bankenverband

Positionspapier

des Bankenverbandes „Digitale staatliche Identität zukunftsfähig gestalten“

19. Oktober 2023

Lobbyregister-Nr. R001458
EU-Transparenzregister-Nr. 0764199368-97

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

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

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

USt.-IdNr. DE201591882

Einleitung

Digitale Identitätsnachweise versprechen einen enormen Nutzen für Verbraucher und Unternehmen. Mit ihrer Hilfe können sich die Bürgerinnen und Bürger verlässlich und sicher digital ausweisen oder den Nachweis über bestimmte persönliche Informationen erbringen. Dies ist nicht nur eine wichtige und dringend notwendige Voraussetzung für die digitale Transformation von Wirtschaft und Gesellschaft, sondern kann auch den Alltag der Verbraucher deutlich erleichtern. Nicht zuletzt sind digitale Identitäten ein wichtiger Baustein für die digitale Souveränität Europas.

Die ab 2010 auf deutschen Ausweisdokumenten eingeführte Online-Ausweisfunktion ermöglicht es allen Bundesbürgern und anderen in Deutschland rechtmäßig lebenden Personen, sich sicher im digitalen Raum auszuweisen – zumindest in der Theorie. Die Realität aber sieht anders aus: Nach wie vor bleibt die Online-Ausweisfunktion weit hinter ihren Möglichkeiten zurück, obwohl inzwischen fast jede in Deutschland aufenthaltsberechtigte Person über einen Online-Ausweis verfügt. Es ist höchste Zeit, dieses Potenzial zu nutzen und die Online-Ausweisfunktion für öffentliche wie für privatwirtschaftliche Zwecke einzusetzen. Die privaten Banken möchten ihren Beitrag zum Erfolg der Online-Ausweisfunktion leisten.

Doch ein digitaler Identitätsnachweis wie die Online-Ausweisfunktion muss heute auch über die Grenzen Deutschlands hinaus genutzt werden können. Daher unterstützen wir mit Nachdruck die Bestrebungen der deutschen und europäischen Politik, ein europäisches Ökosystem für digitale Identitäten zu schaffen, das den Bedarf der Bürger und Unternehmen nach einfachen, sicheren, effizienten und breit akzeptierten Identitätslösungen deckt und die nationale Fragmentierung in Europa überwindet. Ein einheitlicher europäischer Rechtsrahmen würde die EU-weite Nutzbarkeit gewährleisten sowie ein Level-Playing-Field im EU-Binnenmarkt schaffen.

Die Vision einer universell nutzbaren digitalen Identität ist in Teilen heute schon Realität. Dies gilt insbesondere für Länder, die von Beginn an auf die Zusammenarbeit zwischen Staat, Wirtschaft und Zivilgesellschaft gesetzt haben. Warum sich digitale Identitäten mit unterschiedlichem Erfolg in den einzelnen nationalen Märkten wie z.B. in Belgien oder in Schweden durchgesetzt haben, geht auf das Zusammenspiel verschiedener Erfolgsfaktoren zurück (siehe Abbildung). Nun müssen hieraus die richtigen Schlüsse gezogen werden – gerade auch in Deutschland.

Faktoren für eine erfolgreiche Etablierung digitaler ID-Systeme[1]

Aktuell arbeitet die Bundesregierung ressortübergreifend an der Weiterentwicklung des staatlichen digitalen Ausweises (u.a. im Rahmen des sogenannten GovLab-Projekts „Digitale Identitäten"). Ziel dessen ist es, „eine breite Marktakzeptanz und sichere, datenschutz-konforme Nutzung der staatlichen Ident-Lösung bei Nutzern und Service-Anbietern im Kontext von Verwaltung und Wirtschaft" zu schaffen, „die EU-Länder-übergreifend nutzbar und mit anderen europäischen Lösungen kompatibel ist". Wir möchten mit diesem Positionspapier die Bundesregierung dabei unterstützen, die richtigen Weichenstellungen für den staatlichen Online-Ausweis sowie die geplante europäische digitale Identitätswallet (EUDI-Wallet) vorzunehmen. Die aus unserer Sicht zentralen Erfolgsfaktoren haben wir im Folgenden näher beschrieben und in konkrete Vorschläge an die Politik überführt. Denn für unsere Mitglieder – Banken wie FinTechs – ist die Identifizierung und Authentifizierung ihrer Kunden wichtiger Bestandteil ihres täglichen Geschäfts und Grundlage ihres wirtschaftlichen Erfolgs.

