SICHERE DIGITALE IDENTITÄTEN

Impulspapier | Juni 2022

Zusammenfassung

Sichere digitale Identitäten sind wichtige Treiber der Modernisierung der öffentlichen Verwaltung, aber auch der Digitalisierung in Unternehmen. Systeme für den elektronischen Identitätsnachweis (eID) sind Lösungen zur Umsetzung eines digitalen Abbilds für die Anwendung im staatlichen oder privatwirtschaftlichen Umfeld. Derzeit dominieren im privatwirtschaftlichen Bereich die bekannten Anbieter, wie Facebook, Google oder Apple. Diese stellen Bürgerinnen und Bürgern zwar komfortable, einfach zu nutzende Dienste bereit, bieten ihnen jedoch kaum Möglichkeiten, selbstbestimmt zu entscheiden, welche Identifizierungsdaten für welche Dienste genutzt und welche Daten wo gespeichert werden dürfen. Zudem ist das Sicherheitsniveau der Lösungen sehr unterschiedlich; nicht jedes Angebot ist für jeden Onlinedienst oder jede digitale Anwendung geeignet. Ein hohes Sicherheitsniveau bietet die eID-Funktion des elektronischen Personalausweises, der aber noch nicht in der Breite eingesetzt wird. Lösungen zu selbstbestimmten Identitäten – Self-Sovereign Identities (SSI) – ermöglichen es Bürgerinnen und Bürgern, selbst zu entscheiden, welche Form der digitalen Identität sie gegenüber einem Dienstanbieter nutzen, sei es ein Pseudonym, eine hoheitlich bestätigte Identität oder eine an spezielle Attribute gebundene Identität, wie zum Beispiel den Arbeitgeber. Ein Manko existierender SSI-Ansätze ist, dass sie meist nicht nutzungsfreundlich sind und das Prinzip der Datensparsamkeit missachten. Es gibt derzeit viele Angebote am Markt, die alle jeweils Vor- und Nachteile haben. Eine One-Fits-All-Lösung wird es nicht geben und sollte auch nicht angestrebt werden. Jedoch erschwert der derzeit existierende, stark fragmentierte Markt an eID-/SSI-Lösungen eine breit akzeptierte, nutzungsfreundliche, aber gleichzeitig sichere und selbstbestimmte Verwendung digitaler Identitäten. Dies führt zu Verzögerungen, auch bei der Umsetzung von Onlinediensten in der öffentlichen Verwaltung. Durch gezieltes politisches Handeln kann und sollte hier Abhilfe geschaffen werden. So sollte durch das Setzen eines politischen Rahmens darauf hingewirkt werden, dass die Marktteilnehmerinnen und Marktteilnehmer in den Wettbewerb treten können, wobei ihre Angebote an den Nutzerinnen und Nutzern orientiert sind und gleichzeitig die demokratischen Werte der Sicherheit, des Vertrauens und der Selbstbestimmtheit gewährleisten.

Die Wissenschaftliche Arbeitsgruppe des Nationalen Cyber-Sicherheitsrates empfiehlt deshalb, die technologische und regulatorische Basis zu entwickeln, um ein europaweites, gemeinsames eID-Ökosystem zu schaffen, das sowohl staatliche als auch digitale Identitäten des privatwirtschaftlichen Sektors sowie SSI-Lösungen umfasst. Ein solches eID-Ökosystem ermöglicht es, digitale Identitäten grenzüberschreitend für alle digitalen Dienstleistungen und Geschäftsprozesse zu verwenden. Die Nutzung soll, soweit möglich und gewünscht, einfach, selbstbestimmt, sicher und privatsphärenfreundlich sein. Um einen hohen Sicherheitsstandard zu garantieren, sollten Sicherheitsfunktionen mobiler Endgeräte zur Verwaltung der digitalen Identitäten systematisch genutzt werden. Bei der Entwicklung von Lösungen müssen die Themen Benutzbarkeit, Vertrauen, Sicherheit und Datenschutz gleichrangig berücksichtigt werden.

Das Positionspapier erläutert die aktuelle Situation bei eID- und SSI-Lösungen, verdeutlicht die technischen Herausforderungen für sichere, nutzungsfreundliche und breit akzeptierte Lösungen. Zudem leitet es Anforderungen an das zu schaffende eID-Ökosystem ab. Das Papier schließt mit konkreten Handlungsempfehlungen an die Politik. Diese umfassen folgende Empfehlungen: Technische und regulatorische Rahmenvorgaben für ein solches Ökosystem zu schaffen, die frühzeitige Einbindung der Zivilgesellschaft, eine offene Entwicklung sowie einheitliche Normen und Standards aktiv gestaltend voranzutreiben und über mehrwertige eID-basierte Dienstleistungen für die breite Öffentlichkeit den Weg für einen Flächeneinsatz von eID zu ebnen.

1 Ausgangslage

Digitale Identitäten sind wesentliche Impulsgeber für unsere moderne Informationsgesellschaft und essenziell für die Vertrauensbildung. Dies betrifft sowohl alle Interaktionen von Bürgerinnen und Bürgern mit staatlichen Organen und Institutionen der öffentlichen Hand, aber auch Handlungen von Bürgerinnen und Bürgern im wirtschaftlichen Kontext, beispielsweise zur Identifikation gegenüber Banken, und nicht zuletzt die Kommunikation untereinander. Vertrauensbildung basierend auf sicheren digitalen Identitäten ist zudem eine zentrale Basis von geschäftlichen Transaktionen im Business-to-Business- oder auch im Business-to-Government-Umfeld. Benutzbare und sichere digitale Identitäten werden somit nicht nur für die notwendige Modernisierung der öffentlichen Verwaltung benötigt (z. B. im Rahmen des Online-Zugangsgesetzes (OZG)), sondern auch in der Privatwirtschaft. Sichere digitale Identitäten sind damit wichtige Impulsgeber für die Modernisierung der öffentlichen Verwaltung und Treiber der Digitalisierung in Unternehmen. Digitale Identitäten betreffen sowohl natürliche Personen als auch Objekte im sogenannten Internet of Things. Das vorliegende Positionspapier stellt die Frage der sicheren digitalen Identitäten **von natürlichen Personen** in den Mittelpunkt der Betrachtungen.

