Positionspapier

Digitale Identitäten – Schritte auf dem Weg zu einem ID-Ökosystem

18. März 2021

Tobias Tenner
Associate Director
Leiter Digitalisierung
Telefon: +49 30 1663-2323
tobias.tenner@bdb.de

Stephan Mietke
Director
Telefon: +49 30 1663-2325
stephan.mietke@bdb.de

Bundesverband deutscher Banken e. V.
Burgstraße 28
10178 Berlin
Telefon: +49 30 1663-0
Telefax: +49 30 1663-1399
www.bankenverband.de
USt.-IdNr. DE201591882

1 Executive Summary

Digitale Identitäten sind aus dem heutigen Alltag nicht mehr wegzudenken: Neun von zehn Deutschen nutzen das Internet, rund 80 % kaufen online ein[1], zwei Drittel erledigen ihre Bankgeschäfte per Online-Banking[2]. Mit diesen Gewohnheiten einher geht die Nutzung digitaler Identitätsdaten einschließlich persönlicher Log-Ins, die Bestandteil jeder digitalen Customer Journey sind. Jedoch sind es in der Regel Insellösungen, das heißt bei jedem Anbieter werden jeweils anbieterbezogene digitale Identitäten angelegt. In Deutschland fehlt es bisher an verfügbaren und in der Breite akzeptierten Lösungen, mit denen sich Personen mit ihrer digitalen Identität überall (d.h. auch branchenübergreifend) und auf vollständig digitalem Wege gegenüber Geschäftspartnern ausweisen können. Ursache dafür ist einerseits die fehlende Interoperabilität existierender Lösungen, andererseits die Tatsache, dass die in der Wirtschaft vielfach vorhandenen Identitätsdaten nicht übergreifend genutzt werden. Die daraus resultierende mangelnde Verfügbarkeit allgemein nutzbarer digitaler Identitätsdaten bremst die dringend erforderliche Digitalisierung in Deutschland und auch in Europa aus.

Umso wichtiger ist es, ein anbieter- und branchenübergreifendes Ökosystem für die Nutzung und Verwaltung von digitalen Identitäten zu schaffen. Ziel muss es sein, Personen und im Weiteren auch Unternehmen und Dingen („Internet of Things") eine nahtlose Einbindung in digitale Wertschöpfungsprozesse auf Basis digitaler Identitäten zu ermöglichen. Kern eines solchen Ökosystems wäre die Bereitstellung von Identitätsdaten, die bereits einmal durch eine Partei (z.B. durch eine Bank) bestätigt wurden und auf die sich andere Geschäftspartner verlassen können. Sowohl datenschutzrechtlich als auch im Sinne des Grundsatzes der digitalen Souveränität sollte die Kontrolle über die eigenen Identitätsdaten bei dem jeweiligen Identitätssubjekt liegen.

Um das Ziel eines lebendigen ID-Ökosystems zu erreichen, müssen Wirtschaft und Staat an einem Strang ziehen. Dies erfordert eine neue enge Zusammenarbeit zwischen öffentlichem und privatem Sektor, deren Aufgabe soweit reichen kann, einheitliche Verfahrens- und Organisationsregeln („Governance-Struktur") wie auch technische Mindeststandards zu formulieren. Das Ökosystem stellt keine Konkurrenz für bestehende Anbieter von Identitätslösungen dar, sondern würde es ihnen erlauben, ihre Angebote und Innovationen im gemeinsamen System (weiter) zu entwickeln.

Voraussetzung hierfür ist, die in den verschiedenen Wirtschaftsbereichen aktuell divergierenden rechtlichen und regulatorischen Anforderungen an die Identitätsfeststellung zu harmonisieren. Denn nur wenn das Ökosystem den Austausch und die Nutzung von Identitätsdaten für alle Parteien und über alle Branchen hinweg ermöglicht, kann eine hohe Akzeptanz und schnelle Adaption neu geschaffener Standards im Markt gewährleistet werden. Um dies zu erreichen, sind gleichwertige Anforderungen an die Identifizierungsprozesse und eine gegenseitige Anerkennung

[1] https://initiatived21.de/app/uploads/2020/02/d21_index2019_2020.pdf, Seite 10 und Seite 32

[2] Bankenverband (2020)

durch die jeweiligen Aufsichtsbehörden notwendig. Eine solche Vollharmonisierung ließe sich am effektivsten durch eine einheitliche, sektorübergreifende Rechtsgrundlage erreichen.

Das ID-Ökosystem sollte als nationale Initiative gestartet werden, die sich im Weiteren auch für einen einheitlichen europäischen Rahmen und interoperable Identitätslösungen einsetzt. Ein Vorbild für die Vereinheitlichung von Regeln und technologischen Standards ist u.a. der europäische Zahlungsverkehr. Die von der Bundesregierung Ende letzten Jahres gestartete Initiative zur Schaffung eines offenen europäischen Ökosystems digitaler Identitäten wird von den privaten Banken ausdrücklich befürwortet.

Damit ein Ökosystem digitaler Identitäten Realität werden kann, sind folgende Maßnahmen zur Anpassung des bestehenden Rechtsrahmens notwendig:

1. Die generelle Gleichwertigkeit der Anforderungen an Identifizierungsprozesse in den sektorspezifischen Regelungen (u.a. im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung, im Telekommunikationsbereich, im öffentlichen Sektor, bei Vertrauensdiensten) muss hergestellt werden. Sofern diese Regelungen auf einer europäischen Rechtsgrundlage basieren, ist eine Vollharmonisierung im Wege einer europäischen Verordnung erforderlich.

2. Am wirksamsten ließe sich eine Vollharmonisierung durch einen einzigen sektorübergreifenden europäischen Rechtsrahmen erreichen, auf den sich sektorspezifische Regelungen stützen. Hierdurch wäre auch gewährleistet, dass der Umfang der vom Identifizierungspflichtigen erhobenen Daten im Sinne einer Wiederverwendung EU-weit identisch ist.

3. Der Gesetzgeber muss weiterhin Rahmenbedingungen schaffen, die Rechtssicherheit im Verhältnis zwischen Identitätsempfänger (Verifier) und Identitätsaussteller (Issuer) ermöglichen. Hierbei müssen auch haftungsrechtliche Fragen, wie zum Beispiel Haftungsgrenzen, mitgedacht werden, um einen fairen Interessenausgleich sicherzustellen und eine Anreizwirkung zu erzielen.

Die anstehende Novellierung der eIDAS-Verordnung[3] sollte genutzt werden, um horizontal einheitliche Anforderungen im Sinne einer Vollharmonisierung auf europäischer Ebene zu definieren und somit auch grenzüberschreitende Identifizierungsprozesse zu erleichtern.

