Identity Economy – Report

European Digital Identity Wallet (EUDI)

Autor: Ralf Keuper

August 2023

Inhaltsverzeichnis

Einleitung *3*

Umsetzung der eIDAS 2.0 Veordnung – Aktueller Stand *5*

Architektur der EUDI-Wallet **6**

Lebenszyklus einer EUDI-Wallet-Instanz **6**

Anwendungsfälle **7**

Konsultationsprozess des BMI **8**

Organisationsidentitäten **9**

Selbstsouveräne Digitale Identitäten / Blockchain *9*

Innopay **9**

Position des Bundesministeriums des Inneren und für Heimat **11**

BSI **12**

eID und SSI **13**

Zero Knowledge Proof **17**

Large – Scale Pilots *17*

NOBID **18**

Potenzial – Pilotprojekte für das Konsortium für EUid-Brieftasche **19**

EWC – EU Digital Identity Wallet Consortium (EU Digital Identity Wallet Consortium) **19**

DC4EU – Digitale Zertifikate für Europa **19**

Feldtests **20**

Digitaler Euro *20*

Potenzielle Risiken für den Erfolg der EUDI *22*

Schlussbetrachtung und Ausblick *25*

Einleitung

Die European Digital Identity Wallet (EUDI) ist eine digitale Brieftasche, die EU-Bürgern, Gebietsansässigen und Unternehmen zur Verfügung stehen wird. Sie ermöglicht es dem Einzelnen, seine persönlichen Informationen und Dokumente in einem digitalen Format sicher zu speichern und zu verwalten. Die Brieftasche kann für öffentliche und private Online- und Offline-Dienste in der gesamten EU verwendet werden

Die Europäische Geldbörse für digitale Identitäten soll allen EU-Bürgern und -Einwohnern weiterhin ein praktisches Instrument an die Hand geben, mit dem sie sich leicht ausweisen und bei Bedarf persönliche Informationen bestätigen können

Zu den Vorteilen der Europäischen Digitalen Identitätsbörse gehören:

1. Vereinfachter Zugang zu Online- und Offline-Diensten in der gesamten EU
2. Erhöhte Sicherheit und Schutz der persönlichen Daten
3. Verringerung des Verwaltungsaufwands und des Papierkrams
4. Verbesserte grenzüberschreitende Mobilität und leichtere Identifizierung

Da die digitale Brieftasche sensible Informationen enthält, werden Fragen der Sicherheit und des Datenschutzes bis zum heutigen Tag kontrovers diskutiert. Die Kritiker befürchten, dass die Wirtschaft durch die EUDI-Wallet Zugang zu staatlich verifizierten Identitätsdaten bekommt. Andere wiederum warnen vor einem Aus- bzw. Umbau der EUDI-Wallet zu einem Überwachungsinstrument des Staates, ähnlich wie der Social Credit in China. Auf Widerstand stößt weiterhin die Verbindung der EUDI-Wallet mit einem digitalen Euro, was die Machtbefugnisse des Staates und der Zentralbanken deutlich erweitern könnte[1].

Wirtschafts- und Bankenverbände, wie Bitkom und der DSGV, begrüßen die Einführung der EUDI-Wallet, haben aber noch einige Änderungswünsche. Keinesfalls nur Zaungäste sind die großen Technologiekonzerne Apple und Google, die bereits selbst digitale Brieftaschen im Angebot haben, in die staatliche

[1] Offener Brief der Zivilgesellschaft zur eIDAS-Reform

Ausweisdokumente hinterlegt und zur Identifizierung verwendet werden können. Da für die digitale Brieftasche ein mobiles Endgerät fast schon zwingend ist, führt an Apple und Google kaum ein Weg vorbei. Entscheidend ist die Frage, ob und inwieweit vor allem Apple bereit ist, sein mobiles Betriebssystem und das Secure Element für die EUDI-Wallet zu öffnen.

Zu lösen ist auch die Frage, wie die unterschiedlichen Auslegungen der eIDAS 2.0 – Verordnung in den EU-Ländern in Fragen des Sicherheitsniveaus angeglichen werden können.

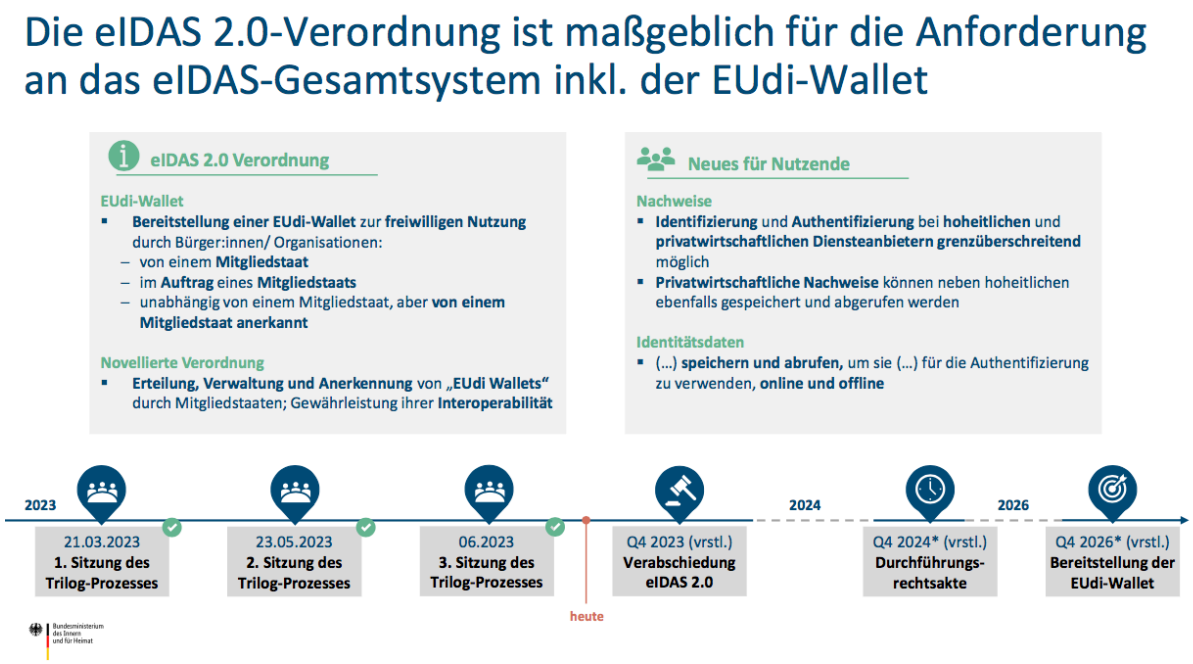
Die Idee einer persistenten Personenkennziffer ist dagegen vom Tisch.

