

Deutscher Bundestag

Ausschuss für Digitales

Ausschussdrucksache

20(23)59

4.07.2022



**Kompetenzzentrum
Öffentliche IT**

An:
Deutscher Bundestag
Ausschuss für Digitales
Platz der Republik 1
11011 Berlin
an: adi@bundestag.de

Kompetenzzentrum Öffentliche IT
am Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin
E-Mail: info@oeffentliche-it.de
Telefon: +49 (0) 30 3463-7173
Fax: +49 (0) 30 3463-997173
www.oeffentliche-it.de

STELLUNGNAHME

Digitale Identitäten

Prof. Dr. Peter Parycek
Kompetenzzentrum Öffentliche IT

Mitautor:innen

Simon Sebastian Hunt, Anna-Sophie Novak, Dr. Gregor Eibl, Gabriele Goldacker,
Dr. Karoline Krenn, Fabian Kirstein

Gestaltung und Redaktion:

Jan Hendrik Gräfe, Niels Kölker



INHALTSVERZEICHNIS

Präambel	2
Nationale Ebene	3
Frage 1	3
Frage 2	5
Frage 3	7
Frage 4	8
Frage 5	10
Frage 6	11
Frage 7	12
Speicherung und Technologie	12
Frage 8	12
Frage 9	14
Frage 10	16
Frage 11	17
Frage 12	17
Frage 13	18
Frage 14	18
Frage 15	19
Frage 16	19
Frage 17	20
Europäische Ebene	20
Frage 18	20
Frage 19	21
Frage 20	21
Frage 21	22
Frage 22	22
Frage 23	22
Frage 24	23
Frage 25	23
Frage 26	23
Frage 27	24
Frage 28	24



Präambel

Der neue Personalausweis (nPA) wurde vor mehr als 12 Jahren eingeführt und hat, nach dem D21 eGovernment Monitor 2021, bis heute eine geringe Verbreitung von 9 %. Deutschland liegt damit weit hinter den skandinavischen Ländern zurück. Die dänische eID bspw. wird von über 90% der über 16-Jährigen genutzt. Selbst Österreich liegt inzwischen mit über 3 Millionen Nutzer:innen bei mehr als einem Drittel der Gesamtbevölkerung und einer regelmäßigen Nutzung von ca. 4 Millionen Transaktionen pro Monat. Der deutsche nPA gilt in Europa als hochsichere eID mit geringer Nutzung und wurde im eIDAS-Notifizierungsverfahren als elektronisches Identifizierungsmittel hoch anerkannt. Allerdings können hochsichere Systeme, die nicht genutzt werden, im Ergebnis zu einem unsicheren gesellschaftlichen Gesamtsystem führen. Aus dieser Perspektive ist nicht nur die technische Sicherheit zu beurteilen, sondern mit der Benutzerfreundlichkeit in Balance zu bringen, dies gilt im Besonderen für eID-Systeme.

Erfolgreiche eID-Ecosysteme zeichnen sich aus durch benutzerfreundliche eID-Services, die zu einer hohen Verbreitung in der Gesellschaft geführt haben, und durch zahlreiche Anbieter von Internet-Services, welche die eID zur Erst-Registrierung und zum Login nutzen. Beim nPA ist beides bis heute nicht gelungen: Es gibt eine geringe Nutzung durch die Bürger:innen und ein geringes Angebot seitens des öffentlichen Sektors, des Gesundheitswesens und auch der Wirtschaft – bei aktuell 175 gelisteten Anwendungen. Somit sind beide Seiten der eID-Plattform und des Ecosystems schwach ausgeprägt und die aktuell geringen Zahlen von Nutzer:innen und Diensten nachvollziehbar.

Ein naheliegender Grund im Fall der Bürger:innen ist die über die Jahre immer wieder kritisierte geringe Benutzerfreundlichkeit des nPA – vom wenig verbreiteten Kartenlesegerät bis zu gekoppelten Prozessen zwischen PC/Laptop und Smartphone über die AusweisApp2. Auch die zweite Seite der Plattform, der Dienste-Anbieter, hat zahlreiche Hürden zu nehmen: organisatorische Hürden der Registrierung, technische Hürden der proprietären Services und etwaige finanzielle Hürden. Somit finden sich auf beiden Seiten der eID-Plattform hohe Einstiegshürden für Nutzer:innen und Dienste-Anbieter und eine geringe Motivation – wenige Services für die Nutzer:innen und wenig potenzielle Nutzer:innen für den Dienste-Anbieter – diese zu überwinden.

Eine der zentralen Maßnahmen ist daher eine Neukonzeption der eID-Architektur und der eID-Prozesse unter Nutzung von Industriestandards und der Sicherheitstechnologien, die in der Breite der Gesellschaft über die aktuellen Smartphones bereits vorhanden sind.

Diskurse über Sicherheitstechnologien, die möglicherweise in der Zukunft eine hohe Verbreitung in der Gesellschaft haben (Smart-eID) oder zusätzliche eID-Services, wie Sichtausweise im Smartphone oder die Speicherung von staatlichen Attributen in einer „EU Digital Identity Wallet“, lenken von den eigentlichen Problemen ab und lösen nicht den Kern des Problems, die unzureichende Benutzerfreundlichkeit des nPA und die proprietäre Architektur für die potenziellen Dienste-Anbieter.

Prof. Dr. Peter Parycek

Leiter Kompetenzzentrum Öffentliche IT



Nationale Ebene

Frage 1

Wo steht Deutschland im Bereich der Digitalen Identitäten (eID, Smart-eID und Wallet)? Wo sehen Sie die größten Hürden?