[3] VERORDNUNG (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

2 Ausgangssituation

Der digitale Wandel schreitet voran, neue Technologien und Services werden überall dort mit Begeisterung angenommen, wo sie einen Mehrwert für die Nutzer versprechen und einfach und komfortabel angewendet werden können. Die aktuelle Studie „Digital-Index 19/20" der Initiative D21 zeigt: Die meisten Bürger erwarten und begrüßen, dass die Digitalisierung künftig noch stärker in sämtliche Lebensbereiche hineinwirken wird.[4]

Im Durchschnitt hat jeder EU-Bürger derzeit rund 90 digitale Identitäten, darunter Zugangsdaten zu Social-Media-Accounts, Online-Shops, Mobilitätsplattformen oder zu Online-Banking-Portalen.[5] Diese Anzahl wird aufgrund vieler Digitalisierungsoffensiven unterschiedlicher Branchen in der Tendenz weiter steigen. Im Bereich des Kunden-Onboarding gibt es aber noch deutliches Verbesserungspotenzial, was den Digitalisierungsgrad anbelangt. Wesentlicher Schwachpunkt: Kunden müssen häufig eine Vielzahl persönlicher Daten manuell in den Antragsprozess eingeben, obwohl diese an anderer Stelle bereits verifiziert zur Verfügung stehen und lediglich in den Antragsprozess übertragen werden müssten. Dieses Manko haben US-amerikanische Tech-Unternehmen schon längst erkannt. Die Nutzer von Apple, Google, Facebook oder Amazon können sich mit ihren jeweiligen Profilen auch auf anderen Websites anmelden.

„Was ist eine digitale Identität"?

Das Spektrum digitaler Identitäten ist breit: Sie können sich auf die einfache Kombination aus Benutzername/Passwort ohne Bezug zu personenbezogenen Attributen beschränken, andererseits aber auch mit persönlich identifizierbaren Informationen aus offiziellen Nachweisen wie einem Ausweisdokument verbunden sein. Darüber hinaus können noch weitere Informationen einfließen wie zum Beispiel Zahlungsdaten, Gesundheitsinformationen oder Ausbildungs- und Beschäftigungsbelege.

Unter einer „verifizierten digitalen Identität" wird ein Datensatz verstanden, der die Identität und gegebenenfalls weitere Identitätsattribute (z.B. besitzt Akademischen Grad „Dr.", ausgestellt von Universität; besitzt Prüfzeugnis für Jagdschein, ausgestellt durch Behörde …; etc.) zu einer natürlichen oder juristischen Person beinhaltet und der durch einen oder mehrere vertrauenswürdige Stellen (z.B. eine Bank) bescheinigt wird.

Eine Zusammenführung dieser Vielfalt an Daten, die in Summe ein umfassendes Bild über die jeweilige Person bzw. Entität geben können, erfordert ein hohes Maß an Integrität und Vertrauen hinsichtlich des Gesamtsystems.

[4] https://initiatived21.de/app/uploads/2020/02/d21_index2019_2020.pdf, Seite 32

[5] https://www.bundesdruckerei.de/de/Fokusthemen/Magazin/So-entwickeln-sie-sich-weiter

Diese „Single-Sign-On"-Angebote der Tech-Unternehmen garantieren allerdings nicht, dass die durch den Kunden angegebenen Daten auch tatsächlich korrekt sind. Regulierte Branchen, wie zum Beispiel Banken oder Mobilfunkanbieter, sind aber dazu verpflichtet, die Daten der Kunden zu verifizieren. Das tun sie gewissenhaft, allerdings kann die rechtsgültige Identifizierung oft nur mit einem Medienbruch durchgeführt werden (Video-Ident, Post-Ident etc.). Die Online-Ausweisfunktion (eID) des Personalausweises findet beim Verbraucher derzeit keine ausreichende Akzeptanz.

Mehrere europäische Länder haben die genannten Probleme erkannt und Lösungen etabliert, allen voran die skandinavischen. In Dänemark verwenden 99 Prozent der Bevölkerung über 15 Jahre eine digitale Identität („NemID")[6], die von Wirtschaft und Regierung gemeinsam angeboten wird. Mit bis zu 100 Millionen Transaktionen im Monat ist NemID ein fester Bestandteil des digitalen Lebens: So nutzen zum Beispiel neun von zehn Kunden NemID, um sich in das Bankkonto einzuloggen oder Verwaltungsleistungen in Anspruch zu nehmen. In Schweden wurde 2003 von einer Reihe großer Banken „BankID" entwickelt. Heute besitzen über acht von zehn Millionen Schweden[7] eine BankID, um sich einzuloggen, digital auszuweisen oder um Verträge digital rechtsverbindlich zu unterschreiben.

Die Basis für den Identitätsnachweis in Deutschland für natürliche Personen bilden hingegen nach wie vor physische Dokumente wie Personalausweis, Aufenthaltstitel oder Reisepass. Zwar sind nahezu alle ausgegebenen deutschen Personalausweise und Aufenthaltsnachweise inzwischen mit einem elektronischen Identitätsnachweis (eID) ausgestattet; auch gibt es teildigitale Identifikationsverfahren wie die Videoidentifizierung. Aber ausschließliche Praxis ist hierzulande noch immer, dass das Ausweisdokument zum Zeitpunkt der Identifizierung dem Verbraucher physisch (per Chipkarte) vorliegen muss, was einem volldigitalen Nutzererlebnis im Wege steht.

Obwohl deutsche Personalausweise und elektronische Aufenthaltstitel bereits seit 2010 mit eID ausgegeben werden, ist diese Funktion nur bei etwa der Hälfte der Dokumente aktiviert.[8] Zudem geben nur sieben Prozent der Bundesbürger an, ihren elektronischen Personalausweis schon einmal genutzt zu haben.[9] Ein Grund dafür besteht darin, dass die Anzahl an Einsatzmöglichkeiten erst seit kurzem zunimmt. Ein anderer Grund könnte die suboptimale Nutzbarkeit durch die bislang zwingende Kombination aus Ausweiskarte und Lesegerät bzw. Smartphone sein. Aktuell werden die rechtlichen und technischen Voraussetzungen dafür geschaffen, dass der elektronische Identitätsnachweis vom Personalausweis oder Aufenthaltstitel auf ein mobiles

[6] https://digst.dk/it-loesninger/nemid/tal-og-statistik-om-nemid/, https://de.statista.com/statistik/daten/studie/19296/umfrage/gesamtbevoelkerung-von-daenemark/, https://de.statista.com/statistik/daten/studie/260255/umfrage/altersstruktur-in-daenemark/ und eigene Berechnungen