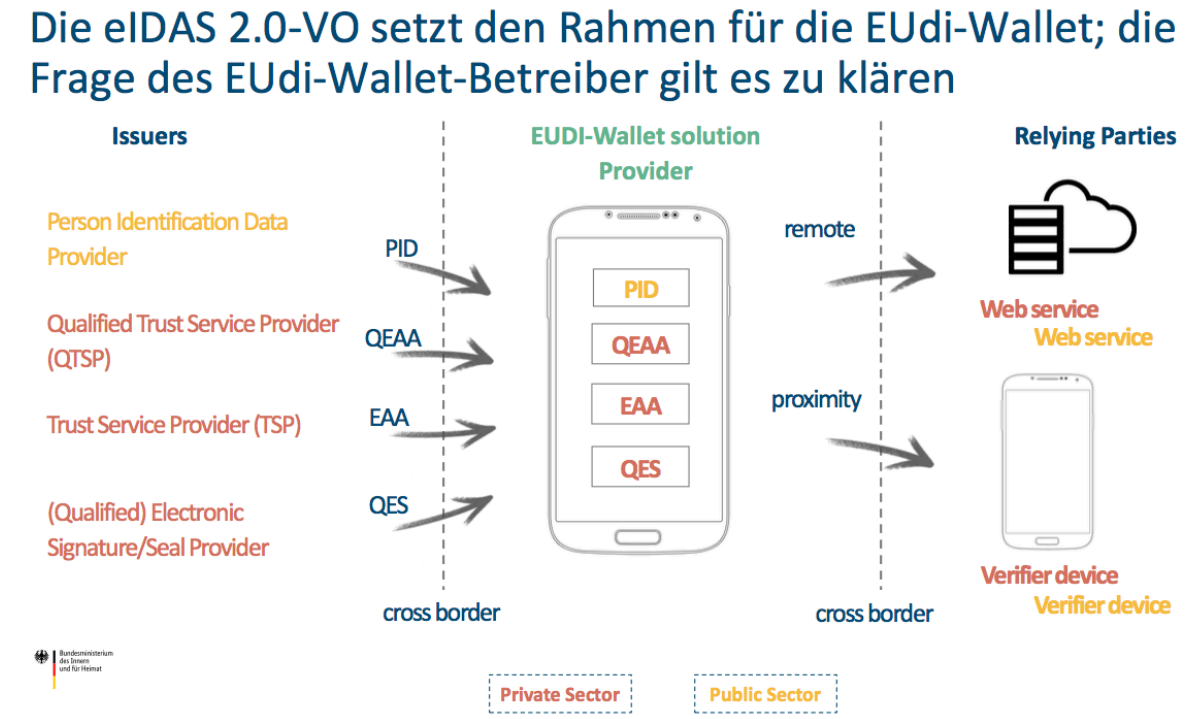
Inzwischen hat die EU die ersten Feldtests zur Erprobung der EUID-Wallet gestartet[2].

[2] Feldtests zu digitalen Identitäten in der EU gestartet

Umsetzung der eIDAS 2.0 Veordnung – Aktueller Stand

Die eIDAS 2.0 – Verordnung, die maßgeblichen Einfluss auf die Gestaltung der EUid hat, befindet sich momentan, d.h. im August 2023, in der Phase unmittelbar vor der Verabschiedung (siehe Grafik).

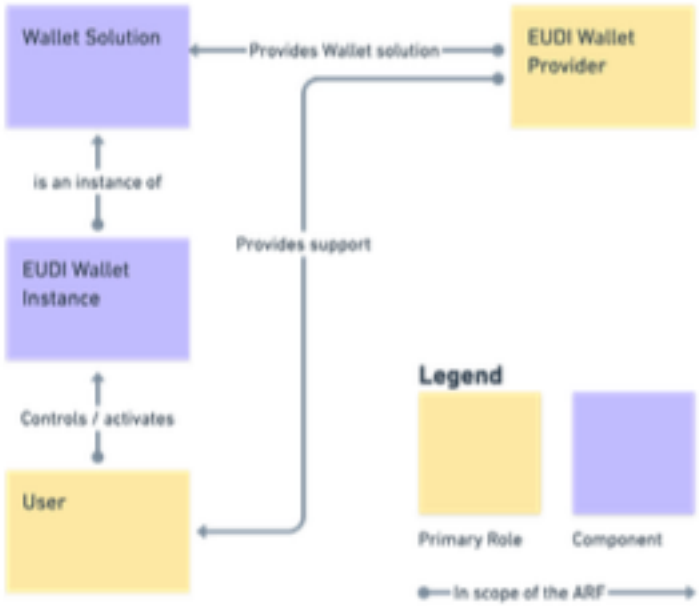




Die Bereitstellung der EUid-Wallet ist für das 4. Quartal 2026 geplant.

Architektur der EUDI-Wallet

Die Architektur der EUDI-Wallet unterscheidet zwischen der EUDI-Wallet -Instanz und EUDI-Wallet-Lösung. Die EUDI-Wallet-Lösung ist das gesamte Produkt und/oder der Dienst eines EUDI-Wallet-Anbieters. Eine EUDI-Wallet-Instanz ist eine persönliche Instanz der EUDI-Wallet-Lösung, die dem Nutzer gehört und von ihm kontrolliert wird[3].



Objektmodell EUDI-Wallet

Es ist keine bestimme Variante vorgeschrieben, sodass eine EUDI-Wallet-Instanz je nach Implementierung aus einer einzigen mobilen Anwendung oder aus einer Reihe von lokalen und entfernten Komponenten bestehen kann, die einem bestimmten Nutzer zur Verfügung stehen.

Lebenszyklus einer EUDI-Wallet-Instanz

Eine EUDI-Wallet-Instanz beginnt ihren Lebenszyklus auf der Grundlage einer gültigen EUDI-Wallet-Lösung. Der EUDI-Wallet-Anbieter stellt dem Nutzer eine

[3] **Architektur und Referenzrahmen für die EUid-Brieftasche**

EUDI-Lösung zur Verfügung, die nach der Installation und Aktivierung durch den Nutzer als betriebsbereite Wallet-Instanz betrachtet wird. Je nach Ausprägung und Implementierung kann die Bereitstellung einer Instanz mehrere Aktionen erfordern, z.B. die Installation und Initialisierung im Falle einer mobilen EUDI-Wallet. Eine solche EUDI-Wallet-Instanz könnte bereits für nicht-EUDI-spezifische Funktionen verwendet werden, z.B. zur Speicherung von Kundenkarten oder nicht personalisierten Zugfahrkarten oder anderen Bescheinigungen, die keine Bindung an eine gültige PID erfordern.