Im Bereich der Verwaltung digitaler Identitäten in der Privatwirtschaft dominieren derzeit die bekannten Anbieter, wie Facebook, Google oder Apple[1]. Der Vorteil dieser Lösungen für die Bürgerinnen und Bürger besteht darin, die gleiche Identität für verschiedene Dienstleistungen verwenden zu können. Dies ist aus Sicht der Nutzenden komfortabel und deshalb breit akzeptiert. Dieser einfachen Nutzung stehen jedoch Gefährdungen gegenüber. So besteht durch die Marktdominanz der großen Identitätsanbieter für die Bürgerinnen und Bürger die Gefahr eines Kontrollverlustes. Es mangelt an der Möglichkeit, souverän über die eigene digitale Identität bestimmen zu können. Die enge Bindung an einen Anbieter birgt zudem die Gefahr eines möglichen Lock-in-Effekts, sodass ein Wechsel zu anderen Anbietern aufgrund hoher Migrationskosten vermieden wird, obwohl andere Anbieter ggf. bessere Optionen bieten könnten, insbesondere im Hinblick auf Datensicherheit und den Privatsphärenschutz. Das Ziel muss deshalb sein, Lösungen von hohem Nutzungskomfort und hoher Akzeptanz bereitzustellen, welche die genannten Gefährdungen ausschließen oder zumindest substanziell verringern.

Hier setzen die Initiativen zur Schaffung von sogenannten **selbstbestimmten Identitäten** – Self-Sovereign Identities **(SSI)** – an[2]. Mit SSI kontrollieren die Bürgerinnen und Bürger jederzeit selbst, welche Form der digitalen Identität sie gegenüber einem Dienstanbieter präsentieren, sei es ein Pseudonym, eine hoheitlich attestierte Identität, wie die eID aus dem amtlichen Personalausweis, oder eine an spezielle Attribute gebundene Identität des privatwirtschaftlichen Sektors. Die beruflichen Qualifikationen oder der Name des Arbeitgebers sind Beispiele für derartige Attribute. Das zugrunde liegende Konzept sieht vor, dass solche Attribute, auch Claims genannt, von zuständiger Stelle, wie beispielsweise dem betreffenden Unternehmen, bestätigt werden. Bestätigungen sind digitale Dokumente, die von der bestätigenden Stelle, dem Aussteller, digital signiert werden. Die so bestätigten Attribute können von den Bürgerinnen und Bürgern selbst, zum Beispiel auf dem Smartphone in einer speziellen App, dem Wallet, verwaltet und Dritten zur Prüfung vorgelegt werden. Die zur Prüfung erforderlichen Informationen werden allgemein zugänglich beispielsweise in einem Verzeichnisdienst oder einer verteilten Datenbank abgelegt. Abbildung 1 visualisiert schematisch die Komponenten eines SSI-Systems.

Selbstbestimmte Identitäten sind technische Lösungen, die ohne eine zentrale Identitätsverwaltung, wie sie klassisch durch Unternehmen wie Facebook, Google und Apple angeboten werden, auskommen. Diese dezentralen Ansätze ermöglichen es Bürgerinnen und Bürgern, digitale Identitäten, bzw. die signierten Identitätsattribute, ohne die Mitwirkung einer vermittelnden Instanz oder einer zentralen Entität zu kontrollieren. Zu unterscheiden ist hier die eigentliche, selbst kontrollierte Verwaltung der Identitätsattribute und die Etablierung von Vertrauen, das benötigt wird, um die Authentizität der signierten Attribute zu prüfen. Während die Verwaltung der Attribute in der Regel dezentral, z. B. auf Geräten der Bürgerinnen und Bürger erfolgt, kann der Aufbau von Vertrauen auch auf klassischen, zentralen Public-Key-Infrastrukturen aufsetzen, mit Wurzelzertifikaten als Vertrauensankern. Eine dezentrale Lösung für den Vertrauensaufbau mittels eines Web-of-Trust oder einer Blockchain-Technologie bzw. Distributed-Ledger-Technologie (DLT)[3] ist somit keine zwingende Voraussetzung für die technische Umsetzung einer SSI-Lösung.

Anwendungsszenarien für SSI-Lösungen – einige Beispiele

SSI- und eID-Lösungen sind ein wesentlicher Schritt in Richtung Digitalisierung, da SSI-Angebote eine Reihe von Vorgängen und Verfahren erleichtern und beschleunigen, bei denen beispielsweise bislang persönliche Anwesenheit, manuelle Dateneingaben oder Unterschriften erforderlich waren. Nachfolgend werden einige Praxisbeispiele skizziert, um den Mehrwert von SSI zu verdeutlichen.