1. Breite (sektorübergreifende) Akzeptanz über gemeinsames Zielbild sicherstellen

Es ist offenkundig, dass eine digitale Identitätslösung nur dann erfolgreich sein kann, wenn sie die Bedürfnisse des Nutzers erfüllt und vom Markt akzeptiert wird. Das gilt gleichermaßen für staatliche wie für privatwirtschaftliche Angebote. Die Bedürfnisse der Verbraucher und Unternehmen müssen daher sorgsam analysiert und bei der Ausgestaltung der Identitätslösung berücksichtigt werden. Hierbei spielen harte Kriterien wie Breite der Einsatzmöglichkeiten, Sicherheit und Kosten, aber auch weiche Faktoren wie Einfachheit in der Bedienung, Nutzervertrauen und Serviceverfügbarkeit eine wichtige Rolle. Nur wenn alle Faktoren in einem

[1] Neun Länder betrachtet: Belgien, Dänemark, Deutschland, Estland, Frankreich, Italien, Kanada, Norwegen, Spanien

richtigen Verhältnis zueinander stehen, kann sich eine breite Marktakzeptanz bei Kunden und Anwendern einstellen.

Bei Entwicklung und Ausgestaltung des deutschen Online-Ausweises standen bisher Anwendungsfälle der öffentlichen Verwaltung im Vordergrund – mit der Konsequenz, dass Anforderungen der Privatwirtschaft vernachlässigt wurden. Dies sollte im Zuge einer Neuausrichtung behoben werden. Denn Fakt ist: Reichweite kann nur durch die Wirtschaft generiert werden. Das setzt einen transparenten und ergebnisoffenen Prozess der Weiterentwicklung voraus, an dem die Nutzer und Anwender der Privatwirtschaft angemessen beteiligt werden. Die bisherigen sporadischen Ansätze zur Einbindung der Stakeholder im Rahmen des laufenden GovLab-Projektes „Digitale Identitäten" der Bundesregierung reichen hierfür nicht aus. Insofern begrüßen wir den jüngst aufgesetzten Konsultationsprozess zur deutschen Umsetzung des eIDAS-Gesamtsystems als Schritt in die richtige Richtung.

Wenn es das Ziel ist, ein Identitäts-Ökosystem für alle Teile der Wirtschaft und Gesellschaft zu schaffen, bedarf es darüber hinaus einer fest institutionalisierten Zusammenarbeit z.B. in Form eines gemeinsamen Steuerungs- und Beratungsgremiums, in dem die öffentliche Hand, die betroffenen Wirtschaftsbereiche, Anbieter bereits bestehender Identifizierungsdienstleistungen und die Zivilgesellschaft gleichberechtigt vertreten sind und gemeinsam über die Leitplanken entscheiden. Nur so kann erfolgreich sichergestellt werden, dass die unterschiedlichen Anforderungen und Präferenzen einzelner Beteiligter im Idealfall nebeneinander berücksichtigt und so austariert werden, dass ein gesamtwirtschaftliches Optimum erreicht wird und eine schnelle Marktverbreitung und Akzeptanz innerhalb der Gesellschaft erfolgt. Ein Zielbild, bei dem staatliche Interessen dominieren und die Bedürfnisse des Marktes an zweiter Stelle kommen, ist von Vornherein zum Scheitern verurteilt. Denn die Akzeptanz der Nutzer steht und fällt mit den Vorteilen, die sie beim alltäglichen Einsatz z.B. im Kontext des Online Bankings verspüren.

2. Ausgewogene Balance zwischen staatlichem Sicherheitsanspruch und gewünschter Nutzerakzeptanz herstellen

Die marktgängige Ausgestaltung des staatlichen Online-Ausweises erfordert einen risikobasierten Ansatz, der die für den konkreten Fall notwendigen Sicherheitsanforderungen mit möglichst einfacher Nutzbarkeit für die Verbraucher verbindet. Es ist unbenommen, dass eine staatliche digitale Identität hohen Sicherheitsanforderungen gerecht werden muss, um für hoheitliche Zwecke oder die Beantragung staatlicher Nachweise wie z.B. einer Geburtsurkunde oder eines Führungszeugnisses eingesetzt werden zu können. Gleichzeitig reicht für die Mehrzahl der Use Cases einer digitalen Identität aber das Vertrauensniveau „substanziell" aus. Dies gilt in gleicher Weise für Anwendungsfälle im öffentlichen wie im privaten Sektor.