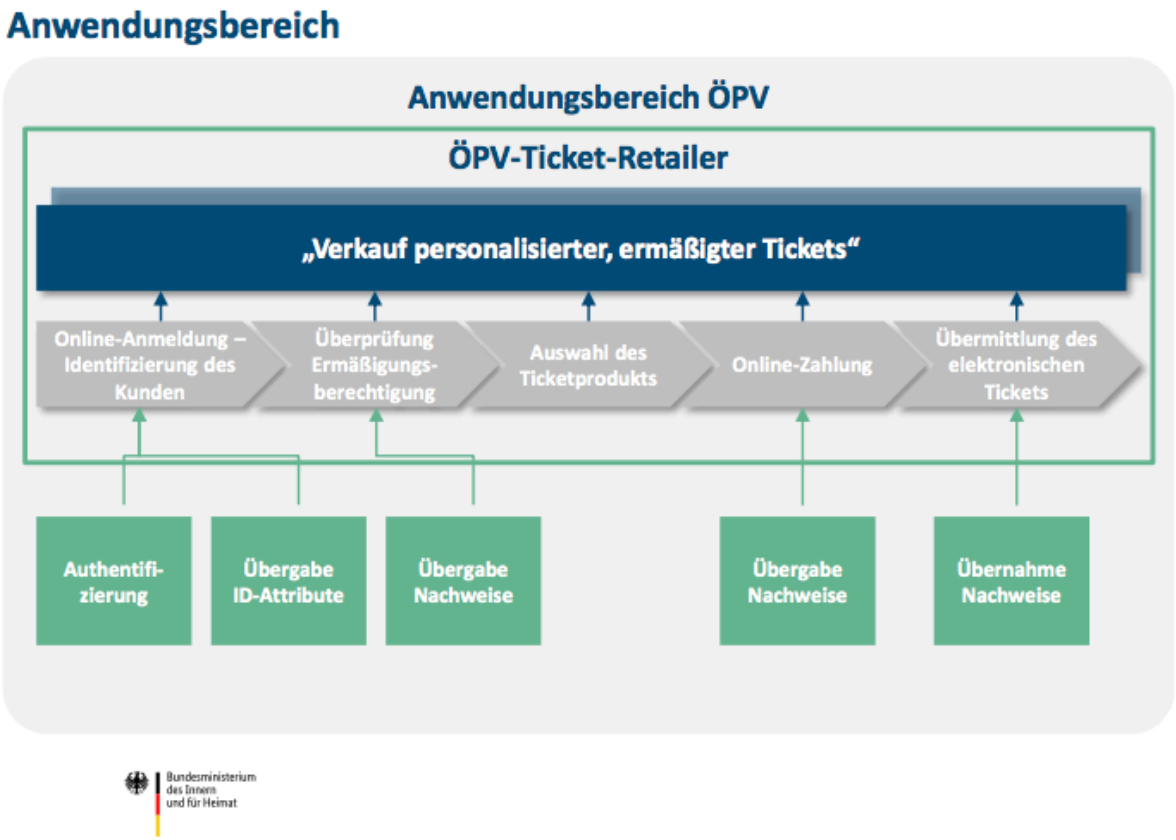
Sobald eine EUDI-Wallet-Instanz initialisiert ist, ist sie gültig, d.h. sie wird von einem PID-Provider erkannt und verfügt über einen gültigen PID-Satz. Wenn die PID abläuft oder widerrufen wird, ist die EUDI-Wallet nicht automatisch unbrauchbar, sondern ihr Status wird lediglich auf betriebsbereit zurückgestuft. Dies kann die Gültigkeit eines (Q)EAA oder eines Zertifikats für QES beeinflussen.

Anwendungsfälle

Die eIDAS-Expertenrunde der EU hat einige typische Anwendungsfällt der EUDI-Wallet definiert.

- Sichere und vertrauenswürdige Identifizierung für den Zugang zu Online-Diensten
- Mobilität und digitaler Führerschein
- Gesundheit
- Bildungsnachweise und berufliche Qualifikationen
- Digitales Finanzwesen
- Digitale Reiseausweise

Das Projektteam für die Umsetzung des eIDAS-Gesamtsystems hat zur Veranschaulichung den Anwendungsfall „Verkauf personalisierter, ermäßigter Tickets“ entworfen (siehe Grafik).

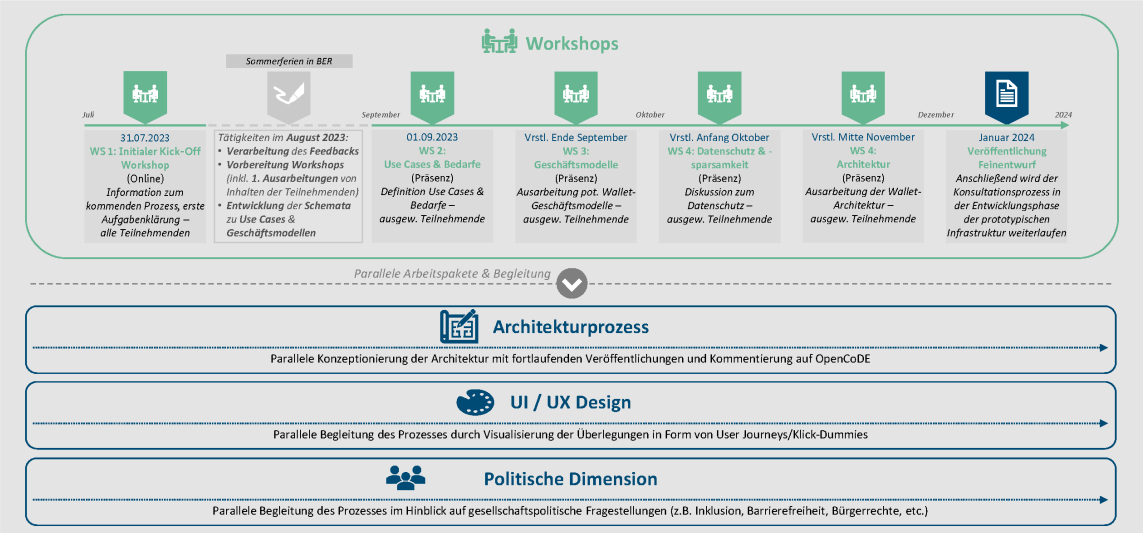


Konsultationsprozess des BMI

Das BMI hat einen öffentlichen Konsultationsprozess zu einem Konzept der deutschen Ausgestaltung von EUDI-Brieftaschen gestartet. Bis zum 30.06.23 hatten Personen, Unternehmen, Organisationen und Institutionen Gelegenheit, ihre Position darzulegen.
Die Positionspapiere stehen mittlerweile unter https://gitlab.opencode.de/bmi/eidas2/-/tree/main/Positionspapiere zur Einsicht und/oder zum Download zur Verfügung.
Der Kick Off fand am 31.07. statt.

Über den weiteren Verlauf des Konsultationsprozesses gibt die folgende Grafik Auskunft.

Zeitleiste der kommenden Monate im Konsultationsprozess



Organisationsidentitäten

Einige in den Konsultationsprozess eingebundene Akteure, wie Bitkom, fordern die Einbeziehung von Organisationsidentitäten in die Erarbeitung einer eIDAS 2.0-konformen Infrastruktur. Bei Bitkom ist man überzeugt, dass Organisationsidentitäten in Zukunft einen Großteil der Use Cases ausmachen werden. Daher müssten auch Organisationswallets mit einer entsprechenden Zertifizierung Teilnehmer des Ökosystems sein.

Selbstsouveräne Digitale Identitäten / Blockchain

Aktuell sind die Chancen eher gering, dass die EUDI-Wallet mit Selbstsouveränen Digitalen Identitäten kombiniert wird.

Innopay

Nach Ansicht von Raluca Ochiana von Innopay kann die EUDI nicht alle SSI-Prinzipien erfüllen]. So könne der Grundsatz der Transparenz verfehlt werden. Dieser verlangt, dass die Systeme und Algorithmen frei, quelloffen, bekannt und möglichst unabhängig von jeder Architektur sind. Der Grundsatz verlangt auch, dass die Verwaltung und die Aktualisierungen transparent sind. Der im Vorschlag beschriebene allgemeine technische Rahmen werde wahrscheinlich transparent

sein, aber da er auch Marktteilnehmern die Möglichkeit geben soll, ihre Dienste anzubieten, bleibe abzuwarten, ob Systeme, Algorithmen, Verwaltung und Aktualisierungen aller einzelnen Wallets vollständig transparent sein werden. Abzuwarten bleibe auch, inwieweit die Grundsätze der Übertragbarkeit von der EU-Wallet erfüllt werden. Der Grundsatz verlangt, dass Informationen und Dienste über die Identität übertragbar sein müssen und dass die Identitäten nicht von einer einzelnen dritten Stelle gehalten werden dürfen. Die vorgeschlagene Verordnung erlaubt es den Mitgliedstaaten, ihre eigene, von der Regierung betriebene EU-Wallet zu entwickeln und zu implementieren oder eine externe Organisation.

