Juli 2025

Die Zeit läuft: Fünf politische Weichenstellungen für ein erfolgreiches eIDAS-Ökosystem

Staat, Zivilgesellschaft und Wirtschaft betrachten die Einführung der EUDI-Wallet und den Ausbau des eIDAS-Ökosystems aus unterschiedlichen Perspektiven – zugleich besteht in vielen Bereichen ein breites Verständnis dafür, dass diese Entwicklungen das Potenzial haben, unsere digitale Gesellschaft maßgeblich zu prägen. Zudem leistet die EUDI-Wallet als interoperables Interface einen essenziellen Beitrag zur Umsetzung der digitalen Souveränitätsziele der EU und der Bundesregierung. Damit dieses Ökosystem erfolgreich wird, muss es einen Mehrwert für Bürger:innen/Verbraucher:innen, Verwaltung und die Wirtschaft bieten. Der Mehrwert ergibt sich durch die Anzahl der staatlichen und privatwirtschaftlichen Nachweise und der Akzeptanzstellen. Daher muss das Ökosystem vertrauenswürdig, breit akzeptiert und die Ausstellung und Nutzung von Nachweisen einfach sein.

Die Gestaltung des Ökosystems ist ein gesellschaftlicher Auftrag, und dabei muss die eIDAS-Verordnung als die alleinige Grundlage für die Regelung digitaler Nachweise und Identitäten in ganz Europa gelten. Daher erfordert es eine enge Zusammenarbeit zwischen Politik, Wirtschaft und Gesellschaft – denn nur durch einen inklusiven, praxistauglichen Ansatz kann das eIDAS-Ökosystem sein volles Potenzial entfalten. Das Interesse in der Bevölkerung ist vorhanden: 55 % der Bürger:innen würden sich gerne zukünftig über das Smartphone mit ihrem Personalausweis ausweisen[1]. Die neue Bundesregierung steht vor der großen Herausforderung, in den kommenden 18 Monaten bzw. bis Ende 2026 die Weichen für eine zukunftsfähige Umsetzung zu stellen. Dabei sind zentrale Weichenstellungen nötig, um Deutschland als starken Akteur im europäischen Identitätsökosystem zu positionieren.

[1] eGovernment MONITOR 2024

Um dieses Ziel zu erreichen, braucht es neben dem politischen Willen klare politische Leitlinien und eine enge Verzahnung aller relevanten Akteure. Vor diesem Hintergrund möchten wir fünf zentrale Forderungen formulieren, die essenziell für den Erfolg des eIDAS-Ökosystems sind.

1) Digitalkompetenz erhöhen

Oft wird im Zusammenhang mit der Digitalkompetenz nur auf die Endnutzenden, also die Bürger:innen abgezielt. Und in der Tat müssen diese Gruppen inhaltlich auf ihrem jeweiligen Wissensstand abgeholt werden. Digitale Brieftaschen mit ihren digitalen Nachweisen und die selbstverständliche Nutzung des digitalen Personalausweises (eID) und des elektronischen Führerscheins müssen fester Bestandteil des digitalen und analogen Alltags werden und die Menschen müssen befähigt werden, diese selbstbestimmt und sicher einsetzen zu können. Aber ohne eine moderne Gesetzgebung und einer zukunftsgewandten Verwaltung geht es nicht: daher plädieren wir dafür, Digitalkompetenzen insbesondere im Bereich digitaler Identitäten und Vertrauensdienste in den Ministerien, Aufsichtsbehörden und Verwaltung – also im gesamten Staatsapparat – aufzubauen. Ziel ist es, das Bewusstsein für das eIDAS-Ökosystem und die EUDI-Wallet deutlich zu erhöhen, deren Funktionen verständlich zu machen und die flächendeckende Nutzung sowohl innerhalb der Verwaltung als auch bei Bürger:innen zu fördern. Ein mahnendes Beispiel ist die Einführung des elektronischen Personalausweises (eID), der bis 2024 nur von 22 % der Bürger:innen genutzt wird[2]. Wir brauchen einen echten Transformationsprozess – weg von althergebrachten Denkmustern und analogen Prozessen hin zu einem digitalen Mindset. Dazu gehört auch, wieder die Interessen der Bürger:innen in das Zentrum zu rücken und anzuerkennen, dass laut einer Bitkom-Umfrage aus dem Jahr 2025 bereits 82 % der Deutschen ab 16 Jahren ein Smartphone nutzen[3].

