Konferenz Digitale Identitäten 2020

Martin Schallbruch, Tanja Strüve und Isabel Skierka
April 2020

Am 4. März 2020 war das Digital Society Institute der ESMT Gastgeber der **Konferenz Digitale Identitäten 2020**, die unter der Schirmherrschaft des Bundesministeriums des Innern, für Bau und Heimat sowie des Bundesministeriums für Wirtschaft und Energie als Teil des Verimi-Begleitforschungsprojekts an der ESMT ausgerichtet wurde. Ziel der Konferenz war es, gemeinsam mit Stakeholdern aus Politik, Wissenschaft und Wirtschaft der Frage nachzugehen, wie eine sektorübergreifende Strategie für digitale Identitäten aussehen kann. Im Plenum und in vier sektoralen Workshops – in den Bereichen Bildung, Gesundheit, Mobilität und öffentlicher Verwaltung – diskutierten die Teilnehmerinnen und Teilnehmer über Anforderungen an digitale Identitäten, innersektorale Strategien zur Flächendeckung innerhalb des Sektors sowie über eine Strategie für eine sektorübergreifende digitale Identität.

1. Digitale Identitäten -Status Quo

Rolle von Staat und Wirtschaft

Digitale Identitäten sind der Schlüssel zur digitalen Welt, sei es im Gesundheitswesen, in der Bildung, der öffentlichen Verwaltung oder der neuen Mobilität. Verlässliche digitale Identitäten sind zentraler Bestandteil jedes Digitalisierungsprojektes, sei es in der Industrie 4.0, der Mobilität der Zukunft oder der erfolgreichen Digitalisierung der öffentlichen Verwaltung. Mit Initiativen aus Politik und Wirtschaft sowie rechtlichen Regelungen wie der eIDAS-Verordnung werden interoperable und vertrauenswürdige Lösungen aus Europa angestrebt. Damit soll auch eine Marktbeherrschung durch digitale Identitätsdienste globaler Plattformanbieter verhindert werden. Doch sektorübergreifende Angebote mit großer Reichweite wurden in Deutschland, anders als in anderen europäischen Ländern, noch nicht erreicht.

Peter Batt, Leiter der Abteilung Digitale Gesellschaft, Verwaltungsdigitalisierung und Informationstechnik im Bundesministerium des Innern, für Bau und Heimat, stellte den Aspekt der digitalen Souveränität Europas in den Mittelpunkt der Diskussion, die auch im Kontext digitaler Identitäten eine zentrale Rolle spiele. Digitale Souveränität Europas erfordere die Reduzierung vorhandener und die Vermeidung zukünftiger Abhängigkeiten. Digitale Souveränität umfasse nach Batt die Dimensionen Politik, Technik, Wirtschaftlichkeit, Recht und Sicherheit und betreffe Verwaltung, Wirtschaft und Bürgerinnen und Bürger gleichermaßen. Ein Beitrag zur digitalen Souveränität im Bereich der digitalen Identitäten leiste im Übrigen die Online-Ausweisfunktion des Personalausweises, die als erste ID-Funktion nach eIDAS-VO notifiziert wurde und durch die Nutzbarkeit auf Smartphones vieler Hersteller derzeit eine größere praktische Relevanz erfahre.

Die Bundesregierung hat in jüngster Zeit zudem staatliche Projekte initiiert, welche digitale Identitäten für breite Anwendungskontexte etablieren sollen. Der Innovationswettbewerb „Schaufenster Sichere Digitale Identitäten“[1] des Bundesministeriums für Wirtschaft und Energie, den der Leiter der dortigen Abteilung Digital- und Innovationspolitik, ***Stefan Schnorr***, vorstellte. Der Wettbewerb habe das Ziel, die digitale Souveränität zu stärken und eID Lösungen, die eine hohe

[1] https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/innovationswettbewerb-schaufenster-sichere-digitale-identitaeten-foerderaufruf.pdf;jsessionid=A379334DDA971818FC4CE1444577D33B?__blob=publicationFile&v=3 (abgerufen am 11.03.2020)

Nutzerfreundlichkeit und Vertrauenswürdigkeit aufweisen und zugleich wirtschaftlich sind, der Verwaltung, der Wirtschaft und Nutzerinnen und Nutzern einfach zugänglich zu machen.