Ebenso könne der Grundsatz der Kontrolle von der EU-Geldbörse nicht in vollem Umfang erfüllt werden. Der Grundsatz erfordert, dass der Nutzer die letztendliche Verfügungsgewalt über seine Identität hat, einschließlich der Möglichkeit, seine Identität zu verbergen. In allgemeinen, öffentlichen oder behördlich geprägten Anwendungsfällen ist dies unmöglich. Man denke nur an die Abgabe einer Steuererklärung, die Erhebung einer Strafanzeige, die Registrierung als Spender oder die Eröffnung eines Bankkontos. In diesen Fällen benötigt der Prüfer ein gewisses Maß an Sicherheit, und der Nutzer hat keine Kontrolle darüber, welche Attribute er angibt. In vielen europäischen Ländern gibt es eine zentrale Registrierung von Personen, die für viele dieser Anwendungsfälle genutzt wird. Für diese Anwendungsfälle gibt es auch rechtliche Verpflichtungen, die es dem Nutzer nicht erlauben, die letzte Autorität über seine Identität zu haben.

Gleiches gelte für den Grundsatz der Persistenz. Das Prinzip erfordert, dass ein Benutzer über seine Identität verfügen kann, wenn er möchte, dass Ansprüche im Laufe der Zeit geändert oder entfernt werden. Dies erfordert eine klare Trennung zwischen der Identität und ihren Ansprüchen. In vielen Anwendungsfällen in einem öffentlichen Umfeld, z. B. bei einer Steuererklärung, ist dies unmöglich. Die Steuerbehörde muss wissen, wer die jeweilige Steuererklärung abgegeben hat. Die Verfügung über die Identität sollte sich im Rahmen der gesetzlichen Bestimmungen bewegen. Ein Nutzer kann eine Vorstrafe nicht ungeschehen machen, weil er/sie vergessen werden möchte. Diese Anwendungsfälle erfordern sogar eine Beziehung zwischen der Identität und ihren Ansprüchen.

In einem öffentlichen Umfeld müssen Nutzer Identitätsattribute an vertrauende Parteien weitergeben, und eine strikte Trennung zwischen der Identität und ihren Ansprüchen ist aufgrund rechtlicher Beschränkungen unmöglich. Aus diesem Grund müsse die EU Digital Identity Wallet die Ambitionen, dem Nutzer die Kontrolle zu geben, mit den Realitäten der öffentlichen Verwaltung in Einklang bringen. Wie dieses Gleichgewicht hergestellt wird, bleibe abzuwarten und werde von den Entscheidungen abhängen, die bei der Überarbeitung von eIDAS noch getroffen werden müssen.

Position des Bundesministeriums des Inneren und für Heimat

Das Bundesministerium des Inneren und für Heimat erteilt in dem Diskussionspapier Beyond EU Digital Identity Wallet - Diskussionspapier zur Erarbeitung einer prototypischen eIDAS 2.0- konformen Infrastruktur für Digitale Identitäten in Deutschland dem Einsatz von Distributed Ledger Technologies eine Absage:

Mit dem GovLabDE Digitale Identitäten hat die Bundesregierung den interministeriellen Austausch zu digitalen Identitäten institutionalisiert. In diesem Rahmen haben sich die Ressorts auf eine gemeinsame Zieldefinition verständigt, welche die Anforderungen an die Realisierung von Lösungen im Bereich der digitalen Identitäten beschreibt. So sollen Lösungen unter dem Leitsatz „Privacy und Security by Design“ entwickelt, eine breite Nutzbarkeit der Öffentlichkeit sichergestellt und Implementierungen als Open Source bereitgestellt werden, u.a. um Nachnutzungsmöglichkeiten einzuräumen. Ansätze, die auf Distributed Ledger Technology (DLT) beruhen, werden in der Zieldefinition für Umsetzungen von Lösungen im Bereich der Digitalen Identitäten auf absehbare Zeit ausgeschlossen.

Das hat in der Krypto-Szene verständlicherweise für Aufregung gesorgt. "*Die anscheinend vorherrschenden Vorurteile und Ängste des BMI lassen die Blockchain-Strategie der ehemaligen Bundesregierung wie einen Witz aussehen. So hatte man in der Blockchain-Strategie von 2019 auch die Erprobung der DLT-Technologie für*

die Verwaltung sowie öffentlichen Register vorgesehen. Von dieser Aufgeschlossenheit scheint man inzwischen nicht mehr viel zu halten"[4]

Ganz so überraschend kommt die Positionierung der aktuellen Bundesregierung indes nicht. Bereits die alte Bundesregierung äußerte sich zu den Einsatzmöglichkeiten der Blockchain-Technologie zurückhaltend, wie im Jahr 2018 in einer Antwort auf eine Anfrage der Bundestagsfraktion der Grünen[5]:

Eine wesentliche Grundlage für die Blockchain-Infrastruktur, in der „SmartContracts" zur Anwendung kommen, sind rechtssichere digitale Identitäten, sowohl für natürliche Personen als auch für Maschinen und Geräte. Bislang gibt es eine Reihe von Pilotprojekten in diesem Bereich, die aber nicht miteinander interoperabel sind. Es gibt derzeit auch noch keinen akzeptierten Standard für digitale Identitäten. Die Bundesregierung wird im Rahmen der Erarbeitung der Blockchain-Strategie prüfen, inwiefern sie über die Vernetzung der „Blockchain-Community", über Pilotprojekte im eigenen Zuständigkeitsbereich und über den Austausch auf europäischer und internationaler Ebene an der Entwicklung von Standards für digitale Identitäten mitwirken kann.

Zwar präsentierte die Bundesregierung bzw. das Bundesministerium für Finanzen im Jahr 2019 eine Blockchain-Strategie; die Vorbehalte in den Einrichtungen des Bundes blieben jedoch.

BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellte im Jahr 2020 fest, dass der Reifegrad der meisten Blockchain-Applikationen gering sei. In ihrem Eckpunktepapier Self Sovereign Identities hatte sich die Behörde bereits kritisch geäußert. Als Claudia Plattner als neue BSI-Chefin vorgestellt wurde, war die Hoffnung in der Kryptosezne auf einen Kurswechsel in Sachen Blockchain groß, galt sie doch als "Blockchain-Enthusiastin". In ihrer Zeit als CIO von DB Systel hatte

[4] Bundesregierung fordert Blockchain-Verzicht
[5] Blockchain und Distributed-Ledger-Technologien – Potenziale und Anwendungsfelder – Anfrage Fraktion BÜNDNIS 90/ DIE GRÜNEN an die Bundesregierung

Plattner sich für Selbstverwaltete Digitale Identiäten (SSI) auf Blockchain-Basis eingesetzt und einen Prototypen entwickelt.
Das BSI ist übrigens dem Bundesinnenministerium unterstellt. Im vergangenen Jahr bewertete die *Wissenschaftliche Arbeitsgruppe des Nationalen Cyber-Sicherheitsrates* die Verwendung der Blockchain bzw. von Distributed Ledger-Technologien für Selbstverwaltete Digitale Identitäten (SSI) kritisch[6]

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

eID und SSI

Daniela Pöhn, Michael Grabatin and Wolfgang Hommel formulieren die Frage*: Was kann man von erfolgreichen eID- und SSI-Projekten lernen, und was sollte beim Start neuer Projekte berücksichtigt werden?* Ziel ist es einen umfassenden Überblick zu geben, einschließlich einiger technischer Hintergründe und der Ableitung von Gestaltungsempfehlungen. Untersucht wurden 23-Lösungen aus allen Teilen der Welt.

