SPRIN-D

BUNDESAGENTUR
FÜR SPRUNGINNOVATIONEN

FEDERAL AGENCY
FOR DISRUPTIVE INNOVATION

DEUTSCHLAND MUSS MUTIG DIGITALISIEREN

V 1.1 – 20240729

ZUSAMMENFASSUNG

Digitale Brieftaschen (Wallets) werden bald unverzichtbar sein. Sie ermöglichen die digitale Verwaltung von Tickets, Bezahlvorgängen sowie Nachweisen und Ausweisen. Die eIDAS-Verordnung schafft den rechtlichen Rahmen für das EU Digital Identity (EUDI) Wallet Ökosystem, das bis 2027 umgesetzt werden soll. Die deutsche EUDI-Wallet benötigt eine digitale Identifizierungsfunktion mit hohem Sicherheitsniveau auf Smartphones. Für einen Erfolg der EUDI-Wallet sind die Kriterien *Datenschutz*, *Sicherheit*, *Nutzendenfreundlichkeit, Reichweite* und *Kosten* entscheidend. SPRIND wendet diese Kriterien im vorliegenden Positionspapier zur Bewertung der zentralen Architekturoptionen "authentifizierter Kanal" und "signierte Daten" für die Identifizierungsfunktion der deutschen EUDI-Wallet an. Die folgende Tabelle fasst die Analyseergebnisse zusammen:

Kriterien	Signierte Daten	Authentifizierter Kanal
Datenschutz	Minimale Beobachtbarkeit durch Aufgabenteilung zwischen Aussteller des Identifizierungsnachweises und Wallet-Anbieter.	Höhere Beobachtbarkeit durch Bündelung der Aufgaben beim Aussteller des Identifizierungsnachweises, staatliche Überwachung lässt sich schwerer ausschließen.
Reichweite	Hohe Reichweite durch Interoperabilität mit anderen EU-Mitgliedsstaaten und deren Wallet-Systemen.	Geringere Reichweite, deutscher Sonderweg, EU-weite Akzeptanz schwieriger.
Kosten	Geringe Kosten durch Nutzung etablierter und standardisierter Technologien	Hohe Kosten durch spezielle Hardwareanforderungen und eigenständige Entwicklung.
Potential	Sehr hoch, Erweiterung für andere Nachweise und qualifizierte Signaturen einfach, Synergien mit Fernsignaturfunktion der Wallet, Vermeidung der Beobachtbarkeit und geringere Betriebskosten durch Erweiterung um voll dezentrale Lösung für Vertrauensniveau normal/substantiell unter Nutzung der existierenden Sicherheitselemente auf den Smartphones der Nutzenden möglich	Begrenzt, da die breite Verfügbarkeit der auf sehr hohem Niveau zertifizierten Hardware-Sicherheitselemente in den Endgeräten derzeit nicht absehbar ist.

Lösungen basierend auf signierten Daten sind weit verbreitet, schnell verfügbar und ermöglichen ein hohes Datenschutz- und Sicherheitsniveau. Sie können mit geringem Aufwand durch Anwendungspartner verarbeitet werden und heben Synergien mit eIDAS-2.0-Aktivitäten anderer EU-Mitgliedsstaaten. Fast alle europäischen Länder nutzen bereits heute signierte Daten in ihren hoheitlichen eID-Systemen und entscheiden sich für diese technische Ausgestaltung zur Initiierung des zukünftigen eIDAS-2.0-Ökosystems für digitale Nachweise. Signierte Daten ermöglichen absehbar die Implementierung einer dezentralen Architektur für die EUDI-Wallet und können Innovationspotenziale aus dem Markt integrieren.

SPRIND empfiehlt daher für die erste Stufe der deutschen EUDI-Wallet die Nutzung von signierten Daten.

EIN ÖKOSYSTEM FÜR EINEN STAATLICHEN DIGITALISIERUNGSSPRUNG

Digitale Brieftaschen werden in Zukunft nicht mehr aus unserem Leben wegzudenken sein. Diese auch als Wallets bezeichneten Brieftaschen werden heute oftmals zum Verwalten von Tickets und Bordkarten oder zum Bezahlen mit dem Smartphone genutzt. Ausweise und vertrauenswürdige Nachweise, die wir heute noch als Plastikkarte im Portemonnaie mit uns herumtragen oder in Ordnern abheften, können in Wallets zukünftig vollumfänglich in digitaler Form verwaltet werden. In solch digitaler Form bieten Nachweise und Ausweise zwei bedeutende Vorteile. Zum einen sind sie einfach zu handhaben und maschinenlesbar, was sie zu einem wichtigen Baustein für den Alltag unserer digitalen Gesellschaft macht. Zum anderen werden sie nach dem neuesten Stand der Technik geschützt, sodass eine Fälschung oder Manipulation praktisch unmöglich ist. Ein Ökosystem für Wallets mit digitalen Nachweisen aus verschiedenen Quellen kann zu einem enormen Digitalisierungssprung für Staat, Wirtschaft und Gesellschaft führen. Im Ergebnis werden so Verwaltungen nutzendenfreundlich und europaweit können Nachweise auf datensparsame Weise auf Basis einheitlicher Rahmenbedingungen Verwendung finden.

