



## Nutzungsqualität im Fokus: Ergebnisse einer Fokusgruppe zur Wahrnehmung der Nutzungsqualität einer SSI-Anwendung mit Dongle

Sarah Ebert<sup>1</sup> , Anna-Magdalena Krauß<sup>2</sup> , Ben Biedermann<sup>3</sup> , Olivia Jürgenssen<sup>4</sup>  und Jürgen Anke<sup>5</sup> 

**Abstract:** Die vorliegende Arbeit untersucht die Nutzungsqualität von Self-Sovereign Identity (SSI) Wallets mit einem zusätzlichen Hardware-Kryptographie-Faktor. Mithilfe einer Fokusgruppe, bestehend aus fünf Teilnehmenden unterschiedlicher technischer Kompetenz, wurde eine Wallet mit Dongle im Kontext eines ÖPNV-Anwendungsfalls getestet und anschließend diskutiert. Die Ergebnisse unterstreichen die Notwendigkeit benutzerfreundlicher Technologien, um das Vertrauen der Nutzenden zu gewinnen. Zudem zeigen sie die Bedeutung von Transparenz und offenen Standards für die Akzeptanz der Lösung auf. Abschließend wurden Propositionen formuliert, die weitere Forschung ermöglichen.

**Keywords:** Self-Sovereign Identity, Fokusgruppe, Nutzungsqualität, Wallet, Dongle, Usability

### 1 Einleitung

Mit zunehmender Digitalisierung durchdringen digitale Dienste und Anwendungen heutzutage alle Bereiche des gesellschaftlichen Lebens - so auch den Bereich der Öffentlichen Verwaltung. Mit der Entwicklung von Anwendungsmöglichkeiten und der damit einhergehenden Konvergenz verschiedener Verwaltungsbereiche und Fachverfahren wächst auch die Zahl der Menschen und Geräte, die sich digital identifizieren müssen [PR21]. Diese Entwicklung bedingt neue wirtschaftliche, soziale, politische, ethische, kulturelle und rechtliche Risiken, die das Vertrauen in internetbasierte Anwendungen schwächen [Wi20]. Bereits Cameron [Ca07] mahnte, dass die Zunahme von Cyberkriminalität das

---

<sup>1</sup> HTW Dresden, Arbeitsgruppe Digitale Dienstleistungssysteme, Friedrich-List-Platz 1, 01069 Dresden, sarah.ebert@htw-dresden.de, <https://orcid.org/0009-0009-1455-9001>

<sup>2</sup> HTW Dresden, Arbeitsgruppe Digitale Dienstleistungssysteme, Friedrich-List-Platz 1, 01069 Dresden, anna-magdalena.krauss@htw-dresden.de, <https://orcid.org/0000-0002-9950-0253>

<sup>3</sup> Islands and Small States Institute, University of Malta, Msida MSD 2080, Malta, bb@acurraent.com, <https://orcid.org/0000-0003-1331-6517>

<sup>4</sup> HTW Dresden, Arbeitsgruppe Digitale Dienstleistungssysteme, Friedrich-List-Platz 1, 01069 Dresden, olivia.juergenssen@htw-dresden.de, <https://orcid.org/0009-0002-7088-2216>

<sup>5</sup> HTW Dresden, Arbeitsgruppe Digitale Dienstleistungssysteme, Friedrich-List-Platz 1, 01069 Dresden, juergen.anke@htw-dresden.de, <https://orcid.org/0000-0002-9324-9387>

Vertrauen der Öffentlichkeit in das Internet gefährde. Die Risiken und negativen Technikfolgen digitaler Transformation fordern Forschende und Entwickelnde die Folgen digitaler Systeme in Transformationsprozessen umfassend zu verstehen, um Hardware und Software verantwortungsvoll anhand menschlicher Werte und Bedürfnisse zu gestalten [Al21a], [Tr22], [Zw21].

Mittlerweile umfasst das E-Government auch digitale Identitätslösungen zur Stärkung des Vertrauens in die Digitalisierung. Aktuelle Studien belegen die Wechselwirkung zwischen Vertrauen in das Internet und in die Nutzung von E-Government-Angeboten [In23], [Pr23], daher müssen auch digitale Identitätssysteme ganzheitlich auf ihre Auswirkungen auf menschliches Wohlbefinden und die Gesellschaft untersucht werden [Sa21]. Nur so kann Vertrauen von Bürger\*innen in digitale Identitäten unter der Garantie des Staates gewährleistet werden [Al21b].

Im Projekt „ID-Ideal“ als Teil des Projektverbundes „Schaufenster Sichere Digitale Identitäten“ werden Bürger\*innen mittels Fokusgruppen in die Technikfolgeabschätzung selbstbestimmter digitaler Identitäten einbezogen [Ve19], da Bevölkerungsbedürfnisse für die Entwicklung und Erprobung niedrigschwelliger Lösungen für die *Regulation on electronic Identification, Authentication, and trust Services (eIDAS)* [Eu21] unerlässlich sind. In enger Zusammenarbeit von Kommunen und Technologieanbietenden wurden so Bevölkerungsbedürfnisse für den Transformationsprozess im Fall der Landeshauptstadt Dresden erfasst.