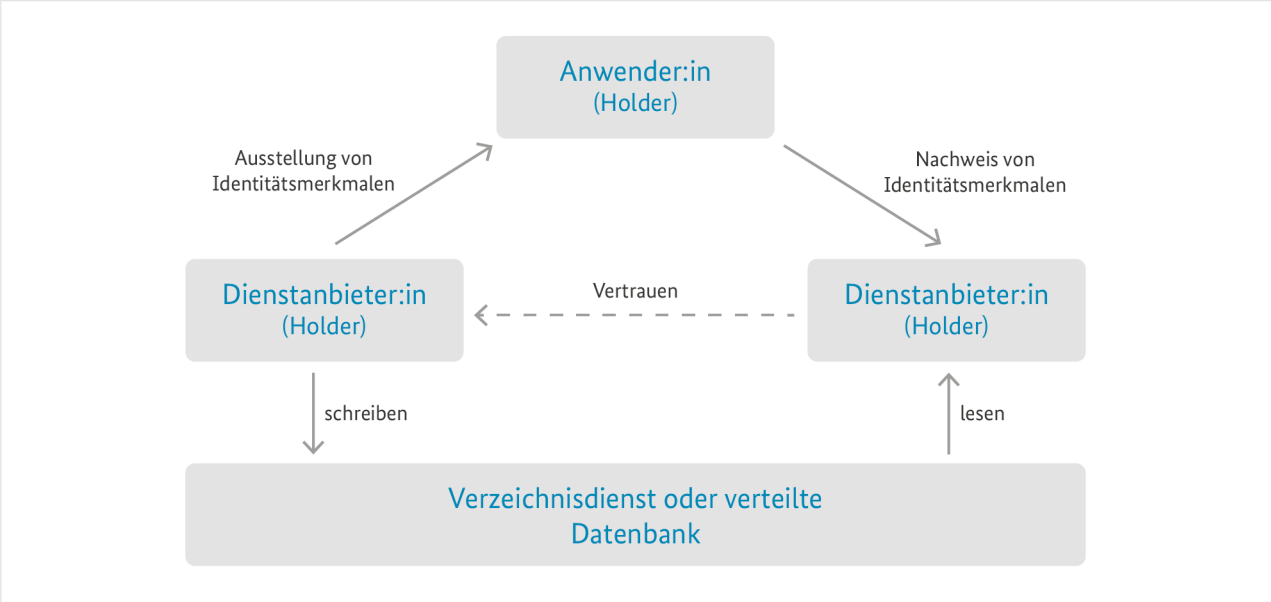

Abbildung 1: Komponenten eines SSI-Systems

Beispiel 1 – Autovermietung
Wer am Bahnhof oder Flughafen ein Auto mieten will, benötigt dafür Ausweis, Führerschein und eine Zahlungsmöglichkeit wie etwa eine Kreditkarte. Müssen Mitarbeitende der Autovermietung alle diese Daten händisch übertragen, kann der gesamte Vorgang inklusive Ausdruck der Vertragspapiere schnell eine Viertelstunde dauern. Mit SSI und ohne fehleranfällige, manuelle Dateneingabe lässt sich der Ablauf medienbruchfrei sicher digitalisieren und auf wenige Sekunden verkürzen.

Beispiel 2 – Bankgeschäfte und Hotelrechnungen
Mit SSI, dem digitalen Personalausweis und einer qualifizierten elektronischen Signatur lassen sich online Bankkonten eröffnen und Verträge mit Mobilfunkprovidern abschließen. Hotels können bei geschäftlichen Aufenthalten von Gästen nach Vorlage digital verifizierbarer Personal- und Dienstausweise die Rechnung direkt an den Arbeitgeber schicken und auch ihren gesetzlichen Meldeverpflichtungen digital nachkommen.

Beispiel 3 – Management von Unternehmensressourcen
Die digitale Identität kann in Unternehmen als Basis für das Management der Zugangs- und Zutrittskontrolle zu Betriebsgebäuden oder zur Freischaltung von Software genutzt werden. Zudem erleichtert eine SSI-Lösung das Flottenmanagement in Betrieben, indem sich die Gültigkeit einer Fahrerlaubnis sofort digital verifizieren lässt.

Beispiel 4 – Digitale Verwaltung
Auch im Bereich Verwaltung und E-Government eröffnen SSI neue Möglichkeiten. So können etwa Vereine und Kammern künftig sichere Onlinewahlen durchführen. Perspektivisch wird dies auch bei Wahlen für politische Gremien aller Art möglich sein, einschließlich Kommunal-, Landtags- und Bundestagswahlen. Alle Nachweise über Genehmigungen und Berechtigungen, die öffentliche Behörden ausstellen, wie Führungszeugnisse oder Parkausweise, lassen sich über SSI abbilden. Ohnehin verpflichtet das OZG Bund, Länder und Kommunen dazu, bis Ende 2023 ihre Verwaltungsleistungen über entsprechende Portale auch digital anzubieten.

Nationale und europäische Initiativen
Aktuell gibt es zahlreiche nationale und europaweite Initiativen, um eID- und auch SSI-Lösungen für digitale Identitäten zu etablieren. Zu den erwähnenswerten Aktivitäten auf Bundesebene gehören die vom Bundesministerium des Innern und für Heimat koordinierten Projekte, um die Online-Ausweisfunktion des Personalausweises auf dem Smartphone einfach und sicher verfügbar zu machen[4]. In dem vom Bundesministerium für Wirtschaft und Klimaschutz orchestrierten Wettbewerb „Schaufenster Sichere Digitale Identitäten“[5] werden bis 2023 die vier Projekte ONCE, IDUnion, ID-Ideal und SDIKA gefördert, um das Thema der sicheren Identitäten in die Breite zu bringen. Auch auf EU-Ebene laufen Anstrengungen zur Etablierung eines EU-weiten Ökosystems für digitale staatliche Identitäten im Rahmen der Strategie für die „Digital Decade“[6]. Von Bedeutung sind dabei die EU-Aktivitäten zur Novellierung der Verordnung „Electronic Identification, Authentication and Trust Services“ (eIDAS) im Juni 2021 gestarteten EU-Aktivitäten, um das Ökosystem auf den privaten Sektor auszudehnen. Durch die eIDAS-Verordnung werden Anforderungen an die Sicherheit staatlicher digitaler Identitäten formuliert und die Harmonisierung des

europäischen Rechtsrahmens weiterentwickelt. In 2022 hat sich eine eIDAS-Expertengruppe der Mitgliedsstaaten gebildet, um gemeinsam an einer technischen Architektur und an Standards zu arbeiten[7]. So soll jeder Mitgliedsstaat verpflichtet werden, seinen Bürgerinnen und Bürgern eine European Digital Identity Wallet (EUid-Wallet) zur Verfügung zu stellen, welche sowohl die bereits existierenden staatlichen Identitäten als auch weitere (z. B. privatwirtschaftliche) Identitäten und Attribute bzw. Nachweise selbstbestimmt verwalten kann.