Mit der neuen eIDAS-Verordnung[1] werden entsprechende Rahmenbedingungen für die Einführung und Nutzung von sogenannten “EU Digital Identity (EUDI) Wallets” geschaffen. Die Verordnung definiert auch einen Implementierungsplan für deren Einführung durch die europäischen Mitgliedsstaaten bis Anfang 2027.

EIN ERSTER SCHRITT ZUR BREITEN AKZEPTANZ DER EUDI-WALLET

Voraussetzung für die Nutzung der EUDI-Wallet ist ein hoheitlicher Identitätsnachweis der Nutzenden auf ihrem Smartphone. Damit können Nutzende sich dann online und vor Ort innerhalb Deutschlands, der EU und in akzeptierenden Drittstaaten mit ihrem Smartphone ausweisen. Außerdem können Nutzende auf dessen Basis auch hochqualitative Nachweise erhalten, z. B. Führerschein, Fahrzeugschein, Zeugnisse oder Studiennachweise.

Deutschland tut sich aus Angst vor Sicherheitsvorfällen und Datenmissbrauch mit digitalen Identitätsnachweisen traditionell schwer. Diese Angst spielte auch bei der Entwicklung der Onlineausweisfunktion des Personalausweises eine wichtige Rolle. Aktuell ist das Sicherheits- und Datenschutzniveau der Online-Ausweisfunktion zwar hoch, diese Ausweisfunktion wurde bisher aber nur von 22 % der Personen überhaupt mindestens einmal genutzt.[2] Stattdessen werden viel häufiger Identitätsnachweisverfahren mit einem niedrigeren Sicherheits- und Datenschutzniveau genutzt,[3] wie z. B. ELSTER- oder Video- und Photo-Ident-Lösungen. Diese Verfahren sind zwar ebenfalls aufwändig, jedoch unkomplizierter in der Handhabung als die Online-Ausweisfunktion des Personalausweises.[4] Gleichzeitig entwickelt das Gesundheitswesen mit der Gesundheits-ID[5] eine sektorspezifische Lösung, um hohen Sicherheitsanforderungen[6] für ihre Anwendungsfälle gerecht zu werden. Statt eines Ansatzes für alle Branchen, werden also mehrere unterschiedliche Identifikationsnachweis-Verfahren in verschiedenen Branchen entwickelt, die miteinander auch nicht interoperabel sind. Ein Großteil der Bürgerinnen und Bürger empfindet diese Vielfalt als kompliziert, wodurch die Akzeptanz gegenüber solchen Verfahren grundsätzlich sinkt. Durch die Vielfalt der Lösungen leiden zudem die Datensparsamkeit und die Sicherheit, vor allem aber die ökonomische Effizienz. Betriebswirtschaftlich wie auch volkswirtschaftlich entstehen Kosten für einen identischen Anwendungszweck, da die Lösungen nebeneinander ohne jedwede Synergieeffekte

[1] Finaler eIDAS Text: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=COM%3A2021%3A281%3AFIN
[2] https://www.heise.de/news/E-Government-Studie-Der-digitale-Ausweis-macht-einen-Sprung-nach-vorn-9795352.html (abgerufen am 12.07.2024)
[3] siehe bspw. Aktivitäten des Chaos Computer Club, nachzulesen unter https://www.ccc.de/en/updates/2022/chaos-computer-club-hackt-video-ident (abgerufen am 12.07.2024)
[4] https://financefwd.com/de/referentenentwurf-video-ident/ (abgerufen am 12.07.2024)
[5] https://www.gematik.de/anwendungen/gesundheitsid (abgerufen am 12.07.2024)
[6] Die gematik definiert hierfür für Anwendungen der TI ein Vertrauensniveau “gematik LoA high” in Anlehnung an eIDAS bzw. entsprechende TRs wie BSI TR-03107-1.

existieren — und das gilt für alle Länder der EU. Diese aktuelle Entwicklung zeigt, wie dringend wir einen einheitlichen Ansatz für digitale Nachweise in EUDI-Wallets in einem interoperablen Ökosystem brauchen, damit der datensparsame Austausch zwischen verschiedenen öffentlichen und privaten Organisationen möglich wird.