2) Vertrauen stärken

Digitale Identitäten und digitale Nachweise müssen Vertrauen im digitalen Raum fördern und nicht das Misstrauen stärken. Daher ist es essenziell, dass die drei zentralen Akteure – also Holder, Issuer und Relying Parties – sich untereinander vertrauen können. Voraussetzung dafür ist, dass jeder weiß, wer der andere ist. Daher braucht jeder Akteur eine eigene digitale Identität. Gleiches gilt für die digitalen Nachweise. Die Echtheit digitaler Nachweise muss sichergestellt werden. Wir fordern daher einen flächendeckenden Einsatz von Vertrauensdiensten wie dem elektronischen Siegel, der elektronischen Signatur und anderen eIDAS-Tools, um Echtheit und Seriosität digital prüfen zu können. Die eIDAS-Verordnung muss die alleinige Grundlage für die Regelung digitaler Nachweise und Identitäten sein und als verbindliche Referenz in allen nationalen Rechtsvorschriften dienen, die diese Themen betreffen. Der Staat sollte den Schwerpunkt klar auf die EUDI-Wallet setzen, und dabei bestehende, funktionierende IT-Komponenten und Bestandslösungen aktiv einbinden, um unnötige Doppelstrukturen und Insellösungen zu vermeiden und die Effizienz und Akzeptanz digitaler Verwaltungsanwendungen zu steigern.

3) Verbraucher schützen

Vertrauenswürdige Daten wecken Begehrlichkeiten. Verbraucher:innen müssen daher vor Überwachung, Missbrauch und Betrug geschützt werden. Es braucht einen effektiven Schutz, am besten durch technische Maßnahmen, die eine „Überidentifizierung“ verhindern, aber gleichzeitig eine bürokratiearme Integration in Anwendungsfälle sicherstellen. Gleichzeitig müssen Verbraucher:innen befähigt werden, entscheiden zu können, wer warum welche Nachweise aus der Wallet erhält. Dafür ist

[2] eGovernment MONITOR 2024
[3] Bitkom 2025, „Mehr als 40 Mrd. Euro Umsatz – Smartphones“

ein kluges Verbraucherschutzkonzept erforderlich, das Verbraucher:innen schützt und gleichzeitig befähigt, selbstbestimmt Entscheidungen treffen zu können. Wir fordern daher, den Verbraucherschutz technisch in der Wallet – u. a. durch die ausreichende Identifizierung und Überprüfung der Relying Parties inkl. Zugriffsrechte – zu verankern, ein Marketingkonzept zur Aufklärung über Risiken und den vertrauensvollen Umgang mit der Wallet zu entwickeln und Datenschutzanforderungen konsequent zu berücksichtigen. Eine zentrale Stelle sollte zudem sicherstellen, dass die Registrierung von Relying Parties unter Einhaltung der eIDAS-Vorgaben erfolgt. Bei der Übermittlung von Daten an Relying Parties ist das Prinzip der Datenminimierung zu beachten. Zudem sollte es für Nutzer:innen möglich sein, ein Pseudonym in der Wallet zu hinterlegen, welches als Standardeinstellung ausgewählt ist. Sensible Ausweisdaten sollten nur auf Grundlage gesetzlicher Anforderungen mit Dienstanbietern geteilt werden. Deshalb plädieren wir für eine klare Trennung zwischen Anwendungsfällen, die auf einer gesetzlichen Identifikationspflicht beruhen, und solchen, bei denen die Identifikation lediglich auf Grundlage von AGB erfolgt. Optional sollte in der EUDI-Wallet die Einstellung möglich sein, dass man den Personalausweis mit der eID-Funktion für (sicherheits)kritische Vorgänge immer wieder neu anhalten und eine PIN eingeben können sollte. Der User kann so selbst entscheiden, ob er seinem Smartphone vertraut, oder ob er bestimmte Vorgänge noch einmal durch das Anhalten der eID haptisch absichern möchte.