Für die Durchführung der Fokusgruppe, deren Ergebnisse im Rahmen dieser Arbeit vorgestellt werden, wurden Privatsphäre-schonende und Wallet-basierte Verfahren mit zwei Faktoren verwendet, die unter dem Paradigma Self-Sovereign Identity (SSI) für sicheren Nachweisaustausch standardisiert werden [PR21]. Für den Anwendungsfall *öffentlicher Nahverkehr* untersuchte die Fokusgruppe subjektiv wahrgenommene Mehrwerte [Wi22], um Nachfragefaktoren für die Nutzung von SSI-Wallets für kommunale Dienste [Bi23] zu identifizieren. In diesem Zusammenhang trug die Forschungsfrage „*wie wird die Nutzungsqualität von Wallets mit hardwarekryptografischem zweitem Faktor wahrgenommen?*“ dem Spannungsfeld zwischen Praktikabilität und Sicherheit explizit folge, da bisher keine Technikfolgeabschätzung für Zwei-Faktor-SSI-Wallets vorliegt.

## 2 Grundlagen

*Self-Sovereign Identity* (SSI) ist ein dezentraler Ansatz zur Identitätsverwaltung, der oft im Zusammenhang mit digitalen Wallets, meist als Smartphone-App, präsentiert wird [Eh21]. Nutzende erhalten Identitätsmerkmale und Berechtigungen, in Form von maschinenlesbaren und kryptografisch gesicherten digitalen Nachweisen [Mü18]. Diese so genannten *verifiable credentials* (VCs) [Sp23] können unabhängig von Ausstellenden in der Wallet verwaltet werden [Eh21]. Die Nutzenden, auf welche die jeweiligen VCs ausgestellt sind, interagieren mit Ausstellenden, sogenannte *issuers*, und Überprüfenden (*veri-*

fiers) direkt und ohne auf eine dritte Partei angewiesen zu sein [Mü18]. Nutzende entscheiden selbst, ob sie Daten teilen möchten, wenn sie dazu aufgefordert werden, und akzeptieren oder lehnen die Anfrage über ihre Wallet ab. Um den Nutzungsversprechen von SSI gerecht zu werden, dass Identitäten persistent, inklusiv, und zugänglich sind, bedarf es neben Sicherheit auch einer guten *usability* [St18]. Nur so kann auch Akzeptanz von SSI-Lösungen erreicht werden [Se22], [Za21].

Obwohl SSI-Ansätze als *work in progress* [Av19] gelten und auch eine philosophische Perspektive auf Identitäts- und Zugangsmanagement umfassen [Bo21], müssen bei der Implementierung von SSI im Gemeinwesen die Nutzungsqualität und die Nutzendenpräferenzen besonders beachtet werden [WK16]. So hat SSI zwar ihren Ursprung in technikorientierten Blogposts [We22], der forstgesetzte Fokus des Diskurses um SSI auf deren technologischen und epistemologischen *Systemqualitäten* gefährdet allerdings die Einbeziehung der Perspektive der Bürger\*innen bei der Erstellung einer neuen massentauglichen E-Government-Lösung [WK17]. Mehr noch, das Hervorheben des Technologie- und Lösungsangebots verhindert die Anwendung einer stringent *serviceorientierten Perspektive* [Wi22] auf die Nutzung von SSI-Applikationen im behördlichen Kontext und Gemeinwesen.

Basierend auf den Säulen *Systemqualität*, *Servicequalität*, als auch *Nutzungsqualität* richtet dieser Beitrag hingegen den Fokus auf die Nachfrageseite von SSI-Lösungen [Wi22]. Während mit Servicequalität grundsätzlich das Leistungsangebot und dessen Gestaltung gemeint ist, bezieht sich Nutzungsqualität auf eine Vielzahl von Eigenschaften, die verwendet werden können, um die Nutzendenerfahrung von *e-government* und deren Auswirkung auf realisierte Nutzung zu beschreiben [Wi22]. Gerade im Hinblick auf besondere Sicherheitsanforderungen durch die von hoheitlichen Identitätsapplikationen auf europäischer Ebene [Sh22], ist die Betrachtung von besonderen Sicherheitsmerkmalen unter dem Aspekt Nutzungsqualität unerlässlich.

Hierfür greift dieser Artikel die Methode einer Fokusgruppe auf und stützt sich auf Studien zur Nutzung von hoheitlichen digitalen Anwendungen in Deutschland [In22a], [Pr23]. Diese clustern Nutzende anhand ihrer Präferenzen, um die Einstellungen von Bürger\*innen zu hoheitlicher digitaler Identität und ihr Vertrauen theoretisch und empirisch abzubilden [In22a], [Pr23]. Es fehlt eine differenzierte Betrachtung der Nutzendenfreundlichkeit in Abhängigkeit verschiedene Sicherheitsbedürfnisse, die durch SSI-Wallets erfüllt werden. Das Erzeugen und Verwalten von Schlüsselmateriale in gehärteten Hardware-Umgebungen, die unzulässiges Teilen digitaler Identitäten verhindern sollen, ist noch auf *Usability* zu untersuchen. Folglich werden Nutzendeneinstellungen zur SSI-gestützten Verwendung von Smartcards untersucht. Diese sind von variierender Abmessung, Bauart, Kommunikationskanälen, und Preis.