Ein weiteres Projekt im Kontext digitaler Identitäten ist das vom Bundesministerium für Wirtschaft geförderten Projekt OPTIMOS der Bundesdruckerei[2] mit dem Ziel, eine Infrastruktur für mobile Dienste in einem offenen Ökosystem für unterschiedliche Sektoren bereitzustellen. Das Projekt soll es Service-Anbietern ermöglichen, über eine Schnittstelle an die sogenannte „Trusted Service Management"-Plattform (TSM) anzudocken, mit Hilfe derer dann das Ablegen der Daten im jeweiligen Hardware-Sicherheitselement auf dem Smartphone der Kunden erfolgt. Neben der Vorstellung des Projektes OPTIMOS hob ***Patrick von Braunmühl*** von der Bundesdruckerei die Bedeutung der Biometrie als Schlüssel zur digitalen Identität hervor und machte in diesem Kontext auf die damit einhergehenden Herausforderungen wie die Möglichkeit des Diebstahls biometrischer Merkmale sowie Deep Fakes aufmerksam.

Artur Burgardt von CORE SE zeigte im Rahmen seines Vortrags die Dimension der Anwendungskontexte digitaler Identitäten auf: die Use Cases von digitalen Identitäten erstreckten sich von der Identifizierung von Personen ebenso wie von Unternehmen, welche sich untereinander und gegenüber Behörden oder Nutzer identifizieren müssen, sowie Maschinen im Internet der Dinge.

Perspektiven aus Europa

NemID ist seit 2010 die einheitliche digitale Identität in **Dänemark**, welche ***Peter Fjelbye*** vom Betreiber Nets DanID A/S auf der Konferenz präsentierte. Mittlerweile nutzen laut Fjelbye bereits 99 % der dänischen Bevölkerung die Login-Lösung von NemID. Eine NemID können Dänische Bürgerinnen und Bürger ab 15 Jahren, die eine nationale Identifikations (CPR)-Nummer haben, erhalten und sich damit gegenüber Onlineverwaltungsleistungen wie beispielsweise den Antrag auf Mutterschaftsgeld, die Beantragung der staatlichen Rente oder die Anmeldung der Kinder an einer neuen Schule über das staatliche Portal borger.dk[3] mittels Logins durch NemID authentifizieren. Den Zugriff auf die eigenen Gesundheitsdaten erhalten Däninnen und Dänen über das staatliche Gesundheitsprotal sundhed.dk[4] via Login mit NemID. Darüber hinaus ist der Login mit NemID nutzbar für Online Banking aber auch für Onlinespiele. Pro Monat werden laut Angaben von Nets DanID 65 Millionen Transaktionen mit NemID durchgeführt. Gründe für die breite Durchdringung der Online Authentifizierung mittels NemID seien unter anderem die entschlossene Zusammenarbeit zwischen dem Staat und der Wirtschaft sowie der Umstand, dass eine Vielzahl von Verwaltungsleistungen obligatorisch nur Online nutzbar sind. Durch die Verknüpfung von NemID mit der dänischen CPR-Nummer, einer nationalen Identifikationsnummer, die im dänischen Zivilstandsregister gespeichert ist, sei eine verlässliche Authentifizierung für einen breiten Anwendungskontext sichergestellt. Die dänische Digitalisierungsbehörde verarbeitet personenbezogene Daten, einschließlich der CPR-Nummer bei Login-Vorgängen mit NemID, um die Identität zu bestätigen.[5] Das Sicherheitsniveau von NemID sei seit ihrem Launch 2010 auf 2FA-Sicherheit angestiegen mit One Time Password per mobiler App nutzbar, was ungefähr dem eIDAS Niveau substanziell entspreche.