Die Akzeptanz gegenüber der EUDI-Wallet ist erfolgskritisch. Um diese bei den Bürgerinnen und Bürgern zu schaffen, muss das Thema Datenschutz eine hohe Priorität haben. Der größtmögliche Schutz von personenbezogenen Daten ist nur mit einer dezentralen Lösung zu realisieren, bei der alle Daten in den Händen der jeweiligen Nutzenden liegen. Für eine gänzlich dezentrale Lösung auf einem hohen Vertrauensniveau fehlt jedoch derzeit die entsprechende Technik. Der erste Versuch, hoheitliche Identitätsdaten sicher im Smartphone zu speichern, ist mit der Einstellung des Smart-eID-Projektes gescheitert. Die Gründe hierfür waren unter anderem die fehlenden technischen Voraussetzungen für eine flächendeckende Skalierung und hohe Kosten.[7] Eine zentrale Erkenntnis aus dem Vorhaben ist, dass die Aspekte Datenschutz, Sicherheit, Nutzbarkeit und Reichweite bei den Nutzenden sorgsam abgewogen werden müssen, um einen erfolgreichen Ansatz zu realisieren.

Statt die Einführung der EUDI-Wallet zu verzögern, indem man erst neue Technik für eine dezentrale Architektur entwickelt und zertifiziert, sollte für die Umsetzung der EUDI-Wallet Technik verwendet werden, die bereits heute auf einem hohen Sicherheitsniveau unmittelbar funktioniert. Die Präsidentin des Bundesamts für Sicherheit in der Informationstechnik, Claudia Plattner, hat daher als sogenannte “Evolutionslösung” die Kombination von etablierten Sicherheitsmodulen auf dem Smartphone und einem Sicherheitsserver mit einem Hardware-Sicherheitsmodul vorgeschlagen.[8] In diesem Sicherheitsmodul werden geheime Schlüssel physikalisch geschützt aufbewahrt. Eine vergleichbare Lösung ist heute bereits in Österreich im Einsatz.[9] Die Bundesagentur für Sprunginnovationen (SPRIND) unterstützt diesen Vorschlag und sieht ihn als sinnvollen ersten Schritt für die Implementierung eines Identifikationsnachweisverfahrens in der deutschen EUDI-Wallet, bis die technischen Voraussetzungen vorliegen, um ein vollständig dezentrales System mit Smartphones zu etablieren.

AUTHENTIFIZIERTER KANAL ODER SIGNIERTE DATEN?

Prinzipiell bestehen zwei technische Optionen zur Umsetzung digitaler Nachweise mit aktuell verfügbaren und praktisch erprobten Verfahren: der “authentifizierte Kanal” und die Nutzung “signierter Daten”. Beide Ansätze werden dabei mit Hilfe von Cloud-Komponenten implementiert, um die hohen Sicherheitsanforderungen an die eID-Lösung kurzfristig zu gewährleisten. Die folgende Analyse basiert auf dem Architekturvorschlag des Architektur- und Konsultationsprozesses zur Umsetzung der eIDAS-Verordnung in Deutschland,[10] den SPRIND im Auftrag des Bundesministeriums des Innern und für Heimat im Rahmen eines öffentlichen Konsultationsprozesses durchführt.

Authentifizierter Kanal

Der authentifizierte Kanal wird heute bereits in der Online-Ausweisfunktion eingesetzt. Kurz beschrieben erfolgt im Rahmen dieses Protokolls ein sogenannter Diffie-Hellman-Schlüsselaustausch zwischen einem Sicherheitselement im Ausweis und derjenigen Akzeptanzstelle, welche die Identität des Nutzers anfragt. Der Prozess beweist einerseits der Akzep-

[7] https://www.egovernment.de/was-ist-die-smart-eid-a-f4e20813066cefa690eef2637680ff57/ (abgerufen am 12.07.2024)
[8] https://www.youtube.com/watch?v=u1SuLBgGIxg
[9] https://www.oesterreich.gv.at/id-austria.html
[10] https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept

tanzstelle, dass ein echtes Sicherheitselement vorliegt (ausgestellt von der Bundesdruckerei). Andererseits beweist er auch dem Sicherheitselement, dass die Akzeptanzstelle berechtigt ist, Daten aus dem Sicherheitselement auszulesen. Nach erfolgreicher Authentifizierung wird im Ergebnis zwischen den beiden dann der Kanal etabliert. An die Stelle des physischen Sicherheitselements im Ausweis würde bei der EUDI-Wallet jedoch eine Hardwarekomponente in einem bundeseigenen Sicherheitsserver treten.[11] Dieser Sicherheitsserver stellt bei jeder Anfrage einen Identifizierungsnachweis für die jeweilige Akzeptanzstelle aus. Im Sinne des Datenschutzes erfährt der Server durch die Zwischenschaltung der Wallet auf dem Smartphone nicht, bei welcher Akzeptanzstelle der Nachweis zum Einsatz kommen wird, sondern nur, dass die Wallet einen Nachweis erbittet. Der Server kann aber nachvollziehen, wann welcher Nutzer von welcher IP-Quelladresse einen Identifizierungsvorgang durchführt. Und abhängig von der verwendeten Technologie erfährt der Server auch, welche Attribute verwendet werden. Das nennt man Beobachtbarkeit (Observability).