- **USB-C Thumbdrive** <sup>6</sup>: Steckverbindung zum Smartphone und LED-basierter Interaktion

---

<sup>6</sup> <https://www.acs.com.hk/en/products/538/acr39t-a5-smart-card-reader/>

- **Bluetooth Dongle<sup>7</sup>:** *Wireless Workflow* in der *Wallet App* und Bestätigung der Gerätekopplung durch LED nach Einstecken der Karte in den Dongle

### 3 Studiendesign

Um die Nutzungsqualität mit den Nutzendenerfahrungen theoretisch zu verknüpfen, stützt sich dieser Beitrag auf das Technology Acceptance Models (TAM), welches bereits zur Evaluation von Nützlichkeit von e-government Anwendungen herangezogen wurde [WK16]. Die Eigenschaften von Zwei-Faktor-Wallets müssen sich mit den Präferenzen der Bürger\*innen überschneiden, um für kommunale Anwendungsfälle als nützlich wahrgenommen zu werden [Da89], [Ra12]. Allerdings fehlt für die Untersuchung von Pull-Faktoren für die kommunale Nutzung von SSI-Wallets mit einem zweiten Faktor – damit auf einem hohen Vertrauensniveau [Sh22] – quantitativ-deduktive Forschung. Daher greift dieser Beitrag auf das qualitativ-induktive Verfahren der Fokusgruppe zurück [CC17], um zur Schließung dieser Forschungslücke beizutragen.

Eine Fokusgruppe bezieht sich nach Nestler [Ne22] auf eine moderierte Diskussion einer Gruppe von Menschen zu einem bestimmten Thema unter der Leitung von UX-Experten und -Expertinnen. Es wurden fünf Teilnehmende mit unterschiedlichen technologischen Kompetenzen und soziodemographischen Faktoren rekrutiert. Diese Eigenschaften wurden vor Beginn der Fokusgruppe über einen Vorabfragebogen ermittelt. Die Teilnehmenden wurden anhand ihrer Antworten in die Segmente eingeteilt, die von der Initiative D21 e.V. im Rahmen der Studie „D21-Digital-Index 2021/2022“ [In22b] ermittelt wurden: digital mithaltend (mittlere Affinität zu Digitalthemen, d.h. Besitz notwendiger Fähigkeiten, neutrale Einstellung gegenüber Digitalisierung [In22b]) und digital vorreitend (großes Interesse an Digitalthemen, vielfältiges Nutzungsverhalten und souveräner Umgang mit Digitalisierungs Herausforderungen [In22b]). Ausschlaggebend für diese Kategorisierung waren vor allem die Dauer der täglichen privaten Nutzung internetfähiger Geräte sowie die genutzten Funktionen und die Anzahl der Geräte im eigenen Besitz. Außerdem wurde die Technikaffinität der Teilnehmenden erhoben. Dies geschah durch Abfragen von Begriffen (z.B. Cloud, Blockchain), aber auch mit der Frage ob sie Details zu ihrem Smartphone nennen können und der Angabe, zu welchen Zwecken sie ihr Smartphone nutzen (insbesondere zur Passwortspeicherung). Daraus ergab sich folgende Einteilung der teilnehmenden Personen:

- **P1:** eher digital vorreitend, besonders technikaffin
- **P2:** digital mithaltend, nicht technikaffin
- **P3:** digital vorreitend, besonders technikaffin
- **P4:** eher digital mithaltend, eher technikaffin

---

<sup>7</sup><https://airid.com/airid2-airid2-mini/>

- **P5:** eher digital vorreitend, eher technikaffin.

Die Fokusgruppe fand in Präsenz statt und wurde in zwei Phasen unterteilt. In der ersten Phase wurden die Teilnehmenden in zwei Gruppen aufgeteilt, die jeweils einen der beiden in Kapitel 2 beschriebenen Dongles in Verbindung mit einer sich in Entwicklung befindenden Wallet auf einem Smartphone ausprobierten. Dazu bekam jede Gruppe die Aufgabe, den jeweiligen Dongle mit der auf dem Smartphone laufenden Wallet zu verbinden. Die Aufgabe war dabei in ein Szenario eingebettet, in dem die Teilnehmenden zur sicheren Buchung eines ÖPNV-Tickets eine Verbindung zum Dongle herstellen sollen. Die Teilnehmenden erhielten hierbei keine Hilfestellung oder Anleitung. Damit sollte sichergestellt werden, dass sich die Teilnehmenden unbeeinflusst mit den Geräten auseinandersetzen und sich zu dem technischen Ansatz eine Meinung bilden können. Anschließend fand in der zweiten Phase eine semi-strukturierte Diskussion mit beiden Gruppen statt. Die gesamte Fokusgruppe wurde audiovisuell aufgezeichnet und transkribiert. Die Auswertung der Daten erfolgte mittels qualitativer Inhaltsanalyse in Anlehnung an Gläser und Laudel [GL10]. Als Kategoriensystem wurden aus den Funktionalen E-Demand-Faktoren der Nutzungsqualität [Wi22] die Folgenden entnommen:

- **Einfache Benutzung/ Benutzerfreundlichkeit:** Maß für den wahrgenommenen Aufwand zum Erlernen und Anwenden einer neuen Technologie
- **Nützlichkeit:** die subjektive Wahrnehmung oder der Eindruck eines Nachfragenden oder Nutzenden, inwiefern Technologie Aufgaben erleichtert oder verbessert
- **Sicherheit/ Privatsphäre:** die wahrgenommene Sicherheit und Vertraulichkeit von Nutzendendaten sowie die systembasierte Informationsverarbeitung
- **Vertrauen:** betrachtet auf den zwei Ebenen: Vertrauen in die Verwaltung bzw. Institution sowie Vertrauen in das Internet
- **Technologie-/ Internetkompetenz:** die Nutzungsfähigkeit angebotener digitaler Dienste seitens der Nachfragenden bzw. Nutzenden
- **Selbstwirksamkeit:** die individuelle Überzeugung, zur Ausführung einer bestimmten Handlung oder zur Erreichung eines Ziels in der Lage zu sein
- **Aufwandserwartung:** je höher die Aufwandserwartung der Nachfragenden bzw. Nutzenden ist, desto eher zögern sie, die neue Technologie zu nutzen

In einer weiteren Iteration wurde das Datenmaterial von zwei unabhängigen Personen nach weiteren relevanten Textstellen durchsucht und identisch auftretende Textstellen neu kategorisiert. Die Kategorie *Benutzendenfreundlichkeit* wurde während der Auswertung mit den Unterkategorien Transparenz (umfasst die Durchschaubarkeit von Vorgängen und Mechanismen), *Benutzendenführung* (beschreibt Aussagen bezüglich des Führens Nutzender innerhalb einer Anwendung bzw. eines Prozesses) und Sichtbarkeit des Systemstatus (die Kommunikation des Systems mit Nutzenden) ergänzt. Die resultierenden Textstellen wurden in allgemeine und explizite Aussagen zu Wallet und Dongle, unterteilt. Anschließend wurden diese Aussagen zusammengefasst und interpretiert.

## 4 Ergebnisse

Im folgenden Kapitel werden die Aussagen und Einstellungen als Ergebnisse der Fokusgruppe nach den verschiedenen Faktoren der Nutzungsqualität dargestellt.

### 4.1 Einfache Anwendung / Benutzendenfreundlichkeit

Alle Teilnehmenden, unabhängig von der eigenen Technikaffinität und Digitalkompetenz, hatten Schwierigkeiten aufgrund fehlender *Benutzendenführung* zum Verbindungsaufbau den Dongle ohne Hilfestellung mit dem Smartphone zu verbinden. Häufig wurde eine kontaktlose Interaktion, wie das Auslesen der Daten über NFC angenommen. Es war für die Nutzenden aufgrund fehlenden Feedbacks nicht erkennbar, ob Smartphone und Dongle miteinander verbunden sind. Auch die Instabilität der Anwendung und Fehlermeldungen an einigen Stellen verwirrten die Nutzenden. Neben den allgemeinen Problemen mit der Anwendung, wurden individuelle Einstellungen deutlich. Während P2, sich stark negativ gegenüber der Abhängigkeit vom Smartphone äußert, betont P3 den Bedarf an neuen, *benutzendenfreundlichen* Technologien, kritisiert aber die Anzahl der notwendigen Geräte und der durchzuführenden Schritte. P3 äußerte hingegen, dass die Wallet und Dongle "nicht *ad hoc* einsetzbar" seien und somit die Zielerreichung, wie z.B. die Online-Ticketbuchung, nicht effizient unterstützt werde.

Die *Transparenz* der Wallet-App wurde, insbesondere von P4, als wichtig herausgestellt. P2 äußerte Bedenken hinsichtlich der Nachvollziehbarkeit einer Wallet in Bezug auf Datenverarbeitung und dem Auslesen der Daten durch Dritte. Die Teilnehmenden hatten Schwierigkeiten die *Benutzendenführung* zu verstehen, sodass P1, P2 und P4 angaben, "wahllos auf dem Smartphone herumzudrücken". P4 äußerte zudem das Bedürfnis nach mehr visueller Unterstützung. Bezüglich der *Sichtbarkeit des Systemstatus* äußerte sich P1 positiv, als eine zur Nutzendenaktion passende Rückmeldung in der Wallet-App erschien. P3 und P4 kritisierten fehlendes Feedback: „[...] dann hat mir eine Rückmeldung [gefehlt]. Das fände ich schön. Das würde bei mir auch Vertrauen schaffen“.