Ein weiteres auf der Konferenz präsentiertes Beispiel ist die SwissID in der **Schweiz**, welche die Swiss Sign Group, ein Konsortium bestehend aus Schweizer Banken und Versicherungen, bereitstellt. **Markus Naef** berichtete, dass der Login mit der Swiss ID zum jetzigen Zeitpunkt bei einigen Behörden, Medien und der IT- und Finanzindustrie möglich sei. Swiss ID weise Nutzerzahlen von >1'300'000[6] auf. Die Funktionalitäten der digitalen Identität würden durch die SwissID modular bereitgestellt, um die spezifischen Kundenbedürfnisse abdecken zu können. Abgebildet werde dieses auf technischer Ebene durch abgestufte Authentifizierungsmöglichkeiten. Um verlässliche digitale Identitäten bereitstellen zu können, solle im zukünftigen eID-Ökosystem die Identitätsdatenbereitstellung durch das Schweizer Register des Bundes erfolgen. Als entscheidenden Erfolgsfaktor setze die Swiss Sign Group auf die Zusammenarbeit zwischen Staat und Wirtschaft in Form einer Public Private Partnership ebenso wie auf geeignete rechtliche Grundlagen. Das Bundesgesetz über elektronische Identifizierungsdienste (BGEID), welches am 27. September 2019 durch Nationalrat und Ständerat angenommen wurde, soll Rahmenbedingungen für die Anerkennung von elektronischen Identifizierungsmitteln und von deren Anbietern schaffen. Das Gesetz sieht «elektronische Identifizierungsmittel» vor, die «staatlich anerkannt» sind, aber nicht vom Staat herausgegeben werden –wie der Schweizer Pass und Schweizer Identitätskarte (Art. 6 BGEID). Über das Inkrafttreten des Gesetzes werde voraussichtlich durch eine Volksabstimmung entschieden.

---

[2] https://www.bundesdruckerei.de/de/Unternehmen/Innovation/Optimos
(abgerufen am 11.03.2020)

[3] https://www.borger.dk/

[4] https://www.sundhed.dk/

[5] https://nemlog-in.dk/login.aspx/noeglekort

[6] https://www.swissid.ch/en/geschaeftskunden.html

Darüber hinaus existiert eine Vielzahl von anderen Lösungen in Europa, welche sektorübergreifende digitale Identitäten auf nationaler, europäischer und internationaler Ebene anbieten.

2. Berichte aus den Workshops

Workshop *Digitale Identitäten im Bildungswesen*

Den Impuls im Rahmen des sektoralen Workshops steuerte **Dr. Anja Hagen** (education 360°) bei und die Moderation übernahm **Beth M. Havinga** (Bündnis für Bildung).

Digitale Identitäten sind im schulischen Kontext Voraussetzung für unterschiedliche Plattform-Funktionalitäten, etwa die digitale Ablage, die Nutzung digitaler Lehrangebote (Berechtigungs- und Lizenzverwaltung), die Kooperation und Kommunikation innerhalb der Schule ebenso wie die Schulverwaltung. Die Teilnehmer des Workshops waren sich einig, dass eine übergreifenden digitale Lern-ID im Bildungssektor erforderlich ist. Als Anforderungen an digitale Identitäten wurden im Rahmen des Workshops unter anderem ein zentraler Verwaltungsdienst, entsprechende Zertifizierungen und die Sicherstellung von Interoperabilität identifiziert. Durch die Implementierung offener, interoperabler Schnittstellen, könnte sich ein Identitäten- Management für alle Akteure des Bildungssektors leichter umgesetzt werden. Eine Lern-ID sollte dabei nicht bei der schulischen Anwendung aufhören, sondern im Zuge des lebenslangen Lernens den gesamten Bildungsweg eines Menschen beinhalten.

