2023
Sztompka P (2003) Trust: a sociological theory. Cambridge University Press (CUP)
Temoshok D, Galluzzo R, LaSalle C, Lefkovitz N, Regenscheid A, Choong Y-Y, Proud-Madruga D, Gupta S (2022) Digital identity guidelines. Initial public draft (SP 800-63-4 ipd) https://doi.org/10.6028/NIST.SP.800-63-4.ipd
UC Berkeley (Hrsg) (2019) Pseudonymous identity—Privacy patterns. https://privacypatterns.org/patterns/Pseudonymous-identity. Zugegriffen: 27.02.2023

Verbraucherzentrale (2021) Welche Folgen Identitätsdiebstahl im Internet haben kann | Verbraucherzentrale.de. https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/welche-folgen-identitaetsdiebstahl-im-internet-haben-kann-17750. Zugegriffen: 27.02.2023

Whitley EA, Schoemaker E (2022) On the sociopolitical configurations of digital identity principles. Data Policy. https://doi.org/10.1017/dap.2022.30