### 4.2 Nützlichkeit

Die Möglichkeit, Tickets des ÖPNV schnell, online und durchgängig mithilfe einer Wallet buchen zu können, wird von P3, P4 und P5 als Erleichterung empfunden. P3 erachtet digitale Identität zur Identifikation bei digitalen Transaktionen als notwendig. Das Konzept der Speicherung von Nachweisen in einer Wallet auf einem mobilen Endgerät wird sowohl von P3 als auch von P5 als nutzenstiftend empfunden. P5 sieht einen Vorteil vor allem darin, einen digitalen Ort für alle Karten zu haben. P5 verwendet bereits eine Bezahlkarte der Sparkasse über eine Apple Watch. Das zusätzliche Mitführen einer Geldbörse zum Vorzeigen eines Ausweises oder der Bahnkarte wird von P5 als störend empfunden. P1 sieht eine Erleichterung darin, ein Gerät und eine Anwendung für sämtliche

Anwendungsfälle nutzen zu können, inklusive der Nutzung des Online-Personalausweises. Darüber hinaus schreibt P3 Online-Kreditkarten, die in einer Wallet gespeichert werden, eine höhere Sicherheit zu, was als wertschöpfend empfunden wird. Die Kombination einer Wallet mit einem hardwarekryptografischen zweiten Faktor stellt für P3 dabei jedoch keinen Mehrwert dar. Ein weiteres Gerät mitführen zu müssen, um eine App auf einem mobilen Endgerät nutzen zu können, erzeugt bei P3 Unverständnis. P2 empfindet die Speicherung von Nachweisen in der Wallet und die damit verbundene Abhängigkeit von einem mobilen Endgerät, das in regelmäßigen Abständen verloren wird, oder Updates benötigt, allgemein als nicht wertschöpfend. Das Konzept einer digitalen Wallet und damit verbundener weiterer Geräte wird von P2 generell abgelehnt.

### 4.3 Sicherheit / Privatsphäre

P1 und P3 argumentieren, dass digitale Lösungen „nie zu 100% sicher“ sind. Dabei sieht P1 aber einen Vorteil im USB-C Dongle, da dieser einen zusätzlichen Schutz für die Daten bieten kann. P3 hebt die Bedeutung der Kontrolle der eigenen Daten hervor und betont, dass im Prozess der Authentifizierung alle Informationen zur Datenfreigabe protokolliert und einsehbar sein müssen. P4 äußert ihre Besorgnis über den Verlust der Kontrolle der geteilten Daten im digitalen Raum. Die Hauptherausforderung wird von P3 bei der Verifizierung einer Person gesehen. Diese teilt die Einschätzung, dass eine Verbesserung der *Benutzendenfreundlichkeit* die Sicherheit verringern würde und damit nicht gewollt sei. P4 betont, dass die Sicherheit nicht durch die Nutzungskomplexität von Anwendungen erhöht werden sollte. Insbesondere die Beziehung und die Rolle des Staates wird diskutiert. P3 plädiert für eine Mithaftung des Staates bei Datenmissbrauch. Es werden vom Staat definierte, offene Standards von P1 gefordert. P3 schließt sich dieser Meinung an und formuliert den Bedarf an Zertifizierungsstellen, die Anbietende, die mit den offenen Standards arbeiten auch überprüfen.

### 4.4 Vertrauen

Die Teilnehmenden der Fokusgruppe äußerten im Hinblick auf den Faktor Vertrauen verschiedene Bedenken und Perspektiven: So äußerten P1 und P2, dass sie dem Konzept zentraler Datenbanken nicht trauen und Zweifel an deren Sicherheit haben. P1 betonte dies sei unabhängig von der Institution zu verstehen ("Das ist mir egal, ob da die Bundesdruckerei dahintersteht, ob da eine Bank dahintersteht (P4 nickt), aber die sind alle nicht vertrauenswürdig."). Zudem äußerte P2 Zweifel am Schutz der Bürger\*innen durch ihr Land. Außerdem wurde Skepsis gegenüber digitalen Entwicklungen der Bundesregierung geäußert, da zu viele unterschiedliche Akteure beteiligt seien und die Interoperabilität fehle, was zu Insellösungen führe (P1).

Teilnehmende haben wenig Vertrauen in die Anbietenden digitaler Dienste, inklusive Wallets, was den Wunsch nach einem Rechtsanspruch auf die ausschließlich zweckgebundene Nutzung freigegebener Daten und deren anschließende Löschung hervorruft.

(P3). Auch die Notwendigkeit einer Historie zur Überprüfung von Transaktionen wurde betont. P2 äußerte zudem, dass es kein Vertrauen in die Technologie an sich bestehe, da Sicherheitslücken in digitalen Anwendungen allgegenwärtig seien. Dennoch brachten einige Teilnehmende (P1, P5) ein generelles Vertrauen in die digitale Authentifizierung zum Ausdruck oder gaben an, der Technologie im Allgemeinen zu vertrauen.

