verbraucherzentrale
Nordrhein-Westfalen

Nils Urbach

SELBSTBESTIMMTE IDENTITÄTEN ZUR STÄRKUNG DER DIGITALEN SOUVERÄNITÄT

Vortrag 8 der Reihe „Zu treuen Händen“ | Januar 2022

Eine Online-Vortragsreihe der Verbraucherzentrale NRW e. V.

VERBRAUCHER INFORMATIK

mit Unterstützung durch das
Institut für Verbraucherinformatik der Hochschule Bonn-Rhein-Sieg

Impressum

Verbraucherzentrale Nordrhein-Westfalen e.V
Kompetenzzentrum Verbraucherforschung NRW.
Mintropstraße 27
40215 Düsseldorf
zutreuenhaenden@verbraucherzentrale.nrw

Gefördert durch

Ministerium für Umwelt, Landwirtschaft,
Natur- und Verbraucherschutz
des Landes Nordrhein-Westfalen

ORIGINALBEITRAG

Verbraucherzentrale NRW, Düsseldorf 2022

AUTOR

Prof. Dr. Nils Urbach ist Inhaber der Professur für Wirtschaftsinformatik, insbesondere Digital Business & Mobilität, sowie Direktor des Research Lab of Digital Innovation & Transformation (ditlab) an der Frankfurt University of Applied Sciences. Zudem ist er stellvertretender wissenschaftlicher Leiter des Kernkompetenzzentrums Finanz- & Informationsmanagement (FIM) und der Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT sowie Mitgründer und -leiter des Fraunhofer Blockchain-Labors.

DOKUMENTION „ZU TREUEN HÄNDEN?“
Alle Videos und Paper der Vortragsreihe finden Sie unter
https://www.verbraucherforschung.nrw/zu-treuen-haenden-tagungsreihe-datenintermediaere-datentreuhaender-60831

INHALT

I. ABSTRACT

Durch die Nutzung von Internetdiensten entstehen derzeit wenig transparente und kaum kontrollierbare Datensilos. Im Sinne einer digitalen Souveränität des Einzelnen ist es daher erstrebenswert, die Nutzer:innen selbstbestimmt darüber entscheiden zu lassen, wann, wie und wofür persönliche Daten übermittelt werden. Das Konzept der selbstbestimmten Identitäten (engl. self-sovereign identities) setzt an dieser Stelle an und versucht, die gegenwärtigen Herausforderungen des digitalen Identitätsmanagements zu adressieren. Dieser Beitrag geht sowohl auf die konzeptionellen Grundlagen als auch auf die Chancen und Herausforderungen von selbstbestimmten Identitäten ein und zeigt auf, wie sie zur Stärkung der digitalen Souveränität von Verbraucher:innen beitragen können.

II. NOTWENDIGKEIT VON WEITERENTWICKLUNGEN IM DIGITALEN IDENTITÄTSMANAGEMENT

Digitale Identitäten spielen bei der Nutzung von digitalen Dienstleistungsangeboten eine immer zentralere Rolle, der Umgang mit ihnen bedeutet jedoch nach wie vor eine Herausforderung für Nutzer:innen und Anbieter. Hintergrund ist, dass das Internet seit seinen Ursprüngen ohne eine Identitätsschicht konzipiert wurde. Hierbei handelte es sich um eine absichtliche Designentscheidung mit dem Ziel, den Nutzer:innen eine möglichst hohe Anonymität und Privatsphäre zu ermöglichen. Diese Eigenschaft des Internets verdeutlicht der populäre Cartoon von Peter Steiner, der 1993 im *The New Yorker* veröffentlicht wurde: „On the internet, nobody knows you're a dog". In Anlehnung daran ging einige Jahre später, im Jahr 2015, der Cartoon „On the internet, nobody knows you're a fridge" in den sozialen Medien viral, um auf die Analogie zum Internet der Dinge hinzuweisen. Während der freiheitliche Ansatz des frühen Internets hinsichtlich der Einhaltung der Persönlichkeitsrechte der Nutzer:innen als grundsätzlich positiv zu bewerten ist, wurde dieser in den vergangenen Jahren durch teilweise im Verborgenen bleibende Nutzerprofile immer weiter aufgeweicht. Des Weiteren stoßen digitale Dienstleistungsangebote immer häufiger an ihre Grenzen, wenn besonders hohe Anforderungen an die Authentifizierung der Nutzer:innen gestellt werden.