Nach dem D21 eGovernment Monitor 2021¹ wird die Online-Ausweisfunktion von 9 % der Bürger:innen genutzt und weitere 26 % geben an, dass die Funktion einsatzbereit ist, aber noch nicht genutzt wurde. Im internationalen Vergleich liegen die Nutzungszahlen insbesondere in den skandinavischen Ländern wesentlich höher, beispielsweise nutzen über 90 % der Einwohner:innen Dänemarks, die älter als 16 Jahre sind, die dänische eID (nemID). Auch im Vergleich innerhalb des DACH-Raumes liegt Österreich mit 54 % und die Schweiz mit 62 % vor Deutschland.²

Der geringen Nutzungsrate steht eine hohe Anzahl von möglichen eID-Lösungen gegenüber. Von AusweisApp2, AUTHADA, Smart-eID, Elster-Zertifikat bis hin zur ID-Wallet App. Zusätzlich werden von den Ländern Bürgerkonten auf der Länderebene etabliert, die wie in Bayern auch mit einer eID-Funktion für die Verwaltung zum Einsatz kommen bzw. kommen sollen, wodurch sich für die Bürger:innen das Bild zunehmend unklarer darstellt. Neben öffentlichen Anbietern drängen auch private Anbieter auf den Markt – von deutschen Initiativen wie IDnow³, Nect⁴ oder Verimi⁵ über unterschiedliche Projekte im Bereich der Self-Sovereign Identity (SSI) auf Basis der Blockchain-Technologie bis hin zu den eID-Lösungen von Apple (AppleID), Google (GoogleID) und Facebook (FacebookID), die nun auch beginnen,⁶. Angesichts der Vielfalt der öffentlichen und privaten Anbieter wird eine klare Kommunikation zunehmend schwieriger.

Neben der bekannt geringen Nutzung und dem immer schwerer durchschaubaren eID-Anbietermarkt werden die Hürden für eine breite Etablierung einer staatlichen eID aus der Perspektive der Bürger:innen und der Service-Anbieter analysiert und dargestellt mit Fokus auf Plattform-Etablierung⁷:

Aus der **Perspektive der Bürger:innen bzw. der eID-Serviceutzer:innen** sind ein klar erkennbarer Mehrwert (a) und eine einfache Nutzung des Onlineservices (b) entscheidend:

- (a) Mehrwerte von eID-Lösungen sind eine schnelle Erstregistrierung und die einfache, verlässliche und sichere Login-Funktion auf bzw. bei möglichst vielen Plattformen und Onlinediensten. Aktuell sind

¹ eGovernment MONITOR 2021, S. 20, Link: <https://initiated21.de/app/uploads/2021/10/egovernmentmonitor2021.pdf>

² eGovernment MONITOR 2021, S.23 f.

³ <https://www.idnow.io/de/produkte/idnow-eid/>

⁴ <https://nect.com/de/>

⁵ <https://verimi.de/>

⁶ Apple bietet in den USA eID Services zu Mobiler Führerscheine oder Studentenausweis, <https://9to5mac.com/2022/06/24/proving-our-identity/>

⁷ In der wissenschaftlichen Literatur werden die Beziehungen zwischen Plattform Beteiligten unter dem Fachbegriff der „two-sided platforms“ seit mehr als 20 Jahren erforscht, 7640 reviewte Artikel nach Google Scholar und nach Scopus 221; Folgende Perspektiven nach, Launching a Two-Sided Platform: The Role of Platform Enhancers June 2018 Conference: 40th R&D Management Conference “R&Designing Innovation: Transformational Challenges for Organizations and Society” [Launching a Two-Sided Platform: The Role of Platform Enhancers \(polimi.it\)](https://www.polimi.it/) + Service providers’ requirements for eID solutions: Empirical evidence from the leisure sector Michael Kubach, Heiko Roßnagel, Rachelle Sellung Fraunhofer IAO <https://dl.gi.de/bitstream/handle/20.500.12116/17204/69.pdf?sequence=1&isAllowed=y;>



nach Angaben der Bundeswebseite 175 Dienste vorhanden, dabei gibt es keine durchgehende Nutzung im öffentlichen Sektor durch Länder und Kommunen, nur geringe Nutzung im Gesundheitsbereich und ebenfalls nur geringe Nutzung durch den privaten Bereich. Somit besteht lediglich eine geringe Motivation und kaum Anlass, die aktuelle eID-Lösung einzurichten und zu nutzen.

- (b) Zweites entscheidendes Element ist die Benutzerfreundlichkeit des eID-Dienstes von der erstmaligen Einrichtung über die regelmäßige Nutzung bis hin zur Beendigung. Bis 2019 war die Nutzung des neuen/elektronischen Personalausweises (nPA/ePA) ausschließlich mit einem Kartenlesegerät möglich. Aufgrund der geringen Nutzungszahlen wurde das bestehende Konzept adaptiert und die Nutzung des RFID-Chips im Personalausweis über NFC-fähige Smartphones und die AusweisApp2 ermöglicht. Damit ist inzwischen die Einstiegsbarriere deutlich geringer. Für elektronische Verfahren, die direkt am Smartphone durchgeführt werden können, ist die Nutzung grundsätzlich möglich. Die Usability der AusweisApp2 ist im direkten Vergleich zu Angeboten wie IDnow eID oder Nect Ident schwächer ausgeprägt. Die aktuell größte Hürde besteht aber in der Nutzung am PC/Laptop. Dazu muss die AusweisApp2 sowohl am PC/Laptop als auch am Smartphone installiert sein, gestartet werden und das Smartphone mit dem PC/Laptop gekoppelt sein. Digitale Verwaltungsleistungen für mobile Endgeräte werden aufgrund der Nachfrage der Bürger:innen ausgebaut. Aktuell sind digitale Verwaltungsverfahren aber im überwiegenden Teil primär für Webbrowsers-Nutzung am PC/Laptop ausgelegt und nicht für mobile Endgeräte wie Tablet oder Smartphone. Selbst bei einem in Zukunft überwiegenden Angebot für mobile Endgeräte, kann eine wesentlich schlechtere Usability im Sinne der Inklusion und Gleichbehandlung nicht verantwortet werden, somit ist die AusweisApp2 in der aktuellen Architektur wenig bis kaum für den Einsatz am PC/Laptop geeignet.