Eine wesentliche Rolle im Bereich digitaler Identitäten im Bildungssektor spielt der Datenschutz. Bei der Nutzung von Online-Lernplattformen zur Aufgabenbearbeitung, für Lernkontrollen, oder für Gruppenarbeiten fallen personenbezogene Daten an, welche dem Anwendungsbereich der Datenschutzgrundverordnung unterfallen. Eine rechtmäßige Verarbeitung personenbezogener Daten bedarf einer der in Art. 6 DSGVO normierten Erlaubnistatbestände. Weitergabe von Daten zwischen Institutionen sollte nur selektiv und nur nach Einwilligung des Lernenden geschehen. Im Bildungskontext sind darüber hinaus die besonderen Anforderungen an Einwilligungen eines Kindes gemäß Art. 8 DSGVO zu beachten. Danach kann das Kind die Einwilligung selbst erteilen, sofern es das 16. Lebensjahr vollendet hat, andernfalls bedarf es der Einwilligung durch den Träger der elterlichen Sorge. Diese Zustimmungen zu verwalten wurde momentan als eines der großen Hindernisse in der Digitalisierung des Schulunterrichts betrachtet. Ein auf einer Lern-ID basierendes System, welches diese Problematik adressiert, könnte einen beachtlichen Beitrag dazu leisten, dass sich E-Learning an deutschen Schulen durchsetzen kann.

Eine Strategie für eine Flächendeckung innerhalb des Sektors existiert bislang nicht, so dass die Teilnehmer darüber übereinkamen, dass der Diskurs mit Entscheidungsträgern der Politik zwingend erforderlich sei. Hinsichtlich einer sektorübergreifenden Strategie wurde konstatiert, dass eine sektorübergreifende ID zuvörderst eine Frage des Willens der beteiligten Stakeholder sei. Hinsichtlich einer sektorübergreifenden digitalen Identität sei auch in europäischen Dimensionen zu denken und es wurde darauf aufmerksam gemacht, dass ein Blick auf andere Länder hier hilfreich wäre.

Workshop *Digitale Identitäten im Gesundheitssektor*

Impulsgeber des Workshops Digitale Identitäten im Gesundheitssektor war **Prof. Dr. Georgios Raptis** (OHT Regensburg). Moderiert wurde der Workshop von **Tanja Strüve** (DSI, ESMT).

Digitale Identitäten spielen eine wesentliche Rolle in der digitalen Gesundheitsversorgung. Zu den Kernanforderungen an digitale Identitäten im Gesundheitswesen zählt aufgrund der Sensibilität von Gesundheitsdaten ein dem Schutzbedürfnis angemessenes Sicherheitsniveau. Die DSGVO ordnet Gesundheitsdaten der besonderen Kategorie personenbezogener Daten aufgrund ihrer besonderen Grundrechtsrelevanz zu und erklärt sie damit für besonders schützenswert. Um den datenschutzrechtlichen Anforderungen zu entsprechen, muss die Datensicherheit in einem ausreichenden Maße gewahrt werden, insbesondere die verarbeitenden Systeme entsprechend robust gegen Angriffe geschützt sein. Dementsprechend muss derjenige, der Gesundheitsdaten verarbeitet, besonders hohe technisch-organisatorische Maßnahmen ergreifen, um den Zugriff unberechtigter auf diese Daten auszuschließen. Um diesen hohen Datenschutzanforderungen zu entsprechen, sollten starke Authentifizierungsmechanismen implementiert werden. Die Sicherheit der Identifizierungs- und Authentifizierungslösungen im Gesundheitswesen ist eine Grundvoraussetzung für den Datenschutz. Es bestand Einigkeit unter den Teilnehmern,

dass neben Datenschutz und Datensicherheit auch eine intuitive Nutzbarkeit der Anwendungen gewährleistet werden muss. Denn digitale Anwendungen im Gesundheitswesen werden sich nur dann durchsetzen, wenn die angebotenen Lösungen auch im Alltag der Menschen praktikabel und einfach nutzbar sind. Dementsprechend muss die Digitalisierung des Gesundheitswesens insbesondere aus Nutzerperspektive gedacht werden. Im Rahmen des Workshops wurde des Weiteren darüber gesprochen, welches eIDAS-Sicherheitsniveau im Kontext digitaler Identitäten im Gesundheitswesen Anwendung finde. Den hohen Datenschutzanforderungen, insbesondere denen des Sozialdatenschutzes der §§ 291 ff SGB entsprechend, wird für die Identifizierungen und Authentifizierungen für den Zugriff bspw. auf die elektronische Patientenakte (ePA) das eIDAS-Sicherheitsniveau *hoch* zu Grunde gelegt. Diese Sicherheitsniveau ließe sich derzeit insbesondere mit der Online-Ausweisfunktion des Personalausweises realisieren.