[7] https://www.bankid.com/en/om-bankid/detta-ar-bankid

[8] https://www.cio.de/a/der-online-ausweis-kommt,3654683

[9] https://initiatived21.de/app/uploads/2020/02/d21_index2019_2020.pdf, Seite 44

Endgerät übertragen werden kann, wodurch die Identifizierung allein mit dem Smartphone erfolgen könnte und Benutzerfreundlichkeit sowie Akzeptanz erhöht werden dürften.[10]

Eine andere Möglichkeit, digitale Identitäten einer breiten Nutzerbasis auf kurze Sicht verfügbar zu machen, liegt in der Wiederverwendung bestehender Identitätsdaten, wie es die zuvor genannten Beispiele aus dem Ausland demonstrieren. Da Banken, aber auch Unternehmen verschiedener anderer Branchen, gesetzlich zu einer Identitätsfeststellung ihrer Kunden verpflichtet sind, können diese verifizierten Informationen über eine Person als Grundlage für die Erstellung einer digitalen Identität dienen. Diese Daten werden auf Grundlage staatlicher Ausweisdokumente erhoben und in regelmäßigem Abstand überprüft, sodass sie eine vergleichbar hohe Qualität und Zuverlässigkeit aufweisen.

Die aktuelle Situation zeigt, dass kleine und große Unternehmen genauso wie Verwaltung und Behörden vor der Notwendigkeit stehen, zukunftsfähige und innovative Identifizierungsverfahren einsetzen zu müssen, damit ihre digitalen Dienstleistungen genutzt und akzeptiert werden. Die Unternehmen trifft dieses Thema sogar in doppelter Hinsicht, schließlich müssen auch sie sich regelmäßig digital ausweisen. Dabei stehen sie vor der zusätzlichen Herausforderung, die digitale Identität der juristischen Person mit der digitalen Identität der für das Unternehmen handelnden natürlichen Person(en) zu kombinieren.

3 Herausforderung

In Deutschland gibt es aktuell mehr als 40 Anbieter von digitalen Identitäten[11], die um die Gunst der Nutzer konkurrieren. Der Datenaustausch zwischen den Identitätsanbietern und den nachfragenden Unternehmen erfolgt zumeist über bilaterale Anbindungen. Solche Anbindungen sind komplex: Sie erfordern wiederkehrende Integrationsaufwände, individuelle Regelungen von technischen Spezifikationen und vertragsrechtliche Vereinbarungen. Hinzu kommt, dass die Portabilität der Daten zwischen verschiedenen Identitätsanbietern nur eingeschränkt möglich ist und es sich häufig um Insellösungen und Datensilos handelt. Zudem genügen die angebotenen digitalen Identitäten nicht immer den hohen Ansprüchen, die die regulierenden Behörden stellen. Schlussendlich steht ein Unternehmen, das seinen Kunden den Zugang zu seinen Services durch eine digitale Identität ermöglichen möchte, vor der Herausforderung, aus der Fülle der Dienstleister die relevanten Anbieter mit Blick auf Implementierungskosten, Kundenreichweite, Conversion Rate und mögliche Skaleneffekte auszuwählen.

Und die Nutzerseite? Obwohl der Bedarf groß ist, fehlt es bislang vor allem an praktischen Anwendungsfällen, in denen ein und dieselbe digitale Identität für vielfältige Zwecke (regelmäßig) und mit hoher Convenience eingesetzt werden kann. Ohne Anwendungsfälle aber sieht der Einzelne keinen Nutzen darin, sich eine solche digitale Identität anzulegen, die Nachfrage bleibt gering. Ein klassisches Henne-Ei-Problem.

[10] Die Bundesregierung hat jüngst einen Gesetzesentwurf zur Anpassung von Personalausweisgesetz, eID-Karte-Gesetz und Aufenthaltsgesetz („Smart eID-Gesetz") vorgelegt.

[11] https://paymentandbanking.com/digital-identity-uebersicht-deutschland/

Wesentlichen Einfluss darauf, wie erfolgreich der Einsatz von digitalen Identitätslösungen sein wird, hat das zukünftige digitale Nutzerverhalten. 74 Prozent der Bürger sind schon heute mit mobilen Endgeräten online, in der Altersgruppe von 14 bis 39 Jahren sind es sogar 93 Prozent. In wenigen Jahren werden mehr Menschen das Smartphone nutzen als einen Desktop-PC oder ein Notebook. Der Einsatz appbasierter Identitätslösungen hängt nicht zuletzt auch von der Anzahl der kompatiblen Smartphones ab.

Doch unabhängig von der Frage des Nutzerverhaltens: Damit digitale Identitätslösungen durchschlagenden Erfolg haben können, muss die Gewissheit bestehen, dass sie sicher, bequem und im Idealfall allgemein akzeptiert und anerkannt sind. Es ist wichtig, dass Standards bequeme Lösungen ermöglichen, aber auch, dass auf ein sorgfältiges Gleichgewicht zwischen Benutzerfreundlichkeit und starker Sicherheit geachtet wird. Die maximale Standardisierung der Identitätslösungen ist daher von entscheidender Bedeutung.

Auf europäischer Ebene war diesbezüglich die eIDAS-Verordnung von 2014 ein Meilenstein, ermöglicht sie doch die gegenseitige Anerkennung von elektronischen Identitätssystemen in der EU. Allerdings wird ihre Wirkung dadurch gemindert, dass diese Anerkennung nur notifizierten eID-Systemen vorbehalten ist. Dadurch mangelt es in Deutschland und der EU nach wie vor an operativen und technischen Standards, insbesondere im privaten Sektor. Das hat zur Folge, dass es immer noch erhebliche Hindernisse für die Entwicklung von sektor- und grenzübergreifenden Lösungen gibt.

Eine weitere Herausforderung stellt der Dschungel unterschiedlicher gesetzlicher Identifizierungsanforderungen dar, sowohl zwischen den verschiedenen Sektoren als auch zwischen nationaler und europäischer Ebene. Dies führt zu uneinheitlichen Rahmenbedingungen, behindert die gegenseitige Anerkennung von geprüften Identitätsdaten im Sinne einer Wiederverwendung und bewirkt je nach Standort eine Benachteiligung einzelner Anbieter im europäischen Wettbewerb.