Generell gilt bei der Einführung landesweiter Lösungen für das Identitätsmanagement: Um eine ID-Lösung erfolgreich einzuführen, muss sie einen

[6] Wissenschaftliche Arbeitsgruppe des Nationalen Cybersicherheitsrates betrachtet Blockchain für SSI skeptisch

bedeutenden Anteil unter den Nutzerinnen und Nutzern erreichen. Die Nutzerinnen und Nutzer werden jedoch die Lösungen nur dann annehmen, wenn genügend Online-Dienste bereitgestellt werden, wie in Estland, wo die Dienste im Zusammenhang mit elektronischen Behördendiensten weit verbreitet sind. In der Literatur werden für die breite Akzeptanz der eID in Estland die geringe Komplexität, Benutzerfreundlichkeit, Funktionalität, Bewusstsein, Vertrauen, Privatsphäre, Sicherheit, Kontrolle, Befähigung sowie Transparenz als Erfolgsfaktoren angeführt. Verschiedene Ansätze versuchen, die genannten Herausforderungen zu lösen, wie die SSI eIDAS Bridge], die derzeit im Rahmen des H2020 NGI ESSIF Lab-Projekts entwickelt wird. Dabei wird eIDAS als Vertrauensrahmen für das SSI-Ökosystem verfügbar gemacht]. Es ist jedoch auf eIDAS – Anwendungen beschränkt. Ein weiterer Ansatz ist die Vertrauensmanagement-Infrastruktur namens TRAIN[, die einen Vertrauensanker und Automatisierung bietet. TRAIN nutzt das globale Domain Name System (DNS) und basiert auf dem Projekt LIGHTest. Es stützt sich dabei auf zentralisierte Komponenten, was dem SSI-Paradigma bis zu einem gewissen Grad widerspricht.

Alternativ werden zwei Optionen beschrieben: (1) ein Web of Trust oder (2) ein hybrider Ansatz, in dem Zertifizierungsstellen und Behörden eine zentrale Rolle übernehmen.

Das SEAL-Projekt der Connecting Europe Facility (CEF) verknüpft Anmeldedaten und verwendet Proxies, um bestehende IDPs und SPs zu integrieren. Diese Proxys ermöglichen es, die bestehenden Systeme mit SSI zu nutzen, widersprechen aber gleichzeitig den Grundsätzen der SSI[6][7][8].

SSI-Systeme könnten mit qualifizierten eID-Daten angereichert werden, die aus bestehenden Quellen importiert werden. Ein solcher Ableitungsprozess muss die Daten transformieren und die Vertrauenswürdigkeit der Daten erhalten. Ein Vorschlag geht dahin, eine datenschutzfreundliche dezentrale eID-Ableitung für SSI zu implementieren, bei der Zwischenparteien nicht auf die reinen Benutzerattribute zugreifen können. Andere Autoren wiederum schlagen die Verwendung von IPv8 als Nachfolger von IPv4 und IPv6 vor, das Identitäten eng mit einer dezentralen Public-

Key-Infrastruktur (PKI) und einem anonymisierenden SSI-Overlay verbindet. Dieser Ansatz hat den Vorteil des Datenschutzes, während föderierte Infrastrukturen möglicherweise nicht mehr nutzbar sind.

Situation in Deutschland

Das Projekt OPTIMOS 2.0 stellt das Ökosystem für die mobile eID bereit, während das Projekt digitale Identitäten versucht, die App zu optimieren. Die mobile App AusweisApp2 kann verwendet werden, wenn das Smartphone mit Nahfeldkommunikation (NFC) ausgestattet ist. Die neue mobile eID-App wird derzeit (Oktober 2021) nur auf der Samsung Galaxy S20-Serie funktionieren, da dies bisher das einzige Gerät ist, das die Anforderungen an einen sicheren Chip für die mobile eID erfüllt.

In Deutschland hat sich das Vorzeigeprogramm Sichere digitale Identitäten zu einem Magneten entwickelt, da sich immer mehr Organisationen einem der ausgewählten Projekte anschließen. Dies könnte sogar Auswirkungen auf die Nachbarländer haben. Insbesondere IDunion und ONCE haben an Dynamik gewonnen, wenn man die ursprüngliche und aktuelle Liste der Partner betrachtet. IDunion konzentrierte sich ursprünglich auf die deutschen Bundesländer Nordrhein-Westfalen und Berlin und nutzte Hyperledger Aries und Konnektoren für OIDC, das Lightweight Directory Access Protocol (LDAP) und SAML. ONCE konzentrierte sich zunächst auf das Bundesland Hessen, sowie auf Städte und Kreise in Bayern und Nordrhein-Westfalen. Die drei Anwendungsfälle umfassen regionales E-Government, Mobilität sowie Hotel und Tourismus. Und nicht zuletzt sind mehrere private Initiativen und Projekte aktiv, darunter FIDES und lissi.

Fazit: Die SSI-Lösung muss bequem und vorteilhaft sein, d. h. sie muss genügend Dienste bieten, damit der Nutzer Vorteile aus der Nutzung zieht. Daher wird ein Gleichgewicht zwischen Benutzerfreundlichkeit und Sicherheit vorgeschlagen.

Gescheiterte Projekte

Allerdings wurden nicht alle früheren Projekte in die Produktion aufgenommen. ZugID in der Schweiz war ein digitaler, Blockchain-basierter Ausweis, der uPort

verwendet. Das Projekt wurde eingestellt, aber eine zukünftige Wiederverwendung der Ergebnisse könnte möglich sein. Am Ende hatten 267 Bürger eine digitale ID. Ein Grund für die geringe Zahl könnte die begrenzte Anzahl von Diensten sein. Im Endzustand waren Wahlen und Fahrradverleih die einzigen beiden verfügbaren Dienste. Die flämische Regierung hat sich aus dem Projekt Blockchain on the Move zurückgezogen. Infolgedessen haben die verbleibenden Initiatoren beschlossen, eine dritte Phase des Projekts nicht weiter voranzutreiben.

Die Autorin und die Autoren kommen angesichts dessen zu dem Schluss, dass ein offenes Umfeld für den Austausch und die Förderung wichtig ist. Bei einem Open-Source-Projekt können sich mehr Menschen beteiligen. Gleichzeitig ist dies jedoch keine Garantie für den Erfolg. Die Ressourcen sind ebenso wichtig. Wenn nur wenige Personen an den Projekten beteiligt sind, hat die Veränderung der Beteiligung eine größere Auswirkung. Außerdem sind Ressourcen im Sinne von Zeit, Hardware und Geld, um nur einige zu nennen, erforderlich. Da sich die SSI noch in der Entwicklung befindet, kann sich die Technologie ändern. Ein sinnvoller Weg ist der Aufbau einer technologieunabhängigen oder technologieneutralen sowie modulare Architektur, um Anpassungen im Falle unvorhergesehener Änderungen zu erleichtern.