4) Bestehende Strukturen nutzen und effizienter gestalten

Die Entwicklung eines eIDAS-Ökosystems benötigt Kontinuität. In der Politik muss an die bisherigen Strukturen bestehend aus Ministerien und SPRIN-D angeknüpft werden, wobei vertikale Themen künftig im Bundesministerium für Digitalisierung und Staatsmodernisierung (BMDS) liegen und verantwortet werden müssen. Wir fordern einen zentralen Ansprechpartner, der auch nach innen ins Ministerium das Thema vorantreibt und andere Referate, die indirekt damit zu tun haben, aufklärt. Im Hinblick auf die Verbreitung und zunehmende Einführung der eIDAS-Regeln in der deutschen Digitalumgebung bedarf es einer zentralen Stelle, die die Organisation, Überwachung und Weiterentwicklung des EUDI-Ökosystems verantwortet. Unter dem Dach des BMDS sollten themenspezifische Expertengremien eingerichtet werden, um regelmäßig zu evaluieren, welche digitalen Nachweise (Credentials) in verschiedenen Anwendungsbereichen von Relying Parties verlangt werden – mit dem Ziel, diese bedarfsgerecht zu gestalten und das eIDAS-Ökosystem effizient weiterzuentwickeln. Zudem sollten künftige regulatorische Gesetzesvorhaben grundsätzlich einem Digital-Check unterzogen werden – mit dem Ziel, die Potenziale des eIDAS-Ökosystems systematisch zu berücksichtigen und, wo möglich, aktiv zu integrieren. Die Nutzung der EUDI-Wallet im Zahlungsverkehr darf beispielsweise nur erfolgen, wenn eine adäquate Berücksichtigung in der sektorspezifischen Regulierung erfolgt ist. Diese muss sowohl die technischen (Sicherheits-)Anforderungen als auch das Haftungsregime konsistent regeln, bei dem eine klare Trennung der Verantwortlichkeiten von Wallet-Anbietern und (Finanz-)Dienstleistern sichergestellt ist, um Rechtssicherheit und Stabilität im Finanzsektor zu gewährleisten.

5) Anwendungsfälle fördern

Dass Digitale Identitäten unter dem Henne-Ei-Problem leiden und die Förderung von Anwendungsfällen in der Verwaltung und Privatwirtschaft essenziell für ihren weiteren Erfolg sind, ist seit 2010 bekannt. Die EUDI-Wallet sollte jedoch in einem ersten Schritt auf ihre Kernfunktion – die digitale Identifizierung und Authentifizierung, insbesondere im Rahmen von KYC-Prozessen – fokussieren. Das BMDS sollte zusätzlich auf einige wenige Schlüssel-Anwendungsfälle als Zusatzleistung konzentrieren, die einen Schneeballeffekt hervorrufen können. Hier sehen wir besonders die folgenden Bereiche als elementar an: Die Förderung von Organisationsidentitäten (z.B. European Business Wallet), die Ausstellung des digitalen Führerscheins, digitale Reiseunterlagen, die Bereitstellung des Organspendeausweises als digitalen Nachweis, eine Lösung zur anonymen oder pseudonymen Altersverifikation sowie die Kombination aus physischen und digitalen Hochschulzeugnissen und Immatrikulationsnachweisen.

Entscheidend für den Erfolg ist dabei die frühzeitige und breite Einbindung sowie Akzeptanz durch die Relying Parties.