Die Online-Ausweisfunktion ist derzeit das einzige Verfahren in Deutschland, das auf dem Vertrauensniveau „hoch" nach der eIDAS-Verordnung notifiziert ist. Ihr Einsatz setzt den Besitz

der physischen Ausweiskarte sowie der persönlichen Ausweis-PIN voraus. Das Auslesen des Online-Ausweises erfolgt kontaktlos über ein NFC-fähiges Lesegerät, in aller Regel ein Smartphone oder Tablet. Der Nutzer benötigt also aktuell stets zwei Devices, Ausweiskarte und z.B. Mobiltelefon, plus seine PIN, um den Online-Ausweis einsetzen zu können. Für die initiale Identitätsbestätigung gegenüber einem Serviceanbieter, z.B. einer Bank im Rahmen einer Kontoeröffnung, bietet das Verfahren eine vergleichsweise hohe Nutzerconvenience und aus Kundensicht zum Teil Vorteile in puncto Schnelligkeit und Datenschutz gegenüber den heute in Deutschland verbreiteten Alternativen. Dennoch gilt es, dem Kunden ein höheres Maß an Convenience über das Smartphone zu offerieren, indem die Ausweiskarte nach erstmaliger Aktivierung gänzlich wegfällt und ein Re-Use ermöglicht wird.

Anders verhält es sich jedoch für den Fall, dass die Online-Ausweisfunktion auch für die Kundenauthentifizierung verwendet werden soll, z.B. beim regelmäßigen Login zum Online Banking. Hier fällt der Einsatz des Online-Ausweises im Hinblick auf eine möglichst einfache und bequeme Bedienung deutlich hinter alternative Authentifizierungsverfahren zurück, die ein angemessenes Sicherheitsniveau unter Verwendung nur eines Authentifizierungs-Devices erreichen. Dies schließt auch eine starke Kundenauthentifizierung mit ein, wie sie von Banken im Kontext des Online-Banking-Zugangs oder der Zahlungsfreigabe gefordert ist. Hierfür haben sich Verfahren unter Beachtung bankaufsichtlicher Vorgaben etabliert, die sicher und komfortabel auf allen gängigen Smartphones ohne zusätzliche Hardware funktionieren und im Regelfall eine Nutzerauthentifizierung per Fingerabdruck- oder Gesichtserkennung unterstützen.

Der Bankenverband begrüßt daher das Vorhaben der Bundesregierung, mit der Smart-eID die Online-Ausweisfunktion auf das Smartphone zu übertragen. Dieser ursprünglich für Ende 2020 angekündigte Schritt soll nun im zweiten Halbjahr 2023 vollzogen werden. Die Smart-eID verspricht eine bessere Kunden-Convenience, indem nach einmaliger Übertragung auf das mobile Endgerät die Online-Ausweisfunktion dauerhaft (z.B. für maximal fünf Jahre) als vollwertiges Substitut zum Ausweis verwendet werden kann. Damit würde die Nutzung der physischen Ausweiskarte durch das Auslesen über die NFC-Schnittstelle des Smartphones entfallen. Allerdings werden hierfür technische Anforderungen an die Hardware des mobilen Devices (Secure Element) gestellt, die bisher und auch absehbar nur von einem Teil der im Markt verfügbaren Endgeräte (zumeist im Hochpreissegment) erfüllt werden kann. Mit der voraussichtlichen Öffnung des Secure-Elements von iOS-Geräten über den ab Mitte 2024 wirksamen Digital Markets Act dürfte zwar eine elementare Hürde genommen werden, um die Smart-eID weiter zu skalieren. Allerdings liegt der Anteil von iOS-Smartphones gegenwärtig nur bei ca. 30 %[2]. Bei der Vielzahl an Herstellern und Modellen wird also nicht jedes Smartphone über ein (freigeschaltetes) Secure-Element verfügen. Da es noch Jahre dauern dürfte, bis die Endgeräte der Nutzer flächendeckend über die erforderliche zertifizierte Hardware verfügen, dürfte folglich nur ein Teil der Nutzer auf mittlere Sicht von der Smart-eID profitieren. Damit geht wertvolle

[2] https://de.statista.com/statistik/daten/studie/256790/umfrage/marktanteile-von-android-und-ios-am-smartphone-absatz-in-deutschland/

Zeit im Wettbewerb mit den BigTechs verloren, die mit ihren Identitäts-Lösungen sukzessive in Richtung verifizierter digitaler Identitäten drängen.