Zusammenfassend ist für die Bürger:innen bzw. die Nutzer:innen des eID-Services der notwendige Mehrwert aufgrund der geringen Anzahl der Dienste vielfach nicht gegeben, noch ist eine hohe Benutzerfreundlichkeit durch einen einfachen, nachvollziehbaren eID-Service gegeben, wodurch die niedrigen Nutzungszahlen nachvollziehbar sind.

Aus der **Perspektive der potenziellen Anbieter von Services (Dienste-Anbieter)** für Endnutzer:innen sind drei Aspekte ausschlaggebend: (a) hoher Mehrwert, (b) eine einfache Integration der Onlineservices in ihre jeweilige bestehende Anwendungsumgebung und ein (c) fortlaufendes Plattformmanagement mit Weiterentwicklungsperspektive:

- (a) Ein grundsätzlicher Mehrwert staatlich gesicherter Online-Identifikation der Bürger:innen ist für die Wirtschaft, aber auch den gesamten öffentlichen Sektor von Daseinsvorsorge bis Gesundheitsdienste vorhanden, dies zeigt sich im eGovernment Monitor 2021: 48 % der Befragten haben Interesse an der Hinterlegung der Ausweisdaten im Smartphone.⁸ Der Mehrwert der Datennutzung für den Dienste-Anbieter entsteht aber erst durch die aktive eID-Nutzung der Bürger:innen und diese liegt nach dem eGovernment Monitor 2021 bei 9 % und somit ist kein hoher Anreiz gegeben, diese eID-Funktion für Erstregistrierung oder wiederkehrenden Login in Webdienste oder Applikationen für mobile Endgeräte (Apps) zu integrieren.
- (b) Die einfache Integration der eID-Lösung aus Sicht des Dienste-Anbieters umfasst drei Aspekte: die (aa) organisatorische Ebene, wie z. B. die Registrierung, die (bb) technische Ebene der Integration in die Umgebung des Dienste-Anbieters sowie die (cc) wirtschaftliche Ebene, z. B. finanzielle Planbarkeit.

⁸ eGovernment MONITOR 2021, S. 22.



Organisatorisch (aa) muss jeder Service beschrieben und beantragt werden, eine Service-interne Differenzierung der Nutzungsart und der genutzten Daten wird den Ausführungen nach dabei nicht vorgenommen. Technisch (bb) setzt die eID-Architektur vom Serviceanbieter den Betrieb eines eigenen „ID-Servers“ oder einen Vertrag mit einem ID-Server-Betreiber voraus. Die technische Integration ist im Vergleich zu den webbasierten Standardprotokollen zur Identifikation als hoch und für den Anbieter als schwer kalkulierbar zu bewerten. Aufgrund der zunehmenden Bedeutung mobiler Applikationen für Smartphones wurde in den letzten Jahren auf Basis der AusweisApp2 (mobile App für Android und iOS) ein Software Development Kit (SDK)⁹ entwickelt, dazu sind große Teile der AusweisApp2 in die Applikationen des Dienste-Anbieters zu integrieren; dies entspricht nicht dem Stand der Technik für Apps mobiler Endgeräte. Eine Integration über Standardprotokolle, die sich in den letzten Jahren entwickelt haben - wie OpenID Connect & OAuth 2.0 - ist nicht (weder für die webbasierte Variante noch für die mobilen Applikationen) möglich, daher ist der technische Integrationsaufwand als hoch einzustufen. Die wirtschaftliche (cc) Ebene bleibt intransparent aufgrund der schwer kalkulierbaren Kosten für den Betrieb des ID-Servers, aber allem voran ist keine Garantie für eine kostenfreie Nutzung der eID-Funktion für Registrierung oder Login für den Dienste-Anbieter auf den Informationsseiten der zuständigen öffentlichen Stellen zu finden bzw. gegeben.

- (c) Das eID-Plattformmanagement scheint schwach ausgeprägt zu sein, auf den zugänglichen Informationsseiten sind keine Usecases, Entwicklungsperspektiven oder detaillierte Darstellungen zu den Kosten zu finden.

Zusammenfassend ist aus der Perspektive eines Anbieters von Diensten für Endnutzer:innen festzustellen: (a) Die Motivation ist durch die geringen Nutzungszahlen beeinträchtigt; (b) die organisatorische, technische und finanzielle Integration bietet Optimierungsbedarf bzw. führt zu hohen Eintrittsbarrieren und (c) ein eID-Plattformmanagement scheint nicht ausreichend vorhanden zu sein. Somit sind alle drei entscheidenden Aspekte für die Zunahme an Onlineservices kaum oder auch nicht gegeben.

In der aktuellen Situation sind somit beide Seiten – eID-Nutzer:in und eID-Dienste-Anbieter der eID-Plattform - aufgrund der jeweilig beschriebenen Nutzungsbarrieren unzureichend motiviert, die Eintrittsbarrieren zu überwinden und somit ist das fehlende Wachstum nachvollziehbar. In einem ersten Schritt sind daher die Wurzeln des Problems zu heilen. Die aktuell in Diskussion stehenden Erweiterungen wie Online-Ausweise (Digital (Identity) Wallets) oder zukunftsweisende Konzepte einer Self-Sovereign Identity (SSI) sind in einer Gesamtbetrachtung und Weiterentwicklung des eID-Konzepts Elemente, die mitberücksichtigt werden können, aber unserer Einschätzung nach nicht für den Erfolg entscheidend sind.

