Krauß, Anna-Magdalena; Sellung, Rachelle A.; Kostic, Sandra

Ist das die Wallet der Zukunft?

HMD Praxis der Wirtschaftsinformatik

Provided in Cooperation with:
Springer Nature

Suggested Citation: Krauß, Anna-Magdalena; Sellung, Rachelle A.; Kostic, Sandra (2023) : Ist das die Wallet der Zukunft?, HMD Praxis der Wirtschaftsinformatik, ISSN 2198-2775, Springer Fachmedien Wiesbaden GmbH, Wiesbaden, Vol. 60, Iss. 2, pp. 344-365, https://doi.org/10.1365/s40702-023-00952-6

HMD Praxis der Wirtschaftsinformatik (2023) 60:344–365
https://doi.org/10.1365/s40702-023-00952-6

SCHWERPUNKT

Ist das die Wallet der Zukunft?

Ein Blick durch die Nutzendenbrille beim Einsatz von digitalen Identitäten

Anna-Magdalena Krauß · Rachelle A. Sellung · Sandra Kostic

Eingegangen: 30. September 2022 / Angenommen: 6. Februar 2023 / Online publiziert: 13. März 2023

Zusammenfassung Heutzutage werden digitale Identitäten oft unsicher umgesetzt und sind mit der Erstellung von vielen unterschiedlichen Accounts durch Nutzende verbunden. Das soll langfristig durch die Nutzung sogenannter Digital Identity Wallets verbessert werden. Diese Wallets ermöglichen die Verwaltung und Nutzung von digitalen Identitäten sowie Nachweisdokumenten. Dazu gehören unter anderem Nachweise wie der Führerschein, der Bibliotheksausweis oder auch Flugtickets. Alle diese Daten können gemeinsam in einer Wallet-App auf den Endgeräten der Nutzenden gespeichert werden. Die Nutzenden verwalten ihre Daten eigenständig und entscheiden selbst darüber, welche und wie viele Daten sie über sich preisgeben wollen.

Aktuelle Forschungen zeigen allerdings, dass die bisher entwickelten Wallets Usability-Probleme aufweisen, sodass Nutzende nur schwer das Konzept dieser Wallets greifen können. Zudem weisen heutige digitale Dienstleistungen zahlreiche Hürden auf, welche den Einsatz von digitalen Identitäten erschweren.

In diesem Beitrag wird basierend auf einer Wallet-Analyse und User-Experience-Anforderungen ein Konzeptvorschlag für eine nutzungsfreundlichere Wallet vorgestellt, bei der die Nutzenden im Mittelpunkt stehen. So sieht dieses Konzept einen umfangreicheren Funktionsumfang im Vergleich zu aktuellen Wallet Umsetzungen vor, mit dem Ziel die Wallet stärker den Bedürfnissen der Nutzenden anzupassen.

Anna-Magdalena Krauß
Arbeitsgruppe Digitale Dienstleistungssysteme, Hochschule für Technik und Wirtschaft Dresden, Dresden, Sachsen, Deutschland
E-Mail: anna-magdalena.krauss@htw-dresden.de

Rachelle A. Sellung
Arbeitsgruppe Identitätsmanagement, Fraunhofer IAO, Stuttgart, Baden-Württemberg, Deutschland
E-Mail: rachelle.sellung@iao.fraunhofer.de

✉ Sandra Kostic
Abteilung Secure Systems Engineering, Fraunhofer AISEC, Garching, Bayern, Deutschland
E-Mail: sandra.kostic@aisec.fraunhofer.de

Darunter fallen Funktionen wie die Kommunikation zwischen Wallet und Dienstanbieter ohne die Notwendigkeit des Teilens von Kontaktdaten, die Option der Dauervollmachten zur Freigabe von Daten, die Möglichkeit der Verwaltung von Daten in Vertretung anderer Personen sowie die Organisation der eigenen Daten.

Schlüsselwörter Identity Wallet · Digitale Identität · SSI · User Experience · Usability · Privatsphäre

Is this the Wallet of the Future?

An Insight through the User's Eyes of Digital Identities

Abstract Today, digital identities are often implemented insecurely and are associated with the creation of many different accounts by users. In the long-term, these challenges should be addressed using so-called digital identity wallets. These wallets enable the management and use of digital identities and verification documents. For example, this includes documents like driver's licenses, library cards and airline tickets. All this data can be stored together in a wallet app on users' smart phones. Users manage their data independently and decide for themselves which and how much data they want to disclose about themselves.

However, current research shows that the wallets developed to date have usability problems, making it difficult for users to grasp the concept of these wallets. In addition, today's digital services have numerous hurdles that make the use of digital identities difficult.

This paper is based the creation of generic user experience requirements and the analysis of wallets and their functionality. We present a conceptual proposal for a more user-friendly wallet that focuses on the user. This concept includes a more extensive range of functions compared to current wallet implementations, with the goal of adapting the wallet more closely to the needs of the users. This contains functions like; communication between the wallet and the service provider without the need to share contact data, the option of enduring powers of attorney to share data, the ability to manage data on behalf of others, and the organization of one's own data.

Keywords Identity Wallet · Digital Identity · SSI · User Experience · Usability · Privacy

1 Einführung

Digital Identity Wallets werden als der nächste große Umbruch in der Digitalisierung öffentlicher und privater Dienstleistungen angesehen (Sawers 2022; The Linux Foundation 2022). Einige Experten in der Tech-Industrie glauben, dass Wallets die bisherigen Geschäftsmodelle für digitale Unternehmen gravierend verändern werden, sodass nicht nur neue Geschäftsmodelle erschlossen, sondern auch bestehende hinsichtlich ihrer aktuell genutzten Ressourcen optimiert werden können (Sawers 2022; The Linux Foundation 2022).

Dieses Konzept einer Digital Identity Wallet (kurz Wallet) wird häufig im Zusammenhang mit Self-Sovereign-Identity (SSI) vorgestellt (Podgorelec et al. 2022). Dabei handelt es sich um einen neuen Ansatz des Identitätsmanagements, welches auf dezentraler Organisation beruht (Ehrlich et al. 2021). Die Nutzenden bekommen „Identitätsmerkmale und Berechtigungen in Form von kryptografisch gesicherten digitalen Nachweisen („Verifiable Credentials“) ausgestellt“ (Ehrlich et al. 2021) und können diese in ihrer Wallet („digitale Brieftasche“) selbstständig verwalten. Die Technologie hinter SSI ermöglicht unter anderem das Speichern hoheitlicher Dokumente wie dem Führerschein, aber auch anderer Nachweise wie Bankkarten, dem Bibliotheksausweis oder einer Kinokarte in einer einzigen Wallet-App. Zur Identifizierung, Authentifizierung und Autorisierung gegenüber Akzeptanzstellen durch die Nutzenden (Sporny et al. 2022) „genügt die Vorlage der geforderten Verifiable Credentials in Form von so genannten ‚Verifiable Presentations‘, die ohne direkten Kontakt zum Herausgeber überprüfbar sind“ (Ehrlich et al. 2021). Derzeit gibt es mehrere Anbieter, welche Anwendungen zur Verwaltung digitaler Identitäten basierend auf SSI bereitstellen. Dazu gehören unter anderem Evernym Inc., Trinsic Technologies Inc., Jolocom GmbH und Neosfer GmbH (Evernym Inc., An Avast Company 2022; Trinsic Technologies Inc. 2022; Jolocom GmbH 2023; Neosfer GmbH 2023).

Das Konzept einer Wallet wird aktuell in Deutschland auch im Rahmen des vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) geförderten Innovationswettbewerbs „Schaufenster Sichere Digitale Identitäten“ (Bundesministerium für Wirtschaft und Klimaschutz 2020) behandelt, um neue Ansätze für offene, interoperable und einfach nutzbare ID-Ökosysteme zu erforschen. Das schließt sowohl die Entwicklung diverser benutzungsfreundlicher Anwendungsfälle als auch die Konzeptionierung von Geschäftsmodellen und die Betrachtung von Sicherheitsfaktoren ein.