#### 4.5 Technologie- / Internet-Kompetenz

Unsicherheiten der Teilnehmenden scheinen die Nutzungsfähigkeit der Wallet mit Dongle zu behindern. So äußerten einige Teilnehmende (P3, P4) Unklarheiten über den Speicherort der Daten bei der Wallet mit Dongle. Es herrschte Unsicherheit darüber, ob der Dongle nur als Schlüssel fungiert oder tatsächlich Daten speichert. Insbesondere P4 fühlte sich generell mit dem Konzept von Wallet und Dongle bzw. deren Nutzung überfordert und hinterfragte die Funktionsweise der Technologie. P3 ging fälschlicherweise davon aus, dass für die Nutzung bestimmter Daten über die Wallet, die entsprechende physische Karte, wie z.B. der Führerschein, in den Bluetooth-Dongle eingesteckt werden muss, so dass zusätzlich die physischen Karten immer mitgeführt werden müssen, da immer nur eine Karte in den Bluetooth-Dongle eingeschoben werden kann. Dies wurde als klarer Nachteil der Technologie angesehen. Es gab zudem während der Diskussion auch Unklarheiten bezüglich der SSI-Terminologie. So vermutete eine Person, dass "Nachweis" ein Synonym für einen digitalen Dienst sei, der in Anspruch genommen werden kann.

#### 4.6 Selbstwirksamkeit

P3 geht davon aus, dass ein Authentifizierungsprozess bzw. Historienverlauf, sie in die Lage versetzt, die Kontrolle über ihre Datenfreigabe- und Nutzung zu behalten. Gleichzeitig ist P3 sich darüber bewusst, dass mit der Nutzung einer Wallet in Verbindung mit einem Dongle viel Eigenverantwortung hinsichtlich des Schutzes der Wallet und der eigenen Daten einhergeht. Sowohl P3 als auch P4 überfordert die Verantwortung, die mit dem Mitführen eines weiteren Gerätes einhergeht, das als Schlüssel für alle Anwendungsfälle wahrgenommen wird. Das Risiko, das zusätzliche Gerät regelmäßig zu Hause zu vergessen oder es zu verlieren, wird als hoch eingeschätzt und somit fühlen sich die Personen unfähig, zu jeder Zeit, die benötigten Online-Transaktionen durchführen zu können. Des Weiteren wird von P3 das Szenario befürchtet, unachtsam mit den eigenen Daten umzugehen, indem die PIN einem anderen Menschen verraten und diesem der Dongle ausgehändigt wird. Das wahrgenommene Haftungsrisiko, wird als zu hoch eingestuft. P1 ist der Ansicht, dass die Nutzenden die Entscheidungsgewalt darüber haben sollten, welche Anwendung sie verwenden möchten.



#### 4.7 Aufwandserwartung

Während P1 und P3 den Einsatz der elektronischen ID unter der Voraussetzung einer weiteren App kritisieren, zeigen sich P1, P4 und P5 offen für die Nutzung von Wallets und Dongles, unter der Voraussetzung den Aufwand bei der Verwaltung von Informationen und Diensten zu reduzieren. Dabei benennt P4 insbesondere als Anforderung zur Nutzung der Wallet die Möglichkeit den PC nicht nutzen zu müssen und P1, dass die Wallet für möglichst viele Anwendungsfälle eingesetzt werden kann. Die Teilnehmenden sprechen über verschiedene Szenarien, z.B. schildert P1 ein Szenario im Supermarkt. P5 äußert sich positiv zu den genannten Szenarien und erhofft sich in der Nutzung eine Reduktion des Portmonee-Inhalts. Weiter führt sie aus, den Dongle eher am Schlüsselbund neben dem *Apple Airtag* anzubringen, was eine bessere Verfolgbarkeit ermöglicht und das Mitführen der Tasche überflüssig macht. Die Karte (beim Bluetooth-Dongle) würde im Portemonnaie aufbewahrt, was auf eine Integration in den Alltag hindeutet.

### 5 Limitationen und Methodenkritik

Im Rahmen dieser Studie konnten anhand einer explorativen Untersuchung erste Anhaltspunkte für mögliche Auswirkungen von der Einführung von Zwei-Faktor-Wallets für diverse Nutzende ermittelt werden. Die vorgestellten Ergebnisse unterliegen folgenden Einschränkungen. Die verwendete Wallet und Dongles befinden sich noch in der Entwicklung. Beeinträchtigte *user experience* ist daher eine erwartbare Limitation, da es sich da es sich um eine frühe Alpha-Version handelt. Darüber hinaus erhielten die Teilnehmenden der Fokusgruppe zu Beginn nur eine kurze Einführung und einen Zeitrahmen von 20 Minuten, um sich mit der Wallet und den Dongles vertraut zu machen, was die aufgetretenen Schwierigkeiten beim Verständnis des Konzepts von Wallet und Dongle erklären könnte. Zudem deckte die Aufgabe im ersten Teil der Fokusgruppe nur einen kleinen Teil eines realen Anwendungsfalls ab. Die Stichprobenauswahl beruhte auf freiwilligen und interessierten Teilnehmenden. Außerdem verringerten kurzfristige Absagen die Anzahl der Teilnehmenden auf nur fünf von ursprünglich sieben geplanten Personen. Daher kann Stichprobenverzerrung nicht ausgeschlossen werden und der qualitative Charakter der Studie lässt keine Rückschlüsse auf die Gesamtbevölkerung zu.