Frage 2

Mit der eID gibt es seit mehr als 12 Jahren eine digitale Identitätslösung. Wie bewerten Sie diese und warum wurde die Lösung vergleichsweise wenig genutzt? Welche Rolle könnte die eID noch in der Zukunft spielen?

Zusammengefasst die Gründe aus Frage 1:

12 Jahre nach der Einführung des „neuen Personalausweises“ (nPA) nutzen insgesamt 9 % der Bevölkerung den nPA für die eine oder andere der 175 Anwendungen der öffentlichen Hand und der Wirtschaft, die auf

⁹ <https://www.ausweisapp.bund.de/software-development-kit-sdk>



dem Personalausweisportal¹⁰ angeführt werden. Von diesem Angebot werden funktional einige mehrfach gezählt, weil sie kommunenspezifisch sind. Die Angebote aus der Wirtschaft bieten beinahe durchgehend zusätzliche Alternativen für die Identifikation bzw. Authentifizierung auf ihren Webseiten an.

Unter anderem führen Projekte wie ID-Wallet-App¹¹, Smart-eID, AusweisApp2 oder auch AUTHADA App¹² zu einem schwer nachvollziehbaren Bild, welche Elemente für den eID-Service zwingend notwendig sind und welche optional genutzt werden können bzw. welche Vor- und Nachteile die konkreten Ausprägungen des Service mit sich bringen. Zusätzlich drängen Anbieter auf den Markt, die auf das Einlesen des Personalausweises aufbauen und bei denen für Bürger:innen kaum nachvollziehbar ist, inwieweit dies vom Staat zertifizierte Angebote sind oder auch nicht, wie bspw. IDnow eID oder Nect Ident.

Aus der Perspektive der Dienste-Anbieter ergeben sich hohe Eintrittsbarrieren von der Registrierung, über die proprietäre technische Lösung bis hin zu Fragen der finanziellen Kalkulation sowie offene Fragen zur Weiterentwicklungsperspektive. Die Motivation der potenziellen Service-Anbieter, diese Barrieren zu überwinden, ist aufgrund der geringen Anzahl von Nutzer:innen aller Voraussicht nach gering.

Neben den genannten Gründen aus Frage 1 gibt es noch weitere, teilweise historische Aspekte¹³, die zu der geringen Nutzung geführt haben:

In den ersten Jahren mussten die Bürger:innen beim Erhalt des Personalausweises die Aktivierung beantragen (Opt-in). Basierend auf historisch tradierten Diskussionen lässt sich vermuten, dass die zuständigen Verwaltungen in den ersten Jahren nach der Einführung des Systems zurückhaltend in der Empfehlung der Aktivierung gewesen sind, auch aufgrund der geringen Anzahl angebotener Dienste. Von Opt-in wurde mit 2017 umgestellt auf Opt-out: Der Personalausweis muss seitdem mit aktivierter Funktion zum elektronischen Identitätsnachweis übergeben werden (§10 I PAuswG). Über die Sperrung nach § 10 VI PAuswG besteht jedoch weiterhin die Möglichkeit, diese Funktion nachträglich im Sinne eines Opt-out abzuschalten. Eine der größten Hürden war und ist, wie bereits in Frage 1 erwähnt, die Notwendigkeit eines Kartenlesegerätes, spezieller Software, bis hin zur Benutzung einer speziellen Firefox ESR (extended support release). Die Technik wurde sukzessiv nachgebessert, jedoch waren die ersten Nutzer:innen aus der Wirtschaft und dem öffentlichen Sektor zu diesem Zeitpunkt bereits abgesprungen, wie Techniker Krankenkasse oder HUK24.

Kartenlesegerät bzw. Ausweisleser wurden über das Konjunkturpaket II bspw. über Computer BILD verteilt. Eines der Geräte war langfristig nicht nutzbar, weil die Hardwaretreiber für die nächste Version von Windows nicht aktualisiert wurden, wodurch evtl. ein weiterer Vertrauensverlust verursacht wurde.¹⁴

Trotz höchster Sicherheitsansprüche wurde das Sicherheitsimage des neuen Personalausweises durch weit beachtete kritische Veröffentlichungen des CCC beeinträchtigt.¹⁵

¹⁰ <https://www.personalausweisportal.de/SiteGlobals/Forms/Webs/PA/suche/anwendungensuche-formular.html>

¹¹ <https://www.bundesregierung.de/breg-de/suche/e-id-1962112> ist aktuell nicht installierbar und wurde aus den App Stores entfernt.

¹² <https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/online-ausweisen/software/software-node.html#doc14626372bodyText3> und dem Produkt <https://authada.de>

¹³ Fraunhofer FOKUS als auch ÖFIT waren bei der Entwicklung des neuen Personalausweises beteiligt, <https://www.fokus.fraunhofer.de/de/dps/projekte/npa>, siehe auch <https://www.oeffentliche-it.de/personalausweis>

¹⁴ <http://www.personalausweis-kartenlesegeraete.de/tipps/kostenlose-lesegeraete-und-gratis-kartenleser/>

¹⁵ <https://www.heise.de/newsticker/meldung/Chaos-Computer-Club-Neuer-Personalausweis-ist-nicht-sicher-1958360.html> oder <https://www.zeit.de/digital/datenschutz/2010-09/ccc-mpa-ausweis/komplettansicht>



Elster (Steuer) bot zunächst einen eigenen vom nPA/ePA unabhängigen Mechanismus zur Anmeldung an (Elster-Zertifikat), welcher auch bis heute genutzt werden kann und aktuell empfohlen wird¹⁶, wodurch einer der wenigen wiederkehrenden E-Government-Services, die jährliche Einkommensteuererklärung, nicht exklusiv über den ePA genutzt werden kann.