Die Beobachtbarkeit kann beim authentifizierten Kanal nur noch weiter reduziert werden, wenn die vertrauenswürdige Komponente in einem Sicherheitselement auf dem Smartphone implementiert wird. Die vertrauenswürdige Komponente im Sicherheitselement kann jede beliebige Identität bestätigen. Sollte also nur ein einziges dieser Sicherheitselemente in einem einzigen Smartphone geknackt werden, ergibt sich ein systemisches Sicherheitsrisiko:[12] Das geknackte Sicherheitselement könnte dann dafür missbraucht werden, jede beliebige Identität gegenüber jeder Akzeptanzstelle zu bestätigen, inklusive der Erstellung gänzlich neuer Identitäten. Kriminelle Aktivitäten wären durch den missbräuchlichen Einsatz gefälschter, aber existierender Identitäten extrem schwierig zu erkennen und zu verhindern. Die sichere Implementierung einer solchen Architektur erfordert deshalb Hardware-Sicherheitselemente im Smartphone, die auf einem sehr hohen Niveau zertifiziert sind (vgl. Smart eID). Derzeit ist jedoch noch nicht absehbar, wann derart zertifizierte Sicherheitselemente breit von allen Smartphone-Herstellern bereitgestellt werden, was einer der Gründe für die Einstellung des Smart-eID-Ansatzes war.

Signierte Daten

Bei der Verwendung von signierten Daten erfolgt eine Aufteilung der Aufgaben zwischen dem bundeseigenen Ausstellungsserver der Identitätsnachweise und dem Betreiber der Wallet-App.[13] Der Ausstellungsserver erzeugt die Identitätsnachweise auf Vorrat, bindet sie an kryptografische Bestätigungsschlüssel und überträgt die Identitätsnachweise an die Wallet-App. Nutzende behalten die Kontrolle über die Bestätigungsschlüssel, die dann auf dem Sicherheitsserver des Wallet-Betreibers in einem Hardware-Sicherheitsmodul liegen. Wenn Nutzende einen Identitätsnachweis verwenden möchten, dann lassen sie den Wallet-Betreiber mit dem entsprechenden privaten Bestätigungsschlüssel eine Signatur erstellen und präsentieren diese Signatur zusammen mit dem Identitätsnachweis gegenüber der Akzeptanzstelle. Durch diese Aufgabenteilung kann der bundeseigene Ausstellungsserver also die Nutzung der von ihm ausgestellten Identitätsnachweise nicht verfolgen. Auf der anderen Seite bekommt der Wallet-Betreiber die Identitätsnachweise niemals zu Gesicht, denn sie werden direkt in der Wallet-App gespeichert und aus dieser an die Akzeptanzstelle übertragen. Der Wallet-Betreiber kann nur die Nutzung von Bestätigungsschlüsseln beobachten (vergleichbar mit Pseudonymen). Insbesondere sieht der Server des Wallet-Betreibers nicht, welche Attribute der Nutzenden weitergegeben werden. Neben dem Ausschluss der Beobachtbarkeit für den Aussteller der Identitätsnachweise kann damit also auch das, was der Wallet-

[11] https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept/-/blob/main/flows/PID-AuthenticatedChannel-cloud.md
[12] https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept/-/blob/main/architecture-proposal.md?ref_type=heads#hardware-security-considerations, Option D
[13] https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept/-/blob/main/flows/PID-IssuerSigned-cloud.md

Betreiber beobachten kann, auf ein Mindestmaß reduziert werden. Um den Datenschutz weiter zu steigern, können auch verschiedene Wallet-Betreiber für diese Aufgabe zugelassen werden, um den Nutzenden die Auswahl zu überlassen, welchem Betreiber sie vertrauen. So werden diejenigen Wallet-Betreiber gewählt und begünstigt, die ihren Nutzen einen hohen Datenschutz bieten. Ein höheres Maß an Nicht-Beobachtbarkeit kann mit der Cloud-basierten Architektur nicht erreicht werden. Dafür ist in Zukunft eine vollständig dezentrale Lösung notwendig.

