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

Fraunhofer FOKUS

Kompetenzzentrum
Öffentliche IT

INHALTSVERZEICHNIS

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 2021[1] 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 IDnow[3], Nect[4] oder Verimi[5] 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-Etablierung[7]:

Aus der **Perspektive der Bürger:innen bzw. der eID-Servicenutzer: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://initiatived21.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) + 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 Webbrowser-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 mitberücksichtig 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 Personalausweisportal[10] 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-App[11], Smart-eID, AusweisApp2 oder auch AUTHADA App[12] 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 Aspekte[13], 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 APpp 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-lesegerate-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-npa-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 wird[16], 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/registrierungauswahl-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 AusweisApp2[19], die Bundesdruckerei[20], 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 beispielswiese 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 Verwaltungsverfahren 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. Konflikt-potenziale 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 Büger: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 Nutzenden gespeichert, dann ist ein öffentlicher Dienst vorteilhaft, in dem bei Verlust dieses Gerätes die Revozierung hinterlegt und abgefragt werden kann (ähnlich zu Zertifikatssperrlisten).

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 Dienste-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

digitale Versionen wichtiger persönlicher Dokumente wie Personalausweise, Reisepässe, Geburtsurkunden oder ärztliche Bescheinigungen erstellt werden.

Die Speicherung der Daten bei den Empfängern ist hierbei Teil des Konzeptes. Der Begriff „self-sovereign" bezieht sich hierbei auf die volle Selbstkontrolle der Identitätsinhaber über ihre persönlichen Daten. Die Verhinderung der Empfangsspeicherung ist nicht vorgesehen. Allerdings werden in den meisten Ausprägungen von SSI nicht die ursprünglichen Dokumente (z. B. der Führerschein) gespeichert, sondern nur relevante Einzeldaten (z. B. die Führerscheinklasse). Im Kern bildet SSI die physische Ausgabe von Identitätsdokumenten digital ab. Beispielsweise wird der Personalausweis mit entsprechenden Sicherheitsmerkmalen den Bürgern übergeben. Diese Sicherheitsmerkmale werden bei SSI durch kryptografische Verfahren umgesetzt, bei denen die Identitätsdaten durch die Ausgabestellen signiert werden.

Die Anwendungsfälle sind jedoch nicht auf persönliche SSI beschränkt, sondern können auch digitale Identitäten von physischen Objekten im Rahmen von IoT-Lösungen umfassen.[23] Dabei wird als einer der relevanten Vorteile von SSI die Kontrolle der Datenfreigabe bei den SSI-Nutzer:innen im Diskurs angeführt. Die Daten werden damit direkt von den SSI-Nutzer:innen zum Dienste-Anbieter (i. e. Datennutzer) in der bestimmten Granularität verschlüsselt weitergegeben, ohne dass der Herausgeber der Nachweise eine Kenntnis von der Nutzung erhält.

Im Kontext von SSI sind vielfältige Standards und Spezifikation entstanden, die auch relevant sind für andere eID-Konzepte. Beispielsweise sind hier die W3C-Standards „Decentralized Identifiers"[24] und "Verifiable Credentials"[25], die hoch-strukturierte Datenmodelle zur Abbildung von Identitätsdaten und Beglaubigungen darstellen. Diese Standards werden eine zentrale Rolle bei der Interoperabilität und Sicherheit von Digitalen Identitäten spielen.

Besondere Aufmerksamkeit aus der Perspektive der Verwaltung sollte dem Widerrufsprozess gewidmet werden. Es muss ein Verfahren definiert werden, mit dem Aussteller:innen, im Fall von Attributen aus den Verwaltungsregistern die zuständige Behörde, einen Nachweis auch widerrufen können, bspw. Im Fall der Änderung des Namens, die Änderung der Meldeadresse oder der Entziehung der Fahrerlaubnis. In der SSI Architektur sind nur die Aussteller:innen berechtigt, Attribute zu widerrufen. Für die Fälle, in denen andere Behörden Attribute widerrufen, sind innerhalb der Verwaltung automatisierte Prozesse zu etablieren, zum Beispiel im Falle eines Führerscheinentzugs durch die Polizei im Rahmen einer Verkehrskontrolle.[26]

Grundsätzlich ist die Datensicherheit von SSI nicht anders zu bewerten als andere Lösungen für Digitale Identitäten. Im Kern setzt das Verfahren auf kryptografische Verfahren, bei denen der private Schlüssel der Nutzer sicher verwahrt werden muss. Auch hier bieten sich die aktuellen technischen Möglichkeiten an, wie Hardware-seitige Verschlüsselung, 2-Faktor-Verfahren etc. Es ist jedoch klar festzustellen, dass in aktuellen Umsetzungen von SSI den Nutzern zu viel Verantwortung bei der sicheren Verwahrung von kryptografischen Schlüsseln zukommt. Hier müssen noch wesentlich bessere Usability-Konzepte und Backup-Mechanismen entwickelt werden (siehe dazu auch Frage 9).

[23] https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Fraunhofer%20FIT_SSI_Whitepaper.pdf, S. 38
[24] https://www.w3.org/TR/did-core/
[25] https://www.w3.org/TR/vc-data-model/
[26] https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Fraunhofer%20FIT_SSI_Whitepaper.pdf, S. 42

Frage 9

Eine sichere Lösung zum Speichern der Daten auf dem Smartphone ist die Nutzung eines Secure Elements. Hieran ist jedoch eine soziale Frage geknüpft: Bisher haben nur neue, teure Smartphones die NFC-Schnittstelle und Secure Elements. Wie bewerten Sie dieses Problem heute sowie mittel- oder langfristig? Wie könnten sozialverträgliche Lösungen aussehen – auch für diejenigen, die gar kein Smartphone besitzen? Eine weitere technische Lösung ist die Nutzung der Secure-Enclave Ebene, die in mehr Smartphones zur Verfügung steht. Wie bewerten Sie diese Ebene in Bezug auf die Sicherheit und Performanz?