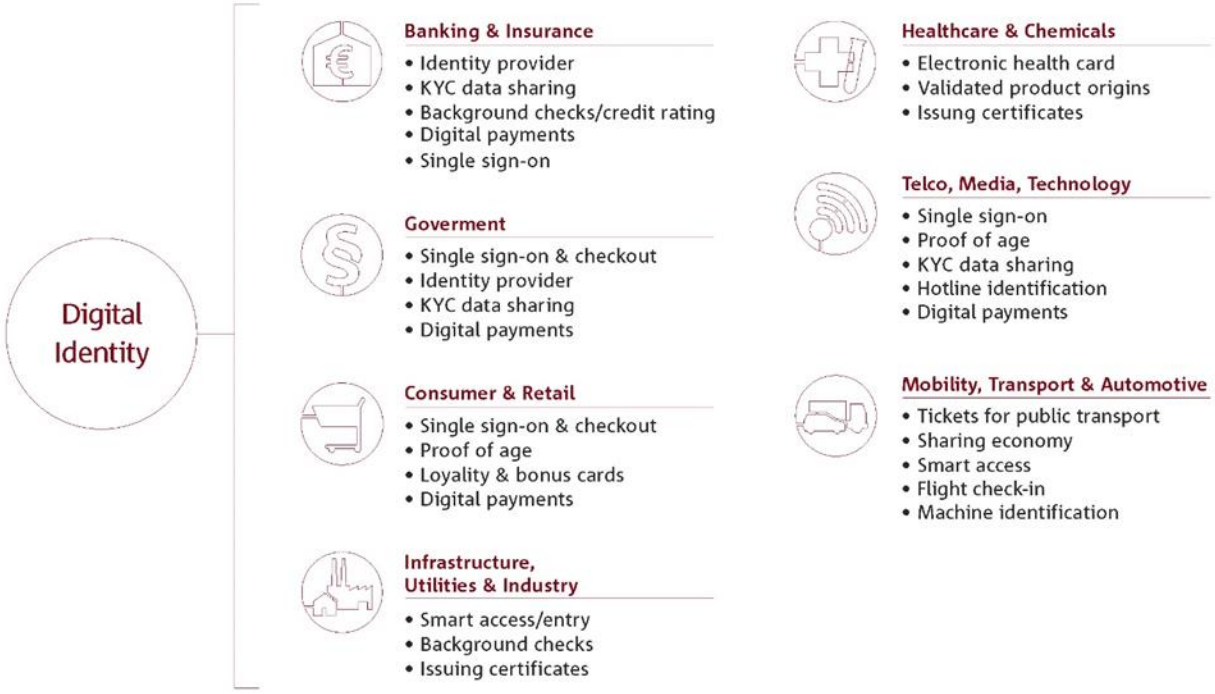
Um den Prozess der Standardisierung und Harmonisierung zu erleichtern, sollten Deutschland und Europa den Ansatz einer Public-Private-Partnership verfolgen. Auf diesem Wege könnte die Entwicklung einer Reihe von Regeln, Praktiken und Standards vorangetrieben und so die Interoperabilität für die Bereitstellung und den Betrieb von Identitätslösungen erzielt werden.

4 Zielbild: Schaffung eines ID-Ökosystems

Ein Ökosystem, in dem digitale Identitätsdaten sicher, zuverlässig, skalierbar und bequem ausgetauscht werden können, ist eine Antwort auf diese Herausforderungen. Es kann die wirtschaftliche Zukunft von Deutschland und Europa im Positiven prägen und dabei gleichzeitig die Privatsphäre des Einzelnen stärken. Damit ein Ökosystem verifizierter digitaler Identitäten erfolgreich ist, muss es

- über einzelne Unternehmen und einzelne Sektoren hinweg nutzbar sein,
- die Interoperabilität zwischen bestehenden Verfahren ermöglichen,
- auf einheitlichen, idealerweise weltweit anerkannten Standards aufbauen,
- von jedem Individuum einer Gesellschaft, unabhängig von der Staatsangehörigkeit, genutzt werden können,
- sicher sein und einen Beitrag dazu leisten, den Verbraucher vor Identitätsmissbrauch zu schützen,
- verbraucherzentriert sein, d.h. Datensouveränität ermöglichen,
- rechtlich nutzbar sein sowie von allen Behörden anerkannt werden und
- gleichermaßen für natürliche und juristische Personen sowie zukünftig auch für Dinge anwendbar sein.

Das folgende Schaubild zeigt die vielfältigen Einsatzmöglichkeiten digitaler Identitäten quer über unterschiedlichste Branchen.



Ziel muss es sein, für Deutschland ein nationales ID-Ökosystem zu entwickeln, das die zuvor genannten Anforderungen erfüllt und zugleich mit anderen europäischen ID-Ökosystemen kompatibel ist. Dabei sollten Wirtschaft und Regierung zusammenarbeiten und gegebenenfalls im Rahmen einer Public-Private-Partnership Vereinbarungen zu funktionalen, technischen, operativen, rechtlichen und wirtschaftlichen Aspekten des Datenaustausches treffen.

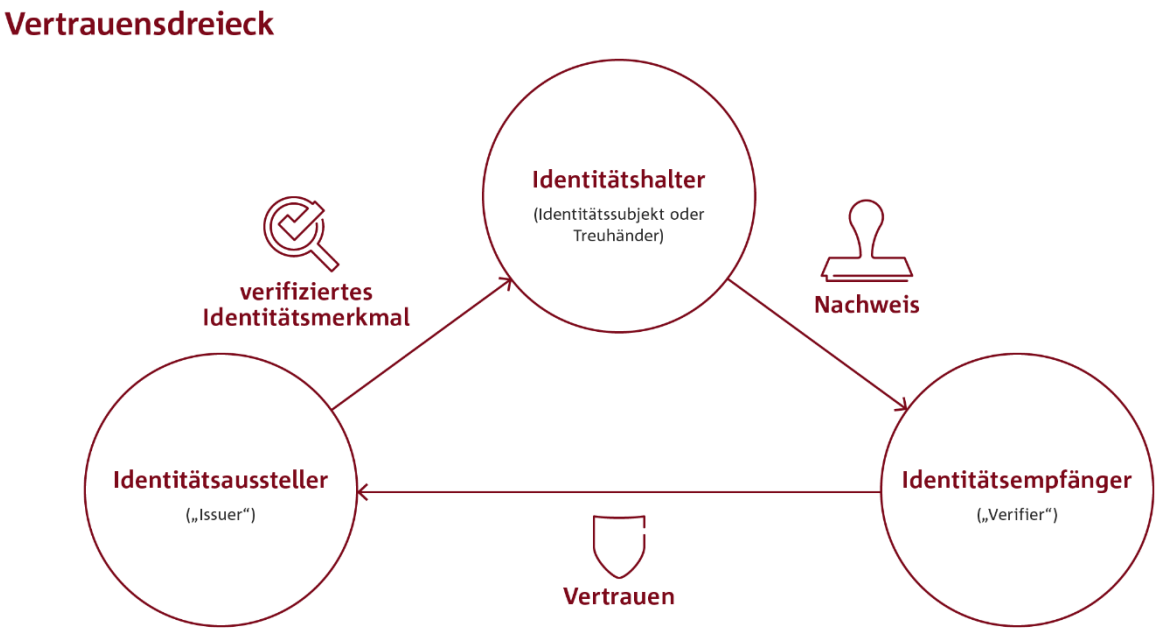
Ein nationales ID-Ökosystem ist im Übrigen kein Konkurrenzangebot zu den bestehenden Identifizierungslösungen wie der Videoidentifizierung, dem elektronischen Identitätsnachweis oder den unterschiedlichen digitalen Identitätsangeboten. Vielmehr bietet ein ID-Ökosystem einen Rahmen, innerhalb dessen Anbieter neue Innovationen in dem Wissen schaffen können, dass die erhobenen Daten untereinander akzeptiert werden und die Spielregeln sowie technischen Anforderungen einheitlich sind. Ein solches nationales ID-Ökosystem trägt zu einem Level Playing Field mit faireren Wettbewerbsbedingungen für alle Teilnehmer bei.