Daneben engagiert sich auch die Privatwirtschaft, um alternative Lösungen für die digitale Identität zu schaffen. Zu nennen sind Initiativen wie netID, ID4me, Verimi oder YES. Deren Anspruch ist es, einen hohen Komfort für Bürgerinnen und Bürger zu bieten sowie die breite Nutzbarkeit der digitalen Identität für verschiedene digitale Dienstleistungen zu ermöglichen. Die genannten privatwirtschaftlichez Lösungen konnten sich jedoch bislang nicht am Markt durchsetzen. Zwar zielen privatwirtschaftliche Lösungen im Unterschied zu den etablierten Lösungen bereits auf das Zertifizieren von Vertrauensniveaus der Informationssicherheit, z. B. nach eIDAS oder technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI), stehen aber insbesondere in Deutschland vor der Hürde, unterschiedliche Anforderungen in unterschiedlichen Domänen zertifiziert umsetzen zu müssen.

2 Herausforderungen

Die Fragmentierung des Marktes für eID- bzw. SSI-Lösungen ist bereits heute Realität. Diese sollte akzeptiert, aber gleichzeitig als Chance und Auftrag für die politische Gestaltung aufgefasst werden. Das bedeutet, dass Anstrengungen, die darauf hinauslaufen, einen One-Fits-All-Ansatz zu etablieren, ins Leere laufen werden, da damit die Realität nicht abgebildet wird und eine solche Lösung keine breite Akzeptanz finden würde. Vielmehr muss dafür Sorge getragen werden, dass die Marktteilnehmerinnen und -teilnehmer nutzungsorientiert in den Wettbewerb treten können und gleichzeitig ihre Angebote die demokratischen Werte der Sicherheit, des Vertrauens und der Selbstbestimmtheit gewährleisten. Hierfür muss der geeignete politische Rahmen gesetzt werden.

Technische Herausforderungen

Diese Transformation von allgemeinen, heute üblichen eID-Lösungen hin zu nutzungsfreundlichen, sicheren, selbstbestimmten digitalen Identitäten erfordert neben der politisch-regulatorischen Unterstützung auch eine technische. Nur so kann die informationelle Selbstbestimmung der Bürgerinnen und Bürger garantiert werden. Aussteller von Nachweisen einzelner Aspekte digitaler Identitäten, den Attributen bzw. Claims, müssen von den Bürgerinnen und Bürger selbstbestimmt ausgewählt und aggregiert werden können. Dies ist eine der Kernideen der SSI-Technologien. Den Bürgerinnen und Bürgern muss die Möglichkeit gegeben werden, situations- und kontextanhängig verschiedene Identitätsnachweise und -varianten verwenden zu können, auch in Abhängigkeit des geforderten Sicherheitsniveaus. Spezifische Sicherheitsbedürfnisse können sich unter anderem aus gesetzlichen Anforderungen ergeben. So enthält die eIDAS-Verordnung beispielsweise verbindliche europaweit geltende Regelungen für die grenzüberschreitende Identifizierung. Andere Anforderungen wären beispielsweise das Erfordernis eines bestätigten Nachweises einer Altersangabe. Statt zu versuchen, einen Dienst zu etablieren, welcher alles leisten kann, sollte die Möglichkeit geschaffen werden, auf einfache und sichere Weise diverse Anwendungsszenarien mit unterschiedlichen Technologien zu bedienen, ohne dass der Komfort für Bürgerinnen und Bürger darunter leidet.

Weiterhin sollten Fortschritte und Chancen der etablierten zentralen Identitätssysteme im Auge behalten werden und soweit möglich in einem eID-Ökosystem nicht verloren gehen. Dazu gehört beispielsweise die effiziente Bereitstellung aktueller Informationen über die Nutzerinnen und Nutzer an Dienste. So ermöglichen es typische Identitätsprovider mit dem OpenID-Verfahren, dass die nutzende Person ihre Identität einer Vielzahl von anderen Diensten zur Verfügung stellt und diese an einer zentralen Stelle auf dem aktuellen Stand halten kann. Die Dienste profitieren von aktuellen Identitätsinformationen und könnten auf eine eigene Speicherung dieser Daten verzichten. Dies würde die Problematik von veralteten Datensätzen umgehen und Angriffsrisiken minimieren, die mit der Speicherung sensitiver Daten in Verbindung stehen. Insbesondere Geschäftsprozesse, die aktuelle Identitätsinformationen im Rahmen einer periodischen Leistungserbringung benötigen, wie beispielsweise monatliche Warenlieferungen, sind auf derartige Informationen angewiesen. Dazu müssen sie aber nicht mit Kundinnen und Kunden wiederholt in Kontakt treten; das Vorgehen erlaubt eine nutzungsfreundliche und gleichzeitig datensparsame Lösung. Gerade diese Funktionalität ist jedoch bei vielen SSI-basierten Lösungen nicht (mehr) möglich. Weitere Entwicklungen im Rahmen einer sicheren und dezentralen Bereitstellung von Identitätsinformationen nach den Prinzipien von SSI sind daher erforderlich. Mögliche Ansätze auf Basis von innovativen, dezentralen Verzeichnisdiensten[8] zeigen einen Weg auf, wie diese Lücke gefüllt werden könnte. Hier werden neue kryptografische Mechanismen mit dezentralen Speichermechanismen kombiniert, wodurch die Defizite von SSI-Lösungen kompensiert werden.