Nutzung von Secure Elements in Smartphones

Ganz grundsätzlich werden in allen aktuellen Smartphones „Sichere Zonen" spezifiziert, die mit hardwarebasierten Secure Elements ausgestattet sind. Sichere Zonen im Smartphone können mit verschiedenen Lösungen von „embedded secure elements" (eSE) bis hin zur eSIM ausgestattet sein. Die sicheren Zonen und deren genutzte Secure Elements unterscheiden sich in technischer Ausführung, technischer Funktion, Zertifizierung, Sicherheitslevel und Hersteller-spezifischen Sicherheitsarchitekturen. Die Sicherheitselemente sind gegen Manipulation geschützt und über kryptografische Schlüssel nur für autorisierte Dienste und Anwendungen zugänglich und dienen unter anderem der Verschlüsselung von Daten oder der Verwaltung von Schlüsseln.

Apple setzt bspw. auf die Secure Enclave[27] während in Android Smartphones ein Hardware Backed Keystore[28] verwendet wird. Beides sind hardwarebasierte kryptografische Module, wie Trusted Execution Environments (TEE) oder im Fall von Apple ein eigener Crypto-Co-Prozessor. Die Verwendung dieser Module führt zu einer verbesserten Sicherheit.[29]

Secure Element OPTIMOS und Smart-eID Projekt

Ein zukunftsgerichteter Standard auf höchster Sicherheitsstufe innerhalb der „sicheren Zonen" von Smartphones und ein Zugang zu den „sicheren Zonen" werden zurzeit durch OPTIMOS-Partner und durch das BSI in die internationale Standardisierung eingebracht.[30] Diese Initiative befindet sich in einem frühen Stadium und findet daher noch keine hohe Verbreitung in den aktuellen Modellen bzw. wird aktuell lediglich in den hochpreisigen Android Modellen von Samsung integriert.

Mit dem Smart-eID-Projekt sollen eine Wallet-Umgebung geschaffen und die Attribute direkt im dedizierten Chip gespeichert werden. Nutzer:innen können die Smart-eID unter einmaliger Verwendung der Ausweiskarte selbst erstellen. Dabei werden die Personendaten aus der Ausweiskarte abgeleitet und in einem hardwarebasierten Vertrauensanker im Smartphone abgelegt.[31] Im Zuge des Projektes „OPTIMOS 2.0" wurde eine Reihe von Sicherheitsanforderungen für die Nutzung der Smart-eID ermittelt, die Geräte der Samsung-Galaxy-S20-Serie waren die ersten, die diese Sicherheitsanforderungen erfüllen. Inzwischen gibt es weitere Modelle, die die Smart-eID unterstützen – die Liste der Geräte und Hersteller soll fortlaufend aktualisiert

[27] https://support.apple.com/de-at/guide/security/sec59b0b31ff/web
[28] https://source.android.com/security/keystore
[29] https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions/@@download/fullReport, Seite 18
[30] https://www.bundesdruckerei.de/files/dokumente/pdf/produktblatt_optimos2.0.pdf, Seite 2
[31] https://www.personalausweisportal.de/SharedDocs/downloads/Webs/PA/DE/informationsmaterial/weiterefuehrendes-material/Handlungsleitfaden_Integration_Smart-eID_Nutzerkonto.pdf, Seite 4

werden.[32] Eine Verbreitung der Smart-eID und deren Nutzung hängen damit zusammen, wie sehr gängige Smartphones die erforderlichen Sicherheitsanforderungen erfüllen.

Inwieweit dieser Standard von allen Smartphone-Herstellern genutzt werden wird, ist aus heutiger Sicht nicht einschätzbar. Somit kann auch keine Aussage darüber getroffen werden, in welchem Zeitraum eine Marktdurchdringung durch eine breite Nutzung innerhalb der Gesellschaft erreicht werden kann. Aktuell ist kein hoher Druck aus Europa auf die Smartphone-Hersteller zu erwarten, diesen Chip-Standard zu integrieren, weil alle anderen Mitgliedstaaten auf die etablierten Sicherheitsarchitekturen für ihre nationalen eID- und Wallet-Lösungen setzen. Insbesondere der Einsatz in Apple-Modellen ist fraglich, weil Apple zur Verschlüsselung eine eigene Sicherheitsarchitektur mit dedizierten Crypto-Co-Prozessor entwickelt hat. Kurz- und mittelfristig sind die hohen Sicherheitsansprüche der Smart-eID aufgrund der aktuell geringen Verbreitung des Chips und der nicht absehbaren Marktdurchdringung keine Option für einen breiten Einsatz. Die Smart-eID hätte mit der angestrebten Wallet-Integration wesentliche Funktionsunterschiede zu den bestehenden eID-Lösungen und ist daher auch aus dem Gleichheitsgrundsatz als kritisch zu beurteilen, weil große Gruppen der Bevölkerung von der Nutzung aktuell und eventuell auch zukünftig ausgeschlossen sind. Sollten sich der Standard international durchsetzen, Marktführer wie Apple oder Samsung das notwendige Secure Element breitentauglich in die Sicherheitsarchitekturen integrieren und eine hohe gesellschaftliche Durchdringung feststellbar sein, können und sollten solche Sicherheitselemente auch zukünftig in weiteren Ausbaustufen der eID integriert werden, aber nicht vor diesem Zeitpunkt.