Einigkeit bestand unter den Teilnehmern, dass Authentifizierungen im Gesundheitswesen für die Nutzer im Alltag nicht durch zu hohe Barrieren erschwert werden dürfen. Wenn die Nutzungshürden zu hoch sind, finden die digitalen Anwendungen im Gesundheitswesen keine Verbreiterung. Lösungen auf dem eIDAS-Sicherheitsniveau substantiell sind derzeit gut abbildbar, aber auch in diesem Kontext stellte sich die zentrale Frage wie man die verschiedenen Verfahren in der Breite in den Markt bekommt, so dass die Verfahren auch nach Bedarf genutzt werden können.

Als Strategie zur Flächendeckung innerhalb des Sektors wurde ein übergreifendes Identitätsmanagement mittels ID-Providern, welche entsprechende Anforderungen an IT-Sicherheit und Datenschutz erfüllen und den Zugang für alle Anwendungen (Portale, Apps und sonstige Services) ermöglichen, vorgeschlagen.

Hinsichtlich einer sektorübergreifenden digitalen Identität bestand Uneinigkeit zwischen den Teilnehmern. Eine sektorübergreifende Nutzung der eGK als Identifizierungs- und Authentifizierungsmittel ist aufgrund der Zweckbindung an das Gesundheitssystem nicht zulässig und darüber hinaus stoße die Vereinheitlichung auf den Widerstand der Datenschützer. In diesem Kontext wurde die Frage aufgeworfen, ob eine Verknüpfung der elektronischen Gesundheitskarte (eGK) mit anderen Identitäten wie dem Personalausweis zur Vereinfachung möglich sei. Eine Herausforderung in diesem Zusammenhang stelle der Umstand dar, dass die eGK an die Krankenversicherungsnummer geknüpft ist, die als lebenslange personenbezogene Identität dient. Zur Nutzung dieser müsste ein Matching über Eckdaten stattfinden, die auf beiden Seiten gehalten werden und hinreichend zur Identitätsbestimmung sind.

Ein Vorschlag zur Umsetzung einer sektorübergreifenden Strategie war demnach eine user-zentrierte Lösung, in der die Identitäten für unterschiedliche Sektoren nur durch den Benutzer selbst verwaltet werden können, beispielsweise in einem digitalen wallet. Denkbar sind auch vertrauenswürdige Anbieter, die das für den Nutzer übernehmen.

Workshop *Digitale Identitäten in der öffentlichen Verwaltung/OZG Umsetzung*

Den Impulsvortrag des Workshops hielt **Dr. Markus Richter** (Bundesamt für Migration und Flüchtlinge, BAMF); die Moderation übernahm **Isabel Skierka** (DSI, ESMT).

Die Digitalisierung der öffentlichen Verwaltung (öV) ist eine obere Priorität der digitalpolitischen Strategie der Bundesregierung. Dienstleistungen in der öV sollen mit dem 2017 verabschiedeten Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (OZG) bis 2022 alle online über den Portalverbund zugänglich sein. Der Portalverbund soll dazu dienen, die Verwaltungsportale von Bund und Ländern zu verknüpfen, so dass Bürger und Unternehmen die Online-Leistungen über das für sie angelegte Nutzerkonto abwickeln können. Einheitliche digitale Identifizierungs- und Authentifizierungslösungen sind Voraussetzung für die erfolgreiche Umsetzung dieser Strategie. Im Hinblick auf das im Portalverbund erforderliche Identitätsmanagement wird sich die jeweils angemessene Identifizierung nach dem erforderlichen Vertrauensniveau der begehrten Verwaltungsleistung richten. Eine Identifizierungs-Lösung im Portalverbund muss die aus der eIDAS-Verordnung folgende Verpflichtung der EU-Mitgliedsstaaten berücksichtigen, die eIDAS-Sicherheitsniveaus zu berücksichtigen und eIDAS-notifizierte Identitätsmanagementsysteme zuzulassen. Private Anbieter eines digitalen Identitätsmanagementssystems müssen im Hinblick darauf eine eIDAS-Notifizierung herbeiführen.

