ZVEI-Seiter

Empfehlungen zum Aufbau eines sicheren Ökosystems digitaler Identitäten

Die Bundesregierung hat in ihrer Digitalstrategie die Umsetzung von „sicheren und nutzerfreundlichen digitalen Identitäten“ als eines von drei Projekten mit besonderer Hebelwirkung zur Erreichung des Zielbildes der Digitalstrategie identifiziert. Das ressortübergreifende Konsortium *GovLabDE Digitale Identitäten* koordiniert den Aufbau des Ökosystems digitaler Identitäten. Zeitgleich setzt das BMI die Verpflichtung aller EU-Mitgliedsstaaten um, entsprechend einer prototypischen eIDAS 2.0- konformen Infrastruktur allen Bürgern eine EUDI-Brieftasche (EU Digital Identity Wallet) bereitzustellen. Diese Brieftasche soll die Speicherung und Bereitstellung von Ausweisdokumenten wie Personalausweis, Führerschein etc. ermöglichen. Mit der eIDAS 2.0 wird nun bewusst auch die Nutzung von digitalen Brieftaschen für halb-öffentliche und private Anwendungen ermöglicht.
Der ZVEI unterstützt die Bestrebungen der Bundesregierung zum Aufbau eines Ökosystems digitaler Identitäten und die Erarbeitung einer prototypischen eIDAS 2.0- konformen Infrastruktur für Digitale Identitäten in Deutschland vollumfänglich, da dies ein Schlüsselfaktor zur Digitalisierung von Gesellschaft und Wirtschaft darstellt. Eine breite Marktakzeptanz wird jedoch nur durch privatwirtschaftliche Anwendungen erzielt. Zudem plädieren wir dafür die Anbindung an industrielle Anwendungen der Industrie 4.0 zu berücksichtigen.

Unsere Positionen

Breite Marktakzeptanz durch privatwirtschaftliche Anwendungen erzeugen

- Beim Aufbau eines eIDAS 2.0-konformen Ökosystems für digitale Identitäten sollte auf eine **Kombination aus staatlich und privatwirtschaftlich angebotenen EUDI-Brieftaschen** bzw. Modulen/SDKs und Komponenten einer (deutschen) EUDI-Brieftasche gesetzt werden. Während der Staat die Kerninfrastruktur und Zertifizierung übernimmt, bringt der Wettbewerb kundenorientierte Lösungen und Innovationen hervor.

- Eine breite **Marktakzeptanz** von digitalen Brieftaschen wird vor allem **durch privatwirtschaftliche Anwendungen** erzeugt. Die Anforderungen an Sicherheitsstandards können für Anwendungen jedoch unterschiedlich hoch sein. Behördenanwendung, Ausweisfunktionen oder Banking-Anwendungen erfordern ein höheres Sicherheitsniveau als die Punktesammelkarte. **Potenzielle Anbieter und Anwender aus den jeweiligen Branchen müssen bei der Schaffung der Sicherheitsarchitektur frühzeitig eingebunden werden.**

- Das *GovLabDE Digitale Identitäten* sollte die **Erweiterung und Anschlussfähigkeit von Brieftaschen für juristische Personen (Organisational Wallets) frühzeitig berücksichtigen**. Dies schließt auch die digitale Anbindung an den öffentlichen Verwaltungsapparat mit ein. **Positiver Effekt: bürokratischer Aufwand für Unternehmen kann dadurch reduziert werden.**

- Die Entwicklung eines eIDAS 2.0-konformen EUDI-Brieftaschen-Prototypens sollte ebenfalls die Anschlussfähigkeit zur internationalen Anwendung berücksichtigen.