RFID-Chip – NFC-Reader-Verbreitung in Smartphones

Weniger kritisch ist die Nutzung von RFID-Chips, die über integrierte NFC-Reader am Smartphone ausgelesen werden können. NFC-Reader auf Apple- und Android-Smartphones sind seit ca. 2017 auch in kostengünstigen Modellen Standardbestandteil. Aufgrund einer durchschnittlichen geringen Nutzungsdauer von ca. 40 Monaten[33] ist heute im Jahr 2022 von einer hohen Verbreitung auszugehen. Die Ausweisapp-Plattform listet derzeit 532 Mobilgeräte, die für die Nutzung der Online-Ausweisfunktion geeignet sind.[34] Der Personalausweis mit seiner RFID-Karte kann somit als zweiter Faktor aus der gesellschaftlichen Perspektive genutzt werden. Aus der Sicht der Nutzerfreundlichkeit der eID-Lösungen sollte nicht jede Transaktion zwingend mit dem Personalausweis vorgesehen sein, da die Handhabung je nach Smartphone mit sehr gut bis ungenügend bewertet wird. Empfehlenswert ist ein risikobasierter Ansatz, der je nach Transaktionsprozess unterschiedliche Anforderungen vorsieht, PIN-Eingabe oder je nach Hersteller oder Modell auch biometrische Absicherungen mit hoher Sicherheitsklasse.

Lösungsansätze und Empfehlungen der ENISA- Agentur der Europäischen Union für Cybersicherheit

Die aktuelle Entwicklung geht deutlich in Richtung der Verwendung von sicheren Zonen der Smartphones[35], die in Kombination mit einem zweiten Faktor abgesichert werden, wie bspw. PIN-Eingabe, RFID-Karten (wie

[32] https://www.personalausweisportal.de/SharedDocs/downloads/Webs/PA/DE/informationsmaterial/weiterefuehrendes-material/Handlungsleitfaden_Integration_Smart-eID_Nutzerkonto.pdf, Seite 10
[33] https://www.allianz-trade.com/content/dam/onemarketing/aztrade/allianz-trade_com/en_gl/erd/publications/the-watch/2022_02_035G.pdf, Seite 3
[34] https://www.ausweisapp.bund.de/mobile-geraete
[35] Apple Secure Enclave: https://support.apple.com/de-at/guide/security/sec59b0b31ff/web oder Android Hardware Backed Keystore, siehe dazu: https://source.android.com/security/keystore#architecture

dem Personalausweis) oder im Smartphone integrierten Sicherheitssystemen (siehe auch Frage 10). ENISA rät ab von Absicherungen wie SMS oder E-Mail zur Absicherung von eID-Lösungen und beschreibt die aktuellen Sicherheitselemente, die in europäischen Lösungen genutzt werden[36]: (a) Konzepte, die auf mobilen Endgeräten wie Smartphones basieren, auch aufgrund der weiterhin zunehmenden Nutzung in der Gesellschaft und der weit überwiegenden Erwartungen der Nutzer:innen – dies bestätigt sich auch im eGovernment Monitor 2021.[37] Dies unter Nutzung der vorhandenen Technologien wie Secure-Enclave (SE) und Trusted Execution Environment (TEE) oder, aus technischer Perspektive, auch SIM-Karten. (b) Nutzung von biometrischen Elementen. Diese variieren in Qualität und Zertifizierung besonders stark von Hersteller zu Hersteller bzw. auch in den Modellreihen. (c) Speicherung von Zertifikaten, PIN-Codes oder Schlüsseln in Remote Hardware-Secure-Modul (HSM), die inzwischen europaweit im Bereich der Fernsignaturen eingesetzt werden. (d) Zertifizierung und Sicherheitsschemata für die genannten Lösungen.

So setzt Österreich auf eine Kombination von Wissen (PIN-Code) und Besitz (Smartphone) und eine optionale Absicherung über integrierte Sicherheitssysteme wie bspw. Face ID bei Apple iOS und sichert zusätzlich über die Speicherung von Zertifikaten und Schlüsseln in Remote Hardware-Secure-Modul (HSM) ab, die auch für die Fernsignatur genutzt werden können. Trotz der zahlreich genutzten Sicherheitselemente ist eine gute Benutzer:innenfreundlichkeit/Usability gegeben. Durch die gute Usability und den Verzicht auf eine kartenbasierte Version der eID (eCard) ist das System über die letzten 10 Jahre linear und während der COVID-19-Pandemie exponentiell gewachsen und liegt derzeit bei ca. einem Drittel aktiver Nutzer:innen der Gesamtbevölkerung.

Empfehlung

Unsere Empfehlung ist daher eine Sicherheitsarchitektur, die auf mobilen Endgeräten aufbaut unter Nutzung der vorhandenen Secure Elements mit aktuell hoher Verbreitung (hardwarebasierte kryptografische Module, Apple Secure Enclave/Android Smartphones Backed Keystore), in Kombination mit Wissen (PIN-Code) und, wenn geboten, der Nutzung eines zweiten physischen Faktors über den RFID-Chip des Personalausweises oder ein Remote Hardware-Secure-Modul (HSM).

Frage 10

Als alternative Lösung wird eine verschlüsselte Speicherung auf dem Hauptspeicher des Smartphones anvisiert. Wie bewerten Sie diese Ebene in Bezug auf die Sicherheit und Performanz?

Stand der Technik ist, dass die Daten verschlüsselt im Speicher der App liegen, die mit einem Schlüssel aus dem TEE (bzw. der Secure Enclave – siehe Frage 9) verschlüsselt werden. Das funktioniert auf den beiden genannten Plattformen (Android/iOS) in gleicher Art und Weise. Ein direktes Speichern der Wallet-Daten in der Hardware ist performance- und speicherplatzmäßig nicht zu empfehlen und die Ausgestaltung des Prozesses ist von den Smartphone-Herstellern bzw. dem jeweiligen Smartphone-Modell abhängig. Darüber hinaus können mit den beschriebenen Sicherheitstechnologien aus Frage 9 in Kombination mit Ablaufprozessen hochsichere Systeme geschaffen werden, die aktuell auch europaweit eingesetzt werden. Der Smart-

[36] https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions/@@download/fullReport, S. 30ff
[37] Der Trend geht immer stärker zur Nutzung mit dem Smartphone, bereits jetzt entscheiden sich 59 Prozent der NutzerInnen für die alleinige Nutzung dieser Variante (+6 Prozentpunkte gegenüber 2020), eGovernment Monitor 2021, S. 21.

eID-Ansatz mit dem Schreiben der Daten in den Hardware-Chip wird nach aktuellem Wissensstand von keinem weiteren europäischen Land verfolgt.