Um der gesamten Bevölkerung kurzfristig eine zeitgemäße Usability beim Einsatz des Online-Ausweises zu bieten, wäre auch im Sinne der Barrierefreiheit eine Software-basierte Smart-eID geboten, die schon heute von allen gängigen Endgeräten unterstützt werden kann. Dass auf diese Weise voraussichtlich nur das Vertrauensniveau „substanziell" anstatt „hoch" erreicht werden kann, stünde dem nicht entgegen. Denn, wie zuvor erwähnt, reicht für die weit überwiegende Zahl der Use Cases ein substanzielles Sicherheitsniveau vollkommen aus. Gerade bei Banken, die rechtlich zur Überprüfung der Identität ihrer Kunden verpflichtet sind, werden daneben weitere Prüfungen im Rahmen des Know-Your-Customer(KYC)-Prozesses vorgenommen, die eine Identifizierung auf dem Vertrauensniveau substanziell zulassen. Daher wäre einem differenzierten Ansatz der Smart-eID Priorität einzuräumen, der je nach Anwendungsfall unterschiedliche Vertrauensniveaus unterstützt und nicht zwingend das Vertrauensniveau „hoch" erfordert. Dieser Weg wird auch von anderen europäischen Ländern (z.B. Italien, Niederlande) eingeschlagen, die ID-Lösungen auf unterschiedlichen Vertrauensniveaus unterstützen.

3. Fehlende Bekanntheit bei Nutzern überwinden und breite Anwendungsmöglichkeiten schaffen

Das Potenzial des Online-Ausweises wird bei weitem nicht ausgeschöpft, insbesondere auch deshalb nicht, weil bislang weder der öffentliche Sektor noch die Privatwirtschaft hinreichende Anwendungsfälle mit Zugkraft für die Nutzer etabliert haben. Auch Banken haben sich in der Vergangenheit mit dem Online-Ausweis schwergetan, unter anderem mangels Verbreitung und Nachfrage auf Nutzerseite. Letzten Endes ist ein erfolgreicher digitaler Identitätsnachweis maßgeblich von der Alltagsrelevanz für den Nutzer abhängig.

Für die nötige Sichtbarkeit und Wahrnehmung des Online-Ausweises in der Bevölkerung und bei den Unternehmen bedarf es einer bundesweiten, öffentlichkeitswirksamen Marketingkampagne, die seine Existenz nicht nur ins Bewusstsein rückt, sondern anhand konkreter Anwendungsbeispiele auch seine Vorteile im Alltag verdeutlicht. Über ein neues Branding ließe sich zudem das Image der Online-Ausweisfunktion verbessern. Eine höhere Wirksamkeit würde eine staatliche Kampagne dann entfalten, wenn sie durch entsprechende Maßnahmen seitens der Wirtschaft flankiert und im Vorfeld gemeinsam vorbereitet wird. Die Mitglieder des Bankenverbandes sind offen für den Dialog.

Öffentlichkeitsmaßnahmen werden aber nur dann die gewünschte Wirkung erzielen, wenn auch gewährleistet ist, dass hinreichend viele und vom Bürger tatsächlich nachgefragte Use Cases vorhanden sind. Dies setzt eine gemeinsame Planung und einen ausreichenden Vorlauf voraus, damit möglichst rasch ein großes Spektrum an interessanten Anwendungsmöglichkeiten auf öffentlicher und privater Seite geschaffen wird. Wenn digitale Identifizierungsverfahren die

Anforderungen der Privatwirtschaft bzw. der Unternehmen erfüllen und zu Ersparnissen durch schlankere Prozessstrukturen beitragen, sind Unternehmen auch gewillt, ihre Kunden aktiv für die neuen Legitimationsprozesse zu sensibilisieren. Dies könnte die Anwendungsquote in der Bevölkerung massiv steigern. Dafür müssen die Unternehmen zu der Überzeugung gelangen, dass es sich lohnt, den Online-Ausweis in ihre Prozesse zu integrieren.

Diese Maßnahmen zusammen genommen sind erfolgskritisch, reichen jedoch für eine zukunftsfähige Lösung nicht aus. Ein heute zeitgemäßes Angebot muss mehr bieten als die reine Übertragung der physischen Ausweiskarte auf das Smartphone. Vielmehr bedarf es zusätzlicher Funktionalitäten in Form eines Wallet-Ansatzes, wie ihn die EU im Rahmen der eIDAS-Überarbeitung verfolgt.

4. Innovationen durch klares Rollenmodell von Staat und Wirtschaft fördern und damit Investitionssicherheit schaffen

Damit sich ein Ökosystem für digitale Identitäten entwickeln kann, das sich durch Innovationen und Angebote entlang der Marktbedürfnisse auszeichnet, bedarf es eines Rahmens, der Anreize an die Marktteilnehmer setzt und einen fairen Wettbewerb zulässt. Aufgabe des Staates sollte es sein, diesen Rahmen im Miteinander mit den wirtschaftlichen Akteuren zu gestalten. Dabei muss Klarheit darüber herrschen, welche Rollen der Staat übernimmt und welche Leistungen dem Markt überlassen bleiben. Denn es braucht Planungs- und Investitionssicherheit für Anbieter und Nachfrager von ID-Lösungen, damit sie sich engagieren und das bestehende Henne-Ei-Dilemma gelöst werden kann.