Sicherheitstechnische Herausforderungen und Nutzungsakzeptanz

Ein Kernproblem bleibt die Entwicklung von nutzbaren Lösungen, die einen möglichst hohen Grad an Sicherheit gewährleisten. Einige der bereits existierenden eID-Marktangebote bestätigen zwar, dass sichere Lösungen entstehen können, allerdings ist bislang deren Reichweite und Verbreitung aufgrund eines verbesserungswürdigen Nutzungserlebnisses noch sehr gering. Darüber hinaus muss die Sicherheit von eID-Lösungen in diversen Sektoren, wie dem Telekommunikations-, dem Finanz- oder auch dem Mobilitätsbereich hinsichtlich unterschiedlich regulierter Anforderungen nachgewiesen werden. Zu nennen sind hier etwa die EU-Anti-Geldwäsche-Richtlinie (AMLD), die Zweite Zahlungsdiensterichtlinie PSD2, die eIDAS-Verordnung, das OZG bzw. die Technischen Richtlinien des BSI, das Telekommunikationsgesetz oder die Telematikinfrastruktur. Insbesondere mit Blick auf den Einsatz der für die Bürgerinnen und Bürger aktuell verfügbaren mobilen Endgeräte ergibt sich aus den Regularien ein Spannungsfeld zwischen den Sicherheitsanforderungen der verschiedenen Vertrauensniveaus und dem breiten Einsatz der eID-Lösungen. Die Herausforderungen gelten in diesem Zusammenhang gleichermaßen für Angebote von eID-Lösungen als auch für Dienstleistungen digitaler Anwendungen. Aus den variierenden technischen Schnittstellen und den unterschiedlichen Vertrauensrahmenwerken für Informationssicherheit ergeben sich zudem hohe Integrationskosten. Bestehende Ansätze haben es bis heute für sich allein nicht geschafft, im Spagat zwischen Sicherheitsanforderungen und Nutzungsakzeptanz am Markt erfolgreich zu sein. Für eine nachhaltige Marktdurchdringung digitaler Identitätslösungen ist zweierlei entscheidend: Einerseits ist es wichtig, eine kritische Masse von Nutzerinnen und Nutzern zu erreichen. Andererseits braucht es eine Vielzahl alltäglicher, nutzbarer Anwendungsfälle sowie die Zulassung der Verfahren in den unterschiedlich regulierten Sektoren.

Klassisch werden für digitale Identitäten Smartcards als Trägermedien eingesetzt. Diese bieten einen hohen Grad an zertifizierter Sicherheit und sind durch ihre weite Verbreitung bereits von den meisten Nutzerinnen und Nutzern akzeptiert. Nachteile dieser Lösungen sind die begrenzten Ressourcen der Hardware, eine beschränkte Interaktion mit den Nutzerinnen und Nutzern sowie zumeist eine umständliche Anbindung an PC und Smartphone. Zusätzlich ist es aufgrund von organisatorischen Prozessen oft nur möglich, eine Identität pro Smartcard zu speichern. Der aktuelle Trend zeigt, dass immer häufiger Smartphones als Speichermedium für digitale Identitäten gewählt werden. Smartphones bieten die Möglichkeit, mit den Nutzerinnen und Nutzern zu interagieren sowie beliebig viele digitale Identitäten zu speichern. Jedoch können Smartphones die hohen Anforderungen nach (zertifizierter) Sicherheit, wie sie im Kontext der stark regulierten Identitäten durch die entsprechenden gesetzlichen Auflagen bestehen, noch nicht vollständig erfüllen. Es wird bereits intensiv gearbeitet, um diese Situation zu verbessern. Zu nennen sind hier Aktivitäten wie OPTIMOS 2.0, die Android Ready SE Alliance oder Identity Credentials API. Es besteht aber zudem eine hohe Abhängigkeit von Smartphone-Herstellern wie Apple und Google. Dies zeigt sich unter anderem, wenn man auf integrierte Sicherheitsfunktionen von Smartphones, z. B. auf das Secure-Element in iPhone-Geräten, zugreifen möchte.

Um eID-Lösungen nach den Prinzipien der SSI in der Breite und mit hohem Nutzungskomfort zur Verfügung stellen zu können, sollten als technische Basis die Sicherheitsfunktionen mobiler Endgeräte zur Verwaltung der digitalen Identitäten systematisch genutzt werden. Gleichzeitig sind weitere Anstrengungen unbedingt erforderlich, um die technische Basis so bereitzustellen, dass das geforderte hohe Sicherheitsniveau ebenfalls gewährleistet werden kann.