Weitere Ergebnisse bzw. Erkenntnisse

Staatlich finanzierte Modelle helfen dabei, zusätzliche Dienste und Dienstleister anzubinden, was zu einem höheren Nutzen für die Endnutzer führt. Während mehrere eID-Lösungen auf SAML aufbauen, helfen die Protokolle OAuth 2.0 und OIDC bei der Integration von Diensten. Dokumentationen und veröffentlichte APIs führen wiederum zu einer einfacheren Initiierung. Ohne die Beteiligung der Nutzer sind eID-Lösungen reine Geldverschwendung. Sicherheit und Datenschutz sind gleichermaßen wichtig. Da unterschiedliche Attribute in jeder Föderation oder sogar in dem lokalen System verwendet werden, ist entweder eine minimale Liste von Attributen (siehe eIDAS) oder Schemata und Attributübersetzung, wie sie in eduGAIN angewendet werden, nötig. Die Gesetzgebung muss Hand in Hand mit der technischen Entwicklung gehen. Weitere wichtige Faktoren sind ausreichende Ressourcen und die Unterstützung durch das Topmanagement.

Die technische Auswahl sollte zukünftige Situationen und Entwicklungen so weit wie möglich antizipieren. Die Neuartigkeit der SSI ist eine Herausforderung, da die Protokolle und begleitenden Verfahren noch entwickelt und verbessert werden. Daher sind die technische Neutralität und der Austausch zwischen Projekten und Interessengruppen wichtig.

Die IT und damit auch das Identitätsmanagement entwickeln sich ständig weiter. Unabhängig von der eingeschlagenen Richtung, ob eIDs oder SSI, müssen die zugrundeliegenden Systeme aktualisiert werden und sich ebenfalls weiterentwickeln. Ein einziges großes Projekt reicht nicht aus: Es sind ständige Anstrengungen erforderlich.

Zero Knowledge Proof

Das EU-Parlament hat die ZK-Proof-Technologie (zero-knowledge proofs) in seinen Vorschlag für das eID-System aufgenommen. Diese Technologie ermöglicht die Überprüfung der Richtigkeit bestimmter Informationen, ohne diese vollständig offenzulegen oder Zugang zu ihnen zu gewähren. So kann man beispielsweise Informationen über sein Alter weitergeben, ohne seinen Reisepass vorzulegen. Diese Funktion könnte ein fester Bestandteil der EUDI-Wallet werden[7]/[8].

Large – Scale Pilots

Mit den Large-Scale-Pilots (LSP) für die European Digital Identity Wallet (EUDI-Wallet) werden die Möglichkeiten einer digitalen "Brieftasche" plastisch dargestellt und die Funktionalitäten und deren Mehrwert anhand von diversen Anwendungsfällen demonstriert. Jeder Lage-Scale-Pilot wird von einem Konsortium betrieben.

[7] EU to Launch Digital Wallet with ZK-Proof Technology
[8] Der Weg zum eIDAS 2.0 Trilog

NOBID

Zu dem Konsortium, das von NOBID (Nordic-Baltic eID Project) geleitet wird, gehören sechs Länder (Dänemark, Deutschland, Island, Italien, Lettland und Norwegen). Das Konsortium will den am weitesten verbreiteten der vorrangigen Anwendungsfälle der Europäischen Union für die Brieftasche zum Leben erwecken – Zahlungen, woraus sich erklärt, dass auch einige Banken sich dem Konsortium angeschlossen haben.

Unter der Leitung von NOBID und nach der erfolgreichen Harmonisierung mehrerer nationaler eID-Programme, die Dutzende Millionen europäischer Bürger umfassen, wird die Gruppe zusammenarbeiten, um zu zeigen, "*wie Zahlungen und ID mühelos, grenzüberschreitend und in mehreren Währungen kombiniert werden können. Das Konsortium wird aktiv von führenden digitalen Regierungsbehörden, Banken, Unternehmen und Technologieanbietern unterstützt und wird die ausgereiften digitalen Identitätsinfrastrukturen der sechs jeweiligen Länder nutzen*".

Der Vorschlag des Konsortiums, eines von vier EU-Pilotprojekten für digitale Identitätsbrieftaschen zu sein, stehe in vollem Einklang mit den Hauptzielen der EU für ihren Rahmen für digitale Identität insgesamt. Bei der Umsetzung des Vorschlags würde die bestehende Zahlungsinfrastruktur genutzt, um die Ausgabe von Zahlungen, Sofortzahlungen, Konto-zu-Konto-Überweisungen und die Annahme von Zahlungen sowohl in Geschäften als auch online zu ermöglichen. Das Projekt soll weiterhin umfassendere EU-Pläne zur Stärkung der Mitgliedstaaten und zur Vereinfachung des grenzüberschreitenden Zahlungsverkehrs ergänzen, wie etwa die Europäische Zahlungsverkehrsinitiative (EPI) und den digitalen Euro. Gestützt wird das Projekt von Banken und Zahlungsdienstleistern wie DSGV in Deutschland, DNB und BankID in Norwegen, Nets in Dänemark, Intesa Sanpaolo, PagoPA und ABILab in Italien und Greiðsluveitan in Island.

Zu den Händlern, die die Zahlungslösung testen werden, gehören Elkjøp in Norwegen und die REWE-Gruppe in Deutschland.

Damit die digitale ID-Brieftasche in der EU florieren kann, braucht sie eine Referenzimplementierung, die die Messlatte hoch legt. Das Konsortium bringe nach eigener Aussage alle Voraussetzungen für den Erfolg mit: "*eine multinationale Beteiligung, umfassende Erfahrung mit digitalen Identitäten, einen äußerst überzeugenden Anwendungsfall und die Unterstützung der Besten aus der Banken- und Zahlungsbranche*".

Potenzial – Pilotprojekte für das Konsortium für EUid-Brieftasche

Dieses Projekt wird von Deutschland und Frankreich unter Beteiligung von 17 Mitgliedstaaten und der Ukraine koordiniert. An ihr sind über 50 öffentliche Verwaltungen und über 80 private Einrichtungen beteiligt. Im Rahmen des Projekts wird die EUDI-Brieftasche auf sechs Anwendungsfälle angewendet.

1. Zugang zu staatlichen Dienstleistungen
2. Eröffnung eines Bankkontos
3. Anmeldung für eine SIM-Karte
4. Mobiler Führerschein
5. elektronische Signaturen
6. elektronische Verschreibungen

EWC – EU Digital Identity Wallet Consortium (EU Digital Identity Wallet Consortium)

Dieses Projekt wird von Schweden unter Beteiligung von 18 Mitgliedstaaten und der Ukraine koordiniert. Mehr als 15 öffentliche Verwaltungen und mehr als 40 private Einrichtungen sind daran beteiligt. Im Rahmen des Projekts werden drei Anwendungsfälle getestet.

1. Speicherung und Anzeige digitaler Reisedaten
2. Organisation digitaler Brieftaschen
3. Die Organisation der Zahlungen

DC4EU – Digitale Zertifikate für Europa

Dieses Projekt wird von Spanien unter Beteiligung von 23 Mitgliedstaaten und der Ukraine koordiniert. An ihr sind über 35 öffentliche Verwaltungen und über 40 private Einrichtungen beteiligt.