Um es konkret zu machen: Mit der Online-Ausweisfunktion steht den Bürgerinnen und Bürgern eine hoheitliche digitale Identität zur Verfügung, es fehlt aber nach wie vor an Einsatzmöglichkeiten in der digitalen Verwaltung und im privaten Sektor. Letzteres könnte überwunden werden, indem die Attraktivität der eID für private Service-Anbieter, u.a. Banken, Versicherungen und Mobilfunkanbieter, erhöht wird, im Idealfall durch eine kostengünstige und leichte Anbindung an die staatliche eID-Infrastruktur. Dieser Effekt könnte dadurch noch verstärkt werden, dass sich die eID ohne die zwingende Einbindung weiterer Dienstleister auf Seiten der Verifizierer in den Identifizierungsvorgang integrieren lässt. Gerade die für Banken komplexen und kostenintensiven Outsourcing-Prozesse würden dadurch vereinfacht. Weiterhin wäre von staatlicher Seite zu erwägen, die Kosten für die Anbindung an den staatlichen ID-Server und die Beantragung von Berechtigungszertifikaten durch eine Umsatzsteuerbefreiung zu reduzieren oder diese übergangsweise sogar gänzlich zu übernehmen, quasi als staatliche Investition in die digitale Transformation.

Gleichzeitig gilt es, Wettbewerb und Innovation an anderer Stelle zu ermöglichen. So sollten Bürgerinnen und Bürger wählen können, über welchen Anbieter bzw. welche App sie ihre digitale Identität verwalten. Ein Wettbewerb unter privaten Anbietern von entsprechenden Identitäts-

Wallets, die – gemäß dem aktuellen Vorschlag für eine europäische digitale Identität – die staatliche eID als Kernbestandteil enthalten und darüber hinaus eine Vielzahl privater und staatlicher Nachweise aufnehmen können, wäre ein Schlüssel für Innovation und Angebotsvielfalt.

Die Kernaufgabe des Staates liegt in der Ausgabe hoheitlicher Identitäten, die Bereitstellung und Ausgestaltung der Wallet-Infrastruktur sollte hingegen der Kreativität und den Erkenntnissen des Marktes überlassen werden. Hierfür bedarf es selbstverständlich staatlich vorgegebener Mindestanforderungen und Rahmenbedingungen, die Vertrauen schaffen und die Risiken eines Identitätsmissbrauchs minimieren. Umgekehrt müssen Anbietern von Identitäts-Wallets aber auch Möglichkeiten eröffnet werden, ein nachhaltiges Geschäftsmodell zu realisieren, z.B. durch entgeltfähige Zusatzleistungen wie die Ausstellung qualifizierter Signaturzertifikate oder verifizierte Zusatzdaten. Auch sollte die Integrationsmöglichkeit in Drittanbieter-Apps gewährleistet sein.

Banking-Apps, die auf Millionen von Endgeräten in Deutschland installiert sind, könnten hier als Multiplikator dienen. Durch die Möglichkeit der EUDI-Wallet-Integration in eine bestehende Banking-App (via SDK) ließen sich Skaleneffekte nutzen und die Verbreitung der EUDI-Wallet beschleunigen.

Eine breite Verpflichtung privater Verifizierer zur Akzeptanz der staatlichen eID bzw. darauf basierender Wallets, wie aktuell im Rahmen der eIDAS2.0-Novelle vorgesehen, ist allein kein Garant dafür, dass die Lösung auch von den Kunden angenommen wird. Nur wenn bei der Umsetzung und Weiterentwicklung die Bedürfnisse aller Beteiligten, also Verbraucher, Wirtschaft und Zivilgesellschaft, berücksichtigt werden, sind die Voraussetzungen für eine allgemeine Akzeptanz gegeben. Daher ist es wichtig, Verbraucher durch Kundenbefragungen sowie die Wirtschaft als Partner bei der konzeptionellen und technischen Ausgestaltung im Rahmen einer Private Public Partnership frühzeitig mit einzubinden.

5. Staatliche Identitätsdaten weiter harmonisieren und einheitlichen Interoperabilitäts- und Wettbewerbsrahmen für europäische Wallet-Lösungen herstellen

Der Erfolg einer staatlichen eID steht und fällt mit ihrer Einbettung in ein Ökosystem digitaler Identitäten, in dem Nutzer verschiedenste digitale Nachweise von öffentlichen und auch privaten Herausgebern, wie z.B. ihren digitalen Führerschein, ihre Ausbildungsnachweise oder auch ihr Bankkonto, gegenüber Dritten universell und digital rechtssicher bescheinigen können. Auf diese Weise ließe sich die gegenwärtige Funktionalität der Online-Ausweisfunktion deutlich erweitern, und es könnten zusätzliche Mehrwerte für die Nutzer und Anwender, also für Verbraucher und Unternehmen, geschaffen werden. In diesem Zuge wäre es auch möglich, die derzeitige Fragmentierung der Identitätslösungen in der EU zu überwinden.