Bei der Verwendung von signierten Daten wird die Fälschungssicherheit durch die Signatur des Ausstellungsservers in einem zertifizierten Rechenzentrum in Deutschland gewährleistet. Daher muss beim Übergang auf eine dezentrale Lösung auf dem Smartphone nur noch sichergestellt werden, dass diese signierten Identitätsdaten nicht von einem Angreifer kopiert und zum betrügerischen Ausweisen verwendet werden können. Das wird verhindert, indem die Identitätsdaten an den Bestätigungsschlüssel im Sicherheitselement des Smartphones gebunden werden, sodass die Identitätsdaten auf dem Sicherheitselement eines Smartphones nicht mit dem Sicherheitselement eines *anderen* Smartphones verwendet werden können. Solch ein Sicherheitselement kann natürlich auch das Ziel von Angreifern werden, allerdings hat das Brechen eines solchen Sicherheitselements ausschließlich Auswirkungen auf die verwalteten Identitätsnachweise auf dem einen gebrochenen Smartphone.

Zwar verfügen viele moderne Smartphones bereits über derartige Sicherheitselemente, die sich in der Regel auch bequem über die biometrischen Funktionen des Smartphones schützen lassen. Leider erfüllen diese Sicherheitselemente derzeit aber nur die Anforderungen an ein sog. substantielles Vertrauensniveau. Dieses Niveau reicht jedoch für viele Anwendungsfälle aus, z. B. für die Einrichtung einer qualifizierten elektronischen Signatur und sogar, nach Zustimmung des Nutzenden, für Anwendungen im Gesundheitswesen[14]. Unter Einbindung von BfDI und BSI hat die gematik mit der Gesundheits-ID und den eRezept-Spezifikationen sogar Ansätze signierter Daten mit einem hohen Vertrauensniveau für den Einsatz innerhalb und außerhalb der Telematikinfrastruktur freigegeben. Weitere Verbesserungen zur Erhöhung des Vertrauensniveaus sind hierbei absehbar, weil es weltweit einen Bedarf für Sicherheitselemente gibt, die Bestätigungsschlüssel auf einem hohen Vertrauensniveau erforderlich machen. In diesem Zusammenhang arbeitet SPRIND auch mit den relevanten Ökosystem-Akteuren im Rahmen des SPRIND Funke “EUDI Wallet Prototypes” zusammen.

DIE KLARE VORTEILHAFTIGKEIT SIGNIERTER DATEN

Trotz der jahrzehntelangen praktischen Bewährung von elektronischen Signaturen wird die Verwendung hoheitlicher Signaturen für Identitätsdaten in Deutschland sehr kontrovers diskutiert, bis hin zur grundsätzlichen Ablehnung durch einige Akteure.[15] **Kern der Ablehnung ist die These, dass hoheitliche Signaturen den Wert der Identitätsdaten erhöhen und damit die Attraktivität für Angreifer und böswillige Akteure steigern.** SPRIND sieht derzeit für eine Erhöhung des Risikos durch hoheitlich signierte Daten keine Belege, weder durch bekannte Sicherheitsvorfälle noch durch akademische Publikationen, was notwendig wäre, um die Auswirkungen und Risiken auf empirischer Basis bewerten zu können. Vielmehr sehen wir sehr wahrscheinlich Evidenzen, dass diese These falsch ist:

Erstens lässt sich die These anhand der Entwicklungen und Erfahrungen der letzten zehn Jahre im Bereich hoheitlicher eID-Systeme überprüfen. In diesem Zeitraum implementierten alle anderen Mitgliedsstaaten der EU hoheitliche eID-Systeme mit digitalen Signaturen, aus-

[14]https://gemspec.gematik.de/docs/gemSpec/gemSpec_IDP_Sek/gemSpec_IDP_Sek_V2.4.0_Aend/#gemSpec_IDP_Sek_V2.3
[15]https://gitlab.opencode.de/-/project/1104/uploads/1c62ab180cdec52505fbf9b3a51271e2/Stellungnahme_eID.pdf

genommen die Niederlande und die Slowakei. Sogar der deutsche Personalausweis beinhaltet im Sinne der technischen Interoperabilität innerhalb von Europa mittlerweile die Personendaten in signierter Form, damit wir uns in Deutschland und im Ausland an automatischen Grenzkontrollanlagen ausweisen können. Würde die These zutreffen, dann wären die eID-Systeme der europäischen Mitgliedsländer mit der Verwendung von signierten Daten ein besonders attraktives Ziel für böswillige Akteure im Vergleich zu den Systemen mit einem authentifizierten Kanal. Es liegen dafür jedoch trotz der breiten Nutzung auch nach über zehn Jahre keine empirischen Belege vor, bei denen signierte Daten ursächlich waren oder die Auswirkungen verschärft hätten. Diese Belege sind auch extrem unwahrscheinlich, da aus Sicht der Angreifer der Herkunftskontext der Identitätsdaten (z. B. von einer Behörde oder einer Bank) relevanter ist als die Frage, ob diese staatlich signiert sind oder nicht. Wenn ein Angreifer böswillig Identitätsdaten von z. B. einer Bank erbeutet, dann kann er sich sicher sein, dass diese authentisch sind, da die Bank zur Erhebung dieser entsprechende Geldwäschegesetzesvorgaben erfüllen musste, was auf die Authentizität schließen lässt. Die Frage, ob diese Daten dann staatlich signiert sind oder nicht, ist in dem Fall zweitrangig. Es gibt auch keine Evidenz dafür, dass so erworbene signierte Datensätze einen höheren Marktwert hätten als unsignierte Daten.