3 Forderung zur Schaffung eines europaweiten eID-Ökosystems

Zusammenfassend ist festzuhalten, dass die Anstrengungen forciert werden müssen, um die Chancen von eID-Systemen in der Breite zu nutzen. Grundsätzlich sollte eine technologische und regulatorische Basis entwickelt werden, um ein **europaweites, gemeinsames eID-Ökosystem** zu schaffen. Ziel kann keine One-Fits-All-Lösung sein. Vielmehr müssen die Anstrengungen darauf ausgerichtet werden, die Lösungen der wichtigsten Initiativen, seien es SSI-basierte Ansätze oder klassische eID-Ansätze, in einem eID-Ökosystem zu integrieren. Ein solches eID-Ökosystem ermöglicht es, digitale Identitäten grenzüberschreitend für alle digitalen Dienstleistungen des Alltags und für digitale Geschäftsprozesse zu verwenden. Die Nutzung soll einfach, selbstbestimmt, aber auch so sicher und privatsphärenfreundlich wie möglich und gewünscht sein, ohne dass dadurch neue Lock-in-Effekte entstehen. Um einen hohen Sicherheitsstandard zu garantieren, sollten Sicherheitsfunktionen mobiler Endgeräte zur Verwaltung der eID-Lösungen systematisch genutzt werden. Abbildung 2 visualisiert das Prinzip eines solchen eID-Ökosystems für Millionen von Nutzerinnen und Nutzern. Über eine integrierende Plattform können sie eID-Lösungen, z. B. der Krankenkassen, des Personalausweises oder auch von Banken, vereinheitlicht und einfach nutzen. Verwaltungsprozesse können dabei ebenso einfach abgewickelt werden wie Geschäfte mit der Privatwirtschaft, z. B. Onlinebanking.

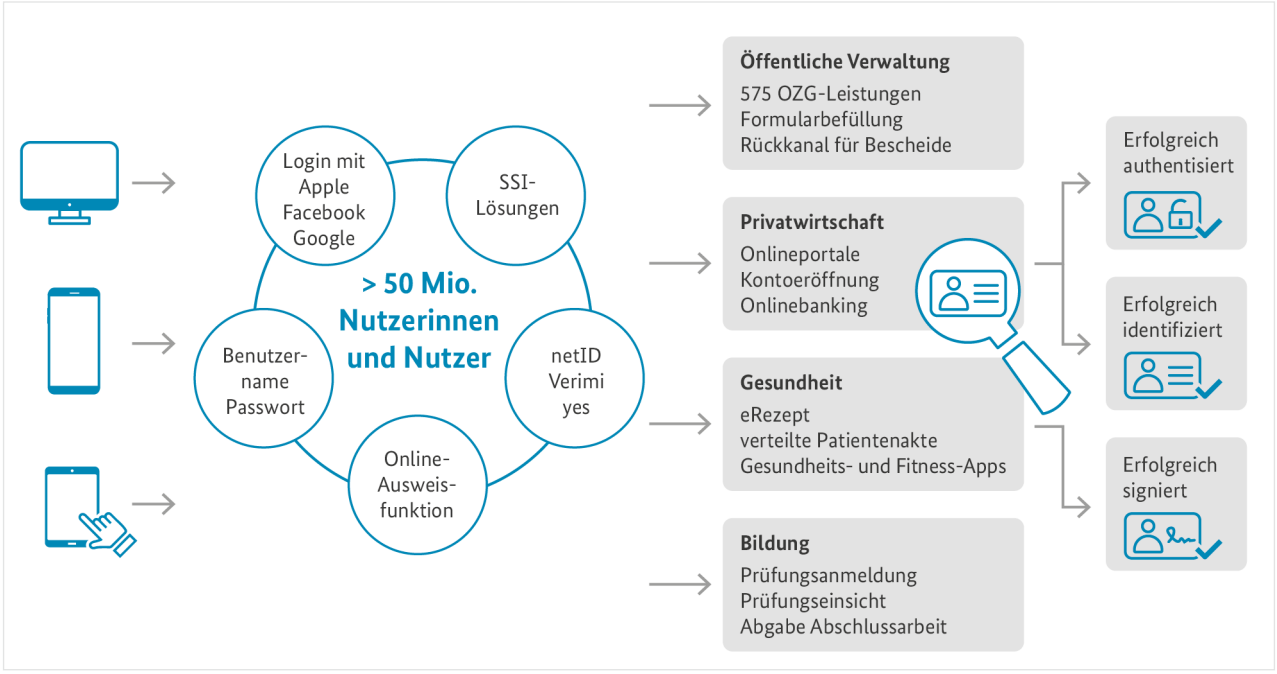

Abbildung 2: Komponenten eines eID-Ökosystems

Nachfolgend werden Anforderungen aufgeführt, die den Rahmen für ein solches eID-Ökosystem definieren und bei der Umsetzung beachtet werden sollten.

Gemeinsame Standards und Interoperabilität

Anerkannte Normen und Standards sind ein wichtiger Baustein für ein eID-Ökosystem, insbesondere hinsichtlich der Interoperabilität von eID-Lösungen und digitalen Dienstleistungen. Die Interoperabilität ist die Voraussetzung dafür, dass technologische Innovationen mit geringen Hürden am eID-Markt erfolgreich sein können und Nutzerinnen und Nutzer tatsächlich hinsichtlich verschiedener ID-Lösungen und Dienstleistungen wählen können. Dabei müssen Standards bezüglich verschiedener Aspekte der Interoperabilität gemeinsam und international entwickelt werden. Dies betrifft die Harmonisierung regulatorischer Anforderungen und die Entwicklung gemeinsamer Protokolle, die von eID-Anbietern und Dienstleistern akzeptiert und genutzt werden sowie die einfache Integration von eID-Lösungen und Dienstleistungen unterschiedlicher Technologien gewährleisten.

Es muss außerdem ein einheitliches Verständnis der grundlegenden Informationseinheiten, Rollen und Vertrauensniveaus von digitalen Identitäten geschaffen werden. Wesentlicher Anknüpfungspunkt für das Entwickeln gemeinsamer Standards eines europaweiten eID-Ökosystems sind die bereits laufenden Bemühungen der Europäischen Kommission und der eIDAS-Expertengruppe zur Überarbeitung der eIDAS-Verordnung. Diesbezüglich ist ein transparenter Austausch zwischen eIDAS-Expertengruppe, Forschung und Industrie notwendig.