Darüber hinaus gibt es auch Bestrebungen auf europäischer Ebene, nicht nur die Digitalisierung und Modernisierung der öffentlichen Dienste und die Verbesserung der elektronischen Behördendienste voranzutreiben (European Commission 2022), sondern auch eine EU-Wallet zu etablieren (European Data Protection Supervisor 2022; Nguyen 2022). Das zeigt auf, dass Wallets nicht nur auf nationaler Ebene, sondern auch EU weit als wichtiges Mittel der Digitalisierung angesehen werden.

Auch wenn den Nutzenden die Kontrolle über die Identitäten gegeben wird, zeigen Untersuchungen wie von Khayretdinova et al. (2022), Sartor et al. (2022), Korir et al. (2022) oder Der et al. (2017) auf, dass die bisher realisierten, auf SSI basierenden Wallets Usability-Probleme vorweisen. So wird unter anderem der in den Wallets verwendete Sprachgebrauch als kritisch angesehen, wodurch den Nutzenden die Verwendung dieser Technologie erschwert, wird (Khayretdinova et al. 2022; Sartor et al. 2022; Son et al. 2021). Um dem entgegenzuwirken und die Akzeptanz bei den Nutzenden zu steigern, ist es wichtig, sie in die Entwicklung der Anwendung oder der Wallets von Beginn an selbst einzubeziehen.

Deshalb werden in diesem Beitrag die Anforderungen an Wallets und digitale Identitäten aus der Sicht der Nutzenden zusammengetragen und ein überarbeiteter Funktionsumfang eines neuen Wallet-Konzepts vorgestellt.

Dafür wird zunächst die diesem Beitrag zugrundeliegende Design-Research-Methode vorgestellt (siehe Kap. 2). Anschließend werden die aktuellen Hürden beim Einsatz von digitalen Identitäten veranschaulicht (siehe Kap. 3). Daraufhin werden in Kap. 4 die Anforderung an ein überarbeitetes Konzept einer nutzungsfreundlicheren Wallet zusammengetragen und in Kap. 5 die Funktionen einer solchen Wallet vorgestellt. Kap. 6 behandelt die Beschreibung der Limitationen und des Ausblicks dieses Beitrags. Abschließend folgt die Zusammenfassung dieses Beitrags in Kapitel 7.

2 Design-Science-Research-Methode

In diesem Abschnitt wird zunächst die Design-Science-Research-Methode (DSR) grundlegend vorgestellt und anschließend genauer auf das Artefakt Wallet eingegangen, das für diesen Beitrag eine wichtige Rolle spielt.

2.1 Grundlagen

In diesem Beitrag wird die Design-Science-Research-Methode angewandt, bei der es sich um einen Ansatz zur systematischen Schaffung von Gestaltungswissen handelt, der für Informationssysteme entwickelt wurde. Die Design-Science-Research-Methode nutzt das Wissen und das Verständnis bezüglich eines Problembereichs zur Erstellung und Anwendung eines Artefakts (Hevner et al. 2004). Das Artefakt wird als Werkzeug zum besseren Verständnis des Problems und zu dessen Neubewertung erstellt, um die Qualität des Designprozesses zu verbessern und den Prozess neu be-

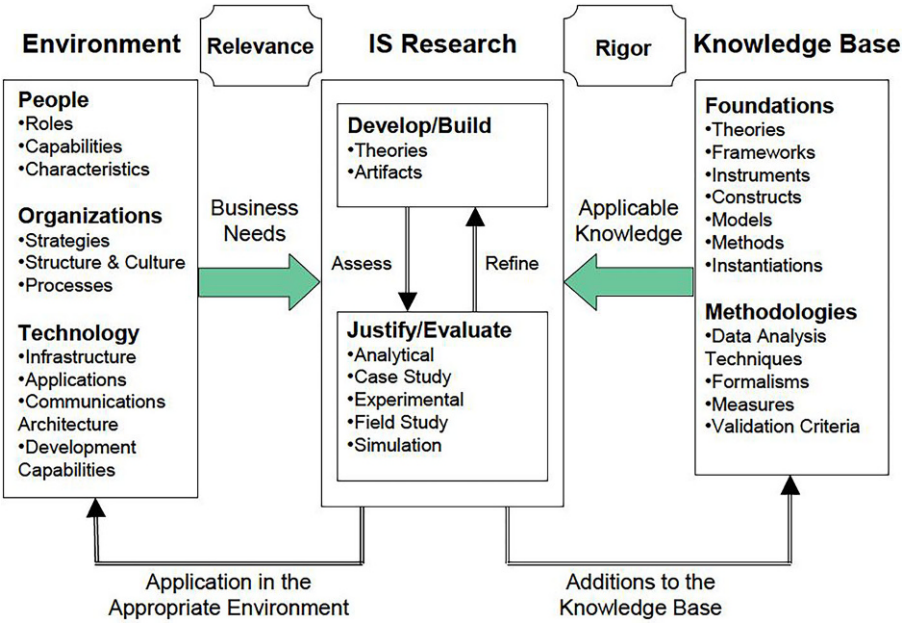

Abb. 1 Schaubild der DSR-Methode (Hevner et al. 2004)

ginnen zu können (Markus et al. 2002). Das übergeordnete Ziel dieses Ansatzes ist es, einen Designprozess zu schaffen, der eine Abfolge von Expertentätigkeiten darstellt und ein innovatives Produkt hervorbringt (Watts et al. 2009). Wie in Abb. 1 zu sehen ist, erfüllt das Design Science-Forschungsmodell zwei Fälle: den Geschäftsbedarf (Relevanz) und die Wissensbasis (Stringenz). Ein wichtiger Schritt in der Methodik ist die Bewertung. Es gibt fünf Kategorien von Evaluierungsmethoden der DSR: Beobachtung, Analyse, Experiment, Test und Beschreibung (Hevner et al. 2004).

Für diesen Beitrag wird eine deskriptive Bewertungsmethode aus der Perspektive der User Experience angewandt. Sie ist eine fundierte Argumentation, bei der Zusammenfassung der aktuellen Forschung in Bezug auf Wallets und deren User Experience vorgenommen wird. Als Ergebnis wird ein Funktionsumfang einer nutzungsfreundlicheren Wallet beschrieben als Optimierungsvorschlag zu aktuellen Modellen.

2.2 Artefakt – Wallet

In diesem Beitrag wird die Design-Research-Methodik auf ein Artefakt, die Wallet, angewendet. Die Basis für die Betrachtung des Artefakts Wallet in diesem Beitrag bildet die Analyse bestehender Wallets und deren Funktionsumfang innerhalb des in Kap. 1 vorgestellten Schaufensterprojekts (Stand Januar 2023). Hierbei wurden folgende Wallets berücksichtigt: SmartWallet, Lissi Wallet, Connect.Me, Trinsic Wallet, helix id Wallet, IRMA (Jolocom GmbH 2023; Neosfer GmbH 2023; Evernym Inc., An Avast Company 2022; Trinsic Technologies Inc. 2022; Blockchain HELIX AG 2020; Privacy by Design Foundation 2023). Im Folgenden sollen der generelle Einsatzzweck sowie die Funktionen der Wallets näher erläutert werden. Dabei sei anzumerken, dass die vorgestellten Funktionen eine Zusammenstellung von Kernfunktionen darstellen, bei der unterschiedliche Wallets von verschiedenen Betreibern betrachtet wurden. Folglich weist nicht jede Wallet die gleichen Kernfunktionen auf. Des Weiteren befinden sich die untersuchten Wallets derzeit noch in Entwicklung und können daher meist nur im Rahmen angebotener Demoszenarien analysiert werden. Da für einige Wallets, wie bspw. IRMA und helix id Wallet zum Zeitpunkt der Untersuchung keine Demoszenarien existierten, kann die Integration einiger Funktionen nur abgeschätzt werden.