Insofern unterstützen wir den vom europäischen Gesetzgeber verfolgten Ansatz einer europäischen digitalen Identität, in der die nationalen staatlichen Identitätssysteme die Grundlage und den Sicherheitsanker für die jeweiligen Identitäts-Wallets bilden. Mit Blick auf eine grenzüberschreitende Nutzbarkeit von europäischen ID-Wallets und Identitätssystemen, die nach dem Gesetzesentwurf weiterhin in der Verantwortung der einzelnen EU-Mitgliedstaaten liegen sollen, sind aus Sicht der privaten Banken folgende Mindestanforderungen hinsichtlich Standardisierung und Interoperabilität zu stellen:

a. Die hoheitlich bereitgestellten Personenidentitätsdaten (PID) sollten für alle 27 Mitgliedstaaten normiert sein und den gleichen Datensatz an Identitätsattributen umfassen

Aus historischen Gründen unterscheiden sich heute die Datenfelder, die auf den einzelnen nationalen (elektronischen) Identifizierungsmitteln enthalten sind. Daher ist bisher nur ein Mindestsatz von Personenidentifizierungsdaten, die eine natürliche oder juristische Person eindeutig repräsentieren, in einem grenzüberschreitenden Umfeld vorgeschrieben[3]. Mit Blick auf eine EU-weit einheitliche Datengrundlage und die Reduzierung der Komplexität für Verifizierer wie z.B. Banken, die auch im grenzüberschreitenden Kontext zur Identitätsprüfung verpflichtet sind, sollte eine europäische Harmonisierung der Datenfelder erfolgen.

Dabei sollte die Wallet alle Kernidentitätsdaten zur Verfügung stellen, die für eine verlässliche Identitätsprüfung, z.B. im Rahmen einer Kontoeröffnung, erforderlich sind. So wäre es wünschenswert, analog der physischen Ausweiskarte auch das Lichtbild einem Verifizierer digital zugänglich zu machen, was im Falle der deutschen Online-Ausweisfunktion bisher Behörden vorbehalten war und kürzlich auch für Notare geöffnet wurde. Durch dieses zusätzliche Sicherheitsfeature könnte die korrekte Identität des Nutzers in Zweifelsfällen per biometrischem Abgleich überprüft werden, was keine Speicherung des biometrischen Lichtbilds durch den Verifizierer erfordert. Etwaigen Datenschutzbedenken könnte dadurch Rechnung getragen werden, dass diese Option auf Anwendungsfälle beschränkt wird, in denen eine Identifizierung gesetzlich vorgeschrieben ist und in denen heute eine Ausweiskopie angefertigt werden darf.

b. Die technische Akzeptanz aller europäischen ID-Wallets durch die vertrauenden Parteien muss über einen Schnittstellenstandard erfolgen können

Aufwand und Kosten der Prozesseinbindung müssen für die Wirtschaft attraktiv sein und im Verhältnis zu der zu erwartenden Kundeninanspruchnahme stehen. Dies gilt umso mehr im Falle einer verpflichtenden Akzeptanz der EUDI-Wallet, wie es im Verordnungsentwurf für Anwendungsfälle der starken Kundenauthentifizierung aktuell vorgesehen ist. Daher muss

[3] DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1501 vom 8. September 2015 über den Interoperabilitätsrahmen gemäß Artikel 12 Absatz 8 der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-Verordnung)

zwingend gewährleistet sein, dass Anbieter über eine EU-weit einheitliche Schnittstelle alle nationalen EUDI-Wallets akzeptieren können. Ein Nebeneinander unterschiedlicher nationaler Standards, die ein Verifizierer sämtlich unterstützen müsste, um Verbraucher und Unternehmen aus allen 27 EU-Staaten zu erreichen, würde das Ziel eines echten europäischen Ansatzes konterkarieren und der Wirtschaft unvertretbar hohe Kosten aufbürden. Denn selbst im Falle einer EU-weiten Standardisierung der Wallet-Schnittstelle werden bestehende Identifizierungs- und Authentifizierungsverfahren, z.B. im Banking, auf absehbare Zeit nicht vollständig ersetzt werden können, was einen dauerhaften Parallelbetrieb verschiedener Infrastrukturen erfordert. Dies hängt auf der einen Seite an der zu gewährleistenden hohen Service-Verfügbarkeit von Bankanwendungen, auf die Banken im Falle einer Akzeptanzpflicht mangels Vertragsbeziehung zum Wallet-Provider keinen Einfluss nehmen können. Auf der anderen Seite müssen Banken ihre digitalen Dienstleistungen auch allen Nutzern anbieten können, die aus unterschiedlichsten Gründen keine EUDI-Wallet nutzen können oder wollen.