4.1 Mit selbstbestimmten Identitäten die digitale Souveränität stärken

Sei es bei der Nutzung sozialer Medien, dem Bestellen von Waren über E-Commerce-Plattformen oder der Recherche von Fachwissen – der digitale Alltag eines jeden Bürgers erzeugt heute zwangsläufig Daten, deren Analyse und Kommerzialisierung häufig in den Händen weniger großer Technologiekonzerne liegt. Aufgrund des Datenschutzrechts und im Sinne der digitalen Souveränität des Einzelnen ist es daher wichtig, jedem Bürger die Möglichkeit zu geben, selbstbestimmt darüber entscheiden zu können, wie und wofür seine Daten genutzt werden. Dies gilt zuallererst für Daten, die unmittelbar die eigene Identität betreffen. Verbraucher sollten jederzeit Transparenz darüber haben, was mit den Daten geschieht, und jederzeit bestimmen können, zu welchen Zwecken sie wem ihre Identitätsdaten zur Verfügung stellen möchten.

Einen Lösungsansatz hierfür bieten digitale selbstbestimmte Identitäten bzw. Self-Sovereign Identities (kurz „SSI"), bei denen Bürger ihre eigenen Identitätsdaten selbst verwalten und bedarfsweise für die Nutzung durch einen Dritten, z.B. bei Begründung einer Vertragsbeziehung oder bei Inanspruchnahme einer Dienstleistung, freigeben. Nur der Nutzer selbst kennt alle seine Identitätsdaten und entscheidet selbstbestimmt, mit wem diese Daten geteilt werden. Dieser Ansatz erlaubt es Identitätsausstellern oder „Issuern" (z.B. Unternehmen, staatliche Behörden), die von ihnen geprüften Identitätsdaten auf den Endgeräten der Nutzer abzulegen und ermöglicht den Nutzern („Identitätshaltern"), sich mit diesen Daten bei Identitätsempfängern („Verifiern") zu identifizieren. Identitätshalter bzw. Identitätssubjekte können dabei sowohl natürliche wie juristische Personen, aber auch Gegenstände (z.B. Fahrzeuge, Züge) sein. Die Verifizierung der Daten erfolgt über ein DLT-Netzwerk, das den Identitätsausstellern lediglich als dezentrale Public-Key-Infrastruktur dient und in dem keine personenbezogenen Daten, noch nicht einmal Pseudonyme (z.B. Hashwert der Nutzer), gespeichert werden. Damit erfüllt es alle Anforderungen des Datenschutzes.

Das Verhältnis zwischen dem Identitätsaussteller, dem Identitätsempfänger und dem Identitätshalter lässt sich abstrakt als Vertrauensdreieck darstellen (siehe Abbildung), und zwar unabhängig davon, wie es technisch (DLT-Netzwerk oder zentrale Infrastruktur) umgesetzt ist.



Die Vorteile eines SSI-Ansatzes lassen sich wie folgt zusammenfassen:

- volle Kontrolle über die Zugriffe auf eigene Identitätsdaten, z.B. über eine ID-Wallet auf dem Smartphone;
- Übertragbarkeit von Identitätsdaten über standardisierte Datenformate und Protokolle;
- Schutz vor Angriffen und zentralen Systemausfällen durch dezentrale Datenhaltung;
- Schutz der Privatsphäre, da Daten von Identitätssubjekten nicht korreliert werden können;
- größere Wachstumschancen durch offene Standards;
- Datensparsamkeit – es werden immer nur die Identitätsattribute weitergegeben, die wirklich benötigt werden.

4.2 Schlüsselrolle für die Finanzindustrie

Beispiele aus anderen Ländern zeigen, dass Banken häufig eine zentrale Rolle in einem erfolgreichen ID-Ökosystem einnehmen. Das hat mehrere Gründe:

- Als regulierte Finanzdienstdienstleister sind Banken gesetzlich verpflichtet, die Identität ihrer Kunden zu überprüfen, z.B. bei der Aufnahme einer Geschäftsbeziehung. Grundlagen hierfür sind das Geldwäschegesetz und die Abgabenordnung, die verbindlich für alle deutschen

Banken gelten und somit auch einen gleichbleibenden Standard für die Verifizierung der Daten darstellen. Die Einhaltung dieser regulatorischen Vorgaben wird durch die Finanzaufsicht (BaFin) überwacht. Damit verfügen Banken in Summe über einen einmaligen Pool an verifizierten Identitäten, der praktisch alle Bürger umfasst, zu denen eine Kundenbeziehung besteht.

- Im Rahmen des Online-Banking haben Banken sichere und hochverfügbare Zugangskanäle für die Kunde-Bank-Kommunikation etabliert. Sichere Authentifizierungsverfahren erlauben es, dass sich Kunden digital gegenüber ihrer Bank ausweisen, um ihr Konto online zu verwalten und beispielsweise Zahlungsaufträge auszulösen. Mit der Umsetzung der zweiten Zahlungsdiensterichtlinie („PSD2") sind die Anforderungen an die Kundenauthentifizierung weiter angehoben worden und erfüllen höchste Sicherheitsstandards. Anders als bei vielen anderen Geschäftsvorfällen, z.B. in der öffentlichen Verwaltung, machen die meisten Bankkunden regelmäßig von der Authentifizierung Gebrauch und sind daher mit der Nutzung dieser Verfahren bestens vertraut. Aufgrund ihrer hohen Sicherheit und der häufigen Nutzungsfrequenz sind diese Authentifizierungsverfahren sehr gut dazu geeignet, digitale Identitäten durch den Kunden zu verwalten.

- Banken genießen hohes Kundenvertrauen, wenn es um den Schutz und die Sicherheit ihrer Daten geht. Nach einer aktuellen Umfrage weisen sie unter allen Branchen das größte Kundenvertrauen auf.[12] Damit haben sie gute Voraussetzungen, die digitale Identität im Auftrag ihrer Kunden vertrauensvoll und sicher zu verwahren.