Das Artefakt Wallet bietet die grundlegende Funktionalität Nachweisdokumente zu digitalisieren und diese z. B. für die Authentisierung sowohl online als auch bei Diensten vor Ort einfach zu nutzen. Das schließt sowohl behördliche als auch privatwirtschaftliche Dienste ein[1]. Die digitalisierten Nachweisdokumente unterliegen der Kontrolle der Nutzenden. Sie selbst speichern die Nachweise in dieser App und entscheiden darüber, welche Daten sie von ihren gespeicherten Nachweisen mit anderen Diensten teilen. Die Speicherung eines Nachweisdokuments in der Wallet kann entweder durch Scannen eines QR-Codes, welches die Übertragung des Nachweisdokuments vom anbietenden Service startet, erfolgen oder durch eine direkte App

[1] Zum Zeitpunkt des Beitrags wurde der Einsatz der Wallets meist nur im Rahmen von Demoszenarien unterstützt, jedoch sowohl für behördliche als auch privatwirtschaftliche Dienstleisungen vorgesehen.

Tab. 1 Übersicht der Funktionen von am Markt bereits vertretenen Wallets

Funktion (ID)	Beschreibung	Wallet
Allgemein		
Übersicht über gespeicherte Nachweise (AF-1)	In der Wallet werden sämtliche von den Nutzenden gespeicherte Nachweise aufgelistet	Lissi Wallet, helix id Wallet, SmartWallet, IRMA, Connect.me
Detailansicht zu gespeicherten Nachweisen (AF-2)	Die Nutzenden können sich die Details zu jedem gespeicherten Nachweis anzeigen lassen	Lissi Wallet, helix id Wallet, SmartWallet, IRMA, Connect.me
Wallet zurücksetzen (AF-3)	Diese Funktion ermöglicht das Löschen sämtlicher gespeicherter Nachweise in der Wallet mit einer Aktion	SmartWallet, IRMA, Trinsic Wallet
Hilfe & FAQ (AF-4)	Die Wallet bietet einen Hilfe- und/oder FAQ-Bereich, in dem Nutzende Antworten auf offene Fragen zur Wallet finden	Helix id Wallet, SmartWallet, IRMA
Backup erstellen (AF-5)	Mithilfe der Funktion können Nutzende ein Backup ihrer Wallet erstellen, um ihre Daten z. B. für den Fall des Verlusts des Smartphones zu sichern. Beispielsweise kann der Zugang zur Wallet oder sogar Nachweise, Kontakte/Verbindungen und die Historie gesichert werden	Lissi Wallet, Trinsic Wallet
Wiederherstellung (AF-6)	Dies ermöglicht die Wiederherstellung des Zugangs zur Wallet oder darüber hinaus aller darin gespeicherten Nachweise, beispielsweise bei einem Umzug auf ein neues Smartphone	Lissi Wallet, helix id Wallet, SmartWallet, Trinsic Wallet
Komfort		
Suche (AF-7)	Die Wallet kann mit einer Suchfunktion sowohl nach Verbindungen als auch nach gespeicherten Nachweisen durchsucht werden	Lissi Wallet
Favoriten (AF-8)	Nutzende können Nachweise in der Wallet favorisieren, um einen schnelleren Zugriff zu ihnen zu erhalten	SmartWallet
Automatische Vorauswahl (AF-9)	Die Nutzenden erhalten bei einer eingehenden Datenanfrage, durch die Wallet eine Vorauswahl, welche Daten aus welchen Nachweisen für die Beantwortung der Anfrage benötigt werden. Dadurch müssen die Nutzenden die benötigten Nachweise nicht manuell suchen und auswählen	Lissi Wallet, SmartWallet
Sicherheit		
Walletschutz (AF-10)	Um zu gewährleisten, dass nur die Nutzenden selbst Zugriff auf die Daten in ihrer Wallet haben, ist ein Zugangsmechanismus zum Entsperren der Wallet vorgesehen, welcher die Sicherheit erhöht. Die Nutzenden selbst legen fest welchen Mechanismus sie einsetzen wollen (Biometrie, Kennwort, PIN, etc.)	Lissi Wallet, helix id Wallet, SmartWallet, IRMA, Connect.me, Trinsic Wallet
Transparenz		
Historie (AF-11)	In der Wallet werden sämtliche Interaktionen zwischen Wallet und Gegenstelle aufgelistet mit denen die Nutzenden in Kontakt getreten sind. Die Auflistung erfolgt in chronologischer Reihenfolge	Lissi Wallet, SmartWallet, Connect.me
Übersicht pro Gegenstelle (AF-12)	In der Wallet wird den Nutzenden angezeigt, welche Daten und Nachweise sie generell pro Gegenstelle freigegeben haben. Es stellt eine Erweiterung der Funktion „Historie“ dar	Lissi Wallet

zu App Verbindung zwischen Wallet und Dienstanbieter. Die in einer Wallet gespeicherten Nachweise werden den Nutzenden in einer Übersicht in der App dargestellt. Sie lassen sich auch als Favoriten markieren, um beispielsweise häufig eingesetzte Nachweise schneller in der Übersicht zu finden. Zudem können sich die Nutzenden sämtliche Details, welche Bestandteil des jeweiligen Nachweisdokuments sind, anzeigen lassen – das meint beispielsweise beim digitalen Studierendenausweis die dazugehörigen Daten, wie Vorname, Nachname und Matrikelnummer etc. (Demoszenario für die Lissi Wallet (Neosfer GmbH 2023)).

Damit nur die Nutzenden Zugriff auf die App und somit ihre gespeicherten Nachweise haben, wird diese mit einem Sperrmechanismus geschützt. Der Zugangsschutz kann mit Hilfe eines Passwortes, einer PIN oder mit einem biometrischen Mittel erfolgen.

Eine Interaktion zum Teilen der Daten erfolgt nur mit Zustimmung der Nutzenden. Diese beginnt meist mit der Initiierung einer Verbindung bzw. des Herstellens eines Kontakts zwischen der Wallet der Nutzenden und einer Gegenstelle. Dies wird durch die Nutzenden initiiert. Die Nutzenden erhalten daraufhin die Anfrage, ob sie dem Verbindungsaufbau zustimmen oder nicht. Dies bietet den Nutzenden die Möglichkeit die eingehende Anfrage zu kontrollieren. Allerdings handhaben verschiedene Wallet Anbieter diesen Schritt unterschiedlich: Die Lissi Wallet sieht beispielsweise eine separate Anfrage zur Verbindung vor und fragt anschließend nach dem Teilen der Daten, die Smart Wallet verbindet die Verbindungsanfrage und die Zustimmung zur Datenübertragung (Neosfer GmbH 2023; Jolocom GmbH 2023). In der Anfrage werden Daten der Nutzenden angefragt, die für z. B. zur Erfüllung einer bestimmten Dienstleistung auf Seiten der Gegenstelle notwendig sind. Die benötigten Daten können die Nutzenden aus ihren in der Wallet gespeicherten Nachweisen auswählen und explizit für die Gegenstelle in diesem bestimmten Anwendungsfall freigeben. Alternativ können die Nutzenden die Datenanfrage ablehnen und damit keinerlei Daten für die Gegenstelle freigeben.

Tab. 1 fasst die beschriebenen sowie weitere Kernfunktionen zusammen, strukturiert sie nach den Kategorien Allgemein, Komfort, Sicherheit und Transparenz und veranschaulicht, bei welcher Wallet die jeweilige Funktion integriert wurde.