Zunächst gab es kaum interessante bzw. verbreitbare Nutzungsszenarien. Den diesbezüglichen Verbesserungen stand allerdings gegenüber, dass immer wieder Grundlagen für die Nutzung der eID-Funktion durch den Rückzug von Dienste-Anbietern verloren gingen, sodass kontinuierliches Wachstum und vor allem "Erfolgsberichte" unter Bürger:innen nur schwer möglich waren.

Alles in allem eine durchwachsene Vergangenheit, die bis heute in die Gegenwart wirkt. Die sehr hohen Sicherheitsanforderungen seitens des BSI haben zu einem fortlaufenden Ungleichgewicht zwischen technischen Sicherheitsanforderungen und Nutzerfreundlichkeit des nPA/ePA geführt, wie das Beispiel der gekoppelten Nutzung der AusweisApp2 am PC/Laptop und Smartphone mit Abbruchquoten von bis zu 100 % zeigt. Die aktuellen Überlegungen zur Smart-eID setzen den Weg fort, Basistechnologien zum Einsatz zu bringen, die noch keine hohen Marktdurchdringungen haben. Die europäischen Staaten mit erfolgreichem eID-Ecosystem setzen auf Industriestandards wie OpenID und auf Sicherheitselemente, die eine hohe Verbreitung bzw. Marktdurchdringung haben und entwickeln die Sicherheitskonzepte fortlaufend weiter.¹⁷ Die Integration von hardware- und softwarebasierten Sicherheitstechnologien wird vorgenommen, wenn bereits eine hohe Durchdringung dieser Technologie in der Gesellschaft vorhanden ist. Dänemark mit einer Nutzung von über 90 % der Gesellschaft älter als 16 Jahre, hat den Personalausweis in der ersten Phase mit TAN-Listen kombiniert und damit auf die niedrigste mögliche Eintrittsbarriere gesetzt und erst zu einem späteren Zeitraum die Lösung zu einer Code-App weiterentwickelt.¹⁸

Frage 3

Was erhoffen Sie sich vom nun geplanten „interministeriellen Laborformat“ für digitale Identitäten?

Das Format bietet grundsätzlich die Möglichkeit, in einen Austausch auf Augenhöhe zu treten und zu einem gemeinsamen Zielbild zu gelangen. Bei guter Steuerung des Formates kann ein zielorientierter Prozess entstehen. Hierfür sollte eine übergreifende Projektleitung etabliert werden, unter Beteiligung von ein bis maximal zwei Organisationen. Als Ergebnisse sind richtungsweisende Entscheidungen wünschenswert. Thematisch sollte eine Fokussierung auf die Nutzer:innen und die Dienste-Anbieter stattfinden und lediglich eine einzige eID-Anwendung ins Zentrum gestellt werden. Zentral wird für diese die Etablierung einer zukunftsgerichteten Architektur mit Sicherheitskonzepten sein, die auf Sicherheitselementen aufbauen, die eine hohe Marktdurchdringung haben. Hierbei sollte berücksichtigt werden, dass die Sicherheitsfunktionen auch fortlaufend weiterentwickelt werden sollten. Ebenfalls ist der Blick auf die technologischen Industriestandards ausschlaggebend, die die eID-Integration bei möglichen Diensteanbietern erleichtern, was neben planbaren organisatorischen und finanziellen Rahmenbedingungen wichtig für eine breite Akzeptanz ist. Damit diese Ziele erreicht werden können, sind entsprechende Priorisierungen im Rahmen der Planungen vorzunehmen und notwendige Ressourcen zur Verfügung zu stellen.

¹⁶ <https://www.elster.de/eportal/wizard/seq/registrierungsauswahl-1/kontotypauswahl-eop>

¹⁷ From platform dominance to weakened ownership: how external regulation changed Finnish e-identification
Anar Bazarhanova, Jesse Yli-Huumo & Kari Smolander <https://link.springer.com/article/10.1007/s12525-019-00331-4>

¹⁸ <https://www.nemid.nu/dk-en/>



Frage 4

Welche konkreten rechtlichen, regulatorischen oder ökonomischen Maßnahmen müssen noch in welcher Reihenfolge ergriffen werden, damit eIDs in Deutschland erfolgreich eingesetzt und von den Bürgerinnen und Bürgern angenommen werden (bspw. Wegfall des Schriftformerfordernisses)? Bitte bewerten Sie diese hinsichtlich Kurzfristigkeit/Langfristigkeit der Wirksamkeit und Priorität sowie benennen Sie möglichst präzise den Adressaten. Welche Erweiterungsmöglichkeiten bieten sich mit Blick z.B. auf Führerschein, Gesundheitskarte, Impfnachweise, Betriebsausweise (siehe Hotel Checkin Pilot)? Gibt es noch weitere Potenziale?

Kurzfristige grundsätzliche Maßnahmen mit hoher Wirksamkeit und hoher Priorisierung

Notwendig ist die Erarbeitung eines Zielbildes gemeinsam mit Bürger:innen und Diensteanbietern sowie einer davon abgeleiteten Strategie und Operationalisierung.

Für den weiteren Entwicklungsprozess ist das iterative, nutzerzentrierte Vorgehen wichtig, daraus leiten sich Weiterentwicklung und Ausbaustufen ab, dies gilt im Besonderen für eine fortlaufende Weiterentwicklung der Sicherheitskonzepte. Die Planung der Weiterentwicklung ist technologieoffen zu gestalten. Erweiterungsmöglichkeiten müssen erkenntnis- und datengetrieben generiert und entwickelt werden. Innovationen, politische Annahmen und Organisationsüberlegungen sollten über datengestützte Analysen verifiziert oder falsifiziert werden und von der Projektleitung je nach Datenlage und Relevanz eigenverantwortlich priorisiert werden.