Frage 11

Eine weitere diskutierte Lösung für die Speicherung der Daten ist die eSIM auf den Smartphones. Wie bewerten Sie dabei die Rolle der Anbieter, die sich teilweise sperren, die eSIM für die staatlichen Lösungen zu öffnen? Inwieweit könnte der Digital Markets Act diese Gatekeeper-Handlung verhindern?

Wie in Frage 9 und 10 angeführt, eignet sich eSIM laut der ENISA grundsätzlich zur Speicherung von Daten und Schlüsseln. Die Nutzung der SIM bzw. der eSIM-Karte zur Absicherung der eID-Funktionen wird seit mehr als einem Jahrzehnt diskutiert und wurde bis 2022 nicht flächendeckend etabliert. Die Etablierung eines auf der eSIM beruhenden Ecosystems ist aufgrund der zahlreichen beteiligten Unternehmen, wie unter anderem den Mobilfunkprovidern oder den Herstellern der mobilen Endgeräte, komplex. Eines der wenigen Länder, die dies erfolgreich umgesetzt haben, ist Estland mit MobileID, allerdings vor mehr als 15 Jahren in einem nationalen Schulterschluss. Aktuell wird eine zusätzliche Lösung, die SmartID, angeboten, die aller Voraussicht nach die MobilID ablöst. Die Koordination und die benötigte Standardisierung der digitalen Austauschprozesse mit der Verwaltung und den Unternehmen sind komplex, wie bspw. die erforderlichen Clearingprozesse im Fall von nicht eindeutigen Zuordnungen. Eine kurzfristige Etablierung ist daher als sehr unwahrscheinlich einzustufen. Kurzfristig ist eine Machbarkeitsstudie denkbar, die mittel- bis langfristige Risiken und Potenziale einer Einführung prüft, der europäische Trend geht aber in eine andere Richtung.

Frage 12

Wie schätzen Sie die Gefahr von Identitätsdiebstählen ein, wenn entsprechende Identifikationsdaten in einer Wallet auf Smartphones gespeichert werden und wie kann diese reduziert werden?

Mit einem zweiten Faktor wie dem RFID-Chip im Personalausweis muss der Angreifer sowohl auf das mobile Endgerät/Smartphone physischen Zugriff haben als auch auf den physischen Personalausweis. Zusätzlich müssen etwaige Zugangscodes zum mobilen Endgerät/Smartphone ausgespäht werden oder biometrische Absicherungen wie Fingerabdruck oder Gesichtserkennung getäuscht werden. Wenn vorgesehen, ist das Remote Secure Element über das ePA/eID-Passwort zusätzlich geschützt. Weitere FIDO-Sicherheitstoken wären zusätzlich einsetzbar, wenn vom Anbieter oder auch den Nutzer:innen gewünscht. Im Design muss eine Balance zwischen guter Nutzbarkeit und Sicherheit gefunden werden und die Usecases sind gegebenenfalls auch unterschiedlich abzusichern. Die Sicherheitselemente sind vorhanden und können in geeigneter Weise kombiniert werden und reduzieren so die Risiken der Nutzung der eID-Funktion und etwaiger Wallets.

Frage 13

In Bezug auf die ID-Wallet-App weist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in seinem 30. Tätigkeitsbericht für das Jahr 2021 auf noch offene datenschutzrechtliche Fragestellungen beim Einsatz der Blockchain-Technologie hin. Wie bewerten Sie den Nutzen und die Erfordernis der Blockchain-Technologie in Konzepten digitaler Identitäten wie ID-Wallets?

„Im Rahmen der SSI-Piloten des Bundeskanzleramts […][dient] [d]ie Verwendung der Blockchain Hyperledger Indy […] nur für die Speicherung öffentlichen Schlüsselmaterials (öffentliche Schlüssel und DIDs) ausstellender Parteien sowie als dezentrale Prüfinfrastruktur. Personenbezogene Daten wurden weder bei der Ausstellung noch bei der Verifizierung von Nachweisen auf den Blockchain Ledger geschrieben. Insbesondere werden nicht nur Identitätsattribute, sondern auch von Personen verwendete öffentliche Schlüssel zu keinem Zeitpunkt auf eine Blockchain geschrieben, sondern lediglich in der digitalen Wallet der Nutzer:innen gespeichert und bilateral mit verifizierenden Parteien geteilt." [38] Basierend auf diesen Informationen liegt für das ID-Wallet-App-System nach unserer Einschätzung keine datenschutzrechtliche Fragestellung vor, weil selbst der öffentliche Schlüssel der Bürger:innen nicht in die Blockchain geschrieben, sondern nur direkt mit der Kommunikationspartei ausgetauscht wird. Somit sind keine Rückschlüsse auf personenbezogene Daten möglich, da diese nicht in der öffentlich zugänglichen Blockchain gespeichert sind. Daraus kann nicht generell abgeleitet werden, dass dies für jeden SSI-Service der Fall sein muss, sondern ist für den jeweiligen Service zu prüfen.