Sicherheit schafft Vertrauen

- **Vertrauen in digitale Identitäten** ist ein zentrales Element zur erfolgreichen Anwendung und Skalierung. Vertrauen kann nur über **nachweisbare und verlässliche Sicherheitsvorkehrungen** erreicht werden. Während im industriellen Kontext risikobasiert und anwendungsabhängig verschiedene Sicherheitslösungen vorstellbar sind, begrüßen wir die Entscheidung der Bundesregierung zum Identitätsnachweis natürlicher Personen primär auf Hardware-Komponenten zu setzen:

  – Bei Mobile Wallet Diensten ist es ratsam, die Nutzerdaten auf einem **physischen Chip**, s.g. **embedded secure elements - eSE** (zertifizierter Hardware-Sicherheits-Elemente) zu speichern, um die Einhaltung der damit verbundenen **Sicherheitsstandards** gewährleisten zu können;

- **Lokale Speicherung** schafft weiteres Vertrauen in die Anwendung, wenn Daten nicht in Clouds gespeichert werden müssen;

- Aufgrund hochkritischer Anwendungen im Bereich der Authentifizierung müssen die auf den Geräten gesicherten Daten **auch im Offline abgerufen** werden können. Embedded secure elements (eSE) mit NFC Schnittstellen (Near Field Communication) ermöglichen auch bei entladenem Akku autorisierten Zugriff auf sensible Daten, die auf dem eSE hinterlegt sind.

- Es bestehen – teils ISO normiert - unterschiedliche kryptographische Verfahren für die **selektive und nicht verknüpfbare Offenlegung elektronischer Bescheinigungsattribute**, die im Einklang mit den zu erwarteten Anforderungen aus der eIDAS 2.0 stehen[1]. Diese ermöglichen es dem Anwender, den Sicherheitsanforderungen entsprechend, darüber zu entscheiden, welche Informationen mit welcher Instanz geteilt werden.

- Bei der Konzeptionierung eines eIDAS 2.0-konformen EUDI-Brieftaschen-Prototypens, muss im Rahmen des *Security-by-Design* und *Privacy-by-Design* zwingend die **Kohärenz relevanter Sicherheitsaspekte und Anforderungen** an Hard- und Software aus Regulierungen, wie der DSG-VO, der Funkanlagenrichtlinie (RED), der überarbeiteten Netz- und Informationssysteme-Richtlinie (NIS2) oder dem **Cyber Resilience Act** gewährleistet werden.

Digitale Identitäten sind ein zentrales Element der Digitalisierung von Wertschöpfungsprozessen der Industrie 4.0[2]

- Beim Aufbau eines Ökosystems digitaler Identitäten muss die **Verknüpfung von digitalen Identitäten**, die an **natürliche und juristische Personen** geknüpft sind, **mit digitalen Identitäten von Objekten (digitaler Zwilling)** berücksichtigt werden – und zwar unabhängig davon, ob das Objekt einer Person zugeordnet ist (z.B. ein Herzschrittmacher), einer Person zuordnungsfähig ist (z.B. ein Fahrzeug mit Kennzeichen und Eintrag des Halters) oder aber auch nicht zuordnungsfähig erscheint (z.B. eine Produktionsanlage im Kontext von Industrie 4.0).

- Die für Industrie 4.0 erforderlichen Identitätskonzepte müssen im rechtlichen Rahmen umsetzbar sein. Anwendungen digitaler Identitäten und Wallets im **industriellen Kontext** stellen im Gegensatz zu öffentlichen Anwendungen (bspw. Personenidentifikation gegenüber der öffentlichen Verwaltung) mitunter **geringere Anforderungen an die Sicherheitsarchitektur dar.** Das notwendige Sicherheitsniveau der Identität im industriellen Kontext ergibt sich aus der Risikobewertung unter Berücksichtigung der entstehenden Kosten. Der ZVEI empfiehlt bei der Wahl des Identifizierungsmittel (unterschiedliche Sicherheitskriterien) sich nach dem jeweils benötigtem Vertrauensniveau (niedrig, substanziell, hoch) aus der eIDAS-VO sowie der internationalen Normreihe IEC 62443 zur IT-Sicherheit industrieller Automatisierungssysteme und weiteren einschlägigen ISO-Standards zu richten.