Unter den Workshop-Teilnehmern bestand Einigkeit darüber, dass die gegenwärtige Strategie der Regierung für flächendeckende digitale Identitäten zu kurz greift. Digitale Identitäten in der öV müssen angemessen sicher, einfach nutzbar und interoperabel bzw. in vielen Anwendungsbereichen über die öV hinaus einsetzbar sein. Wie einige Teilnehmer bemerkten, werden in anderen europäischen Ländern digitale Identitäten dann flächendeckend genutzt, wenn eine nationale Identität für das ganze Land gilt, die Interoperabilität in Richtung Privatwirtschaft (zum Beispiel Banken) gewährleistet wird und die Nutzerperspektive bei der Gestaltung der Identitäten und Anwendungen im Zentrum steht. In Deutschland standen jedoch bisher vor allem die Sicherheitsanforderungen an digitale Identitäten in der öV im Vordergrund. Die Nutzbarkeit (Usability) und der Nutz-

wert digitaler Identitäten wurden laut Teilnehmern dagegen zu sehr vernachlässigt. Um eine Flächendeckung zu erreichen und die Akzeptanz digitaler Identitäten zu steigern, müssen diese Prioritäten sein und die Bedürfnisse der Nutzer im Zentrum stehen. Nutzer können Individuen, aber auch Unternehmen und Maschinen sein. Der Personalausweis reicht in diesem Kontext als Identifizierungsmittel nach Meinung der Teilnehmer nicht aus. Identifizierungsmittel müssen mobil zugänglich, durch biometrische Methoden nutzbar sein und eine Reihe von unterschiedlichen Identitätsattributen abbilden können.

Für einheitliche und sichere Identitäten bietet die eIDAS-VO und die darin enthaltenen Sicherheitsniveaus bereits einen „Werkzeugkasten". Jedoch werden diese bisher nicht ausreichend einheitlich umgesetzt und sowohl innerhalb der öV als auch in unterschiedlichen Sektoren uneinheitliche Standards genutzt.

Als ein Problem wurde die Fragmentierung von Kompetenzen und Verantwortlichkeiten innerhalb des föderalen Systems benannt. Formal löst die Änderung des Art. 91c Grundgesetz, worauf auch das OZG aufsetzt, einige dieser Konflikte. Der IT-Planungsrat kann demnach IT-Standards in der öV beschließen und Interoperabilität fördern. In der Praxis werden solche Beschlüsse jedoch nicht immer einheitlich umgesetzt oder nehmen sehr viel Zeit für die Abstimmung und Implementierung in Anspruch. Zentrale Ansätze auf Bundesebene sind wünschenswert. Einige Teilnehmer befürworteten jedoch zusätzlich einen dezentralen Ansatz, in dem einzelne Bundesländer als „first mover" Best Practice Standards setzten und mit gutem Beispiel vorangingen.

Die Fragmentierung entlang sektoraler Silos ist nach Einschätzung vieler Teilnehmer ein mindestens ebenso großes Problem wie jenes, das der Föderalismus bedingt. In unterschiedlichen Sektoren gelten oft uneinheitliche Anforderungen an digitale Identitäten. Die Sicherheitsniveaus der eIDAS-VO gelten beispielsweise für digitale Identitäten in der öV, jedoch nicht für das Gesundheits- oder Mobilitätswesen. Dieser Mangel an Interoperabilität von Standards behindert die Durchsetzung sektorübergreifender ID-Lösungen. Zudem liegt der Fokus in Deutschland viel zu sehr auf der Sicherheit der Lösungen. So wird Sicherheit oft binär als sicher/unsicher definiert. Ein risikobasierter Ansatz, welchen auch die eIDAS-VO vorgibt, ist jedoch realistischer und umsetzbar. Das Sicherheitsniveau muss sich daher nach der tatsächlichen Sensibilität der Daten richten.