Frage 14

Die derzeitige Beschreibung des eID-Systems lässt noch technische Details offen. Weitere Verfeinerungen können einen Einfluss auf Datenschutz und Sicherheit haben. So könnte eine auf der Wallet basierende Architektur, bei der die Wallet immer dann mit einem zentralen Cloud-Anbieter interagiert, wenn sich die oder der Nutzer*in bei einem Dienst authentifiziert, zu unerwünschtem Informationsverlust führen (etwa, wann und bei welchem Dienst die Wallet verwendet wird). Wird dies berücksichtigt? Nach welchem Verfahren werden diese technischen Einzelheiten festgelegt, und welches Maß an demokratischer Kontrolle ist vorgesehen?

Die eID-Architektur ist ganz grundsätzlich aus der Perspektive „Privacy by Design" zu entwickeln und daher sollte nicht jede Transaktion über staatliche Dienste oder private, nationale oder internationale Anbieter stattfinden. In dieselbe Richtung zielt auch der Vorschlag, vor allem wiederkehrende Transaktionen direkt über Standardprotokolle und das Endgerät der Nutzer:innen zu initiieren. Dieses Argument spricht auch dafür, Daten zumindest für einen definierten Zeitraum in der Wallet vorzuhalten. Ebenso sollte von einem streng durchgeplanten Vorgehen Abstand genommen werden. Die Erfahrung hat gezeigt, dass sich digitale Großprojekte nicht gut mit den alten Planungsmethoden umsetzen lassen. Hier sind moderne iterative Vorgehensweisen deutlich besser aufgestellt, um der Komplexität angemessen Rechnung zu tragen. Dies gilt im Besonderen für die fortlaufende Weiterentwicklung der Sicherheit. Die demokratische Kontrolle sollte für diesen iterativen Prozess die Ziele vorgeben und bei Bedarf das Endergebnis abnehmen.

[38] https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Whitepaper_Mythbusting_Self-Sovereign_Identity.pdf, S. 29

Frage 15

Sollten aus Ihrer Sicht alle Funktionen einer eID-Wallet auch offline verfügbar sein?

Wenn eine eID-Wallet auch eine vollwertige Alternative zu den physischen Sichtausweisen bilden soll, dann ist eine Offlinevariante notwendig, bspw. zum „Vorzeigen" des Führerscheins in ländlichen Regionen.

Allerdings muss eine Offlinenutzung für die prüfende Seite zeitlich limitiert sein, da ein regelmäßiger Abgleich mit zentralen Daten notwendig ist. Das beinhaltet zum Beispiel die Bereitstellung von aktuellen öffentlichen Schlüsseln oder Widerruflisten.

Frage 16

Wie bewerten Sie Berechtigungszertifikate, die verhindern sollen, dass bei einfachen Logins (bspw. Online-Shopping, Social Media) immer der Personalausweis vorgezeigt wird? Wer stellt diese Zertifikate aus? Wie schätzen Sie allgemein die Sicherheitsrisiken in diesem Kontext ein? Welche alternativen Möglichkeiten zur Verhinderung von Over-Identification gibt es? Bitte unterscheiden Sie diese nach technischen und regulatorischen Ansätzen.

In der Frage 4 zu den Maßnahmen empfehlen wir, wie 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 beispielswiese Face ID von iOS. (c) Wiederkehrende Logins über biometrische Absicherungen und Freigabe am Smartphone.

In diesen typischen Usecases von umfangreicher Erstregistrierung eines Bankaccounts bis hin zum wiederkehrenden Login sollten somit einerseits die Sicherheitselemente zur Absicherung des Prozesses und auch die zu übertragenden Daten definiert werden. Die richtige Wahl der Absicherung kann die Akzeptanz bei Dienste-Anbietern und -Nutzern wesentlich erhöhen. Unter der Nutzung der aktuellen Industriestandards können so Login-Prozesse und Single-Sign-On-Dienste im Rahmen der staatlichen eID-Lösung realisiert werden, wie wir sie von den führenden Anbietern tagtäglich nutzen und im Idealfall auch erfolgreich in Konkurrenz zu den bestehenden Systemen treten.

Das angesprochene Berechtigungszertifikat kann unterschiedlich ausprägt sein. Im Sinne einer spezifischen, eingeschränkten Datenübertragung eignen sie sich nicht, weil das Zertifikat unterschiedliche Facetten eines Dienstes abdecken muss und die Summe aller Subsets im Zertifikat abgebildet ist. Mit der Bereitstellung des Zertifikats wären die Nutzer:innen auf das Wohlverhalten des Anbieters angewiesen, dass dieser nur die benötigten Daten herunterlädt.

Eine andere Form von Berechtigungszertifikaten wäre das temporäre Hinterlegen bei einem Dienst. Dies würde eine sehr hohe Nutzerfreundlichkeit bedeuten, jedoch mit der Gefahr des Missbrauchs, wenn auf das Endgerät der Nutzer:innen zugegriffen werden kann. Dieses Risiko müsste transparent dargestellt und temporär begrenzt werden.

Frage 17

Wie kann aus Ihrer Sicht die Benutzerfreundlichkeit bei digitalen Identitäten noch besser berücksichtigt werden?

Um eine hohe Akzeptanz und Verbreitung bei den Bürger:innen und den Anwender:innen zu bekommen, ist die Benutzerfreundlichkeit bei digitalen Identitäten in den Mittelpunkt zu stellen, ohne dabei Sicherheitsaspekte zu vernachlässigen. Wie in den unterschiedlichen Fragen bereits dargestellt, ist dies aktuell nicht gegeben.