Zweitens setzen selbst zentrale Komponenten für hoheitliche Identitätssysteme der öffentlichen Verwaltung in Deutschland bereits heute signierte Daten ein. Zum Beispiel verwenden die Schnittstellen der meisten eID-Server für die Online-Ausweisfunktion und die Bürgerkonten[16] Protokolle wie SAML[17] oder OpenID Connect[18], die als Ergebnis des Prozesses signierte Identitätsnachweise an die Akzeptanzstelle liefern. Auch im Kontext der EUDI-Wallet stellen die meisten Experten die Nutzung von Signaturen intuitiv überhaupt nicht infrage, da diese seit Jahrzehnten das effizienteste Mittel für den Schutz der Integrität und Authentizität von Daten sind. Die Niederlande, als eines der wenigen Länder, die in ihrem bestehenden eID-System auf den authentifizierten Kanal setzen, hat seine Wallet-Lösung nun mit Signaturen implementiert und deren Quellcode als Open Source veröffentlicht.[19] Die Schweiz hat nach einem parlamentarischen Prozess vor kurzem beschlossen,[20] ihre neue eID auf der Basis der in Smartphones verfügbaren Hardware-Sicherheitselemente und damit unter Nutzung von Signaturen zu implementieren[21]. Neben den hoheitlichen Identitätsnachweisen werden im Rahmen des EUDI-Wallet-Ökosystems zudem auch weitere qualifizierte elektronische attestierte Attribute herausgegeben, welche die Authentizität unterschiedlicher Nachweise in der EUDI-Wallet zusätzlich bestätigen, bspw. ein Zeugnis oder die Vertretungsberechtigung für eine juristische Person. Die aktualisierte eIDAS-Verordnung sieht für deren Absicherung ausschließlich die Verwendung digitaler Signaturen vor.[22] Dies zeigt, dass die Verwendung von digitalen Signaturen in der Vergangenheit bei Identitätssystemen und auch mit Blick auf die Umsetzung von Wallet-Lösungen im Zuge der neuen eIDAS-Verordnung für die meisten EU-Staaten und Partnerländer die Wahl der technischen Ausgestaltung ist.

Drittens wurde der authentifizierte Kanal in der Online-Ausweisfunktion des Personalausweises verwendet, um die missbräuchliche Weitergabe von Daten mit einer “hoheitlichen Echtheitsgarantie” zu verhindern.[23] Insbesondere ging es darum, den Weiterverkauf von Identitätsdaten zu verhindern. Die Entwicklung im deutschen Markt hat jedoch gezeigt, dass dieser Weiterverkauf trotz des authentifizierten Kanals nicht verhindert werden konnte. Es gibt diverse Unternehmen, die bei der Nutzung des Personalausweises über die Online-Aus-

[16] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03160/BSI-TR-03160-2.pdf
[17] https://www.oasis-open.org/standard/saml/
[18] https://openid.net/specs/openid-connect-core-1_0.html
[19] https://github.com/MinBZK/nl-wallet
[20] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-101414.html
[21] https://github.com/e-id-admin/open-source-community/blob/main/tech-roadmap/tech-roadmap.md
[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20240520
[23] Bender, Kügler, Markgraf, Naumann, Sicherheitsmechanismen für kontaktlose Sicherheitselemente im deutschen elektronischen Personalausweis, Datenschutz und Datensicherheit, 3/2008,

weisfunktion Identitätsdaten der Nutzenden erlangen und diese danach zur erneuten Identifizierung des betreffenden Nutzenden bei Anwendungspartnern wiederverwenden. Das deutsche Geldwäschegesetz (§ 17) erlaubt diesen Austausch zwischen Finanzinstituten sogar explizit. Hierbei wird deutlich, dass sich die Behauptungen zu den Vorteilen des authentifizierten Kanals beim elektronischen Personalausweis nicht bewahrheitet haben, da entsprechende Möglichkeiten zur Weitergabe von Identitätsdaten durch den Gesetzgeber explizit vorgesehen sind. Dies ist ein weiterer Beleg, dass das Vertrauen in die Authentizität von Identitätsdaten auf das Vertrauen in die ausstellenden Partei und deren Prozess und Haftungszusagen basiert und nicht die staatliche Signatur entscheidend ist.