### 6 Diskussion und Fazit

Dieser Beitrag zeigte, dass Vertrauen bei Bürger\*innen aktiv geschaffen werden muss. Die Herausforderungen bei der Verwendung von Dongles mit dem Smartphone wurden unabhängig von Technikaffinität gezeigt. So bedarf es benutzendenfreundlichen Technologien um Vertrauen bei Bürger\*innen zu schaffen. Eine Wallet mit Dongle benötigt eine gute Nutzendenführung und Anleitung, um von den Nutzenden richtig verstanden werden zu können. Der nachgewiesene Zusammenhang zwischen positiver Nutzungsqualität sowie Sicherheitsgefühl fordert mehr Serviceorientierung, um Akzeptanz von Zwei-Faktor-

Wallet-Apps im Szenario ÖPNV zu schaffen. Diese Ergebnisse decken sich mit den Befunden der serviceorientierte Perspektive auf die Nützlichkeit von E-Government-Lösungen und deren Nachfrage [Wi22].

Die Nützlichkeit der getesteten Zwei-Faktor-Wallets hängt somit maßgeblich von Verbesserungen der Nutzungsqualität ab, denn Teilnehmende schrieben geringer Nutzbarkeit Risiken für die Privatsphäre zu. Die Reaktionen der Nutzenden legen kritische Haltungen gegenüber komplexem Identitätsmanagement offen und sind auf zwei Hauptaspekte zurückzuführen. Einerseits übersteigt die Verbindungsherstellung mit dem zweiten Faktor Alltagswissen. Andererseits bleibt für Nutzende unklar, auf welchem Gerät Daten verarbeitet und gespeichert werden. Daher wird ein Transparenzmangel wahrgenommen, welcher das Nutzendenvertrauen und die Nutzungsqualität einschränkt. Es ist daher notwendig, die Funktionsweise und die Aspekte der Sicherheit den Nutzenden vor bzw. während der Nutzung deutlich zu machen. Der Dongle wird allerdings auch positiv als Möglichkeit bewertet, Portemonnaies zu ersetzen und Nachweise aller Art portabler zu gestalten. Aus diesen Befunden leiten sich folgende Propositionen ab, welche durch zukünftige Untersuchungen überprüft werden können.

- Offene Standards und Zertifizierungsstellen sind Schlüsselemente, um Vertrauen in digitale Identitätslösungen durch Transparenz zu stärken.
- Vertrauen in die digitale Authentifizierung kann als Basis für die Akzeptanz und Nutzung digitaler Identitätslösungen dienen.
- Obwohl der Dongle als Single-Point-of-Failure wahrgenommen wird, übersteigt seine wahrgenommene Nutzungsqualität diejenige von Portemonnaies.
- Je mehr Geräte für eine Interaktion benötigt werden, desto geringer die Akzeptanz des Verfahrens.

Der Nachweis einer gemischten Wahrnehmung *der Nutzungsqualität von Wallets mit hardwarekryptografischem zweitem Faktor* durch die Fokusgruppe beantwortet die Forschungsfrage und fordert eine systematische Untersuchung von SSI-Wallets mit zweitem Faktor, um die Ergebnisse mit Hinblick auf ähnliche Befunde verwandter Studien [Pr23] theoretisch zu rahmen.

#### **Danksagung und Förderhinweise**

Wir danken den Teilnehmenden der Fokusgruppe.

Das dieser Veröffentlichung zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Wirtschaft und Klimaschutz unter dem Förderkennzeichen 01MN21001A gefördert.

Diese Forschung wurde im Rahmen des Projektes „Menschenzentrierte digitale Daseinsvorsorge in Stadt und Land“ (SIGNAL, Förderkennzeichen: 100693812) aus Mitteln des Europäischen Sozialfonds Plus (ESF Plus) und aus Steuermitteln auf Grundlage des vom Sächsischen Landtag beschlossenen Haushalts gefördert.

Diese Veröffentlichung wurde gefördert als Teil des Projekts WIDE "Web3 Identity for DAOs and Education" als Teil des TRUSTCHAIN Horizon Europe Grants mit der Fördernummer: 101093274.