3 Herausforderungen

In diesem Abschnitt wird ein Überblick über einige der aktuellen Herausforderungen gegeben, die beim Einsatz von digitalen Identitäten mit den derzeitigen Diensten und Wallets verbunden sind.

3.1 Hürden bei der Inanspruchnahme von Dienstleistungen

Auch wenn die Digitalisierung Einfluss darauf nimmt, wie Dienstleistungen zur Verfügung gestellt werden können, stehen sowohl behördliche als auch private Dienstleister noch immer vor vielen Herausforderungen. Der Einsatz einer Wallet kann als Hilfsmittel zur Lösung dieser Herausforderungen dienen.

Bei vielen öffentlichen Diensten in Deutschland werden die Dienstleistungen nur als quasi-digitaler Dienst angeboten (USU Software AG 2020; forsa Politik- und Sozialforschung GmbH 2020), bei dem immer noch das persönliche Erscheinen der BürgerInnen erforderlich ist (IDnow GmbH 2023), um abschließend zu überprüfen, ob es sich um die Person handelt, die die Dienstleistung in Anspruch nehmen möchte. Neben der persönlichen Vorsprache zur Erledigung einer Dienstleistung sind viele öffentliche Dienste nur begrenzt flexibel und bieten nur feste Öffnungszeiten an (IDnow GmbH 2023).

Für Dienstleistungen, die ein höheres Maß an Identitätssicherheit erfordern, muss vor der Inanspruchnahme des Dienstes ein Ausweisdokument vorgelegt werden, was nicht nur bei öffentlichen, sondern auch bei einigen privaten Diensten Herausforderungen mit sich bringt (z. B. Vorlage des Personalausweises für die Anmietung eines Autos als Identitätsnachweis) (Bundesministerium der Justiz 2009). Mit Hilfe des Onlinezugangsgesetzes (Bundesamt für Justiz 2017) soll durch die Digitalisierung von Verwaltungsleistungen unter anderem der Pflicht des persönlichen Erscheinens entgegengewirkt werden. Der Bericht zum eGovernment Monitor 2022 zeigt jedoch auf, dass Vielen die Verfügbarkeit von Online-Leistungen nicht bekannt ist und zudem nur 43 % der Personen, welche einen Bedarf einer Verwaltungsleistung haben diese auch online nutzen (Initiative D21 e. V. und TU München 2022). Darüber hinaus wird der Einsatz der digitalen Angebote erschwert auf Grund von Hardware-Problemen bei den Nutzenden (Schwab et al. 2019) oder dem Mangel bezüglich des Fehlens einer medienbruchfreien Abwicklung des Prozesses (Schwab et al. 2019). Gleiches lässt sich beim Einsatz der eID (Bundesministerium des Inneren und Heimat 2023) (Online-Ausweisfunktion des Personalausweises) beobachten. Diese Funktion setzten ausschließlich 10 % der Deutschen ein (Initiative D21 e. V. und TU München 2022). Die Gründe sollen unter anderem im mangelnden Vertrauen in die Technologie, sowie in den Kosten z. B. zur Anschaffung eines Kartenlesegeräts liegen (eco – Verband der Internetwirtschaft e. V. und techconsult GmbH 2022).

Damit die Nutzenden behördliche Online-Dienste in Anspruch nehmen, müssen diese daher eine hohe Zuverlässigkeit, eine einfache Bedienbarkeit sowie einen garantierten Schutz der Daten vorweisen.

3.2 Bedürfnisse der Nutzenden

Ein anderes Problem, mit denen die Nutzenden derzeitiger Dienste konfrontiert sind, stellt die Vielzahl von Kundenkarten, Coupons, Tickets und Jahreskarten dar. Sie nehmen nicht nur viel Platz im Portemonnaie ein, den Nutzenden fällt es auch immer schwerer die Übersicht zu wahren (Reposito GmbH 2013). Daher stehen Nutzende auch dem Konzept von selbstverwalteten digitalen Identitätsmerkmalen und Berechtigungen gesammelt in einer App offen gegenüber (eco – Verband der Internetwirtschaft e. V. und techconsult GmbH 2022). Insbesondere, da diese eine einfache und unkomplizierte Nutzung sowie eine schnellere Abwicklung von Prozessen ermöglichen kann (eco – Verband der Internetwirtschaft e. V. und techconsult GmbH 2022), so wie es auch durch eine Wallet möglich ist. Sollte eine sichere digitale Identität bereitstehen, würden Nutzende auch mehr digitale Dienste verwenden,

als sie derzeit nutzen (eco – Verband der Internetwirtschaft e. V. und techconsult GmbH 2022).

Neben den genannten Herausforderungen besteht bei den digitalen Diensten in Deutschland noch immer ein großes Hindernis in der mangelnden Interoperabilität bei Accounts von Nutzenden und beim Identitätsmanagement. Bei vielen Diensten ist es nach wie vor erforderlich einen Account mit Anmeldenamen und Passwort für den jeweiligen Dienst zu erstellen, um diesen zu nutzen. Dies führt dazu, dass die Nutzenden gezwungen sind, die Übersicht über die Vielzahl ihrer Konten zu behalten und sich zu erinnern, welches Passwort sie für welche Anwendung vergeben haben. Auch hier sehen die Nutzenden einen Vorteil im Einsatz einer gebündelten Identität, da ihnen diese die Reduzierung der Anzahl an Anmeldenamen sowie zu merkender Passwörter ermöglicht (eco – Verband der Internetwirtschaft e. V. und techconsult GmbH 2022). Darüber hinaus sprechen sich die Nutzenden für eine selbstverwaltete Lösung aus, so wie sie auch vom SSI-Prinzip beschrieben wird, und wollen die Verwaltung ihrer Identität nicht aus der Hand geben (eco – Verband der Internetwirtschaft e. V. und techconsult GmbH 2022). So haben auch 20 % der Befragten aus der Studie eco – Verband der Internetwirtschaft e. V. und techconsult GmbH (2022) geäußert, dass sie bereits einmal etwas von einer Wallet gehört haben. Darüber hinaus können die Nutzenden auch Erfahrungen beim Einsatz von mobilen Verwaltungsangeboten vorweisen (43 % der Befragten) und zeigen darüber hinaus auch Interesse hinsichtlich der Nutzung dieser Angebote (Initiative D21 e. V. und TU München 2022). Dies stellt die passende Voraussetzung für den Einsatz einer Wallet dar.

Zu den primären Gründen, weshalb Online-Behördendienste nicht intensiv genutzt werden, gehört auch die Sorge bezüglich des Datenschutzes (Initiative D21 e. V. und TU München 2022). Aktuelle Beobachtungen, bei denen die Nutzenden z. B. bei einer Altersverifikation vor Ort weiterhin unfreiwillig mehr Daten teilen müssen, als nötig ist (z. B. das Vorzeigen des gesamten Personalausweises, obwohl nur das Geburtsdatum benötigt wird) könnten die Sorgen um den Datenschutz verstärken. Solche Hürden lassen sich durch ein von den Nutzenden kontrollierten Einsatz des Datenteilens mit einer Wallet überwinden.

3.3 Hürden bei der Nutzung aktueller Wallet-Lösungen

Da sich aktuelle Wallets derzeit in einem frühen Entwicklungsstadium befinden, stehen sie noch vor Herausforderungen (Khayretdinova et al. 2022; Sartor et al. 2022; Korir et al. 2022; Der et al. 2017). So wird grundsätzlich angemerkt, dass den Nutzenden nur unzureichend die Innovation und die Vorteile von Wallets erklärt wird (Sartor et al. 2022; Khayretdinova et al. 2022). Dies führte zu erheblichen Problemen und soll den Einsatz der Technologie beeinträchtigt haben:

Die Studie von Khayretdinova, et al. untersuchte Wallets, die auf SSI-Technologien basieren (Khayretdinova et al. 2022). Sie führten einen Usability-Test mit 18 Personen für unterschiedliche Wallets durch und deuteten auf einige verbleibende Herausforderungen für digitale Wallets hin, die überwunden werden müssen, um erfolgreich zu sein. Grundsätzlich weist die Autorenschaft darauf hin, dass zum Zeitpunkt der Studiendurchführung die Technologie den Nutzenden nicht die Mög-

lichkeit bot, die Vorteile einer Wallet hinsichtlich des Datenschutzes oder Sicherheit zu wahrzunehmen (Khayretdinova et al. 2022). Dabei wurden die Lösungen jedoch als praxistauglich vermarket.