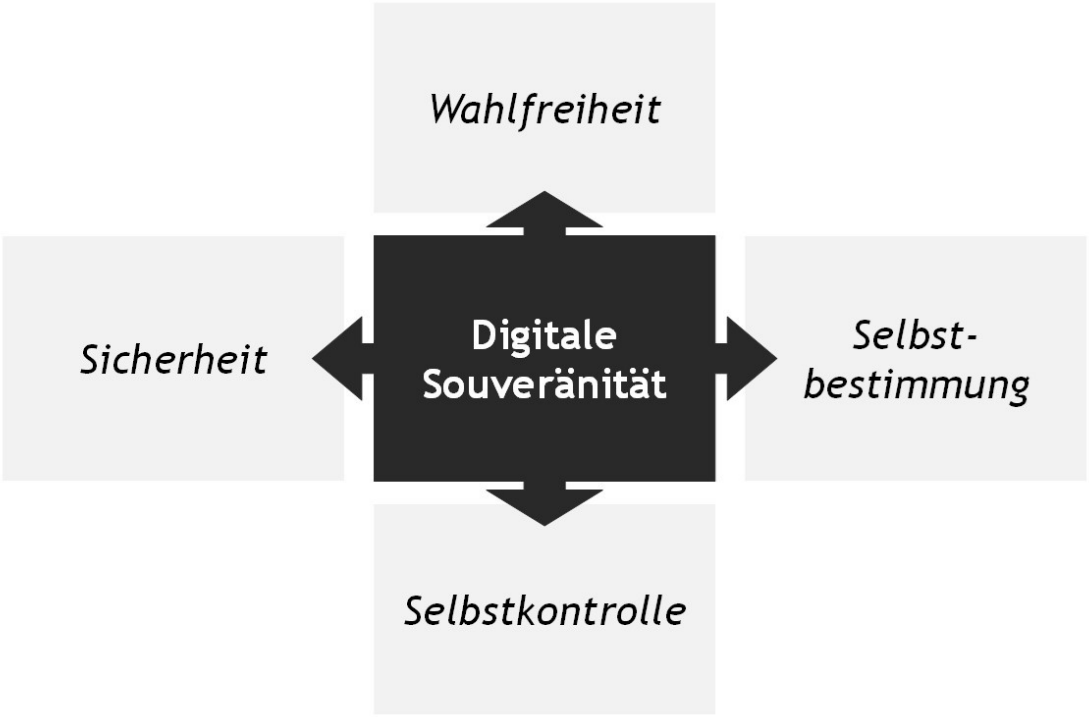
Die Bedeutsamkeit und Notwendigkeit einer Weiterentwicklung des digitalen Identitätsmanagements im Zeitalter der Digitalisierung wird zunehmend von Wirtschaft und Politik erkannt. So stellt beispielsweise das Bundeskanzleramt in einem im Jahr 2021 erschienenen Whitepaper zum Thema Digitale Identität heraus, dass „[d]as Fehlen digitaler Nachweise eines der drängendsten Digitalisierungshemmnisse unserer Zeit [darstellt]" (Bundeskanzleramt 2021, 2). Ebenso weist der Präsident des Branchenverbands der deutschen Informations- und Telekommunikationsbranche, Bitkom, darauf hin, dass „[d]ie Einführung einer digitalen Identität und die Abschaffung der Schriftformerfordernisse […] es möglich machen [würden], sämtliche Behördengänge digital zu erledigen" (Stiens 2021). Tatsächlich wird die Schaffung eines vertrauenswürdigen digitalen Identitätsmanagements auch bereits durch verschiedene Initiativen vorangetrieben. Forschungsprojekte wie die Schaufensterprojekte Sichere Digitale Identitäten des Bundeswirtschaftsministeriums, die Pilotierungsprojekte des Bundeskanzleramts sowie das Blockchain Machine Identity Ledger der Deutschen Energie-Agentur (Dena) stellen

vielversprechende Ansätze in diesem Kontext dar. Es ist zu erwarten, dass auch die neue Bundesregierung nach dem Regierungswechsel im Jahr 2021 den eingeschlagenen Kurs fortsetzen wird. Zumindest weist der zwischen den Regierungsparteien vereinbarte Koalitionsvertrag, in dem „[e]in vertrauenswürdiges, allgemein anwendbares Identitätsmanagement sowie die verfassungsfeste Registermodernisierung“ mit Priorität versehen werden, explizit darauf hin (Koalitionsvertrag 2021, 15).

III. ANFORDERUNGEN AN EIN DIGITALES IDENTITÄTSMANAGEMENT AUS SICHT DER DIGITALEN SOUVERÄNITÄT

Bei der Entwicklung digitaler Angebote – gerade, wenn diese von öffentlicher Hand gefördert oder gar maßgeblich vorangetrieben werden – spielt das Ziel der digitalen Souveränität der Nutzer:innen eine immer bedeutsamere Rolle. Durch eine datenschutzfreundliche Gestaltung von Technologie, durch Stärkung der digitalen Kompetenz der Verbraucher:innen und durch umsichtige Regulierung sollen die Vorteile der Digitalisierung möglichst vielen Verbraucher:innen zugutekommen. Der Sachverständigenrat für Verbraucherfragen hat in einem im Jahr 2017 veröffentlichten Gutachten vier Leitlinien identifiziert (siehe Abbildung 1), die im Zusammenhang mit digitaler Souveränität stehen: Wahlfreiheit, Selbstbestimmung, Selbstkontrolle und Sicherheit (Sachverständigenrat für Verbraucherfragen 2017).

Abbildung 1: Leitlinien der digitalen Souveränität



Quelle: Eigene Darstellung

Die Leitlinie der *Wahlfreiheit* umfasst sowohl Aspekte negativer Handlungsfreiheit („Freiheit von etwas“) wie auch positiver Handlungsfreiheit („Freiheit zu etwas“). Die Verbraucher:innen sollen demnach weitgehend frei darin sein, etwas zu tun oder auch

zu unterlassen (zum Beispiel möglichst geringe Lock-in-Effekte bei digitalen Diensten). Zur Wahlfreiheit gehört ebenso die Entscheidung, ob anderen die Einsicht in personenbezogene Daten der Nutzer:innen erlaubt sein soll oder nicht.