Digitale Identitäten sollten nach Ansicht der Teilnehmer als wesentliche Infrastruktur begriffen werden, für die der Staat eine maßgebliche Verantwortung trägt. Der Staat muss daher entschlossen vorangehen und gemeinsame Standards und Anwendungskriterien schaffen. Eine Öffnung und Interoperabilität von digitalen Identitäten in Richtung Privatwirtschaft, welche ein sehr viel breiteres Anwendungsgebiet zur Verfügung stellt als die öV, sei zudem unabdingbar. Eine Strategie für flächendeckende, sektorübergreifende digitale Identitäten kann in Deutschland nach Ansicht der Teilnehmer daher nur innerhalb einer öffentlich-privaten Partnerschaft (ÖPP) erreicht werden. Durch die Form einer ÖPP können privatwirtschaftliche Anwendungen mit einbezogen werden, die für eine breite Akzeptanz, Nutzbarkeit und Nutzwert, Verbreitung, unabdingbar sind. Hier könne Deutschland dem Beispiel anderer Länder in Europa wie den skandinavischen Ländern oder den Niederlanden folgen. Das „Schaufenster digitale Identitäten" des BMWi sei ein erster Schritt in diese Richtung. Jedoch bedürfe es noch an stärkerem politischem Druck bzw. Willen, um eine gemeinsame Lösung durchzusetzen. Das Beispiel des BAMF hat gezeigt, dass funktionierende Lösungen innerhalb kürzester Zeit gefunden werden können, wenn es nötig ist. Beim Staat sollte es innerhalb der ÖPP und allgemein eine klare Rollentrennung zwischen Issuer (Ausgeber), Regulierer und Kontrollinstanz von digitalen Identitäten geben. Es darf dementsprechend keine Wettbewerbsverzerrung stattfinden. Auch das bisher uneinheitliche Registerwesen solle reformiert, sortiert und mit digitalen Identitäten verknüpft werden.

Workshop *Digitale Identitäten im Mobilitätssektor*

Impulsgeber des Workshops Digitale Identitäten im Mobilitätssektor war **Jens Hantke** (Digital:Lab Volkswagen). Moderiert wurde der Workshop von **Martin Schallbruch** (DSI, ESMT).

Die Diskussion im Mobilitätssektor findet vor dem Hintergrund einer starken Veränderung des Mobilitätsverhaltens stand. Neue Mobilitätsangebote (z.B. Sharing) und flexibleres Mobilitätsverhalten betreffen alle Mobilitätsanbieter. Eine zentrale Anforderung an digitale Identitäten im Mobilitätssektor ist daher die übergreifende Kundenperspektive. Die Nutzer möchten während ihrer Reise eine durchgängige Reisekette vorfinden, d.h. sowohl die Buchung der Bahnfahrt als auch das Carsharing und das Leihfahrrad müssen mit einer Identität online buchbar sein. Dazu müssen die vielen unterschiedlichen Akteure zusammenwirken, insbesondere auch private, im Wettbewerb stehende Akteure, und öffentliche Akteure, die in Monopolbereichen Leistungen der Daseinsvorsorge erbringen. Das Zusammenwirken wird dadurch erschwert, dass die Mobilitätsanbieter wegen der starken Veränderung im Markt hohes Interesse am Erhalt der Kundenbindung und Sorge vor

einem Verlust der Kundenschnittstelle an andere Anbieter (z.B. Plattformunternehmen haben).

Eine Strategie für eine Flächendeckung digitaler Identitäten innerhalb des Verkehrssektors existiert insbesondere aus diesem Grund bislang nicht. Ein Vorschlag unter den Teilnehmern war eine Art „Mindestinteroperabilität". Einvernehmen bestand, dass die Rolle des Staates und der von ihm wesentlich gestalteten Mobilitätsbereiche hierfür entscheidend sein wird.

Sektorübergreifende digitale Identitäten haben für die Anbieter im Mobilitätssektor noch keine große Bedeutung. Sektorübergreifende Lösung müssten zwingend auch global – oder zumindest europäisch – anschlussfähig sein. eIDAS-Konformität spielt im Verkehrssektor bislang keine Rolle.