Wie in der Antwort auf Frage 1 dargelegt, ist die Benutzerfreundlichkeit der AusweisApp2 im direkten Vergleich zu Angeboten wie IDnow eID oder Nect Ident schwächer. Die größte Hürde ist derzeit jedoch die Nutzung am PC/Laptop. Obwohl die digitalen Verwaltungsdienste für mobile Geräte aufgrund der Nachfrage der Bürger:innen ausgebaut werden, sind die digitalen Verwaltungsverfahren derzeit in erster Linie für die Nutzung von Webbrowsern auf PCs/Laptops und nicht für mobile Geräte wie Tablets oder Smartphones konzipiert. Für die Nutzung am PC/Laptop ohne eigenen Kartenleser muss die AusweisApp2 sowohl am PC/Laptop als auch auf dem Smartphone installiert und gestartet sein und das Smartphone mit dem PC/Laptop gekoppelt werden

Die Vielzahl an Projekten ID-Wallet-App[39], Smart-eID[40], AusweisApp2[41] oder auch AUTHADA App[42] führen zu einem schwer nachvollziehbaren Bild und sollten daher möglichst reduziert und gemeinsam vermarktet werden.

Regelmäßige erfolgreiche Nutzung von digitalen Services trägt zum Vertrauensaufbau bei. Eine flächendeckende Integration von digitalen Services im öffentlichen Sektor und der Privatwirtschaft ist dementsprechend, ebenso wie der fortlaufende Ausbau der Services wie bspw. Sichtausweise am Smartphone oder eine elektronische Zustellung, notwendig.

Europäische Ebene

Frage 18

Wie bewerten Sie die Beratungen und Diskussionen um die eIDAS Verordnung auf europäischer Ebene? An welcher Stelle der VO müsste nachgebessert werden?

Insbesondere die dominierenden Wallet-Überlegungen sind sowohl technisch als auch organisatorisch sehr ambitioniert, dabei technisch fokussiert und mit zahlreichen Annahmen zum Bedarf der Bürger:innen aufgeladen, die bisher nicht überprüft wurden. Somit besteht die Gefahr einer Regulierung, die am Bedarf der Bürger:innen vorbeigeht. Daher wäre es empfehlenswert, zum jetzigen Zeitpunkt Usecases aus unterschiedlichen Ländern zu erheben, die sich am Bedarf der Büger:innen orientieren. Darauf aufbauend sollte eine

[39] https://www.bundesregierung.de/breg-de/suche/e-id-1962112 ist aktuell nicht installierbar und wurde aus den APpp Stores entfernt.
[40] https://www.personalausweisportal.de/SharedDocs/downloads/Webs/PA/DE/informationsmaterial/weiterefuehrendes-material/Handlungsleitfaden_Integration_Smart-eID_Nutzerkonto.pdf;jsessionid=8985328C891210D01D163E8119C76EE9.1_cid373?__blob=publicationFile&v=10
[41] https://www.ausweisapp.bund.de/home/
[42] https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/online-ausweisen/software/software-node.html#doc14626372bodyText3 und dem Produkt https://authada.de

Ableitung der technischen Konzepte und wiederum darauf aufbauend die rechtlichen Ableitungen erfolgen – siehe dazu auch die Antwort zu Frage 21.

Die in dem Entwurf der zukünftigen eIDAS-Verordnung vorgesehene hohe Anzahl von Rollen erhöht die Komplexität im Zusammenspiel zwischen Wallet, Vertrauensdiensteanbieter und den Quellregistern der Mitgliedstaaten, auf welche durch die Vertrauensdiensteanbieter direkt zugegriffen werden können soll. Mit der Implementierung der zusätzlichen Schnittstellen sind hohe Aufwände verbunden, die in vielen Mitgliedstaaten über Registerbussysteme und die Übergabe an den eIDAS-Knoten mit geringem Aufwand lösbar sind.

Frage 19

Wie positionieren Sie sich zur Frage, ob es eine einheitliche technische Lösung geben soll, oder (lediglich) einheitliche Standards zur Sicherstellung der Interoperabilität?

Eine einheitliche (und damit einzige) technische Lösung ist stets riskant: Stellt sie sich als fehlerhaft heraus, kann es zu umfassender Nichtverfügbarkeit der damit realisierten Dienste kommen. Die daraus resultierenden Probleme hat erst kürzlich in einem vergleichbaren Fall der tagelange Ausfall der Verifone-Terminals zum Bezahlen mit der EC-Karte gezeigt. Falls es gelingen sollte, eine einheitliche Lösung oder auch nur wesentliche Komponenten davon anzugreifen bzw. zu unterwandern, besteht ein hohes europäisches Systemrisiko.

Dieses Risiko kann gerade in Europa über die Mitgliedsstaaten und dank einer dezentral verteilten Architektur minimiert werden und steht daher nicht einer einheitlichen Europäischen eID entgegen, die als Standard-Anwendung allen europäischen Büger:innen zur Verfügung steht. Dieser Ansatz stand und steht auch immer wieder im Raum. Diesem wird entgegengehalten, dass Identitäten unter die nationalstaatliche Kompetenz fallen, die Mitgliedstaaten bereits hohe Investments getätigt haben und in einigen Mitgliedsstaaten bereits eine hohe Verbreitung und Nutzung vorliegt. Aus diesen Gründen ist eine Neukonzeption auf europäischer Ebene als sehr unwahrscheinlich einzustufen. Zusätzlich wäre dies ein IT-Projekt in erheblicher Dimension und somit einem Risiko des Scheiterns verbunden. Insbesondere der öffentliche Sektor hat diesbezüglich wenig positive Projekte aufzuzeigen, die in Zeit und Budget umgesetzt wurden.

Der eingeschlagene Weg der wechselseitigen Anerkennung über eIDAS erscheint in Anbetracht der Rahmenbedingungen als der geeignetste, trotz der Kompromisse, die in der Usability der Auswahl des jeweiligen nationalen eID-Dienstes gemacht werden müssen.

Verknüpfend zur Frage 23 wäre auf längere Sicht eine Prüfung denkbar, inwieweit nicht ein einheitliches eID-Protokoll, das über ETSI oder W3C entwickelt wird, und schrittweise in die nationalen eID Lösungen integriert werden könnte.