Zudem weisen die Wallets auch große Usability-Probleme auf (Korir et al. 2022; Khayretdinova et al. 2022). Diese zeigten sich z. B. in einer schlechten Beschreibung der Terminologie in den Wallets (Sartor et al. 2022; Khayretdinova et al. 2022). Die Usability-Probleme führten aber auch dazu, dass Nutzenden Bedenken äußerten zu viele Daten zu teilen (Korir et al. 2022). So haben Nutzenden den Gedanken aufgegeben die Möglichkeit zu haben ihre Daten zu kontrollieren. Dies wurde deutlich durch Aussagen wie: „You know I work in information technology already and part of me says the idea that you keep your information secure and people not knowing it is a ship that has probably already sailed“ (Korir et al. 2022).

Außerdem wurde darauf hingewiesen, dass die Wallet über keine Sicherungs- und Wiederherstellungsfunktion verfügen (Khayretdinova et al. 2022). Diese wurde als wesentlicher Bestandteil des Lebenszyklus (Cameron und Grewe 2022) einer Wallet identifiziert (Khayretdinova et al. 2022). Die Funktionen der Wallets waren darüber hinaus waren nicht selbsterklärend. Zudem fehlte den Nutzenden eine einfache zu Handhabung sowie gute Benutzungserfahrung (Khayretdinova et al. 2022). Da das Konzept der Wallets auf einer neuen Technologie basieren, setze dies laut (Khayretdinova et al. 2022) eine gute Erklärung der Funktionen voraus und das über die Erläuterung von grundlegenden Anweisungen hinaus. Das meint z. B. wieso bestimmte Funktionen in einer gewissen Art und Weise umgesetzt werden müssen. Als Nächstes erwähnen Khayretdinova et al. (2022), dass die Erlernbarkeit der Funktionalität in Verbindung mit den Anwendungsfällen der digitalen Wallet noch immer eine Hürde für Nutzende darstellt. Diese Erlernbarkeit könnte durch die Einbeziehung von Nutzungsstudien oder anderen Erfahrungsansätzen mit Nutzenden während des Entwicklungsprozesses verbessert werden. Daher fassen Khayretdinova et al. (2022) zusammen, dass die Benutzungsfreundlichkeit der betrachteten Wallets noch nicht ausgereift ist.

4 Anforderungen an eine zukünftige, nutzungsfreundlichere Wallet

Nach der Beschreibung des aktuellen Standes des Artefakts Wallet besteht der nächste Schritt darin, die Anforderungen zu ermitteln, die für das Erreichen einer höheren Usability (dt. Benutzungsfreundlichkeit) relevant sind. Zu diesem Zweck wurde eine Zusammenfassung von Definitionen, Methoden und Beobachtungen aus der Forschung zu Usability und User Experience (dt. Nutzungserlebnis) erstellt und daraus Anforderungen abgeleitet.

Allgemein werden in der ISO 9241-11 Kernanforderungen festgelegt, um die Usability-Definition zu erfüllen. Diese Kernanforderungen sind Effektivität, Effizienz und Zufriedenheit der Nutzenden (Deutsches Institut für Normung e. V. 2018). Um diese Usability-Kernanforderungen weiter zu verfeinern, definiert die ISO 9241-110 sieben Aspekte dieser allgemeinen ergonomischen Prinzipien: Aufgabenangemessenheit, Erlernbarkeit, Benutzerbindung, Erwartungskonformität, Selbstbeschreibungsfähigkeit, Steuerbarkeit und Robustheit gegen Benutzungsfehler (Deut-

sches Institut für Normung e. V. 2020). Zweitens definiert Nielsen (2012) Usability mit fünf Qualitätskomponenten.

1. **Erlernbarkeit:** Die Einfachheit, mit der grundlegende Aufgaben zum ersten Mal ausgeführt werden. (Wie einfach fällt es Nutzenden grundlegende Aufgaben zu erledigen, wenn sie das System zum ersten Mal benutzen?)
2. **Effizienz:** Die Geschwindigkeit, mit der Aufgaben ausgeführt werden, sobald die Nutzenden Erfahrung mit dem System haben. (Wie schnell können Nutzende Aufgaben erledigen, wenn/sobald sie mit dem System vertraut sind bzw. es einmal kennengelernt haben?)
3. **Einprägsamkeit:** Die Fähigkeit, sich die Komponenten der Schnittstelle zu merken. (Wenn die Nutzenden nach einer gewissen Zeit der Nichtbenutzung zum System zurückkehren, wie leicht können sie ihre Kenntnisse wiederherstellen?)
4. **Fehler:** Die Regelmäßigkeit und Schwere von Fehlern und deren Behebung. (Wie viele Fehler machen die Nutzenden, wie schwerwiegend sind diese Fehler, und wie leicht können sie sie beheben?)
5. **Zufriedenheit:** Das allgemeine Wohlbefinden mit dem Produkt. (Wie angenehm ist es das System zu benutzen?)

Bei den meisten Produkten ist jedoch mehr als nur eine benutzbare Schnittstelle erforderlich, weshalb eine positive User Experience mit der Usability einhergeht. Die von Hassenzahl (2008) beschriebene User Experience ist ein momentanes, primär bewertendes Gefühl (positiv – negativ) bei der Nutzung technischer Produkte und Dienstleistungen. Eine positive User Experience entsteht durch die Befriedigung menschlicher Grundbedürfnisse. Diese Bedürfnisse sind Autonomie, Kompetenz, Stimulation, Zugehörigkeit und Beliebtheit (Hassenzahl 2008). Die Gestaltung einer guten User Experience ist wichtig, da sie die Nutzenden anspricht, erfreut und Vertrauen in eine Lösung aufbaut.

Zusätzlich zu dieser kurzen Zusammenfassung wurden bei der Erstellung der Anforderungen an eine zukünftige, nutzungsfreundlichere Wallet auch die folgenden Quellen berücksichtigt:

1. Usability-Anforderungen an Sicherheitsanwendungen (Whitten und Tygar 1999),
2. Untersuchung zu Sicherheit und Usability im Kontext von Identitätsmanagement (Wohlgemuth et al. 2003),
3. Richtlinien für sicheres Interaktionsdesign (Yee 2004),
4. Prinzipien und Muster zum Abgleich von Usability und Sicherheit (Garfinkel 2005),
5. Heuristiken zur Evaluation von IT-Sicherheitsmanagement-Tools (Jaferian et al. 2011),
6. Richtlinien zur Barrierefreiheit (W3C 2018; Bundesministerium für Arbeit und Soziales 2019),
7. Untersuchung von Usability-Kriterien für behördliche Dienstleistungen (Sellung et al. 2022).

Zusammengefasst folgenden daraus folgende Benutzungsanforderungen (BA):

BA-01 – Usability Eine Wallet sollte eine hohe Usability aufweisen, sodass Nutzende eigenständig und intuitiv die Wallet einsetzen können. Dabei ist zu beachten, dass die Nutzenden potenziell über unterschiedliches Vorwissen im Umgang mit dieser Technologie verfügen können.