Selbstbestimmung im Umgang mit digitalen Medien zielt darauf ab, dass die Verbraucher:innen selbst die Hoheit über wichtige Entscheidungen behalten. Demnach sollen sie grundsätzlich nicht das Objekt automatisierter Entscheidungen auf der Grundlage von Algorithmen sein, die von erheblicher Bedeutung für ihre Lebensführung sind. Die Zweckbindung bei der Erhebung und Verwendung personenbezogener Daten ist daher ein wichtiger Faktor, ebenso die Option, dass diese Daten anonymisiert gespeichert und ausgewertet werden. *Selbstkontrolle* bedeutet in diesem Kontext, dass Nutzer:innen in der Lage sind, selbst die Grenzen der eigenen Nutzung digitaler Angebote festzulegen und die Konsequenzen ihres Verhaltens abzuschätzen. Diese Leitlinie umfasst nicht nur die Gestaltung eines souveränen Agierens innerhalb der digitalen Welt, sondern fordert einen ebenso souveränen Umgang mit der digitalen Welt im Sinne der Fähigkeit, digitale Dienste bei der Nutzung kontrollieren zu können, nicht aber kontrolliert oder im Verhalten maßgeblich beeinflusst zu werden. Die Leitlinie *Sicherheit* soll schließlich den Schutz von Verbraucherdaten und digitalen Infrastrukturen durch den Staat und Unternehmen sowie durch Verbraucher:innen selbst gewährleisten. Zu diesem Zweck sollen Infrastrukturen bereitgestellt werden, die eine sichere Erhebung, Speicherung sowie eine kontrollierte Weitergabe von Daten ermöglichen (Sachverständigenrat für Verbraucherfragen 2017, 4–5).

Im Sinne einer Stärkung der digitalen Souveränität können diese vier Leitlinien als Anforderungen an digitale Lösungen verstanden werden. Entsprechend gilt es auch bei der Weiterentwicklung des digitalen Identitätsmanagements, diese Anforderungen bestmöglich zu adressieren. Inwiefern der in diesem Artikel vorgestellte Ansatz der selbstbestimmten Identitäten dafür geeignet ist, die digitale Souveränität der Nutzer zu stärken, wird in Kapitel 4 diskutiert.

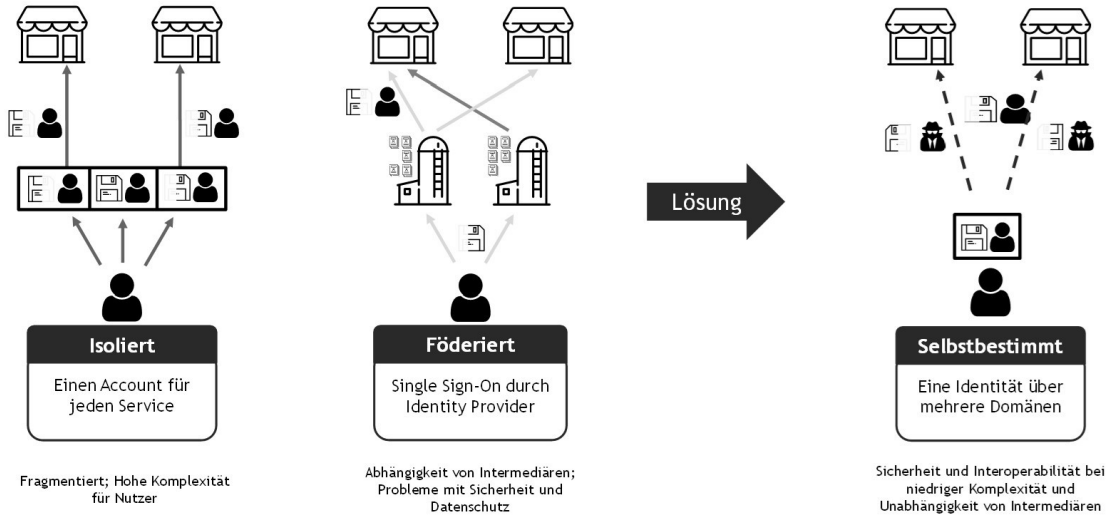
IV. DAS KONZEPT DER SELBSTBESTIMMTEN IDENTITÄTEN ALS MÖGLICHER LÖSUNGSANSATZ

Zur Adressierung der herausgestellten Notwendigkeit von Weiterentwicklungen im digitalen Identitätsmanagement unter Berücksichtigung der Anforderungen der digitalen Souveränität der Nutzer:innen hat sich im Laufe des Jahres 2021 der Ansatz der selbstbestimmten Identitäten (Self-sovereign identities, kurz: SSI) als möglicher Lösungsansatz herauskristallisiert.

1. ENTWICKLUNGSSTUFEN DES DIGITALEN IDENTITÄTSMANAGEMENTS

Der Ansatz der selbstbestimmten Identitäten kann als Weiterentwicklung früher Ansätze des digitalen Identitätsmanagements angesehen werden (Strüker et al. 2021) (siehe Abbildung 2).