Eine Standardisierung der Sichtausweise in digitaler Form (Digitaler Ausweis in der Wallet) ist, für die gängigen Ausweise wie Personalausweis, Führerschein, Fahrzeugpapiere, etc., dringend zu empfehlen.

Frage 20

Wie schätzen Sie die Verhandlungen zur eIDAS-Verordnung im Kontext der deutschen eID-Strategie ein? Wie wird beides zeitlich aufeinander abgestimmt?

Aufgrund der generellen Fragestellungen zur deutschen eID-Strategie und -Architektur könnten in einer grundsätzlichen Neukonzeption der deutschen eID, die europäischen Dimensionen – sowohl strategisch als

auch in der technischen Architektur und unter der Voraussetzung, dass die Neukonzeption zeitnahe gestartet und umgesetzt wird – gut berücksichtigt werden.

Frage 21

Wie bewerten Sie den Plan der EU KOM, in sogenannten „Large Scale Pilots" die „European Digital Identity Wallet" zu testen? Wie schätzen Sie die Chancen ein, dass in jenen Pilots Standards – auch zum Datenschutz und der IT-Sicherheit gesetzt – werden?

Die bisherigen Large Scale Pilots haben zum überwiegenden Teil technische und organisatorische Grundlagen zur Interoperabilität von digitalen Verwaltungsverfahren beigetragen. Unter anderem wurden auch die Grundlagen für die wechselseitige Nutzung der europäischen eID-Systeme darüber erarbeitet. Insofern kann ein eigenes Large-Scale-Pilot-Projekt sich eignen, Wallet-Usecases aus Sicht der Bürger:innen zu entwickeln und darauf aufbauend die Standardisierungen vorzunehmen; allerdings werden die Ergebnisse in der Diskussion zur Verordnung nicht mehr berücksichtigt werden können. Ganz generell ist über die Einführung der „Digital Identity Wallet" eine stärkere Standardisierung zu erwarten, wie beispielsweise auch bei Fernsignaturen, die in Wallets über eine standardisierte Schnittstelle miteingebunden werden können. Standardisierung kann sowohl positive Wirkungen auf die Sicherheit haben als auch zu einem Mehrwert für die Nutzer:innen - über Integration weiterer Services – führen, somit bestehen gute Chancen, Erkenntnisse zu Datenschutz und IT-Sicherheit gewinnen zu können.

Frage 22

Auf europäischer Ebene wird darüber diskutiert, die technische Ermöglichung von Zero-Knowledge-Proofs (ZKP), also sich rechtssicher auszuweisen ohne Daten preiszugeben, als verpflichtenden Standard in die eIDAS-VO aufzunehmen. Wie bewerten Sie das?

Zero-Knowledge Proofs ermöglichen ein hohes Maß an Datensparsamkeit und sind daher unter Datenschutzgesichtspunkten oft erstrebenswert. Es gibt gut funktionierende Beispiele für ZKPs, allerdings sind häufig kontextspezifische Daten oder Methoden erforderlich. Es kann derzeit nicht davon ausgegangen werden, dass in absehbarer Zeit für alle erstrebenswerten Einsatzfälle eine massentaugliche Lösung verfügbar sein wird. Daher erscheint es zum jetzigen Zeitpunkt allenfalls möglich, ganz konkrete ZKPs für ganz konkrete Kontexte verpflichtend zu machen (weil für andere Kontexte evtl. noch gar keine, keine sichere oder keine wirklich praktikable Lösung existiert).

Frage 23

Welche Rolle spielen aus Ihrer Sicht gemeinsame internationale Standards im Hinblick auf die Interoperabilität von eID-Lösungen?

Interoperabilität mit privatwirtschaftlichen Lösungen würde die Benutzerfreundlichkeit und damit auch die Akzeptanz staatlicher Lösungen erhöhen. Allerdings besteht zwischen den führenden digitalen Plattformen keine hohe Interoperabilität, sondern der Anspruch die jeweils eigene eID-Lösung möglichst marktdominierend zu positionieren. Insofern ist noch nicht absehbar, wie sich dieses gesamte Feld der eID-Services entwickeln wird.

Zwischen den EU-Mitgliedsstaaten wurde über die Wechselseitige Anerkennung und Klassifizierung der nationalen eIDs ein Minimum von Interoperabilität hergestellt, ohne in die unterschiedlichen nationalen Ansätze zu stark einzugreifen. Nach mehr als 10 eIDAS-Verordnungen finden sich die ersten positiven

Entwicklungen. Inwieweit dies aber eine hohe Verbreitung erhält, ist weiterhin offen und hängt natürlich sehr stark vom Erfolg der einzelnen nationalen eID-Lösungen ab.

Ganz grundsätzlich ist allerdings ein Wettbewerb zwischen privatwirtschaftlichen und staatlichen Lösungen zu erwarten bzw. ist dieser bereits vorhanden. Wie in den vorhergehenden Fragen aufgezeigt wurde, gibt es sowohl internationale als auch nationale Anbieter auf dem eID-Markt. Einige deutsche Anbieter bieten Lösungen an, die den Personalausweis in ihren Registrierungsprozess integrieren und eine wesentlich höhere Benutzerfreundlichkeit bieten als die aktuelle staatliche deutsche eID-Lösung und sich auch aus der Perspektive der Service-Anbieter einfacher in bestehende Internetservices integrieren lassen.

Auf der technischen Ebene zu einzelnen Sicherheitsstandards oder auch Authentifizierungs-Protokollen, haben sich Standards entwickelt wie in den Fragen 2 und 4 festgehalten. Diese werden von den führenden Internetdienste-Anbietern, wie OpenID Connect, OAuth 2.0 oder FIDO, eingesetzt. Diese werden in der aktuellen eID-Architektur noch nicht ausreihend berücksichtigt.