Banken können in einem ID-Ökosystem somit mehrere Funktionen übernehmen. Als **Identitätsempfänger (Verifier)** von digitalen Identitäten könnten sie auf diese Weise ihre gesetzlich geforderten Identifizierungspflichten erfüllen. Aufgrund der stetigen Nachfrage nach Identitätsprüfungen beim Kunden-Onboarding können sie einen häufigen Anwendungsfall mit vergleichsweise hohen Nutzungsraten zum Ökosystem beisteuern.

Sie können aber auch eine zentrale Rolle als **Aussteller (Issuer)** von digitalen Identitäten einnehmen. Denn Banken sind nicht nur verpflichtet, die Identität ihrer Kunden zu verifizieren und sich kontinuierlich zu vergewissern, dass die Daten aktuell sind. Sie verfügen auch über weitere Daten ihrer Kunden, die sie mit deren Zustimmung anderen Nutzern in einem ID-Ökosystem zur Verfügung stellen können. Beispiele hierfür sind Nachweise bzw. Bestätigungen zum Einkommen, über Kontosalden, zur Volljährigkeit, bis hin zu Bonitätsauskünften. Indem sie Sicherheit und Integrität der Daten garantieren, können sie die Wirtschaft und Verwaltung dabei unterstützen, ein ID-Ökosystem zu beleben und den Verbrauchern eine Vielfalt an Services zugänglich zu machen.

Darüber hinaus kommt noch eine weitere Rolle in Betracht: Banken können als **Treuhänder (Trustee)** und Identitätshalter im Auftrag ihrer Kunden fungieren und neben den durch sie selbst als Issuer bereitgestellten Identitätsdaten weitere Daten ihrer Kunden verwalten, die von

[12] https://de.eos-solutions.com/data-survey-2020

anderen Herausgebern in ein ID-Ökosystem eingebracht werden. Denn schon heute vertrauen Kunden ihrer Bank hochsensible Finanz- und Identitätsdaten an.

Derzeit fehlt es jedoch noch an regulatorischen und technischen Rahmenbedingungen, damit Banken oder andere Unternehmen ihren Kunden Mehrwertdienstleistungen auf Grundlage sicherer und breit nutzbarer digitaler Identitäten anbieten können.

4.3 Harmonisierung des Rechtsrahmens für Identifizierungsprozesse

Für die Förderung eines digitalen ID-Ökosystems bedarf es branchenübergreifender Standards für Identifizierungsprozesse, insbesondere für die Identitätsfeststellung sowie die Wiederverwendung von Identifizierungsdaten. Das gilt vor allem für Identitäten, die aufgrund gesetzlicher Vorgaben erhoben werden müssen. Hiervon speziell betroffen sind Banken und andere geldwäscherechtlich Verpflichtete, Telekommunikationsanbieter, Vertrauensdiensteanbieter sowie öffentliche Stellen.

Mit wenigen Ausnahmen sind die Möglichkeiten, einmalig festgestellte, verifizierte Identitäten zwischen einzelnen Unternehmen oder einzelnen Sektoren auszutauschen und dadurch sektorübergreifend wiederzuverwenden, bis heute stark eingeschränkt. Grund dafür ist, dass in den jeweiligen Branchen sektorspezifische gesetzliche Anforderungen an die Identifizierung bestehen, die nicht miteinander abgestimmt sind. Um ein Ökosystem digitaler Identitäten kurzfristig zum Erfolg zu führen, bedarf es daher einer Harmonisierung der sektorspezifischen Regelungen sowie einer einheitlichen Verwaltungspraxis der jeweils zuständigen Aufsichtsbehörden in den verschiedenen Sektoren. Dies würde maßgeblich dazu beitragen, dass verifizierte Identitäten unternehmens- und sektorübergreifend wiederverwendet werden können.

In den sektorspezifischen Regelungen des Geldwäschegesetzes (GwG), des Onlinezugangsgesetzes (OZG) und des Telekommunikationsgesetzes (TKG) gibt es zwar sowohl hinsichtlich des Inhalts der einzuholenden Informationen (bei natürlichen Personen bspw. Vorname und Nachname, Geburtsdatum und Anschrift) als auch hinsichtlich der notwendigen Unterlagen und ihrer erforderlichen Speicherung zahlreiche Überschneidungen. Nach wie vor bestehende Unterschiede zwischen den Regularien erschweren bzw. verhindern aber unnötigerweise eine Wiederverwendung bereits erhobener Identifizierungsdaten. Diese Unterschiede betreffen beispielsweise den Umfang des Identifizierungsdatensatzes: So müssen etwa nach GwG und OZG Angaben zur Staatsangehörigkeit und zum Geburtsort erhoben werden, jedoch nicht nach TKG. Zudem unterscheiden sich die Möglichkeiten der Identitätsüberprüfung anhand bestimmter Nachweise, die neben den Ausweisdokumenten explizit zugelassen sind. Im GwG etwa ist die Identitätsüberprüfung anhand einer Qualifizierten Elektronischen Signatur (QES) ausdrücklich vorgesehen, im TKG jedoch nicht. Häufig werden die Anforderungen an die Identitätsfeststellung durch die jeweils zuständigen Behörden in Form von Verfügungen und Technischen Richtlinien weiter konkretisiert, was zur Divergenz zusätzlich beiträgt.

Grundsätzlich sehen sowohl das Geldwäschegesetz als auch das Vertrauensdienstegesetz (VDG) die Möglichkeit der Wiederverwendung einer bereits zuvor durch einen Dritten ordnungsgemäß durchgeführten Identifizierung vor. Während dies nach VDG beispielsweise Banken oder andere Unternehmen sein können, die gesetzlich (z.B. nach GwG oder TKG) zur Identifizierung ihrer Vertragspartner verpflichtet sind, sieht das GwG diese Möglichkeit lediglich für andere GwG-Verpflichtete vor.

Bei der sektorübergreifenden Nutzung von Identitätsdaten ergeben sich für Vertrauensdienste-anbieter (VDA) in der Praxis operative Herausforderungen durch die bereits beschriebenen sektorspezifisch unterschiedlichen Detailanforderungen. Dies betrifft beispielsweise den Aktualisierungsprozess bereits erhobener Identitätsdaten in den jeweiligen Branchenverfahren. So ist derzeit offen, inwieweit die in der Kreditwirtschaft vorgeschriebenen Prozesse zur Sicherstellung der Aktualität von Kundendaten (KYC-Prozesse) auch die diesbezüglichen Anforderungen für Vertrauensdiensteanbieter erfüllen, oder ob – beispielsweise bei Änderungen von Meldedaten – zwingend eine Neuidentifizierung durchzuführen ist. Zudem muss der VDA für jede einzelne Bank prüfen, ob die seitens der Bank eingesetzten Prozesse und Identifizierungsverfahren den Anforderungen an VDAs genügen, auch wenn die Bank im Zusammenhang mit einer Kontoeröffnung alle einschlägigen Anforderungen (z.B. aus GwG, Abgabenordnung etc.) eingehalten hat. Dies führt zu einem erheblichen Aufwand auf beiden Seiten und stellt eine merkliche Barriere für die sektorübergreifende Wiederverwendung von Identitätsdaten dar.