Dementsprechend sollte der aktuell in Arbeit befindliche Rahmen einer gemeinsamen technischen Architektur (Architectual Reference Framework – ARF) eine einheitliche Schnittstelle verbindlich vorgeben und den Mitgliedstaaten keinen individuellen Gestaltungsspielraum lassen. Mit Blick auf eine einfache Anschlussfähigkeit an bereits genutzte Identifizierungs- und Authentifizierungsinfrastrukturen sowie auf mögliche Einsatzszenarien außerhalb der EU wäre es ratsam, auf geeigneten internationalen Standards aufzusetzen. Etwaige proprietäre nationale Identitätsstandards sollten sich nahtlos in europäische oder internationale Lösungen integrieren lassen.

c. Die Ausgabe der EUDI-Wallet sollte einem einheitlichen Interoperabilitätsrahmen folgen und innerhalb der EU skalierbar sein

Für den Erfolg der europäischen digitalen Identität ganz wesentlich wird auch die Möglichkeit sein, diese auf sich verändernde Nutzerbedürfnisse und neue Einsatzszenarien fortlaufend anzupassen. Hierbei spielen Wettbewerb und Angebotsvielfalt eine entscheidende Rolle, denn sie sind maßgebliche Innovationstreiber und tragen dadurch wesentlich dazu bei, die Akzeptanz der Nutzer sicherzustellen. Daher sollten die Bereitstellung und Ausgestaltung von EUDI-Wallets weitestmöglich marktgetrieben erfolgen. Lediglich die Rahmenbedingungen, die für das Zusammenspiel des gesamten Ökosystems zwingend erforderlich sind, sollten durch den Staat festgelegt werden.

Hierzu gehört ein einheitliches technisches Rahmenkonzept, wie es mit dem Architectual Reference Framework angestrebt wird. Dieses muss die Interoperabilität zwischen den nationalen ID-Systemen als Kern der jeweiligen Wallets sicherstellen, woran es heute mangelt. Eine länderübergreifende Öffnung der Wallet-Bereitstellung für private Anbieter auf Basis eines einheitlichen Referenzrahmens würde es den Anbietern erlauben, ihre Wallet-Lösungen über nationale Grenzen hinweg zu skalieren. Nur so kann ein echtes pan-europäisches Identitäts-

Ökosystem in einem integrierten Binnenmarkt entstehen, das EU-weit gleiche Möglichkeiten für Anbieter und Nutzer gewährleistet.

Dabei gilt es, auch digitale Identitäten für Organisationen bzw. Unternehmen rechtzeitig mit in den Blick zu nehmen. So könnte die Rechtssicherheit im digitalen Geschäftsverkehr zwischen Unternehmen schlagartig erhöht werden, was enormes Potenzial für eine rasche Verbreitung der EUDI-Wallet verspricht. Obwohl die eIDAS2.0-Novelle die Bereitstellung von digitalen Identitäts-Wallets nicht nur für Bürgerinnen und Bürger, sondern auch für Unternehmen verbindlich vorsieht, wird dieses Thema auf deutscher wie auf europäischer Ebene bislang als nachrangig gesehen. Die zugegeben höhere Komplexität darf nicht als Vorwand benutzt werden, denn es ist ein Game-Changer für den dringend zu verbessernden Digitalisierungsgrad in Wirtschaft und Verwaltung und entscheidender Faktor im internationalen Standortwettbewerb.

Kernvorschläge im Überblick:

1. Für eine bedarfsgerechte Weiterentwicklung der staatlichen digitalen Identität bedarf es einer **Private Public Partnership**, in der öffentliche Hand, betroffene Wirtschaftsbereiche, Anbieter von Identifizierungsdienstleistungen und Zivilgesellschaft gleichberechtigt über die Leitplanken entscheiden. Hierzu sollte ein gemeinsames Steuerungs- und Beratungsgremium institutionell eingerichtet und paritätisch besetzt werden.