Frage 24

Ein Kritikpunkt, ist die Verpflichtung der Unternehmen oder relying Parties, die EUid-Wallets als Identifizierungsmittel zu akzeptieren. Dies sei eine größere Herausforderung, da sie bisher keine hoheitlichen Identifizierungsprozesse innerhalb ihrer Services vorsehen. Wie schätzen Sie diesen Punkt ein? Ist die Kritik berechtigt? Welche Folgen hat diese Regelung und wie könnte eine Alternative aussehen?

Siehe Antwort auf Frage 26.

Frage 25

Die Novellierte eIDAS-Verordnung sieht vor, dass qualifizierte Webseitenauthentifizierungszertifikate automatisch von Webbrowsern anerkannt und der Vertrauensstatus visualisiert dargestellt werden muss. Die Kritik ist, dass die Unabhängigkeit von Webbrowsern und die von Unternehmen entwickelten Sicherheitsvorkehrungen durch diese Regelungen beeinträchtigt werden. Aus diesem Grund soll Artikel 45 eIDAS-VO gestrichen werden. Teilen Sie die Kritik und was wären die Folgen einer automatischen Anerkennung?

Die Kritik war und ist nachvollziehbar, daher wäre die Streichung des Artikels 45 als positive Anpassung zu bewerten.

Frage 26

Der Artikel 12b des Kommissionsentwurfs zur eIDAS-Verordnung sieht vor, neben den großen Plattformbetreibern auch zahlreiche Branchen zur Akzeptanz der EU-Wallet zu verpflichten. Wie schätzen Sie diese Verpflichtung ein? Aktuell wird auf europäischer Ebene diskutiert, ob es nur eine staatliche Wallet geben soll oder verschiedene Wallets, die zertifiziert sind. Welchen Weg bevorzugen Sie und warum?

Die verordnete Verpflichtung der Wirtschaft, eine für hoheitliche Zwecke entwickelte Lösung zu unterstützen, ist unserer Einschätzung nach keine zielführende Strategie, um hoheitlichen Lösungen zu Akzeptanz, Verbreitung und Nutzungszahlen zu verhelfen. Wenn ein Mehrwert für die Bürger:innen angestrebt wird,

sollten gemeinsam mit der Wirtschaft Lösungsansätze entwickelt werden, die den Anforderungen aller Seiten gerecht werden. Diese Lösungsansätze sollten so modular und z. B. nach Sicherheitsanforderungen kombinierbar sein, dass unangemessener Aufwand für die Wirtschaft und eine zu weitgehende Datenpreisgabe der Bürger:innen effektiv vermieden werden. Siehe dazu auch Frage 18 mit kritischen Aspekten, wie den zahlreichen Annahmen, den fehlenden Usecases und der fehlenden Involvierung der Bürger:innen und der Wirtschaft.

Frage 27

Gemäß Art. 6a des Kommissionsentwurfs soll die Benutzung der Europäischen Wallet für natürliche Personen kostenfrei sein. Auf welche Aspekte der Nutzung einer Wallet sollte sich diese Vorgabe beziehen?

Im Sinne der Regulierung einer europäischen Wallet sollte der Fokus primär auf staatlich verantwortete Attribute gerichtet sein, die sich bspw. als Sichtausweise auf mobilen Endgeräten darstellen lassen können, bzw. deren Datenpunkte in zivilrechtliche Prozesse integriert werden können, unter der Freigabe durch die natürliche Person. Inwieweit natürliche Personen (Bürger:innen) daran Interesse haben, private Attribute aus Gesundheit, Finanz, Versicherungen und sozialen Netzwerken in eine staatliche betriebene oder beauftragte Wallet zu speichern, sollte vorab noch untersucht werden; die Wahrscheinlichkeit eines hohen derartigen Bedarfs wird jedoch als gering eingestuft.

Die kostenfreie Nutzung durch die natürliche Person ist nachvollziehbar, weil der wirtschaftliche Mehrwert der staatlichen verifizierten Daten bei den Unternehmen entsteht und somit die Geschäftsmodelle im B2B verortet werden sollten.

Frage 28

Die Mitgliedsstaaten haben möglicherweise unterschiedliche Interpretationen bestimmter Attribute der eID, etwas was Geschlecht oder Heiratsstatus angeht. Wird ein von einem Mitgliedsstaat ausgegebener Wert eines Attributs immer von den anderen anerkannt werden? Wie wird das durchgesetzt werden? Falls nein, wird ein Rechtsbehelf vorgesehen? Wie sollen die Semantiken der Typen und Werte von Attributen standardisiert?

Insbesondere zur Umsetzung von grenzüberschreitenden Once-Only-Prinzipien sind europaweite Standardisierungen auf Attributsebene notwendig. Eine EU-weite Standardisierung jeglicher Attribute in anderen Sprachen gibt es derzeit noch nicht, die Arbeiten daran haben aber begonnen. Die Aufgabe ist eine langfristige, da es unterschiedliche Formate und Interpretationen von Begrifflichkeiten gibt. So wird beispielsweise der Begriff „Unbescholtenheit“ in vielen Mitgliedstaaten unterschiedlich definiert und nachgewiesen. Eine Mindestliste der Attribute, die standardisiert werden sollen, ist im Annex 6 des Vorschlags der Kommission zur Änderung der eIDAS-Verordnung[43] genannt. Innerstaatlich sind die Standardisierungen einfacher, weil bekannt ist, welches Format Postleitzahlen haben oder ob diakritische Zeichen in einem Strafregister verwendet werden. Orientierungshilfe könnte bei einigen Attributen aus ICAO-Vorgaben für Reisedokumente übernommen werden.

[43] https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:52021PC0281