Abbildung 2: Entwicklungsstufen des digitalen Identitätsmanagements



Quelle: Eigene Darstellung

Die etablierteste Form des digitalen Identitätsmanagements ist der *isolierte* Ansatz, der gegenwärtig bei den allermeisten digitalen Dienstleistungsangeboten Anwendung findet. Hierbei verwalten die Nutzer:innen die Zugänge zu den verschiedenen Diensten selbst, mit jeweils eigenen Accounts für jeden genutzten Service. Sofern die Nutzer:innen für jeden genutzten Dienst unterschiedliche Passwörter verwenden, kann dieser Ansatz als vergleichsweise sicher angesehen werden. Gleichzeitig bedeutet ein solcher fragmentierter Ansatz jedoch eine relativ hohe Komplexität für die Nutzer:innen und hat somit eine sehr geringe Nutzungsfreundlichkeit.

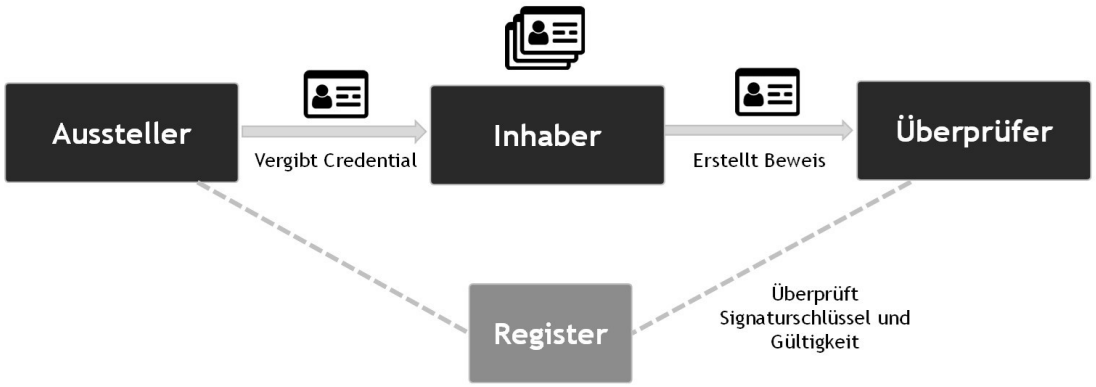
Eine *föderierte* Identität stellt die nächste Entwicklungsstufe im digitalen Identitätsmanagement dar und zielt vor allem darauf ab, die geringe Nutzungsfreundlichkeit vorheriger Ansätze zu verbessern. Dies soll erreicht werden, indem den Nutzer:innen durch eine zentrale Log-in-Instanz die Möglichkeit eröffnet wird, ihre Identitätsdaten mit anderen Anbietern zu teilen. Dieses Prinzip wird unter dem Begriff Single Sign-on vor allem von etablierten Internetdiensten wie Facebook, LinkedIn oder Google angeboten. Nach einmaliger Registrierung bei einem dieser (Identitäts-)Anbieter können die Nutzer:innen ihre Identitätsdaten per Knopfdruck zu einem anderen Dienst transferieren. Die Weitergabe der Daten erfordert dabei stets den Zugriff auf den zentralen Log-in-Dienst. Die erhöhte Nutzungsfreundlichkeit dieses Ansatzes ist unbestritten. Gleichzeitig entsteht hierbei jedoch eine hohe Abhängigkeit von immer mächtiger werdenden zentralen Log-in-Diensten mit inhärenten Problemen hinsichtlich Datensicherheit und Datenschutz.

Die Kernidee des Ansatzes der *selbstbestimmten* Identitäten besteht nun darin, die Vorteile der beiden zuvor genannten Ansätze zu verbinden, ohne dabei die jeweiligen Nachteile in Kauf nehmen zu müssen. Der Ansatz sieht vor, dass die Nutzer:innen ihre digitale Identität von zentraler Stelle, nämlich bei den Nutzer:innen selbst, über verschiedene Anwendungsdomänen hinweg verwenden. Als zentraler Verwalter ihrer digitalen Identitäten soll den Nutzer:innen so ermöglicht werden, über alle verschiedenen Dienste hinweg die Kontrolle über ihre Identität zu wahren und damit eine Autonomie in der Verwaltung dieser Dienste zu erzielen. Dadurch soll ein hohes Niveau an Sicherheit und Interoperabilität bei gleichzeitig niedriger Komplexität und Unabhängigkeit von Intermediären erreicht werden.

2. GRUNDLEGENDE FUNKTIONSWEISE VON SELBSTBESTIMMTEN IDENTITÄTEN

Im Wesentlichen sind selbstbestimmte Identitäten wie Nachweise in einer Brieftasche zu verstehen. Analog zur Sammlung von unterschiedlichen Ausweisen wie Personalausweis, Führerschein oder Kreditkarte in der physischen Welt, dient eine Digital Wallet zur Speicherung von digitalen Zertifikaten (engl. credentials). Diese Credentials können entweder selbst attestierte Identitätsattribute enthalten oder solche, die durch Dritte attestiert wurden. Durch Dritte attestierte Credentials werden als Verifiable Credentials bezeichnet. Die Digital Wallets der Nutzer:innen können dabei als Steuerzentrale des Austauschs der Identitätsdaten verstanden werden. Der Ansatz der selbstbestimmten Identitäten sieht vor, dass Interaktionen immer und ausschließlich nutzerzentriert gesteuert werden. Durch die in der Digital Wallet enthaltenen Verifiable Credentials werden die Nutzer:innen zu bilateralen Interaktionen befähigt. Ein solches Verifiable Credential besteht dabei sowohl aus den Identitätsdaten selbst als auch aus einer Signatur des Ausstellers, über die die Echtheit der ausgestellten Identitätsdaten überprüft werden kann. Der Prozess der Ausstellung von Verifiable Credentials und der Echtheitsüberprüfung sowie die am Gesamtprozess beteiligen Rollen (siehe Abbildung 3) sollen im Nachfolgenden näher erläutert werden (siehe auch Strüker et al. 2021 für eine detailliertere Darstellung).