2. Die marktgängige Ausgestaltung des staatlichen Online-Identifikationsverfahrens erfordert einen **risikobasierten Ansatz**, der die notwendigen Sicherheitsanforderungen des jeweiligen Anwendungsfalls mit möglichst einfacher Nutzbarkeit für die Verbraucher verbindet. Für eine möglichst niederschwellige Nutzung sollten die Smart-eID und die EUDI-Wallet einen differenzierten Ansatz zur Unterstützung unterschiedlicher Vertrauensniveaus verfolgen. Hierzu sollte der Online-Ausweis – in Form der Smart-eID oder auch der künftigen EUDI-Wallet – zusätzlich zu dem Vertrauensniveau „hoch" auch das Niveau „substanziell" mit niedrigerer Nutzerschwelle unterstützen, um so eine bestmögliche Kunden-Usability zu erlauben und geringere Anforderungen an die Kundenhardware zu stellen.

3. Für die nötige Sichtbarkeit und Wahrnehmung des Online-Ausweises bei Bevölkerung und Unternehmen ist eine **bundesweite, öffentlichkeitswirksame Marketingkampagne** notwendig, um Bewusstsein für die Vorteile zu schaffen und konkrete Anwendungsbeispiele im Alltag aufzuzeigen. Eine erfolgreiche Kampagne setzt allerdings hinreichende praktische Einsatzmöglichkeiten voraus und muss durch Maßnahmen seitens der Wirtschaft flankiert und gemeinsam mit ihr vorbereitet werden.

4. Ein zeitgemäßes Angebot einer digitalen Identität sollte über die reine Übertragung der physischen Ausweiskarte auf das Smartphone hinausgehen. Hierfür bedarf es zusätzlicher Funktionalitäten sowie einer Öffnung für private Herausgeber von Identitätsmerkmalen, wie es der **Ansatz einer Europäischen Digitalen Identitäts-Wallet (EUDI-Wallet)** vorsieht.

5. Die Attraktivität der Einbindung des Online-Ausweises in die Kundenidentifikationsprozesse bei Banken, Versicherungen und anderen Service-Anbietern ließe sich durch eine kostengünstige und unkomplizierte **Anbindung an die staatliche eID-Infrastruktur** erhöhen. Um Finanzinstituten aufwendige Outsourcingprozesse zu ersparen, sollte es Verifizierern freigestellt sein, staatliche Infrastrukturen direkt zu nutzen.

6. Die **Bereitstellung und Ausgestaltung von EUDI-Wallets** sollte marktgetrieben erfolgen, um Innovationen und Angebotsvielfalt zu fördern. Lediglich die Rahmenbedingungen sollten staatlichen Mindestanforderungen unterliegen. Anbietern von Identitäts-Wallets müssen dabei die Möglichkeit haben, entgeltfähige Dienstleistungen zu erbringen und somit ein nachhaltiges Geschäftsmodell zu realisieren. Über eine Integrationsmöglichkeit in Drittanbieter-Apps könnten z.B. Banken und FinTechs als Multiplikator zu einer schnellen Verbreitung der EUDI-Wallet beitragen.

7. Die **hoheitlich bereitgestellten Personenidentitätsdaten (PID**) sollten perspektivisch für alle 27 Mitgliedstaaten harmonisiert werden und den gleichen Datensatz an Identitätsattributen umfassen. Auf diese Weise ließen sich Komplexitäten für Verifizierer aufgrund einer uneinheitlichen Datengrundlage signifikant reduzieren.

8. Eine staatliche digitale Identität sollte alle **Kernidentitätsdaten** zur Verfügung stellen, die für eine verlässliche Identifizierung erforderlich sind. Analog zum physischen Ausweis sollte der Ausweisinhaber das Lichtbild für bestimmte Zwecke auch privaten Verifizierern digital zugänglich machen können, damit diese die korrekte Identität des Nutzers in Zweifelsfällen validieren können, beispielsweise für die Überprüfung der Kundenidentität im Rahmen der geldwäscherechtlichen Verpflichtungen.

9. Die Akzeptanz aller europäischen ID-Wallets durch die vertrauenden Parteien muss über einen **EU-weit einheitlichen Schnittstellenstandard** erfolgen können. Dies ist ein Schlüssel zur Akzeptanzverbreitung und reduziert nicht zuletzt auch den notwendigen Implementierungs- und Pflegeaufwand für private vertrauende Parteien, die durch die EU-Verordnung zur Akzeptanz der EUDI-Wallet verpflichtet werden sollen.

10. **Digitale Identitäten für Unternehmen und Organisationen** müssen von der Politik stärker und zeitnah in den Fokus genommen werden. Mit diesen könnte die Rechtssicherheit im digitalen Geschäftsverkehr zwischen Unternehmen deutlich erhöht, eine rasche Verbreitung der EUDI-Wallet beschleunigt und letztlich die Wettbewerbsfähigkeit Europas durch konsequente Digitalisierung in Wirtschaft und Verwaltung effektiv gesteigert werden.