Ein weiteres Beispiel sind unterschiedliche Anforderungen an die Identitätsfeststellung mittels Videoidentifizierungsverfahren in den verschiedenen Sektoren: Jede Aufsichtsbehörde stellt separate Anforderungen, beispielsweise die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in ihrem Rundschreiben 03/2017 für geldwäscherechtlich Verpflichtete oder die Bundesnetzagentur (BNetzA) in ihrer Verfügung zu § 11 (1) VDG, 11/2018 für die Vertrauensdiensteanbieter sowie in ihrer Verfügung gemäß § 111 (1) Satz 4 TKG für die Telekommunikationsanbieter. Dies kann mitunter zu erheblichen Wettbewerbsnachteilen für deutsche Anbieter gegenüber ihren europäischen Mitbewerbern führen, die nicht diesen speziellen deutschen Aufsichtspraktiken unterliegen, wie es für Vertrauensdiensteanbieter zu beobachten ist.

Um die oben skizzierten Hindernisse zu beseitigen, sind folgende Maßnahmen zur Anpassung des bestehenden Rechtsrahmens notwendig:

1. Es muss eine generelle Gleichwertigkeit der Anforderungen an Identifizierungsprozesse in den sektorspezifischen Regelungen auf nationaler bzw. europäischer Ebene hergestellt werden. Hiervon müssen alle Bereiche erfasst sein, in denen eine Identifizierung von natürlichen oder juristischen Personen von Gesetz her vorgeschrieben ist, beispielswiese im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung, im Telekommunikationsbereich, im öffentlichen Sektor sowie bei Vertrauensdiensten. Sofern diese Regelungen auf einer europäischen Rechtsgrundlage basieren, ist eine Vollharmonisierung im Wege einer europäischen Verordnung erforderlich, wie es von der EU-Kommission im Bereich der Geldwäschebekämpfung angekündigt ist.

2. Am wirksamsten ließe sich eine Vollharmonisierung durch einen einzigen sektorübergreifenden europäischen Rechtsrahmen erreichen, auf den sich sektorspezifische Regelungen stützen. Hierdurch wäre auch gewährleistet, dass der Umfang der vom Identifizierungspflichtigen erhobenen Daten EU-weit identisch ist. Damit ließen sich die aufwendigen Nacherhebungen einzelner Merkmale, wie sie heutzutage bei der Wiederverwendung regelmäßig erforderlich sind, auf ein Minimum reduzieren.

3. Der Gesetzgeber muss weiterhin Rahmenbedingungen schaffen, die Rechtssicherheit im Verhältnis zwischen Identitätsempfänger (Verifier) und Identitätsaussteller (Issuer) ermöglichen. Denn der Identitätsempfänger muss sich im eigenen Interesse und zur Erfüllung seiner aufsichtsrechtlichen Pflichten darauf verlassen können, dass die vom Issuer bereitgestellten Identitätsdaten ordnungsgemäß unter Einhaltung der ihn (Issuer) betreffenden Regularien (z.B. bzgl. Identifizierung und Aktualisierung) erhoben wurden. Hierbei müssen auch haftungsrechtliche Fragen, wie zum Beispiel Haftungsgrenzen, mitgedacht werden, um einen fairen Interessenausgleich sicherzustellen und eine Anreizwirkung zu erzielen.

Die anstehende Novellierung der eIDAS-Verordnung sollte genutzt werden, um auf europäischer Ebene horizontal einheitliche Anforderungen im Sinne einer Vollharmonisierung zu definieren und grenzüberschreitende Identifizierungsprozesse zu erleichtern. Auf diesem Wege könnte eine kohärente, EU-weite Lösung für eine branchenübergreifende Anwendung digitaler Identitäten und deren Wiederverwendung geschaffen werden. Über die vorhandenen eIDAS-Vertrauensniveaus („niedrig", „substanziell", „hoch") wären zudem fall- oder sektorspezifische Bedarfe und Risiken abbildbar, analog zu dem heutigen Anwendungsbereich im E-Government. Darüber hinaus sind verbindliche Regelungen darüber erforderlich, welches eIDAS-Vertrauensniveau für den entsprechenden Anwendungsfall notwendig ist. Für die geldwäscherechtliche Identifizierungsanforderung wäre das eIDAS-Level „substanziell", wie es für qualifizierte VDAs bei der Erstellung einer QES vorausgesetzt wird, das angemessene Vertrauensniveau.

4.4 Interoperabilität zwischen den einzelnen Identitätsanbietern

Das Angebot an digitalen Identitätslösungen ist innerhalb der EU unterschiedlich stark entwickelt, wobei bestehende Angebote auf die nationalen Märkte begrenzt sind. Dabei ist der deutsche Markt besonders fragmentiert, es existieren zahlreiche Anbieter, von denen derzeit noch keiner eine kritische Masse aufweisen kann. Ein ID-Ökosystem würde die Chance eröffnen, die Nutzbarkeit von digitalen Identitäten über verschiedene Identitäts-Schemes zu gewährleisten und damit digitalen Identitäten zur breiten Anwendung zu verhelfen. Aktuell krankt es daran, dass die bestehenden Identitätslösungen untereinander nicht kompatibel sind. Sie sind als in sich geschlossene Lösungen konzipiert, mit eigenen Schnittstellen, eigenen Daten-Attributen und eigenen Rahmenwerken. Die Interoperabilität der Daten zwischen einzelnen Identitätsanbietern und internationalen Netzwerken ist eine wichtige Voraussetzung, um einen schnellen und nachhaltigen Austausch von Daten zu ermöglichen.