An der aktuellen Online-Ausweisfunktion sind bisher unterschiedliche Organisationen mit unterschiedlichen Lösungen beteiligt: Das BSI, Governikus mit der AusweisApp2¹⁹, die Bundesdruckerei²⁰, das Kanzleramt mit dem ID-Wallet sowie das BMI, um die zentralen Einheiten zu nennen. Eine Reduzierung auf ein führendes Projekt mit einer technischen Lösung durch einen Anbieter sollte dringend geprüft werden. Das definierte und dezidierte Projekt sollte nur an eine Behörde berichten.

Kurzfristige technische Maßnahmen mit hoher Wirksamkeit und hoher Priorisierung

Die Gesamtarchitektur wurde vor mehr als 12 Jahren entwickelt mit dem primären Fokus der traditionellen Anwendung am PC/Laptop. Die Architektur wurde schrittweise erweitert, beispielsweise mit der AusweisApp2, aber nicht grundsätzlich überarbeitet oder infrage gestellt. Die Prüfung der Gesamtarchitektur unter besonderer Berücksichtigung der Sicherheitsanforderungen sollte vorgenommen werden, unter der Berücksichtigung der aktuell im hohen Ausmaß verbreiteten hardwarebasierten Secure Elements in den führenden Smartphone-Plattformen (Android/iOS).

Bisher wurde die technische Sicherheit über eine einfache Nutzbarkeit (hohe Usability) gestellt und technische Vorgaben wurden für Sicherheitselemente mit geringer Marktdurchdringung definiert – beim neuen Personalausweis (nPA) das Kartenlesegerät und bei der geplanten Smart-eID ein zertifiziertes Secure Element, das heute nur von einigen wenigen Geräten genutzt wird und bei welchem nicht sicher ist, ob eine Marktdurchdringung stattfinden wird. Hochsichere Systeme, die nicht genutzt werden, können im Ergebnis zu einem unsicheren gesellschaftlichen Gesamtsystem führen mit einhergehendem Vertrauensverlust in die

¹⁹ <https://www.governikus.de/loesungen/produkte/ausweisapp2/>

²⁰ <https://www.bundesdruckerei.de/de/was-ist-eine-digitale-identitaet>, <https://www.bundesdruckerei.de/de/innovation-hub/das-smartphone-als-personalausweis>



digitale Gestaltungsfähigkeit des Staates. Dieser Trend spiegelt sich bereits im eGovernment Monitor 2021 wider, mit einem starken Rückgang von 15 % in der Zufriedenheit mit den E-Government-Angeboten.²¹

Daraus können folgende Maßnahmen abgeleitet werden: (a) Sicherheitsanforderungen sollten zumindest in Balance mit der Usability stehen. (b) Sicherheitselemente innerhalb einer IT-Architektur sollten in der Umsetzung eine hohe Verbreitung haben und nicht erst in einer prognostizierten Zukunft. (c) Sicherheit sollte als fortlaufender Weiterentwicklungsprozess gesehen werden, in welchem Hard- und Softwarelösungen und deren Marktdurchdringung beobachtet und bei hoher Nutzung in die Sicherheitskonzepte integriert werden. (d) Dabei sollte der Fokus auf der Nutzung von Industriestandards liegen, wie beispielsweise OpenID Connect, OAuth 2.0 oder FIDO. Die Nutzung der Standards kann sowohl den Nutzen für die Anwender:innen als auch die Integration beim Dienste-Anbieter maßgeblich erhöhen. (e) Nutzung der eID mittels Smartphones sollte als Standardfall (mobile first) definiert und prioritär entwickelt werden. (f) Entwicklung von Sicherheitskonzepten und Architekturen, die spezifisch auf die beiden mit weitem Abstand führenden Smartphone-Plattformen (Android/iOS) ausgerichtet sind.

Darüber hinaus sollte die Kanalbindung in der PC/Laptop-Nutzung, welche die Koppelung zwischen PC/Laptop und dem Smartphone voraussetzt, aufgrund geringer Usability und hohen Abbruchquoten dringend durch aktuelle Authentifizierungskonzepte, wie eine Zwei-Faktor-Authentifizierung, die über das Smartphone freigegeben wird, ersetzt werden.

Darauf aufbauend sollten risikobasierte Authentifizierungsprozesse definiert werden, die bspw. nicht bei jedem Login-Vorgang das Auslesen des Personalausweises über NFC verpflichtend vorgeben, bspw.: (a) Erstmalige Registrierung mit Datenübermittlung bei einem Dienste-Anbieter wie Bank oder Einkaufsplattform, Nutzung des physischen Personalausweises als zweiten Faktor über NFC. (b) Registrierung mit Pseudonym und Altersnachweis über biometrische Absicherungen der Smartphone-Hersteller, wie beispielsweise Face-ID von iOS. (c) Wiederkehrende Logins über biometrische Absicherungen und Freigabe am Smartphone.

Kurzfristige organisatorische Maßnahmen mit hoher Wirksamkeit und hoher Priorisierung

Etablierung eines eID-Plattformmanagements zum Aufbau eines Ecosystems mit Usecases aus dem öffentlichen, dem Gesundheits- und dem privaten Sektor gemeinsam mit den potenziellen Serviceanbietern.

Finanzielle Garantien für die kostenfreie Nutzbarkeit des eID-Dienstes für die Dienste-Anbieter, die für 5 bis 10 Jahre als Investment in eine sichere digitale Gesellschaft gesehen werden sollten.

Mittelfristige rechtliche Maßnahmen mit hoher Wirksamkeit und hoher Priorisierung

Unter Voraussetzung einer **wirksamen** technischen und organisatorischen **Umsetzung** sollte mittelfristig die verwaltungsseitige zwingende Nutzung der eID und der digitalen Zustellung für alle Verwaltungsvorfahren geprüft werden: (a) Verpflichtende Unterstützung der eID für alle Behördenwege mit Login- oder Signatur-Erfordernissen über OZG 2.0. (b) Einführung einer verpflichtenden digitalen Zustellung gegenüber der Verwaltung für Wirtschaft und Bürger:innen.