3. Ergebnisse der Konferenz und Empfehlungen des DSI

Ergebnisse

1. Digitale Identitäten sind für die meisten digitalen Geschäftsmodelle ebenso Voraussetzung wie für die Digitalisierung der Daseinsvorsorge.
2. Mit der weitergehenden Vernetzung digitaler Dienste wird eine übergreifende Lösungsarchitektur für digitale Identitäten als zwingender Bestandteil der digitalen Souveränität Europas angesehen.
3. Deutschland hat bislang – anders als andere europäische Länder – keine sektorübergreifende, Staat und Wirtschaft verbindende Lösungsarchitektur mit einem oder wenigen „Standardanbietern" bzw. übergreifender Interoperabilität.
4. eIDAS-Konformität als im Wesentlichen nur rechtliche Anforderungen an digitale Identitäten im öffentlichen Bereich ist weder sektorübergreifend relevant, noch löst sie derzeit das Interoperabilitätsproblem.
5. Die Anforderungen der öffentlichen Verwaltung im Hinblick auf digitale Identitäten sind EIN Faktor, dürfen aber die Lösungsarchitektur nicht allein bestimmen, weil andere Faktoren wie die Tauglichkeit für alltägliche Identifizierungsvorgänge und die internationale Kompatibilität ebenso berücksichtigt werden müssen.
6. Eine entsprechende Lösungsarchitektur muss sich stark an den Bedürfnissen der Nutzerinnen und Nutzer ausrichten. Die Nutzer wollen intuitiv benutzbare Lösungen für ein breites Anwendungsspektrum.
7. Sicherheit ist conditio-sine-qua-non, aber allein kein Grund zur Nutzung der Lösung. Sicherheitsanforderungen dürfen nicht eine gute UX verhindern.
8. Übergreifende Identifizierungslösungen auf nationaler Ebene sind meist nicht von Beginn an profitabel und benötigen für die Anfangsphase ausreichendes Startkapital.

Empfehlung 1

Staat und Wirtschaft sollten eine gemeinsame Lösungsarchitektur für sektorübergreifende digitale Identitäten entwickeln und umsetzen.

Auch für Deutschland empfiehlt sich die Gründung einer Public Private Partnership für sektorübergreifende digitale Identitäten, wie sie bereits in einigen europäischen Ländern besteht. Die PPP sollte eine Plattform darstellen (und ggf. auch technisch bereitstellen) für sektorübergreifende Standardisierung sowie Herstellung von Interoperabilität und Übertragbarkeit. Einzuschließen sind mindestens Identifizierung und Authentifizierung. Private und öffentliche ID-Anbieter müssen sich der PPP ebenso anschließen können wie Anwendungsanbieter. Für eine solche sektorübergreifende digitale Identität ist ein eigenes Brand zu entwickeln, das Staat und Wirtschaft gemeinsam nutzen.

Empfehlung 2

Bund und Länder müssen diese Lösungsarchitektur wie in anderen europäischen Ländern durch aktive Maßnahmen unterstützen.

Erforderlich ist erstens eine Verknüpfung einer sektorübergreifenden digitalen Identität mit einer staatlichen Identität. Dies kann erfolgen, indem im Rahmen des geplanten registerübergreifenden Identitätsmanagements ein staatlich garantierter verlässlichem Unique Identifier eingeführt, zur Bestätigung einer Identität nutzbar gemacht und auch – im Rahmen der Registermodernisierung - mit den Verwaltungsanwendungen verknüpft wird.

Erforderlich ist zweitens eine Berücksichtigung der gemeinsamen Lösungsarchitektur bei der Ausgestaltung der staatlichen Angebote ebenso wie der Rahmenbedingungen der Daseinsvorsorge-Bereiche (Gesundheitswesen, Bildung, Kultur, öffentliche Verwaltung, Mobilität etc.). Wo der Staat durch eigene Projekte oder Regulierung eine vertrauenswürdige digitale Identität verlangt oder voraussetzt, sollte auf die gemeinsame Lösungsarchitektur Bezug genommen und eine entsprechende digitale Identität eingesetzt werden.