Im Rahmen des Projekts wird der Einsatz der EUDI-Brieftasche im Bildungssektor und im Bereich der sozialen Sicherheit getestet. Das Pilotprojekt wird mit dem Europäischen Sozialversicherungspass und dem europäischen Lernmodell im Einklang stehen. Sie wird die europäische Blockchain-Diensteinfrastruktur (EBSI) im Rahmen der EUDI-Brieftasche nutzen.

Feldtests

Mittlerweile sind die ersten Feldtests zur Erprobung der Anwendungsfälle gestartet[9].

Digitaler Euro

Aus dem Entwurf der EU-Kommission zum Digitalen Euro geht hervor, dass die EUiD-Wallet bei der Einführung eines Digitalen Euros eine zentrale Rolle übernehmen soll.

Auszüge:

Die EU-weit interoperable Europäische Geldbörse für digitale Identitäten (EUiD) ermöglicht den Nutzern auf freiwilliger Basis bei Zahlungen eine starke Kundenauthentifizierung und Zahlungen vorzunehmen, wie in Artikel 97 der PSD2 gefordert. Die gleichen Funktionalitäten sollten auch den Nutzern des digitalen Euro angeboten werden.

Europäische Geldbörsen für digitale Identitäten könnten digitale Transaktionen erleichtern, indem sie Folgendes ermöglichen: Authentifizierung, Identifizierung und den Austausch von Attributen, einschließlich Lizenzen und Zertifikaten. Die Europäische Geldbörsen für digitale Identitäten sollten zum universellen Zugang zum

[9] **Projekte zur Erprobung der EUDI-Brieftasche gestartet**

digitalen Euro und zu dessen Verwendung beitragen. Die Mitgliedstaaten sollten europäische Geldbörsen für digitale Identitäten auf der Grundlage gemeinsamer Standards und Praktiken ausgeben, die in den Durchführungsvorschriften festgelegt sind. Die Europäische Geldbörse für digitale Identitäten sollte über strenge und spezifische Schutzmaßnahmen zur Gewährleistung des Datenschutzes und des Schutzes der Privatsphäre sowie eine hochrangige Sicherheits-Zertifizierung verfügen.

Die von der Europäischen Zentralbank zu entwickelnden Front-End-Lösungen sollten daher die technischen Spezifikationen für die europäischen Geldbörsen für digitale Identitäten berücksichtigen. Dies würde die entsprechende Interoperabilität mit den Europäischen Geldbörsen für digitale Identitäten ermöglichen, die es erlauben würden, diese Vorteile zu nutzen. Basierend auf der Wahl des Nutzers sollte die Interoperabilität mit der Europäischen Digitalen Identitäts-Wallet es auch ermöglichen, die Sorgfaltspflicht gegenüber Kunden gemäß der Verordnung (EU) XX/YY [bitte Referenz einfügen – Vorschlag für eine Verordnung zur Geldwäschebekämpfung Verordnung – KOM/2021/421 endgültig) einzuhalten. Um ein kohärentes Kundenerlebnis zu erreichen, könnten sich die Intermediäre dafür entscheiden, ihre digitalen Euro-Front-End Dienstleistungen vollständig in die Spezifikationen für die europäischen digitalen Identitätsbrieftaschen zu integrieren.

Die Nutzer sollten in der Lage sein, wenn sie dies wünschen, Zahlungen mit dem digitalen Euro unter Verwendung der europäischen Geldbörsen für digitale Identitäten zu autorisieren. Die Zahlungsdienstleister sollten daher verpflichtet werden, die Europäischen Geldbörsen für digitale Identitäten für die Identitätsüberprüfung sowohl potenzieller als auch bestehender Kunden zu akzeptieren, im Einklang mit Verordnung (EU) XX/XX [bitte Fundstelle einfügen – Vorschlag für eine Verordnung zur Bekämpfung der Geldwäsche – KOM/2021/421 endgültig). Zur Erleichterung der Eröffnung von digitaler Euro-Konten in der gesamten Union, sollten die Zahlungsdienstleister auch die Möglichkeit haben, sich auf qualifizierte Bescheinigungen der europäischen digitalen Identitätsbrieftaschen verlassen zu können, auch für die Durchführung der Sorgfaltspflicht gegenüber Kunden aus der Ferne. Zahlungsdienstleister sollten auch die Verwendung

europäischer digitaler Identitätsbrieftaschen akzeptieren, wenn der Zahler die Brieftasche für die Zahlungsautorisierung von digitalen Euro-Zahlungen verwenden möchte. Zur Erleichterung von Offline- Zahlungen in digitalen Euros sollte es außerdem möglich sein, die Europäischen Geldbörsen für digitale Identitäten für die Speicherung von digitalen Euros im Zahlungsgerät zu verwenden.

Um digitale Euro-Zahlungen online oder offline abwickeln zu können, ist es unerlässlich, dass Front-End- Dienstleister-Anbieter für den digitalen Euro und Emittenten europäischer digitaler Identitätsbrieftaschen Zugang zur Nahfeldkommunikationstechnologie (NFC) auf mobilen Geräten erhalten. Diese Komponenten umfassen insbesondere, aber nicht ausschließlich, NFC-Antennen und die so genannten sicheren Elemente mobiler Geräte (z.B.: Universal Integrated Circuit Card (UICC), eingebettete SE (eSE) und microSD usw.). Es muss daher verhindert werden, dass Erstausrüster von Mobilgeräten oder Anbieter von elektronischen Kommunikationsdiensten den Zugang zu NFC-Antennen und sicheren Elementen verweigern. Um sicherzustellen, dass Zentralbankgeld in der digitalen Wirtschaft verwendet werden kann, müssen die Anbieter von Frontend-Diensten für den digitalen Euro und die Betreiber von Europäischen Geldbörsen für digitale Identitäten das Recht haben, Software auf der Hardware der betreffenden mobilen Geräte zu speichern, um Transaktionen mit dem digitalen Euro sowohl online als auch offline technisch möglich zu machen.

Potenzielle Risiken für den Erfolg der EUDI

In 4 ways the EU Digital Identity Wallet could fail werden vier Risiken vorgestellt, die den Erfolg der EUDI-Wallet gefährden können.

- Fehlende Akzeptanz bei den wichtigsten Parteien und den EU-Bürgern
- Ein Wallet-Ökosystem, das kommerziell nicht nachhaltig ist
- Technische Unausgereiftheit und eine zu komplexe Lösung
- Rechtliche Unvereinbarkeit mit bestehenden Vorschriften

Ohne Zugang zu nahtlosen und vertrauenswürdigen Identitätslösungen, die grenzüberschreitend anerkannt werden, werden Bürger und Unternehmen auf

Lösungen angewiesen sein, die nicht mit den von den Mitgliedstaaten ausgestellten legalen Identitäten von den Mitgliedstaaten arbeiten werden und daher weniger sicher sind. Dies steht im Widerspruch zu der zunehmenden Nachfrage nach einer sicheren digitalen Identität für den Zugang zu allen Online-Diensten in der EU, die den Nutzern Kontrolle über die Verwendung ihrer persönlichen Daten gibt und den Austausch von persönlichen Daten Attributen und Berechtigungsnachweisen ermöglicht.