BA-02 – User Experience Aufbauend auf der Usability soll bei der Entwicklung einer Wallet die User Experience berücksichtigen, um eine gute Akzeptanz bei den Nutzenden zu gewährleisten. Insbesondere die menschlichen Grundbedürfnisse Sicherheit und Kompetenz sind wichtige Faktoren bei der Gestaltung einer Applikation, welche personenbezogenen Daten bündelt. Idealerweise sollte eine Wallet diese Bedürfnisse ansprechen, um eine gute User Experience zu schaffen.

BA-03 – Etablierte Usability-Richtlinien und -Prinzipien Bei der Entwicklung einer Wallet sollten etablierter Standards, Heuristiken und Richtlinien der Usability berücksichtigt werden, um ein benutzungsfreundliches Produkt zu gewährleisten.

BA-04 – Befähigte Nutzende Die Nutzenden sollten immer das Gefühl haben, die Kontrolle über die Vorgänge in der Wallet zu haben.

BA-05 – Kognitive Belastung Die kognitive Belastung der Nutzenden sollte so weit wie möglich minimiert werden. Wenn die Nutzenden sich zu viel merken oder zu viele Prozessschritte durchlaufen müssen, um das gewünschte Ziel zu erreichen, werden sie die Wallet nicht dauerhaft nutzen. Daher sollten die Prozessschritte verständlich und so kurz wie möglich gehalten werden.

BA-06 – Erlernbarkeit Erlernbarkeit ist ein wichtiges Usability-Design-Prinzip. Dies ist umso wichtiger, wenn die Nutzenden nur über geringe Vorkenntnisse bezüglich Wallets und SSI verfügen. Dies bedeutet, dass die Nutzenden lernen müssen, wie eine Wallet funktioniert. Daher sollte die Lernförderlichkeit für die Gestaltung des User Interfaces (UI) eine relevante Rolle spielen.

BA-07 – Konsistente Sprache Alle Wallets sollten kontext- und anwendungsfallübergreifend eine konsistente Sprache verwenden. Bei Nichteinhaltung erschwert es die Verständlichkeit des Konzepts einer Wallet.

BA-08 – Benutzungsfreundliche Terminologie und Metaphern Alle in einer Wallet verwendeten Begriffe und Metaphern sollten auch für Nutzende mit geringem technischem Verständnis oder für jene, die mit der Applikation oder Technologie nicht vertraut sind, verständlich sein. Einfach zu verstehende und greifbare Begriffe und Metaphern können den Nutzenden helfen, das Konzept von SSI auf abstraktem Niveau zu verstehen.

BA-09 – Verfügbare Informationen und Hilfe Die Nutzenden sollten die Möglichkeit haben, innerhalb einer Wallet Antworten zu etwaigen Fragen und Hilfestellungen bezüglich der Wallet und den unterstützten Dienstleistungen zu erhalten.

BA-10 – Transparenz Die Nutzenden müssen nicht jedes kleine Detail, das im Hintergrund der Wallet abläuft, verstehen. Die UI der Wallet sollte jedoch transparent genug sein, damit die Nutzenden das Gesamtkonzept verstehen können und somit wissen, was geschieht und was sie tun sollen. Zu jedem Zeitpunkt sollten die Vorgänge der Wallet transparent genug sein, ohne die Nutzenden zu überfordern.

BA-11 – Minimalistische und einfache Gestaltung der UI Die UI einer Wallet sollte keine unwichtigen Informationen enthalten oder unübersichtlich sein, die die Nutzenden verwirren könnten. Ein einfaches Design ermöglicht es den Nutzenden, sich auf die wichtigsten Funktionen der Wallet zu konzentrieren.

BA-12 – Fehlerbehandlung In allen vorhersehbaren Fällen sollte eine Wallet die Nutzenden daran hindern, Fehler zu machen. Allerdings sollte eine Wallet einen Vorgang nicht einfach blockieren, sondern die Nutzenden über die Fehlerursache informieren. Diese Erklärung sollte in einer einfachen, aber informativen Weise erfolgen und klare Anweisungen enthalten, wie die Nutzenden den Fehler beheben können.

BA-13 – Zugänglichkeit Die UI einer Wallet sollte für Nutzende mit Beeinträchtigungen geeignet sein. Dies bedeutet, dass es keinen Ausschluss einer bestimmten Nutzendengruppe geben sollte. Eine Wallet sollte daher barrierefrei bedienbar sein.

5 Funktionen einer zukünftigen, nutzungsfreundlicheren Wallet

Anhand der untersuchten Wallets (Kap. 3), den daraus identifizierten Hürden bzw. Schwächen (Abschn. 3.3) sowie den genannten Anforderungen hinsichtlich der User Experience und Usability (Kap. 4) konnten im nächsten Schritt Funktionen einer zukünftigen nutzungsfreundlicheren Wallet abgeleitet werden. Das Konzept erweitert dabei die bestehenden Funktionen aktueller Wallets, um Nutzenden das volle Potenzial von SSI zugänglich zu machen. Die Anforderungen in Kap. 4 wurden mit einem sehr hohen Abstraktionsgrad entworfen, um User Experience und Usability möglichst ganzheitlich abzubilden. Da jede der erarbeiteten Funktionen einen Beitrag zur verbesserten User Experience leisten und damit entsprechend eine hohe Usability aufweisen soll, sind alle Anforderungen aus Kap. 4 für jede der beschriebenen Funktionen zu berücksichtigen. Zukünftige Wallets können nicht nur von Privatpersonen, sondern auch von Organisationen, Familien oder für Objekte eingesetzt werden. Mithilfe der Wallets sollen Nutzende in die Lage versetzt werden, ohne große technische Anforderungen und ohne tiefgreifendes technisches Verständnis verschiedene Nachweisdokumente zu digitalisieren (Hoepner et al. 2019). Diese Dokumente liegen in der Wallet in verifizierter Form vor (Sovrin Foundation 2023). Die Wallet kann sowohl für kommunale Anwendungsfälle wie für die Bibliothek oder das Bürgerbegehren, als auch bei privaten Unternehmen eingesetzt werden, wie beim Carsharing oder Scooter Sharing. Die Nutzenden werden intuitiv durch die Wallet geleitet, in der ihnen selbsterklärend das Ausstellen, Speichern sowie Freigeben ihrer Daten aufgezeigt wird.