Recht auf Anonymität nach den Prinzipien der informationellen Selbstbestimmung und Datensparsamkeit

Während die Identifikation von Nutzerinnen und Nutzern eine zentrale Sicherheitsfunktion darstellt, ist das Recht auf Privatheit auch im Internet von hoher Bedeutung. Anwenderinnen und Anwendern muss es freigestellt bleiben, sich auch weiterhin anonym oder pseudonym im Internet (wie auch in der Realität) zu bewegen. Es sollte ihnen möglich sein, nach dem Prinzip der Datensparsamkeit der Situation entsprechende Identitätsausprägungen zu nutzen. Diese Ausprägungen reichen von Pseudonymen hin zu vertrauenswürdigen, hoheitlichen digitalen Identitätsnachweisen, abhängig vom jeweiligen konkreten Anwendungsfall. Insbesondere Technologien im Bereich der kryptografischen Zero-Knowledge-Verfahren erlauben es, die Privatsphäre der Nutzerinnen und Nutzer zu schützen. Dabei handelt es sich um Beweissysteme, die anzeigen, dass jemand über geheimes Wissen verfügt, ohne dafür dieses Wissen explizit preiszugeben. Die Möglichkeiten und Vorteile solcher Technologien sind in der Öffentlichkeit sowie bei Diensteanbietern noch relativ unbekannt, weshalb hier ein verstärkter Wissenstransfer und Technologieaustausch notwendig ist.

Keine künstliche Technologiebindung
Während die Notwendigkeit von dezentralisierten Technologien im Rahmen der Förderung einer informationellen Selbstbestimmung naheliegend ist, sollte daraus keine Technologiebindung abgeleitet und damit künstlich eine Einschränkung erzeugt werden. Es ist abzuwägen, ob beispielsweise die Blockchain-Technologie als eine Ausprägung der DLT im Rahmen von eID- bzw. SSI-Umsetzungen notwendig ist oder ob die Nachteile überwiegen[9]. So sind klassische „Proof of Work"-Konsensmechanismen von DLT energiewirtschaftlich und ökologisch nicht nachhaltig und Konsortialmodelle behindern eine unbeschränkte Teilnahme ebenso wie den Wettbewerb. Eine Neubewertung, wo und ob überhaupt DLT-Technologien im Rahmen der dezentralen Identitätsverwaltung einen Mehrwert bieten, ist dringend anzuraten. Eine künstliche Technologiebindung in Ausschreibungen und Standards ist zu vermeiden, da diese Innovationen behindert.

Stärkung der Sicherheitsmechanismen auf Smartphones
Moderne Smartphones enthalten eine wachsende Anzahl von hardwarebasierten Sicherheitsmechanismen. Der Hersteller Apple kann durch seine homogene Gerätelandschaft dabei ein uniformes Sicherheitsniveau bieten, eine Zertifizierung der Mechanismen besteht aber aktuell nur teilweise. Das Android-Ökosystem ist im Gegensatz dazu sehr heterogen. Dies führt zu unterschiedlichen Betriebssystemversionen und Funktionsumfängen, gerade im Hinblick auf die angebotenen Sicherheits- und Privatsphäremechanismen. Eine durchgehende, nachvollziehbare Zertifizierung fehlt. Um Smartphones als Trägermedien digitaler Identitäten auch für stark regulierte Kontexte zu etablieren, müssen weitere Maßnahmen zur Stärkung der Sicherheitsmechanismen solcher Endgeräte umgesetzt werden. So könnte die Etablierung einer Smartphone-Device-Security-Datenbank eID-Diensteanbietern ermöglichen, die Vertrauenswürdigkeit von einzelnen Smartphone-Modellen nachzuvollziehen und ihre Dienste daran zu orientieren. Eine solche Datenbank könnte zum Beispiel auf einer Einschätzung wie dem Android Device Security Rating[10] basieren. Über Standardisierung und Normierung sollten einheitliche, standardisierte, diskriminierungsfreie Schnittstellen für Identitätslösungen auf Smartphones geschaffen werden. Erste Schritte in diese Richtung wurden bereits beschritten; diese sind stringent fortzuführen und auch umzusetzen. So spezifiziert beispielsweise der Standard ISO/IEC DIS 18013-5[11] eine Schnittstelle zur Umsetzung von Führerscheinen auf mobilen Endgeräten. Weiterhin sollte auch die Zertifizierung der Hard- und Softwarekomponenten vorangetrieben werden.

Transparenz
Weite Teile der Zivilgesellschaft stehen großen Digitalisierungsprojekten sehr kritisch gegenüber. Gerade beim Aufbau eines eID-Ökosystems, an dem potenziell alle Bürgerinnen und Bürger sowie Dienstanbietende teilnehmen sollen, muss das Thema Transparenz von Anfang an berücksichtigt werden. Hierfür ist es nicht nur wichtig, dass Open-Souce-Software verwendet wird. Es müssen auch die Konzepte öffentlich zur Verfügung gestellt und frühzeitig mit der Zivilgesellschaft diskutiert werden, unter Einbindung von Sicherheitsexpertinnen und- experten.

Benutzbarkeit und Vertrauenswürdigkeit
Neben der einfachen Benutzbarkeit ist eine wesentliche Voraussetzung, dass digitale Identitäten auch genutzt werden, dass Bürgerinnen und Bürger in solche Lösungen vertrauen. Hier ist nicht nur wichtig, die Lösungen transparent zu gestalten oder entsprechende Zertifizierungen durchzuführen, sondern den Bürgerinnen und Bürgern auch über entsprechende Anwendungsmöglichkeiten bewusst zu machen, dass ihre digitalen Identitäten sicher und datenschutzfreundlich gestaltet sind. Digitale Identitäten müssen also einfach benutzbar sein, ohne allerdings die erforderlichen Sicherheitsmechanismen komplett zu verstecken, da Bürgerinnen und Bürger in diesem Fall kein Vertrauen in die Lösung entwickeln können.