Abbildung 3: Rollen und Prozess des selbstbestimmten Identitätsmanagements



Quelle: Eigene Darstellung

Der Ansatz des selbstbestimmten Identitätsmanagements sieht drei zentrale Rollen vor. Die Aufgabe des *Ausstellers* (engl. issuer) besteht in der Vergabe der Verifiable Credentials, die der Inhaber in der jeweiligen Digital Wallet speichern kann. Die Rolle des Ausstellers übernehmen vertrauenswürdige Parteien, deren Identität und damit einhergehend deren Public Key, der zur Überprüfung der Signaturen eines Ausstellers notwendig ist, öffentlich einsehbar sind. Ein Aussteller kann beispielsweise eine öffentliche Institution wie etwa ein Einwohnermeldeamt, eine Führerscheinstelle oder eine Hochschule sein. Der *Inhaber* (engl. holder) ist der Besitzer und meist auch das Subjekt des vom Aussteller vergebenen Verifiable Credentials. Er kann ein Mensch, eine Organisation oder aber auch ein Ding (zum Beispiel eine Maschine) sein. Der Inhaber kann die in seiner Digital Wallet gespeicherten Verifiable Credentials verwenden, um sich bei verschiedenen Diensten auszuweisen. Der *Überprüfer* (engl. verifier) fragt spezifische Identitätsinformationen beim jeweiligen Inhaber an. Er erhält diese in Form einer Verifiable Presentation auf Basis zuvor von ihm festgelegter Anforderungen sowie einen Beweis ihrer Korrektheit. Hierzu wird über ein Register der Signaturschlüssel des Ausstellers sowie die Gültigkeit der verwendeten Verifiable Credentials überprüft.

Ein wesentlicher Vorteil des selbstbestimmten Identitätsmanagements gegenüber alternativen Ansätzen besteht in der Möglichkeit, Identitätsdaten via Verifiable Presentations selektiv preiszugeben. Das bedeutet, dass die Nutzer:innen gerade so wenige Informationen von sich weitergeben, wie tatsächlich aufseiten der Überprüfer erforderlich sind. Das Beispiel einer Kreditaufnahme bei einer Bank soll dies verdeutlichen. Der Bankkunde in der Rolle des Inhabers hat neben seinem (digitalen) Personalausweis auch seinen Steuerbescheid in der Digital Wallet. Mittels einer Verifiable Presentation kann er nun neben den erforderlichen Stammdaten zu seiner Person die von der Bank geforderte Mindesthöhe des Einkommens beweisen. Hierfür muss er nicht einmal die konkrete Höhe seines Einkommens preisgeben. Das eigentliche Verifiable Credential und alle weiteren dort enthaltenen Daten verbleiben dabei ausschließlich beim Nutzer. Die öffentlichen Signaturen der Bundesdruckerei und der Steuerbehörde sorgen für die Vertrauenswürdigkeit der digitalen Zertifikate, deren Gültigkeit von der Bank überprüft werden kann.

Ein weiterer Vorteil des selbstbestimmten Identitätsmanagements gegenüber seinen analogen Alternativen ist, dass Verifiable Credentials nach ihrer Ausstellung widerrufen werden können. Dies geschieht entweder über ein zuvor definiertes Gültigkeitsattribut analog zu den meisten physischen Ausweisdokumenten, wie beispielsweise das Ablaufdatum eines Personalausweises. Die Besonderheit liegt aber darin, dass Verifiable Credentials auch ad hoc widerrufen werden können, beispielsweise beim temporären Einzug eines Führerscheins im Fall eines Verkehrsdeliktes. Hierbei erlaubt der Ansatz der selbstbestimmten Identitäten jedoch explizit nicht, das Verifiable Credential des Inhabers aus seiner Digital Wallet zu löschen, da die Kernidee ja gerade darin besteht, dass die Nutzer:innen die Hoheit über ihre Daten behalten. Daher werden die Gültigkeitsinformationen auf öffentlich zugänglichen Listen gespeichert, die dem Überprüfer für die Gültigkeitsprüfung vorgelegt werden können. Hierbei ist anzumerken, dass nur der Inhaber die Gültigkeit beweisen kann. Eine externe Person hingegen kann diese Liste nicht durchsuchen und Informationen über Gültigkeiten beziehen. Entsprechend können auch die Informationen über Gültigkeiten immer nur vom Inhaber ausgegeben werden. Häufig werden Blockchains als Register für Gültigkeiten, Strukturinformationen (Schemata) und öffentliche Identitäten genutzt. Alternativ könnte grundsätzlich aber auch ein zentraler Server einer Organisation, der alle Teilnehmer des jeweiligen Ökosystems vertrauen, für das Hosting eines solchen Registers verwendet werden. Es ist auch denkbar, dass mehrere unterschiedliche Register zum Einsatz kommen, sodass Verifiable Credentials aus verschiedenen Quellen kombiniert werden könnten.