**Literaturverzeichnis**

- [Al21a] Alt, R. et al.: Life Engineering. *Bus Inf Syst Eng* 2/63, S. 191–205, 2021.
- [Al21b] Alamillo-Domingo, I.: From eIDAS to SSI in the European union. In (Preuschkat, A.; Reed, D. Hrsg.): *Self-Sovereign Identity. Decentralized Digital Identity and Verifiable Credentials*. Manning, S. 394–407, 2021.
- [Av19] Avellaneda, O. et al.: Decentralized Identity: Where Did It Come From and Where Is It Going? *IEEE Communications Standards Magazine* 4/3, S. 10–13, 2019.
- [Bi23] Biedermann, B. et al.: Nutzen und Grenzen von SSI für Verwaltung und öffentliche Institutionen, S. 437–457, 2023.
- [Bo21] Boysen, A.: Decentralized, Self-Sovereign, Consortium: The Future of Digital Identity in Canada. *Frontiers in Blockchain* 4, 2021.
- [Ca07] Cameron, K.: The Laws of Identity. [https://learn.microsoft.com/en-us/previous-versions/dotnet/articles/ms996456\(v=msdn.10\)](https://learn.microsoft.com/en-us/previous-versions/dotnet/articles/ms996456(v=msdn.10)), Stand: 2023-12-20.
- [Eh21] Ehrlich, T. et al.: Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. *2198-2775* 2/58, S. 247–270, 2021.
- [Eu21] European Commission: Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, 2021.
- [GL10] Gläser, J.; Laudel, G.: *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen*. VS Verlag, 2010.
- [In22a] Initiative D21 e.V.: eGovernment MONITOR 2022. <https://initiated21.de/publikationen/egovernment-monitor/2022>, Stand: 2024-04-22.
- [In22b] Initiative D21 e. V.: D21-Digital-Index 2021/2022. <https://initiated21.de/publikationen/d21-digital-index/2021-2022>, Stand: 2022-04-22.
- [In23] Initiative D21 e.V.: eGovernment MONITOR 2023. <https://initiated21.de/publikationen/egovernment-monitor/2023>, Stand: 2024-04-22.
- [Mü18] Mühle, A. et al.: A survey on essential components of a self-sovereign identity. *Computer Science Review* 30, S. 80–86, 2018.
- [Ne22] Nestler, S.: Usability. In (Nestler, S. Hrsg.): *Menschzentrierte Digitalisierung*. Springer Fachmedien Wiesbaden, Wiesbaden, S. 79–121, 2022.
- [PR21] Preuschkat, A.; Reed, D.: Why the internet is missing an identity layer — and why SSI can finally provide one. In (Preuschkat, A.; Reed, D. Hrsg.): *Self-Sovereign Identity. Decentralized Digital Identity and Verifiable Credentials*. Manning, S. 3–20, 2021.

- 
- [Pr23] PricewaterhouseCoopers GmbH: Digitaler Personalausweis und digitale Briefschaften 2023, 2023.
  - [Sa21] Sabadello, M.: Decentralized identity for a peaceful society. In (Preuschkat, A.; Reed, D. Hrsg.): Self-Sovereign Identity. Decentralized Digital Identity and Verifiable Credentials. Manning, S. 293–299, 2021.
  - [Se22] Sedlmeir, J. et al.: Transition Pathways towards Design Principles of Self-Sovereign Identity, 2022.
  - [Sh22] Sharif, A. et al.: The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes. 2076-3417 24/12, S. 12679, 2022.
  - [Sp23] Sporny, M.; Steele, O.; Jones, M. B.; Cohen, G.; Terbu, O.: Verifiable Credentials Data Model v2.0. World Wide Web Consortium (W3C), 2023.
  - [St18] Stevens, L.: Self-Sovereign Identities for Scaling Up Cash Transfer Projects: Designing a blockchain based digital identity system. Master Thesis, Delft, 2018.
  - [Tr22] Trier, M.; Kundisch, D.; Beverungen, D.; Müller, O.; Schryen, G.; Mirbabaie, M.: Digital Responsibility, 2022.
  - [Ve19] Verband Sichere Digitale Identitäten (VSDI): BMWi-Förderaufruf: Schaufenster Sichere Digitale Identitäten. <https://vsdi.de/bmw-förderaufruf-schaufenster-sichere-digitale-identitaeten/>, Stand: 2024-04-22.
  - [We22] Weigl, L. et al.: The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility: Proceedings of the 55th Hawaii International Conference on System Sciences. HICCS, S. 2543–2552, 2022.
  - [Wi20] Wirtz, B. W.: Electronic Business. Springer Gabler, 2020.
  - [Wi22] Wirtz, B. W.: E-Government. Springer Gabler, 2022.
  - [WK16] Wirtz, B. W.; Kurtz, O. T.: Local e-government and user satisfaction with city portals – the citizens’ service preference perspective. 1865-1992 3/13, S. 265–287, 2016.
  - [WK17] Wirtz, B. W.; Kurtz, O. T.: Determinants of Citizen Usage Intentions in e-Government: An Empirical Analysis. 1573-7098 3/17, S. 353–372, 2017.
  - [Za21] Zaeem, R. N. et al.: On the Usability of Self Sovereign Identity Solutions, 2021.
  - [Zw21] Zweig, K. A. et al.: Sozioinformatik. In (Zweig, K. A. et al. Hrsg.): Sozioinformatik. Carl Hanser Verlag GmbH & Co. KG, S. I–XIV, 2021.