Mögliche Szenarien:

- In Ermangelung einer gemeinsamen Lösung für den Identitätsabgleich wird die grenzüberschreitende Verwendbarkeit von eIDs begrenzt bleiben, was auch ein Risiko für das Funktionieren anderer EU-Rechtsvorschriften, wie der Verordnung über das einheitliche digitale Portal, und insbesondere das Funktionieren des Grundsatzes der einmaligen Zulassung darstellt.
- Die Fragmentierung des Marktes für private eID-Lösungen wird ohne einheitlichen Rechtsrahmen auf EU-Ebene wahrscheinlich zunehmen. Es ist davon auszugehen, dass einige wenige mächtige Akteure (z. B. Online-Plattformen) ihre Dominanz ausbauen werden. Dies wird zu Abhängigkeiten für die Anbieter von Online-Diensten und zur Bindung der Nutzer führen (Lock-In). Eine geringere Wertschöpfung und eine Bedrohung für die digitale Autonomie der EU sind die Folge.
- Die Nutzer werden nicht in der Lage sein, die Verwendung ihrer Identitätsdaten zu kontrollieren, wenn keine klaren, einheitlichen Datenschutz- und Datenschutzgarantien für Identitätsanbieter, einschließlich Online Plattformen existieren.
- Das Risiko, dass IoT-Geräte als Vermittler genutzt werden, um auf betrügerische Weise an die Daten von Bürgern Daten von Bürgern und Unternehmen zu gelangen, wird voraussichtlich ebenfalls zunehmen, da immer mehr verbundene Geräte im Umlauf sein werden

Der eco-Verband der Internetwirtschaft e.V. mahnt an, dass die EU die Mitgliedstaaten dazu anhalten müsse, Lösungen digitaler Identitäten wie ID-Wallets

so anzubieten, dass sie für Nutzerinnen und Nutzer attraktiv und überzeugend genug sind, um sie auch wirklich zu nutzen. Für einen erfolgreichen Wettbewerb mit bestmöglichen Lösungen und einer erfolgreichen Durchsetzung des Wallets sollte sich die EU laut eco-Vorstand Prof. Norbert Pohlmann dafür einsetzen, dass mehrere zertifizierte Wallets nebeneinander im Markt existieren können; von einer rein staatlichen Lösung sei unbedingt abzusehen[10].

Bitkom macht sich für eine flexible Anpassung des notwendigen Sicherheitsniveaus an die jeweiligen Anwendungsfälle stark. Einige eID-Systeme in Europa funktionierten bereits erfolgreich auf einem niedrigerem, aber ebenfalls sicheren Niveau, an das sich viele Bürgerinnen und Bürger bereits gewöhnt hätten.

Ein anderer Risikofaktor ist der Datenschutz. So fordert Epicenter Works, dass eine Identifizierung über die EUDI Wallet bestenfalls auf Fälle von gesetzlichen KYC-Anforderungen beschränkt sein und nicht auf Nutzungsbedingungen beruhen sollte. *„Die überwachungsgetriebenen Geschäftsmodelle von Geschäftsmodelle dieser Big-Tech-Unternehmen erfordern besondere Sicherheitsvorkehrungen, um zu verhindern, dass die EUDI-Wallet zu Verletzungen der Privatsphäre beitragen, die bei diesen Diensten üblich sind“.*

Lilith Wittmann gibt in ihrer Stellungnahme zu bedenken: *„Wallet Apps sind i.d.R. Softwarelösungen, welche verschiedene digitale Identitätsnachweise sowie signierte Dokumente zusammenführen und elektronisch bereitstellen können. Sie sind ein exzellentes Angriffsziel für böswillige Akteure sowie Unternehmen, die gerne Datenreichtum erlangen wollen, weil die Wallet Apps eben so viele sensible Dokumente an einem Ort mit Internetzugang bereitstellen.*

Es existieren keine sicheren, softwarebasierten Wallet-Lösungen. Und es ist nur eine Frage der Zeit, bis jedes dieser Systeme (erfolgreich) angegriffen wird. Das Risiko mag aktuell für Menschen, die sich immer das neueste Smartphone leisten können, überschaubar sein, allerdings wird diese staatliche Risikoakzeptanz folglich dazu

[10] Die digitale Brieftasche der EU

führen, dass sich eben nicht alle Menschen Datensicherheit leisten können. Ohnehin benachteiligte Gruppen sind besonders gefährdet oder werden gar von sozialer Teilhabe ausgeschlossen".

Nach dem „ID-Walltet – Desaster" der Vorgängerregierung, sei es *„traurig, dass diese (Risiken) nun noch einmal ausdiskutiert werden müssen und am Ende eine Lösung stehen wird, die ganze gesellschaftliche Gruppen digital noch weiter ausschließen und in einem weiteren technischen Desaster enden wird", so Wittmann.*

Die Erfolgsaussichten der EUDI-Wallet könnten deutlich getrübt werden, wenn Apple und Google sich weigern würden, den Zugriff auf ihre NFC-Schnittstellen und Secure Elements freizugeben. In dem bereits erwähnten Entwurf der EU-Kommission zum Digitalen Euro heißt es: *Um digitale Euro-Zahlungen online oder offline abwickeln zu können, ist es unerlässlich, dass Front-End- Dienstleister-Anbieter für den digitalen Euro und Emittenten europäischer digitaler Identitätsbrieftaschen Zugang zur Nahfeldkommunikationstechnologie (NFC) auf mobilen Geräten erhalten. Diese Komponenten umfassen insbesondere, aber nicht ausschließlich, NFC-Antennen und die so genannten sicheren Elemente mobiler Geräte (z.B.: Universal Integrated Circuit Card (UICC), eingebettete SE (eSE) und microSD usw.). Es muss daher verhindert werden, dass Erstausrüster von Mobilgeräten oder Anbieter von elektronischen Kommunikationsdiensten den Zugang zu NFC-Antennen und sicheren Elementen verweigern.*

Schlussbetrachtung und Ausblick

Der Weg zur EUDI-Wallet, welche die Anforderungen der Wirtschaft, des Staates und der Zivilgesellschaft in einem zufriedenstellen Maß erfüllt, ist steinig und lang – schon alleine in Deutschland.

Eine möglichst einheitliche Lösung, die in allen EU-Ländern verwendet werden kann und die auch von den Nutzerinnen und Nutzern im Alltag eingesetzt wird, zu entwickeln und umzusetzen, ist eine Herausforderung. Neben unterschiedlichen gesetzlichen Vorgaben und voneinander abweichenden Gewohnheiten in den jeweiligen Ländern beim Umgang mit der EUDI-Wallet sind es auch technische

Herausforderungen, wie Fragen der Sicherheit und des Datenschutzes, die zu Akzeptanzproblemen führen können.

Viel hängt für den Erfolg von der Rollenverteilung zwischen dem Staat und der Privatwirtschaft ab. Sofern die Wirtschaft keinen Nutzen für sich erkennen kann, wird sie sich bei der Unterstützung der EUDI-Wallet zurückhalten.

Zu klären ist auch die Frage, welches Sicherheitsniveau für die verschiedenen Anwendungsfälle gelten und wie verhindert werden soll, dass Teile der Bevölkerung ausgeschlossen werden.

Und über allem schwebt das Szenario des Digitalen Euro und die Frage, ob Apple und Google bereit sein werden, ihre Software für die EUID-Wallet zu öffnen.

Impressum

Kontakt

Ralf Keuper

Kolpingstr. 3

33428 Harsewinkel

E-Mail: ralf.keuper@identity-economy.de

Autor: Ralf Keuper

V.i.S.d.P.: Ralf Keuper