3. ANWENDUNGSMÖGLICHKEITEN SELBSTBESTIMMTER IDENTITÄTEN

Die Anwendungsmöglichkeiten selbstbestimmter Identitäten sind vielfältig. Im Folgenden sollen zwei exemplarische Anwendungsfälle zur Verdeutlichung von Funktionsweise und Potenzial vorgestellt werden (siehe auch Strüker et al. 2021 für eine detailliertere Darstellung und weitere Anwendungsbeispiele).

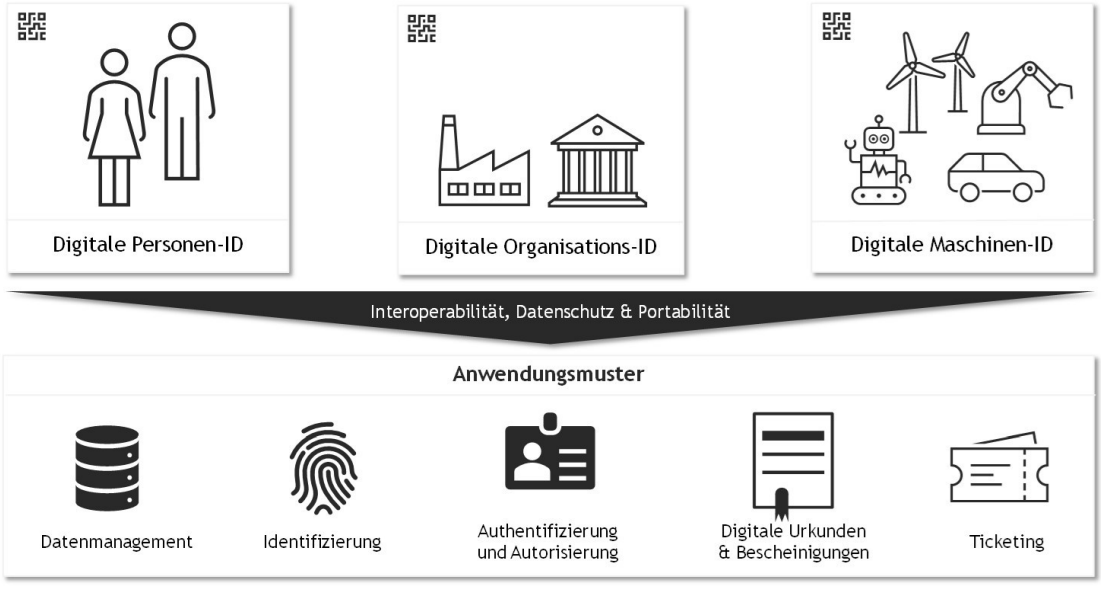
Das erste Anwendungsbeispiel bezieht sich auf den E-Commerce. Die rasante Verbreitung von entsprechenden Angeboten hat das Bewusstsein vieler Nutzer:innen für Privatsphäre und Datenschutz erhöht. Da die Zahlungsabwicklung oder auch der Versand von Waren stets die Nutzung von Teilidentitäten erfordern, sind insbesondere die Verifizierung und die Nutzung der Nutzeridentitäten eine Herausforderung. So kann aktuell beispielsweise das Alter der bestellenden Person einzig durch den Paketdienst geprüft werden. Durch eine personenbezogene digitale Identität könnten im E-Commerce viele Prozesse vereinfacht und beschleunigt werden. So ließe sich neben einem sicheren

Nachweis der Kundenidentität auch die Zahlung der Ware dezentral abwickeln. Außerdem können Nutzer:innen selbstbestimmte Identitäten einsetzen, um ihr Alter nachzuweisen, etwa beim Erwerb alkoholhaltiger Getränke. Auch ein Identitätsdiebstahl (Bestellung auf den Namen einer anderen Person) könnte so vermieden werden.

Das zweite Anwendungsbeispiel bezieht sich auf die Ausstellung von Universitätszeugnissen. Diese werden den Absolvent:innen gegenwärtig nach erfolgreichem Studium nach wie vor in Papierform bereitgestellt. Bisher gibt es bis auf die Erstellung beglaubigter Kopien durch ein Notariat keinerlei Möglichkeiten, die Übereinstimmung des Dokuments mit einem Original nachzuweisen. Insbesondere durch die fortschreitende Digitalisierung von Bewerbungsprozessen in Unternehmen werden bei Bewerbungen häufig nur eingescannte und damit leicht manipulierbare Dokumente gefordert. Um möglichem Missbrauch entgegenzuwirken, könnten Universitäten mittels selbstbestimmter Identitäten ihren Studierenden digitale Zertifikate über erbrachte Leistungen und nach Studienende ein Verifiable Credential mit der Abschlussnote ausstellen. Über dieses Verifiable Credential könnten Studierende beispielsweise bei einem Wechsel der Universität bereits bestandene Leistungen nachweisen. Des Weiteren könnten die Leistungen auch von Unternehmen im Rahmen eines Bewerbungsprozesses verifiziert werden.