Tab. 2 Funktionen einer zukünftigen nutzungsfreundlicheren Wallet

Funktion (ID)	Grundlage	Beschreibung
Allgemein		
Verwaltung unterschiedlicher Nachweisarten (NF-1)	Keine Vielzahl an Accounts für unterschiedliche Anwendungsfälle gewünscht (Initiative D21 e. V. 2022; Schnepf et al. 2021) Einfacher Zugang zu verschiedenen Online-Portalen gewünscht (Schnepf et al. 2021) Speicherung verschiedener Dokumente in einer Wallet gewünscht (Schnepf et al. 2021) Vielzahl an Anwendungsfällen gewünscht (Schnepf et al. 2021)	In der Wallet können sowohl hoheitliche Dokumente, wie der Personalausweis oder Führerschein, als auch nicht hoheitliche Dokumente, wie Kinotickets oder Kundenkarten, gespeichert werden
Online- und Offlinefähigkeit (NF-2)	Einsatz der Wallet auch ohne Verbindung zum Internet gewünscht (Budiu 2015; Schnepf et al. 2021) Vorschlag aus eIDAS 2.0 (Europäische Kommission 2021)	Die Wallet kann sowohl offline vor Ort als auch online eingesetzt werden. In Online-Anwendungsfällen können zur Interaktion mit Gegenstellen z. B. QR-Codes oder, bei Nutzung desselben Mediums (z. B. im mobilen Browser oder einer anderen App) Deep Links zum Einsatz kommen. In Offline-Anwendungsfällen können statt Deep Links noch Technologien wie NFC oder Bluetooth genutzt werden
Portabilität und Interoperabilität (NF-3)	In Ansätzen zwischen Lissi Wallet und Trinsic Wallet bereits umgesetzt (Neosfer GmbH 2023; Trinsic Technologies Inc. 2022) SSI-Prinzip Portabilität und Interoperabilität (Sovrin Foundation 2023) Weite Verbreitung bei Anbietern und Unternehmen und Einsatz im Ausland gewünscht (Schnepf et al. 2021; Hoepner et al. 2019) Wahlfreiheit bei Wallet-Anbieter gewünscht (IDnow GmbH 2023)	Nachweise aus der Wallet eines Anbieters können exportiert und in die Wallet eines anderen Anbieters importiert werden. Die Wallet ist Teil eines Ökosystems und bietet aufgrund von offenen Standards sowie interoperablen Nachweisformaten die Möglichkeit, Daten und Nachweise über verschiedene Anwendungskontexte hinaus nutzen zu können
Kommunikation über Wallet (NF-4)	Ggf. bereits umgesetzt in helix id Wallet (Blockchain HELIX AG 2020) Nutzende haben Sorge beim Daten teilen und wollen daher wenige teilen (Korir et al. 2022; USU Software AG 2020) Benachrichtigung über neue Services gewünscht (USU Software AG 2020)	Die Wallet bietet die Möglichkeit mit den Dienstanbietern direkt über die Wallet zu kommunizieren. Somit stellt das Teilen von Kontaktdaten keine Notwendigkeit mehr dar
Komfort		
Schnellzugriff auf gespeicherte Nachweise (NF-5)	Effizienz (Deutsches Institut für Normung e. V. 2018; Nielsen 2012) Schnellzugriff gewünscht (Sartor et al. 2022)	Die Nutzenden erhalten mit einer Aktion den direkten Zugriff auf die Generierung z. B. eines QR-Codes vom Nachweis, um diesen vorweisen zu können
Automatisierte Favorisierung (NF-6)	Effizienz (Deutsches Institut für Normung e. V. 2018; Nielsen 2012) Erwartungskonformität (Deutsches Institut für Normung e. V. 2018)	Die Wallet bietet die Option einer automatisierten Favorisierung von Nachweisen, je nach Zugriffshäufigkeit

Tab. 2 (Fortsetzung)

Funktion (ID)	Grundlage	Beschreibung
Dauervollmachten (NF-7)	Individualisierung und Anpassung an das Sicherheitsbedürfnis gewünscht (Deutsches Institut für Normung e. V. 2020; Schade 2016)	Nutzende können der Wallet Vollmachten erteilen bis zu ihrem Widerruf. Dazu zählt etwa die automatisierte Annahme eingehender Verbindungen und Nachweise generell, je Gegenstelle bzw. Anwendungsfall oder Grad der Vertrauenswürdigkeit (z. B. nur bei verifizierten Gegenstellen). Darüber hinaus ist auch die automatisierte Freigabe festgelegter Daten für festgelegte Zwecke an festgelegte Gegenstellen möglich (bei häufigem Gebrauch z. B. des Dienstausweises zum Betreten des Firmengebäudes)
Archiv (NF-8)	Individualisierung gewünscht (Deutsches Institut für Normung e. V. 2020; Schade 2016)	Nutzende können in der Wallet einstellen, was mit ungültigen Nachweisen geschehen soll. Sie können automatisch gelöscht oder archiviert werden
Kategorisierung, Filterung & Sortierung (NF-9)	Individualisierung gewünscht (Deutsches Institut für Normung e. V. 2020; Schade 2016) Vielzahl von Dokument vorstellbar (Schnepf et al. 2021) und daher eine Übersicht gewünscht Filtermöglichkeit gewünscht (Sartor et al. 2022)	Nutzende können gespeicherte Nachweise kategorisieren. Beispiele für Kategorien wären etwa die Art der Gegenstelle, Gültigkeitsdauer oder Anwendungsfall. Zusätzlich können die Nutzenden ihre Nachweise filtern oder sortieren (z. B. nach Datum, nach Dienstanbieter, etc.)
Hinweis auf fehlende Nachweise (NF-10)	Robustheit gegen Benutzungsfehler (Deutsches Institut für Normung e. V. 2020; Nielsen 2012)	Die Nutzenden werden beim Einsatz der Wallet darauf hingewiesen, dass geforderte Nachweise fehlen. Darüber hinaus erhalten sie Informationen darüber, wo sie sich die jeweiligen Nachweise ausstellen lassen können
Mehrgerätenutzung (NF-11)	Angepasst an die beschriebenen Bevölkerungsgruppen aus den Studien der Initiative D21 e. V. (Initiative D21 e. V. 2022; Initiative D21 e. V. und TU München 2022). Sie besitzen im Durchschnitt 3,5 Endgeräte. Endgeräteübergreifende Nutzbarkeit gewünscht (Hoepner et al. 2019)	Die Wallet lässt sich über mehrere Geräte der Nutzenden synchronisieren und somit nutzen
Kollektiv		
Übertragung von gespeicherten Nachweisen (NF-12)	SSI-Prinzip Delegation (Sovrin Foundation 2023)	Mit der Wallet können Nutzende digitalisierte Nachweisdokumente an Wallets anderer Nutzender übertragen, ohne, dass das Nachweisdokument an Gültigkeit verliert. Dabei kann entschieden werden, inwieweit eine Kopie des Nachweises oder der originale Nachweis selbst übertragen wird
Verwalten von Nachweisen anderer Personen (NF-13)	SSI-Prinzip Delegation (Sovrin Foundation 2023) Nutzung von Online-Services rund um die Familie und Kind (USU Software AG 2020)	In der Wallet können sowohl Daten und Nachweise einer Person als auch von mehreren Personen verwaltet werden, z. B. im Kontext einer „Familienwallet“, in der eine erziehungsberechtigte Person auch die Daten und Nachweise der zugehörigen Kinder verwaltet

Tab. 2 (Fortsetzung)

Funktion (ID)	Grundlage	Beschreibung
Profilansicht (NF-14)	Aufteilung der Informationen für Übersichtlichkeit und minimale geistige Belastung gewünscht (Moran 2016)	Nutzende können verschiedene Profile in ihrer Wallet erstellen und zwischen diesen Ansichten hin- und herwechseln. Beispielsweise können Nutzende zwischen der „Familienansicht", in der die Nachweise von Familienmitgliedern angezeigt werden, und der Ansicht des eigenen Profils wechseln. Hier werden nur die eigenen Nachweise der Nutzenden aufgelistet
Sicherheit		
Optionaler zusätzlicher Schutz bei Datenfreigabe (NF-15)	Individualisierung und Anpassung an das Sicherheitsbedürfnis gewünscht (Deutsches Institut für Normung e. V. 2020; Schade 2016)	In der Wallet wird den Nutzenden überlassen, ob sie die Freigabe ihrer Daten stets zusätzlich mittels z. B. Eingabe eines Bestätigungs-PINs autorisieren oder dies nur angepasst auf bestimmte Anwendungsfälle erfolgt (z. B. nur bei Interaktionen mit einem hoheitlichen Dokument oder bei Bezahldaten)
Transparenz		
Übersicht über freigegebene Daten & Nachweise (NF-16)	Nachvollziehbare und transparente Übersicht über die Nutzung der Daten gewünscht (Hoepner et al. 2019) SSI- Prinzip Transparenz (Sovrin Foundation 2023)	In der Wallet wird den Nutzenden angezeigt, welche Daten und Nachweise sie generell pro Gegenstelle freigegeben oder auch selbst ausgestellt haben. Es stellt eine erweiterte Option der Funktion „Historie" dar. Um auch ein Verhältnis zur geteilten Datenmenge zu erhalten, können die Nutzenden die Ansicht ändern und die Menge oder Sensibilität der Daten spezifisch angezeigt bekommen
Prüfung der Vertrauenswürdigkeit der Gegenstelle (NF-17)	Geringes Risiko für die Nutzenden gewünscht (Hoepner et al. 2019) SSI-Prinzip Überprüfbarkeit & Authentizität (Sovrin Foundation 2023)	Die Wallet prüft automatisch bei der Initiierung einer Interaktion mit einer Gegenstelle, inwieweit diese vertrauenswürdig ist
Darstellung der Vertrauenswürdigkeit der Gegenstelle (NF-18)	In Ansätzen zwischen Lissi Wallet und Trinsic Wallet bereits umgesetzt (Neosfer GmbH 2023; Trinsic Technologies Inc. 2022) Geringes Risiko für die Nutzenden gewünscht (Hoepner et al. 2019) SSI-Prinzip Überprüfbarkeit & Authentizität (Sovrin Foundation 2023) Unterstützung bei Entscheidungsfindung via Guiding (Kohler 2022) Vertrauen in Organisation notwendig vor weitere Interaktion (Sherwin 2016)	Nach der Prüfung wird der Grad der Vertrauenswürdigkeit den Nutzenden z. B. mit Symboliken eines Ampelsystems veranschaulicht. Die Nutzenden können dann basierend auf diesem Grad der Vertrauenswürdigkeit entscheiden, ob sie die Verbindung eingehen wollen
Prüfung des Nutzungszwecks freizugebender Daten (NF-19)	Geringes Risiko für die Nutzenden gewünscht (Hoepner et al. 2019) Angelehnt an das Onlinezugangsgesetz (OZG) (USU Software AG 2020)	Bei einer eingehenden Datenanfrage prüft die Wallet automatisch, ob die Gegenstelle überhaupt berechtigt ist, die entsprechenden Daten im jeweiligen Anwendungsfall abzufragen