Die Verpflichtung zur Nutzung durch Bürger:innen und Wirtschaft kann zu einer hohen Verbreitung führen, wie am Beispiel Dänemarks zu sehen ist. Nutzungsverpflichtungen sollten allerdings erst eingeführt werden, wenn ein angemessener Teil der Bevölkerung die Services bereits nutzt sowie eine hohe Usability und

²¹ eGovernment MONITOR 2021, S. 23



Akzeptanz dieser Services vorhanden ist. Liegen diese Voraussetzungen nicht vor, kann eine Verpflichtung zu einer grundlegend ablehnenden Haltung führen.

Mittelfristige strategische Maßnahmen mit (hoher) Wirksamkeit und mittlere Priorisierung

Ausweisfunktionen wie Führerschein oder KFZ-Zulassung können beispielsweise am Smartphone einen hohen Mehrwert bieten, dazu sind aber im Vorfeld Fragestellungen zu klären, bspw.: „Wie kann die Exekutive die Ausweise überprüfen?“, „Wie kann bei Führerscheinentzug sichergestellt werden, dass der Führerschein nicht mehr angezeigt werden kann?“, „Wie kann erreicht werden, dass im Fall einer Eigentumsübertragung die KFZ-Zulassung nicht mehr in der Wallet hinterlegt ist?“. Ganz generell ist mittelfristig die Absicherung der Aktualität der digitalen Ausweise (auch z. B. der Gesundheitskarte und der Impfnachweise) sicherzustellen.

Die Relevanz und Machbarkeit weiterer Usecases, wie der Integration einer qualifizierten Fernsignatur (Dänemark und Österreich haben die qualifizierten Signaturen in ihren eID-Services integriert) oder der elektronischen Zustellung in die mobile Anwendung, sollte fortlaufend geprüft werden. Mit der Wirtschaft sollte fortlaufend die Entwicklung von Usecases - wie Hotel-Check-in - idealerweise in einem dann etablierten eID-Plattform-Ökosystem diskutiert und priorisiert werden. Die Potenziale und die notwendigen Weiterentwicklungen des Self-Sovereign-Identity-Ansatzes sollten gemeinsam mit den Dienste-Anbietern und der SSI-Community strategisch geprüft werden. Sowohl die Zuständigkeit des Staates für konkrete Aspekte („Staatsaufgaben“) als auch die Beteiligung des Staates an gemeinsamen Serviceentwicklungen mit der Wirtschaft sollte fortlaufend strategisch geprüft werden. Die Wirtschaft könnte auch für gemeinsam entwickelte Services eigene bzw. weitere Geschäftsmodelle entwerfen, umsetzen und betreiben. Eine weitere Möglichkeit ist, die Wirtschaft zusätzlich über APIs einzubinden, von Self-Sovereign-Identity-Services bis hin zum Führerschein als Bestandteil von privatwirtschaftlich verantworteten Wallets, wie iOS Apple Wallet. Voraussetzung dazu sind technische und organisatorische Prozesse, die eine Veränderung der Attribute an Wallets weitergeben bzw. die Gültigkeit von Einträgen zurückziehen können (z. B. Namensänderungen, Änderungen der Meldeadresse, Eigentumsübergänge oder auch Führerscheinentzug).

Die Gründung einer Betreibergesellschaft und die Beteiligung der Wirtschaft an dieser sollte mittelfristig geprüft werden.

Voraussetzung für alle Erweiterungen ist die Bearbeitung und Lösung der Hauptursache/n, wie in Frage 1 dargestellt. Solange diese nicht eingehend analysiert wurden und gelöst sind, sollte keine Funktionserweiterung vorgenommen werden.

Frage 5

Welche möglichen Interessenkonflikte könnten durch die Verteilung von Entscheidungshoheiten und „Schaufensterprojekten“ zwischen Ministerien, der Privatwirtschaft und der Gesellschaft entstehen? Gibt es mögliche Widersprüche bzw. Konfliktpotenziale zwischen den gesellschaftlichen Zielen und möglichen Gewinnwirtschaftsabsichten?

Aus der eID-Nutzung in spezifischen Anwendungen lassen sich möglicherweise personenbezogene Merkmale ableiten, die zur Profilbildung und für gezieltes Marketing verwendet werden können. Daher ist, um die gesellschaftlichen Ansprüche an den Datenschutz zu gewährleisten, über die Architektur sicherzustellen, dass möglichst wenige Prozesse über einen zentralen Punkt geleitet bzw., wenn notwendig, die kritischen Daten zeitnah nachweislich gelöscht werden.



Hinsichtlich der Gewinnabsichten sollten folgende Data-Governance-Prinzipien eingehalten werden:

- (a) Transparenz hinsichtlich der Zwecke für die die eID verwendet werden darf/soll.
- (b) Transparenz über Datennutzung durch Privatwirtschaft und den öffentlichen Sektor, mit enger Zweckbindung der Nutzung der eID bzw. der daraus erschließbaren Daten.

Ein allgemeiner Zielkonflikt existiert zwischen dem Ziel der Steigerung von Effizienz (Vereinfachung und Beschleunigung der Prozesse sowohl für Bürger:innen als auch Verwaltung) und dem Ziel der Verringerung/Vermeidung von Vulnerabilitäten (Risiko des Systemmissbrauchs steigt durch zentrale ID (potenzielle Folgen von eID-Phishing; Function Creep, also der Zweckentfremdung der Daten (z. B. für Gewinnsteigerungsabsichten der Privatwirtschaft anstelle einer reinen Identifikationsfunktion)).

Ministerien brauchen jedoch auch die IT-spezifischen Kompetenzen der Privatwirtschaft, dabei scheint die wichtigste Frage, wie es gelingen kann, die Interessen und die Anforderungen an die technische Umsetzung gesellschaftlich ausbalanciert in die Entscheidungsprozesse einfließen zu lassen.