4 Empfehlungen an die Politik

Das übergeordnete Ziel sollte sein, ein europaweites eID-Ökosystem aufzubauen, das die eID-Lösungen der einzelnen Initiativen integriert und die Themen Benutzbarkeit, Vertrauen, Sicherheit und Datenschutz gleichrangig berücksichtigt. Damit können eID-Lösungen in der Breite, grenzüberschreitend für Bürgerinnen und Bürger, Unternehmen und Diensteanbieter nutzbar und die Chancen digitaler Dienste für alle Bürgerinnen und Bürger zugänglich gemacht werden. Um dieses herausfordernde Ziel zu erreichen, empfiehlt die Wissenschaftliche Arbeitsgruppe des Nationalen Cyber-Sicherheitsrates:

- Die Entwicklung technischer und regulatorischer Rahmenvorgaben, damit Bürgerinnen und Bürger selbstbestimmt über die Ausstellung von digitalen Identitäten entscheiden und kontext- sowie situationsabhängig festlegen können, welche Identität genutzt werden soll. SSI-Lösungen müssen dazu stärker an Kundinnen und Kunden orientiert gestaltet werden.
- Das Einbeziehen der Zivilgesellschaft in den gesamten Entwicklungsprozess, insbesondere bereits während der Konzeptionsphase.

- Das aktive Vorantreiben einheitlicher Normen und Standards, die Harmonisierung der Anforderungen für verschiedene Sektoren sowie die Entwicklung standardisierter Protokolle, um die Integrierbarkeit unterschiedlicher Lösungen zu gewährleisten.
- Das Vorantreiben von Initiativen zur Stärkung der Sicherheitsmechanismen auf Smartphones und die weitere Forcierung der Zertifizierung der Hard- und Softwarekomponenten.
- Ein verstärkter Fokus auf die Einführung einer Vielzahl von mehrwertigen eID-basierten Dienstleistungen, insbesondere im Bereich der öffentlichen Verwaltung, um der eID-Technologie über das Ökosystem den Weg in den Massenmarkt zu ebnen. Hierbei sollte man sich an den Prinzipien der agilen Entwicklung orientieren. Empfohlen wird also, schnell tragfähige Lösungen bis zur Einsatzreife zu entwickeln, die die Mehrwerte eines solchen eID-Ökosystems für die breite Öffentlichkeit verdeutlichen. Die Lösungen sollen sich auf Kernfunktionen konzentrieren, die einfach nutzbar sind, hohe Sicherheitsanforderungen erfüllen und nach Transparenzprinzipien entwickelt wurden.
- Das frühzeitige Klären der Frage nach geeigneten Betreibermodellen.

Mögliche Kriterien zur Nachverfolgung / Beurteilung des Umsetzungserfolgs der Empfehlungen:

- Messen der Anzahl der Vorfälle im Kontext von Identitätsdiebstählen: Zeigen die Maßnahmen die Wirkung zur Erhöhung der Cybersicherheit?
- Kenngrößen, die den Erfolg der Akzeptanz und Verbreitung des Angebots fokussieren:
  - Messung der Anzahl der eID-Lösungen im Ökosystem (national, europaweit)
  - Messung der Anzahl der angeschlossenen Dienstangebote (national, europaweit und international)
  - Messung der Zahlen zur Nutzung (national, europaweit)

1 Vgl. Daniel Träder, Alexander Zeier und Andreas Heinemann. „Design-und Implementierungsaspekte mobiler abgeleiteter Identitäten.“ DACH Security (2017).
2 Eckpunktepapier für Self-Sovereign Identities (SSI), BSI, 2021.
3 Blockchain sicher gestalten, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Studie-374.pdf.
4 www.personalausweisportal.de/Webs/PA/DE/wirtschaft/projekt_digitale_identitaeten/projekt_digital.
5 www.digitaletechnologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html.
6 2030 Digital Compass: the European way for the Digital Decade, European Commission, https://ec.europa.eu/info/sites/info/files/communication-digital-compass-2030_en.pdf.
7 European Digital Identity Architecture and Reference Framework – Outline – , eIDAS.
8 u. a. re:claimID Fraunhofer AISEC, www.aisec.fraunhofer.de/de/fields-of-expertise/projekte/reclaim.html Expert Group, 02.2022.
9 vgl. BSI-Eckpunktepapier für Self-Sovereign Identities (SSI), BSI, 2021.
10 Vgl. Institute of Networks and Security, JKU Linz, www.android-device-security.org.
11 Personal identification – ISO-compliant driving licence – Part 5: Mobile driving licence (mDL) application.

Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat

Seit Oktober 2018 unterstützt die Wissenschaftliche Arbeitsgruppe den Nationalen Cyber-Sicherheitsrat. Sie berät aus Perspektive der Forschung zu Entwicklungen und Herausforderungen im Hinblick auf eine sichere, vertrauenswürdige und nachhaltige Digitalisierung.

Mitglieder der Wissenschaftlichen Arbeitsgruppe sind: Thomas Caspers, Prof. Dr. Gabi Dreo Rodosek, Prof. Dr. Claudia Eckert (Hauptautorin dieses Impulspapiers), Prof. Dr. Jörn Müller-Quade, Prof. Dr.-Ing. Christof Paar, Prof. Dr. Alexander Roßnagel, Prof. Dr. Michael Waidner