GovLabDE Digital Identitäten: Klarer kommunizieren, Ziele definieren

- eID, smart eID und EUDI-Brieftasche (EUDI Wallet): Für Laien ist kaum nachvollziehbar, welche Funktionen und Dienste sich hinter den Namen verbergen (werden). Die Regierung muss daher **mehr und verständlicher kommunizieren, worin der jeweilige Nutzen der Angebote für den Anwender (Bürger, Unternehme, Vereine etc.) liegt**. Mehr geschaffene Akzeptanz fördert vermehrte Anwendung und schlussendlich die Skalierung digitaler Identitäten.

- Die Komplexität des Gesamtprojektes zum Aufbau eines Ökosystems digitaler Identitäten ist sehr hoch. Für Außenstehende, wie Bürger und auch für Projektpartner aus der Wirtschaft ist nur schwer nachvollziehbar, welche konkreten Projekte und Ziele unter welcher Arbeitsweise das *GovLabDE Digitale Identitäten* verfolgt, und wie die Einbindung und Koordinierung mit dem BMI zur Umsetzung einer eIDAS 2.0 konformen Infrastruktur erfolgt. **Prioritäten müssen klar benannt**, **Stakeholder und potentielle Anwender aus der Wirtschaft** müssen früher und enger in Prozesse und Entscheidungen eingebunden werden, um so mehr Transparenz zu schaffen. Nur so kann Sorge getragen werden, dass die **Technologie anwendungsgerecht ausgeführt** wird.

- Das *GovLabDE Digitale Identitäten* sollte sich **quantifizierbare Ziele und Meilensteine setzen sowie ein Monitoring** zum Umsetzungsstand implementieren.

[1] ETSI 2023: Electronic Signatures and Infrastructures (ESI); Analysis of selective disclosure and zero-knowledge proofs applied to Electronic Attestation of Attributes
[2] Plattform Industrie 4.0 - Technischer Überblick: Sichere Identitäten (plattform-i40.de)

Hintergrund: Zahlen, Daten, Fakten

Deutschland hinkt bei der Umsetzung mobiler digitaler Identitäten hinterher
In 16 europäischen Ländern sind mobile digitale Identitäten in der Anwendung, z.T. seit deutlich mehr als 5 Jahren. In 8 EU-Ländern sind diese sogar nach eIDAS notifiziert und könnten von EU-Bürgern auch in Deutschland angewendet werden.

eID-Transaktionen in Deutschland ausbaufähig
Gerade einmal **6,2 Mio. eID-Transkationen** für Identifizierungen wurden im Jahr 2022 durch natürliche und juristische Personen durchgeführt. Die Bundesregierung prognostiziert, dass diese Zahl der eID-Transaktionen bis 2026 **auf 0,7- 1,3 Milliarden** ansteigen wird. Dies gelingt jedoch nur durch privatwirtschaftliche Anwendungen.

Skalierung erfolgt nur über private Anwendungen
Bundesbürger haben im Schnitt **nur 1,4x im Jahr Kontakt mit öffentlichen Behörden**. Entsprechend selten werden in diesem Kontext Anwendungen über die Wallet genutzt. Eine hochfrequente Nutzung der Wallet wird nur über privatwirtschaftliche Anwendungen des alltäglichen Bedarfs (49€-Ticket, Ticket-Buchungen, Punktesysteme etc.) erzielt.

6. November 2023

Kontakt

Dominic Doll • Manager Digitalisierung -und Innovationspolitik• Abteilung Digital- und Innovationspolitik •
Telefon: +49 30 306960 19 • Mobil: +49 151 26441 132 • E-Mail: Dominic.Doll@zvei.org

ZVEI e. V. • Verband der Elektro- und Digitalindustrie • Charlottenstraße 35/36 • 10117 Berlin • www.zvei.org
Lobbyregisternr.: R002101 • EU Transparenzregister ID: 94770746469-09 • www.zvei.org