Die Privatwirtschaft ist an Service Level Agreements interessiert, wenn sie vor ihre eigenen Services (z. B. Onlinebanking) externe eIDs, wie jene der öffentlichen Hand, schaltet. Die öffentliche Hand ist andererseits wenig daran interessiert, zusätzlich zur freien Bereitstellung noch Service Level Agreements zu garantieren. Eine Betreibergesellschaft, die dieses Risiko verwaltet und die Services fortlaufend weiterentwickelt, kann ein mögliches Lösungsszenario sein. Darüber hinausgehend wären eine Beteiligung aus der Wirtschaft und ein PPP-Modell als Möglichkeit zu prüfen.

Frage 6

Welche Verfahren sind für die Revozierung eines Wallet vorgesehen? Was werden die Folgen für Bürger*innen sein, die den Zugang zu ihrem eID-Wallet nicht mehr haben, etwa weil ein Wallet revoziert (deaktiviert) wurde, weil sie ihre PIN vergessen oder ihr Smartphone verlieren oder es gestohlen wird?

Diese Frage ist abhängig von der Datenquelle, dem Anbieter der Wallet und dem gewählten Speicherverfahren für die Wallet.

Unter der Annahme, es handele sich um eine „Wallet“ des Staates, können über einen erneuten Einrichtungsvorgang die Daten aus den staatlichen Registern wiederhergestellt werden.

Im Fall eines privaten Wallet-Anbieters ist dessen Prozessgestaltung entscheidend, aber aus heutiger Sicht spricht nichts dagegen, die Daten aus den staatlichen Registern erneut in die Wallet zu übertragen.

Bei Verlust der PIN besteht nur die Möglichkeit, eine neue Wallet anzulegen und alle in der ursprünglichen Wallet enthaltenen Nachweise erneut einzupflegen.²² Die ursprüngliche Wallet sollte spätestens nach einer derartigen Wiederherstellung des Wallet-Zustandes gelöscht werden, um einen zukünftigen Missbrauch sicher auszuschließen, da nicht ausgeschlossen werden kann, dass die PIN zukünftig doch von Dritten ermittelt werden könnte.

²² <https://digital-enabling.eu/>



Ist die Wallet auf einem physischen Gerät des Nutzens gespeichert, dann ist ein öffentlicher Dienst vorteilhaft, in dem bei Verlust dieses Gerätes die Revozierung hinterlegt und abgefragt werden kann (ähnlich zu Zertifikatssperlisten).

Frage 7

Wo sollten staatlich beglaubigte elektronische Personendaten eingesetzt werden dürfen? Wie kann gewährleistet werden, dass bei digitalen Identitäten Offenbarungsverbote (§ 5 Transsexuellengesetz) auch weiterhin eingehalten werden können? Wer legt fest, welche Arten von Attributen die eID dokumentiert und mitteilt (bspw. Alter, Gender) und wer legt fest, welche „Werte“ diese Attribute haben können (im Fall von Gender: männlich, weiblich, noch weitere)?

Prinzipiell können staatlich beglaubigte elektronische Personendaten auch in Rechtsgeschäften der Bürger:innen bspw. mit der Wirtschaft eingesetzt werden, wenn dies transparent für die Bürger:innen erfolgt. Im Verfahren sollte sichergestellt werden, dass keine für den jeweiligen Service unerheblichen Daten abgefragt werden und kein Druck ausgeübt wird, derartige Daten „freiwillig“ bereitzustellen. Sollen zukünftig weitere, über die heute üblichen Daten des Personalausweises hinausgehende Daten übermittelt werden können, sind dazu spezifische, auf den Typ und Inhalt der Daten bezogene Regeln erforderlich, die z. B. der Sensibilität der Daten Rechnung tragen. In Teilen sollten die Bürger:innen selbst für das Teilen ihrer Informationen zuständig sein und müssen entsprechend umfassend transparent abfragen und kontrollieren können, wie, wann und wo diese Daten genutzt werden.

In der aktuellen Architektur ist dies zweifach gesichert. Im ersten Schritt muss der Service registriert werden, dabei wird geprüft, inwiefern die vom Dienst-Anbieter gewünschten Daten tatsächlich relevant für den gewünschten Service sind. In einem weiteren Schritt müssen die Bürger:innen die Datenübertragung freigeben.

Die Attribute und Werte, die auf der eID gespeichert und von dieser geteilt werden, hängen dabei von verschiedenen Faktoren ab. Grundsätzlich ist es eine Entscheidung des Gesetzgebers und gegenwärtig sind diese in §18 III PAuswG gelistet. Das Geschlecht gehört nicht dazu, darf entsprechend nicht gespeichert und kann somit auch nicht geteilt werden.

Speicherung und Technologie

Frage 8

Wie definieren und bewerten Sie das Self-Sovereign Identity (SSI)-Konzept? Eine Kritik an SSI ist, dass beglaubigte Daten bei den Empfängern gespeichert würden. Wie bewerten Sie die Datensicherheit des SSI-Konzepts? Gibt es aus Ihrer Sicht technische Wege, wie diese Empfangsspeicherung durch SSI vermieden werden kann?

Self-Sovereign Identity (SSI) ist ein vielversprechendes Konzept im angewandten Forschungsstadium. Aufgrund der grundlegenden Probleme der eID (beschrieben mit den Antworten zu Frage 1 und 2) und der notwendigen Maßnahmen (Frage 4) sollte keine hohe Priorität auf SSI gesetzt werden, um die Komplexität nicht weiter zu erhöhen.

SSI bietet besondere Vorteile in Bezug auf die individuelle Kontrolle, die Datensicherheit und die vollständige Übertragbarkeit der Identität zwischen verschiedenen Diensten. So können beispielsweise fälschungssichere