Schon heute bedienen sich Schemes internationaler Standards: Mit OAuth 2.0 und OpenIDConnect existieren gängige Konventionen, die im Kontext von Identifizierungs- und Authentifizierungsdiensten weltweit genutzt werden. Sie funktionieren allerdings nur innerhalb der jeweilig geschlossenen Schemes und sind untereinander in den wenigsten Fällen interoperabel. Dies führt dazu, dass Internetportale zuweilen bis zu sieben verschiedene Single-Sign-On-Anbieter unterstützen. Daneben entstehen vermehrt dezentrale Ansätze für eine Speicherung der Identitätsdaten nach dem Prinzip sogenannter Self-Sovereign Identities (selbstbestimmten Identitäten) unter Nutzung der Distributed Ledger Technologie (DLT). Diese dezentralen Ansätze beruhen auf standardisierten Kommunikationsprotokollen (DIDcomm) sowie Datenstandards für Decentralized Identifiers (DID) und verifiable Credentials, die von der Decentralized Identity Foundation (DIF) und dem World Wide Web Consortium (W3C) global definiert werden und deren Ziel eine Interoperabilität über Schemes und Ländergrenzen hinweg ist.

Mit Self-Issued OpenID Connect Provider (OP/SIOP) gibt es aktuell Bestrebungen in der Standardisierung, die Vorteile von SSI auch mit existierenden Schnittstellen interoperabel zu machen. Auf diese Weise könnte den Abnehmern von Identitätsdaten eine einfache Integration von SSI-Lösungen auf Basis bekannter Schnittstellen bei gleichzeitiger Erhöhung der Reichweite zur Verfügung gestellt werden.

Neben der technischen Interoperabilität spielt die regulatorische Interoperabilität eine wichtige Rolle. Mit der eIDAS-Verordnung besteht bereits ein EU-weiter Rechtsrahmen für Vertrauensdienste, beispielsweise zur Ausstellung von qualifizierten elektronischen Signaturen und Siegeln. Im Rahmen der geplanten Überarbeitung der eIDAS-Verordnung wäre eine rechtlich bindende Verankerung von Verifiable Credentials sowie der Zertifizierungsmöglichkeit von Identifizierungsanbietern (entsprechend eIDAS bei Vertrauensdiensteanbietern) wünschenswert.

Damit ein Ökosystem wirtschaftlich funktionieren kann, sind neben Rahmenvereinbarungen zu funktionalen, technischen, operativen und rechtlichen Aspekten auch Rahmenbedingungen zu wirtschaftlichen Aspekten des Identitätsaustauschs notwendig. Denn eine Identifizierung ist in der Regel Teil eines Wertschöpfungsprozesses; die Erbringung einer Identitätsleistung stiftet einen wirtschaftlichen Nutzen für den Verifier. Daher muss diese Dienstleistung, die mit Aufwand verbunden ist, für den Issuer einen wirtschaftlichen Vorteil versprechen, sprich: die Identitätsdienstleistungen müssen entweder gegenüber dem Verifier oder den zu Identifizierenden bepreist werden können. Es bedarf daher eines vertraglichen Rahmens für Monetarisierungsmodalitäten, der Unternehmen nachhaltig Anreize bietet, in die notwendige Infrastruktur zu investieren. Die hohe Komplexität bilateraler Verträge ließe sich z.B. durch ein Rahmenvertragswerk auf Ebene des Ökosystems reduzieren. Hierzu bedarf es der Etablierung einer Governance, die übergreifende Regeln und Vereinbarungen (z.B. Haftungsmechanismen) in Übereinstimmung mit dem geltenden Rechtsrahmen schafft und eine bedarfsgerechte Weiterentwicklung fördert.

4.5 Enge Zusammenarbeit zwischen öffentlichem und privatem Sektor

Ein Ökosystem digitaler Identitäten kann dann erfolgreich sein, wenn es ein Miteinander von öffentlicher und privatwirtschaftlicher Seite gibt. Dies zeigt auch ein Blick ins Ausland, wo sich digitale Identitätslösungen zumeist im Zusammenspiel mehrerer Akteure einschließlich des Staates etabliert haben. Erst auf diese Weise entstehen die notwendigen Skaleneffekte und Synergien, die für eine hohe Attraktivität des Gesamtsystems und für Akzeptanz bei den Nutzern sorgen.

Für eine maximale Skalierbarkeit und möglichst breite, branchenübergreifende Akzeptanz eines ID-Ökosystems müssen Bedarfe und Anforderungen aller Stakeholder in der Konzeption des Ökosystems in gleicher Weise berücksichtigt werden. Um dies zu gewährleisten, ist eine enge Zusammenarbeit zwischen öffentlichem und privatem Sektor womöglich in Form einer Public-Private-Partnership anzustreben, in der Vertreter der einzelnen Stakeholder (Staat, Wirtschaft, Verbraucher) gemeinsam an der Entwicklung eines ID-Ökosystems arbeiten und entsprechende branchenübergreifende Standards definieren. Anhand ausgewählter Use-Cases könnten sowohl technische Standards, die Kombination staatlicher und privater eID-Verfahren, regulatorische Anpassungen als auch prozessuale Abfolgen und Maßnahmen für eine maximale Usability definiert und in Praxistests erprobt werden. Neben der Bündelung von Wissen ließen sich Entwicklungskosten innerhalb der Partnerschaft teilen oder fördern, sodass nutzerzentrierte Innovationen bei verhältnismäßig niedrigem Kostenaufwand der einzelnen Parteien entstehen können.

5 Ausblick

Die von der Bundesregierung Ende letzten Jahres gestartete Initiative zur Schaffung eines europäischen Ökosystems digitaler Identitäten ist ein bedeutender Schritt in diese Richtung und wird von den privaten Banken ausdrücklich unterstützt. Im Rahmen eines Projektes mit Vertretern ausgewählter Branchen und Unternehmen sollen Anwendungsfälle mit hoher Sichtbarkeit gemeinsam ausgewählt und kurzfristig umgesetzt werden. Gleichzeitig hat die Bundesregierung in Aussicht gestellt, notwendige regulatorische Voraussetzung zu schaffen, um eine breite Nutzung der entwickelten Lösungen in den jeweiligen Sektoren zu ermöglichen. Hierbei ist es allerdings wichtig, eine Plattform zu schaffen, die allen interessierten Parteien und Stakeholdern eine Partizipation und Mitgestaltung an dem Ökosystem ermöglicht – auch mit Blick auf einen fairen Wettbewerb. Zudem darf nicht erneut der Fehler begangen werden, durch eine ausschließliche Fokussierung auf die staatliche Online-Ausweisfunktion als Kern des Ökosystems den Erfolg der Initiative zu gefährden. Denn in einer marktwirtschaftlichen Ordnung wird am Ende die Nutzerakzeptanz über Erfolg und Misserfolg entscheiden. Angesichts der hohen Bedeutung privatwirtschaftlicher Anwendungsfälle in einem solches Ökosystem und der heutigen globalen Vernetzung sind mittelfristig Lösungen unverzichtbar, die über die nationalen Grenzen hinaus gehen und mindestens auf europäischer Ebene zum Tragen kommen. Diesem Anspruch müssen sich nationale Initiativen stellen.