Viertens rückt die polarisierende Diskussion zu den Risiken von signierten Daten leider in den Hintergrund, dass Digitalisierung generell mit dem Risiko des Diebstahls von personenbezogenen Daten verbunden ist. Entsprechende Vorfälle treten mittlerweile sehr häufig auf, da nicht jedes System, das personenbezogene Daten verarbeitet, geprüft und zertifiziert werden muss und kann. Es ist eine gesamtgesellschaftliche Aufgabe von Staat, Organisationen und Individuen, die IT-Sicherheit unter Berücksichtigung technischer, regulatorischer, ökonomischer Aspekte sowie dem Nutzendenverhalten im Umgang mit IT-Systemen zu verbessern. Auf die Adressierung dieses Problems müssen wir uns fokussieren, da es aus Sicht der Nutzenden die unautorisierte Weitergabe von personenbezogenen Daten das Problem ist, egal ob diese Daten signiert sind oder nicht.

Für den authentifizierten Kanal spricht einzig die Möglichkeit der Abstreitbarkeit der Authentizität einer bestimmten Identität. Dafür existiert jedoch kein praktisch relevantes Risikopotenzial. Der hohe Grad an Beobachtbarkeit in der Cloud-basierten Architektur wiegt dafür umso schwerer, denn sie nährt die Kritik, dass das EUDI-Wallet das Potenzial zur Massenüberwachung durch den Staat besitzt[24]. Aus dem eGovernment Monitor 2023 geht hervor, dass nur 35 % der Befragten der Regierung Vertrauen entgegenbringen. Folglich könnte eine Möglichkeit der Überwachung durch den Staat dieses Vertrauen weiter reduzieren.[25] Gleichsam ist zu erwarten, dass eine effizientere Verwaltung mit digitalen Diensten den Staat leistungsfähiger erscheinen lässt und das Vertrauen der Bürger steigert. Des Weiteren wäre der authentifizierte Kanal ein deutscher Sonderweg. Kein anderes Land in der EU nutzt gemäß den derzeitigen Implementierungsansätzen den authentifizierten Kanal. Deutschland müsste die Entwicklungskosten für den authentifizierten Kanal vollkommen alleine tragen und ebenso die Kosten, um die deutsche EUDI-Wallet in Europa sicher nutzbar zu machen. In der Folge ist zu befürchten, dass der deutsche Sonderweg nur schleppend oder gar nicht im europäischen Ökosystem implementiert wird und zur faktischen Ausgrenzung deutscher Bürgerinnen und Bürger hinsichtlich pan-europäischer digitaler Dienste führt.

Im Gegensatz zum authentifizierten Kanal hat der europaweite Einsatz von signierten Daten mit Blick auf die Schaffung eines Ökosystems für digitale Nachweise entscheidende Vorteile. Erstens setzen diese Verfahren auf etablierte und erprobte technische Konzepte auf, was die Komplexität reduziert und die Widerstandsfähigkeit gegen Angreifer erhöht. Zweitens ist der Ansatz interoperabel mit den Wallets anderer EU-Mitgliedsstaaten und ermöglicht dabei große Synergien durch die Open-Source-Bereitstellung im Zuge einer gemeinsamen Entwicklung (z.B. durch die EUDI Wallet Reference Implementation[26]) und Standardisierung. Drittens ist die Weiterentwicklung der ersten Stufe der deutschen EUDI-Wallet zur vollständig dezentralen Wallet-Lösung mit Sicherheitsmodulen im Smartphone deutlich effizienter und früher zu erreichen, denn die Anforderungen an die Sicherheitsmodule beim Umgang mit Signaturen sind viel einfacher zu erfüllen, als mit einem authentifizierten Kanal. Gleiches

[24] https://netzpolitik.org/2023/eidas-trilog-hunderte-wissenschaftlerinnen-und-dutzende-ngos-warnen-vor-massenueberwachung/
[25] https://initiatived21.de/uploads/03_Studien-Publikationen/eGovernment-MONITOR/2023/eGovMon2023_eng.pdf
26 https://github.com/eu-digital-identity-wallet/.github/blob/main/profile/reference-implementation.md

gilt auch für den Ausbau des Ökosystems für digitale Nachweise, da weitere Nachweisattribute wie Bildungszeugnisse ohnehin auf signierte Daten setzen und durch eine einheitliche Architekturbasis zahlreiche Synergien im Vergleich zum authentifizierten Kanal existieren.