Selbstbestimmte Identitäten können grundsätzlich für unterschiedliche Bezugsobjekte, beispielsweise digitale Personen-IDs für menschliche Akteure, digitale Organisations-IDs für Unternehmen und öffentliche Einrichtungen sowie digitale Maschinen-IDs im industriellen Kontext eingesetzt werden. Die vielfältigen Anwendungsfelder lassen sich in mehrere Anwendungsmuster gruppieren (siehe Abbildung 4).

Abbildung 4: Anwendungsmuster für selbstbestimmte Identitäten



Quelle: Eigene Darstellung

Das *Datenmanagement* kann durch selbstbestimmte Identitäten dahin gehend vereinfacht werden, dass ein Management von Stammdaten an unterschiedlichen Stellen nicht mehr notwendig ist. Vielmehr können Personen, Organisationen und Maschinen hierdurch ihre Stammdaten selbst verwalten und individuell freigeben. Das Anwendungsmuster *Identifizierung* bezieht sich auf die inhärente Eigenschaft selbstbestimm-

ter Identitäten, selektiv verifizierbare Identitätsdaten der Bezugsobjekte in unterschiedlichen Kontexten und zu unterschiedlichen Zwecken zu präsentieren, die wiederum eine eindeutige Identifizierung der Bezugsobjekte ermöglichen. Diese Identitätsdaten können entsprechend auch in verschiedenen Anwendungsfällen zur *Authentifizierung und Autorisierung* der Bezugsobjekte herangezogen werden. Neben Stammdaten können auch weitergehende Informationen wie ein digitales Zeugnis im oben dargestellten Beispiel als Verifiable Credential bereitgestellt werden. Entsprechende Anwendungsfälle lassen sich dem Anwendungsmuster *Digitale Urkunden und Bescheinigungen* zuordnen. Nicht zuletzt lassen sich digitale Identitäten einsetzen, um gegenwärtige Herausforderungen im *Ticketing* (zum Beispiel bei Großveranstaltungen) zu adressieren.

V. EINORDUNG VON SELBSTBESTIMMTEN IDENTITÄTEN AUS SICHT DER DIGITALEN SOUVERÄNITÄT

Eine Betrachtung des Ansatzes des selbstbestimmten Identitätsmanagements vor dem Hintergrund der Anforderungen einer digitalen Souveränität zeigt, dass selbstbestimmte Identitäten das Potenzial aufweisen, einen bedeutsamen Beitrag zur digitalen Souveränität von Verbraucher:innen liefern zu können. Im Vergleich zu den etablierten Ansätzen des digitalen Identitätsmanagements behalten die einzelnen Nutzer:innen sehr viel mehr Kontrolle über ihre jeweiligen Identitätsdaten. Die individuell ausgestellten Verifiable Credentials verbleiben immer als Originale bei den Nutzer:innen. Lediglich Verifiable Presentations werden geteilt. Die Verifiable Presentations wiederum können so datensparsam wie möglich gestaltet werden, sodass idealerweise nur solche Attribute geteilt werden, die tatsächlich für den spezifischen Anwendungsfall erforderlich sind. Die Nutzer:innen nehmen bei der Initialisierung der Datentransfers eine proaktive Rolle ein und es findet niemals ein Austausch von Daten ohne die explizite Zustimmung der Nutzer:innen statt. Wechselnde Pseudonyme verhindern zudem die Korrelation von Identitätsdaten auf Anbieterseite und schützen vor Identitätsmissbrauch.

Bei der Einordnung von selbstbestimmten Identitäten aus Sicht der digitalen Souveränität lässt sich festhalten, dass die in Kapitel 2 dargestellten Leitlinien sehr weitgehend adressiert werden. Zur Stärkung der Wahlfreiheit trägt bei, dass die Nutzer:innen aktiv darüber entscheiden können, ob anderen die Einsicht in personenbezogene Daten erlaubt sein soll oder nicht. Die Selbstbestimmung wird dadurch erhöht, dass die Nutzer:innen die alleinige Hoheit über ihre eigenen Daten behalten und selektiv über die Freigabe personenbezogener Daten entscheiden können. Die Selbstkontrolle wird über die Möglichkeit unterstützt, personenbezogene Daten sparsam und über wechselnde Pseudonyme weiterzugeben. Schließlich wird die Sicherheit dadurch erhöht, dass das selbstbestimmte Identitätsmanagement eine sichere Erhebung, Speicherung sowie eine kontrollierte Weitergabe von Daten erlaubt. Zusammenfassend lässt sich festhalten, dass der Ansatz des selbstbestimmten Identitätsmanagements zur Stärkung der digitalen Souveränität der Nutzer:innen beiträgt.