EMPFEHLUNG: SIGNIERTE DATEN MIT FOKUS AUF DEZENTRALE LÖSUNG

Deutschland benötigt dringend eine funktionierende Identifizierungslösung als erste Iteration der EUDI-Wallet. Denn nur so können wir den Innovationsstau in der Digitalisierung unserer Gesellschaft angehen. **Unter Abwägung der zentralen Erfolgsfaktoren Datenschutz, Sicherheit, Nutzbarkeit, Reichweite und Kosten zur Einführung der ersten Iteration der zukünftigen deutschen EUDI-Wallet empfiehlt SPRIND die Nutzung von digitalen Signaturen.** Diese Architekturoption erfüllt neben hohen Datenschutz- und Sicherheitsanforderungen die Anforderung nach einer schnellen, kosteneffizienten und nachhaltigen Implementierung auf Basis maximaler europäischer Interoperabilität. Die Vorteile ergeben sich auch für die Bürgerinnen und Bürger sowie die Anwendungspartner, da diese durch eine geringe Komplexität und Synergien bei der Anbindung und Verwendung profitieren. Genauso wie deutsche Organisationen andere europäische EUDI-Wallets einfach integrieren wollen, muss es das Ziel sein, dass die Bürgerinnen und Bürger ihre deutsche EUDI-Wallet-Lösung unkompliziert zum Beispiel während eines Urlaubes im EU-Ausland einsetzen können.

Gleichzeitig ermöglicht uns der Einsatz von digitalen Signaturen im Zuge dieser Lösung gegenüber dem Status quo mit einer Vielzahl von öffentlichen und privaten Identifizierungslösungen das Sicherheits- und Datenschutzniveau signifikant anzuheben und die Nutzbarkeit deutlich zu verbessern. Durch den produktiven Einsatz von digitalen Signaturen können wir eigene Erfahrungen im Umgang mit hoheitlich signierten Daten sammeln und auf dieser Basis das Thema in einigen Jahren erneut evaluieren. Wir müssen die *German Angst* vor hoheitlichen Signaturen überwinden, sonst werden zum wiederholten Male enorme Gelder und viel Zeit fehlinvestiert, ohne bei den eigentlichen Herausforderungen mit Blick auf die Entwicklung eines Ökosystems von digitalen Nachweisen und allgemein der Digitalisierung von Deutschland voranzukommen.

Unser langfristiges Ziel ist eine dezentrale Lösung. Im Rahmen des SPRIND-Funkens “EUDI Wallet Prototypes” werden gerade innovative Ansätze für das Architekturdesign von Wallets experimentell erprobt, die das langfristige Ziel einer vollständig dezentralen Lösung bei noch mehr Sicherheit, Datenschutz und Nutzungsfreundlichkeit ermöglichen sollen. Wir sind überzeugt, dass Erkenntnisse aus diesem Innovationswettbewerb in die deutsche Implementierung zukünftig einfließen werden und einen positiven Beitrag zur Entstehung des Ökosystems für digitale Nachweise in Europa leisten können.

Nachdem die Grundlagen mit der ersten Iteration einer deutschen EUDI-Wallet geschaffen worden sind, kann die Digitalisierung Deutschlands gemeinsam vorangetrieben werden. Mehr als 11.000 Kommunen, die Länder und der Bund müssen ertüchtigt werden, die diversen Bescheinigungen und Nachweise zu digitalisieren. Ähnliches gilt für die Zeugnisse der über 30.000 Schulen und Hochschulen in Deutschland. Es besteht ein enormes Potenzial für Effizienzgewinne, Prozessbeschleunigung und Kosteneinsparung. Nicht zuletzt gewinnen alle stark überlasteten Behörden deutlich an Handlungsspielraum, sodass sie ihre Aufgaben wieder in einer Qualität erledigen können, die ihren eigenen Ansprüchen gerecht wird.

Es gibt viel zu tun. Lassen Sie uns auf Basis signierter Daten als Architekturoption für die Evaluationslösung einen überfälligen und großen Digitalisierungssprung in Deutschland nach vorne machen! Jetzt ist der Moment, endlich die notwendigen Entscheidungen zu treffen und die digitale Transformation aktiv zu gestalten. Gemeinsam können wir die Grundlage

für ein sicheres, effizientes und nutzendenfreundliches digitales Identitätssystem schaffen, das nicht nur Deutschland, sondern ganz Europa voranbringt. Treten Sie mit uns ein für eine innovative Zukunft und machen Sie den Mut zur Digitalisierung zu unserer gemeinsamen Mission. Zusammen schaffen wir ein digitales Ökosystem, das Vertrauen, Sicherheit und Fortschritt in den Mittelpunkt stellt. Lassen Sie uns die Chancen der Digitalisierung nutzen und Deutschland an die Spitze der digitalen Innovation führen!