VI. FAZIT UND AUSBLICK

Digitale Identitäten spielen bei der Nutzung von digitalen Dienstleistungsangeboten und auch in der analogen Welt eine immer zentralere Rolle. Aktuelle Ansätze weisen aber noch verschiedene Schwachstellen sowohl auf Nutzer:innen- als auch auf Anbieterseite

auf, was als Hemmnis in verschiedenen Digitalisierungsvorhaben anzusehen ist. Die Bedeutsamkeit und Notwendigkeit von Weiterentwicklungen des digitalen Identitätsmanagements im Zeitalter der Digitalisierung wird bereits von Wirtschaft und Politik erkannt. Zur Adressierung der Weiterentwicklungen im digitalen Identitätsmanagement unter Berücksichtigung der Anforderungen der digitalen Souveränität hat sich der Ansatz der selbstbestimmten Identitäten als möglicher Lösungsansatz herauskristallisiert. Dieser Ansatz sieht vor, dass die Nutzer:innen ihre digitale Identität von zentraler Stelle, nämlich bei den Nutzer:innen selbst, über mehrere Anwendungsdomänen hinweg verwenden. Als zentrale Verwaltungsinstanzen ihrer jeweiligen digitalen Identität soll den Nutzer:innen so ermöglicht werden, über verschiedene Dienste hinweg die Kontrolle über ihre Identität zu wahren und damit eine Autonomie in der Verwaltung dieser Dienste zu erzielen. Dadurch soll ein hohes Niveau an Sicherheit und Interoperabilität bei gleichzeitig niedriger Komplexität und Unabhängigkeit von Intermediären erzielt sowie die digitale Souveränität der Nutzer:innen gestärkt werden. Das Paradigma der selbstbestimmten Identitäten verspricht eine neue Entwicklungsstufe des digitalen Identitätsmanagements, aus der sich vielfältige Einsatzmöglichkeiten ableiten. Entsprechend wird das Konzept bereits in unterschiedlichen Initiativen auf regionalen, nationalen und internationalen Ebenen diskutiert, erprobt und umgesetzt.

Als Voraussetzung für eine Massenverbreitung von selbstbestimmten Identitäten gilt es, verschiedene Herausforderungen zu adressieren. Es besteht die Notwendigkeit der technischen, fachlichen und rechtlichen Standardisierung, wenngleich in den letzten Monaten bereits zahlreiche Initiativen in diese Richtung arbeiten und teilweise beachtliche Fortschritte erzielen konnten. Eine weitere Vereinheitlichung ist für eine langfristige Interoperabilität entsprechender Systeme unabdingbar. Ein weiteres Handlungsfeld stellt die Kompetenzentwicklung dar. Mit der Schlüsselrolle als Initiator:innen und Halter:innen ihrer Daten wird zukünftig mehr Verantwortung bei den einzelnen Nutzer:innen liegen. Daher ist die Aufklärung über die neu entstehenden Möglichkeiten, aber auch über die zunehmende Eigenverantwortung von großer Relevanz. Zudem muss der Zugang zu selbstbestimmten Identitäten und die Teilhabe an Ökosystemen für alle Verbraucher:innen sichergestellt werden. Hierbei sollten sich entsprechende Systeme hinsichtlich Optik und Bedienbarkeit an den gängigen Anwendungen orientieren. Auch sollten Gruppen ohne große digitale Affinität die notwendigen Kompetenzen vermittelt werden, um eine Teilhabe sicherzustellen. Nicht zuletzt bedarf es entsprechender Angebote, damit eine Akzeptanz und Nutzung durch Verbraucher:innen und durch die Privatwirtschaft erfolgt. Frühere Initiativen haben gezeigt, dass digitale Lösungen oftmals nur im Rahmen nutzerstarker Ökosysteme Mehrwert schaffen. Entsprechend sollte über entsprechende Förderungen sichergestellt werden, dass selbstbestimmte Identitäten weitreichend eingesetzt werden können.

VII. ABBILDUNGSVERZEICHNIS

VIII. LITERATURVERZEICHNIS

Bundeskanzleramt. 2021. *Digitale Identität: Wie ein Ökosystem digitaler Identitäten zu einem selbstbestimmten und zugleich nutzerfreundlichen Umgang mit dem digitalen Ich beitragen kann*. Referat Digitaler Staat. https://www.bundesregierung.de/resource/blob/975292/1898280/d9819a40553a9543b9e8f3acb620b0c2/digitale-identitaet-neu-download-bundeskanzleramt-data.pdf?download=1 (Zugriff: 18.01.2022).

Koalitionsvertrag. 2021. *Koalitionsvertrag 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN und den Freien Demokraten (FDP)*. https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf (Zugriff: 18.01.2022).

Sachverständigenrat für Verbraucherfragen. 2017. Digitale Souveränität: Gutachten des Sachverständigenrats für Verbraucherfragen. https://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_Digitale_Souver%C3%A4nit%C3%A4t_.pdf (Zugriff: 29.11.2021).

Stiens, Teresa. 2021. Sicherheitsprobleme und Zuständigkeitschaos: Der Weg zur digitalen Identität in Deutschland ist lang. *Handelsblatt*. 22. November. https://www.handelsblatt.com/politik/deutschland/digitalisierung-der-verwaltung-sicherheitsprobleme-und-zustaendigkeitschaos-der-weg-zur-digitalen-identitaet-in-deutschland-ist-lang/27816984.html (Zugriff: 18.01.2022).

Strüker, Jens, Nils Urbach, Tobias Guggenberger, Jonathan Lautenschlager, Nicolas Ruhland, Vincent Schlatt, Johannes Sedlmeir, Jens-Christian Stoetzer und Fabiane Völter. 2021. Self-Sovereign Identity – Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT. https://www.fim-rc.de/wp-content/uploads/2021/06/Fraunhofer-FIT_SSI_Whitepaper.pdf (Zugriff: 18.01.2022).