Tab. 2 (Fortsetzung)

Funktion (ID)	Grundlage	Beschreibung
Darstellung des Nutzungszwecks freizugebender Daten (NF-20)	Geringes Risiko für die Nutzenden gewünscht (Hoepner et al. 2019) Angelehnt an das Onlinezugangsgesetz (OZG) (USU Software AG 2020) Unterstützung bei Entscheidungsfindung via Guiding (Kohler 2022) Nachvollziehbare und transparente Nutzung der Daten gewünscht (Hoepner et al. 2019)	Bei einer eingehenden Datenanfrage wird den Nutzenden in der Wallet angezeigt, wofür die Gegenstelle die angefragten Daten benötigt. Des Weiteren werden die Nutzenden über das Ergebnis der automatischen Prüfung des Nutzungszwecks der Daten informiert

Wenn die Nutzenden aufgefordert werden ihre Daten mit einer Gegenstelle zu teilen, müssen sie lediglich die geringste Menge an benötigten Daten aus ihrer Wallet freigeben (Datenfreigabe nach dem Minimalprinzip (Sovrin Foundation 2023; Europäisches Parlament und Rat 2016; Bhargav-Spantzel et al. 2006)). Das können auch nur einzelne Bestandteile von Nachweisen sein, z. B. statt des gesamten Personalausweises nur die Freigabe des Geburtsdatums oder nur einzelne Informationen, wie statt des gesamten Geburtsdatums nur die Freigabe des Alters. Im kleinstmöglichen Fall ist auch die Freigabe einzelner Aussagen möglich, wie z. B. die Aussage „ist volljährig“, ohne die Preisgabe des tatsächlichen Alters.

Neben den existierenden Interaktionen, wie der Kontaktherstellung und dem Teilen einzelner Daten oder ganzen Nachweisen, bietet das Konzept einer zukünftigen nutzungsfreundlichen Wallet auch die Möglichkeit für Nutzende Gegenstellen selbst bestimmte Nachweise auszustellen. Dazu zählt beispielsweise die Erteilung einer Lastschrift vom Konto der Nutzenden oder die Berechtigung zur gewerblichen Nutzung der für die Gegenstelle freigegebenen Daten. Entsprechend können Nutzende allerdings auch von ihnen ausgestellte Nachweise widerrufen, sodass diese der Gegenstelle entzogen werden. Darüber hinaus veranschaulicht Tab. 2 weitere Funktionen einer möglichen verbesserten Wallet. Sie wurden dabei in die fünf Kategorien Allgemein, Komfort, Kollektiv, Sicherheit und Transparenz unterteilt und zur jeweiligen Anforderung in Bezug gesetzt.

6 Limitationen und Ausblick

Die in Kap. 5 vorgestellten Funktionen stellen einen ersten Vorschlag für eine mögliche Erweiterung bisheriger Wallets mit dem Ziel einer nutzungsfreundlicheren Wallet dar. Hierfür wurden die Herausforderungen bei den Dienstleistungen ausschließlich im deutschen Raum betrachtet. Eine erweiterte Betrachtung von Herausforderungen nicht nur auf nationaler Ebene, sondern auch auf europäischer oder internationaler Ebene ist für die Ausarbeitung zukünftiger Arbeiten vorgesehen und könnte Änderungen und Erweiterungen im Funktionsumfang nach sich ziehen.

Im Rahmen dieses Beitrags wurde eine limitierte Auswahl an Wallets untersucht, die teils aufgrund fehlender Demoszenarien zum Zeitpunkt der Analyse nur einen begrenzten Einblick in den Funktionsumfang ermöglichten. Da sich die bisherigen Wallet Umsetzungen aktuell rasant weiterentwickeln, ist eine kontinuierliche und

regelmäßige Neubetrachtung des Funktionssets im Hinblick einer nutzungsfreundlicheren Wallet ratsam. Zudem liegt in diesem Beitrag bewusst der Fokus allein auf der Sicht der Nutzenden. Das bedeutet, dass mit diesem Beitrag keine interdisziplinäre Betrachtung des Konzepts Wallet stattgefunden hat. Demnach sind beispielsweise eine rechtliche oder technische Anforderungsermittlung und Evaluation noch ausstehend.

Im Kontext der diesem Beitrag zugrundeliegenden Design-Science-Research-Methode stehen für eine vollständige Iteration des Artefakts die Phasen der Demonstration und Evaluation aus (Hevner et al. 2004). Um die erarbeiteten Funktionen zu veranschaulichen ist die Erstellung von Nutzungsszenarien für zukünftige Arbeiten geplant. Diese sollen unter Berücksichtigung verschiedener Personas erstellt werden und den Einsatz der Funktionen anhand ausgewählter Anwendungsfälle demonstrieren.

Darüber hinaus ist die Einbeziehung von Nutzenden im Rahmen von Studien zur Evaluierung der neu vorgestellten Funktionen für zukünftige Arbeiten vorgesehen. Die Studien sollen zur Validierung dienen, inwieweit der neue Funktionsumfang auf Akzeptanz trifft und ob eine Erweiterung um zusätzliche Funktionen notwendig erscheint.

7 Fazit

In der vorliegenden Arbeit wurde ein erweiterter Funktionsumfang für eine nutzungsfreundlichere Wallet vorgestellt. Dazu zählt unter anderem die Verwaltung hoheitlicher Daten, um Nutzenden den Einsatz einer Wallet auch bei Anwendungsfällen ermöglichen zu können, bei denen ein hoheitlicher Nachweis benötigt wird (bspw. Personalausweis und Führerschein). Des Weiteren ist eine Funktion zur Kommunikation mit Gegenstellen vorgesehen, bei Anwendungsfällen ohne den Bedarf einer Internetverbindung vor Ort (z. B. mit Hilfe von NFC oder Bluetooth). Darüber hinaus können sind die Nutzenden nicht an einen festen Wallet Anbieter gebunden, sondern können aufgrund der Portabilität mit ihren gespeicherten Nachweisen zu einer beliebigen anderen Wallet umziehen. Zusätzlich wird die Privatsphäre stärker gewahrt, weil die Nutzenden sich mit den Dienstanbietern nur mit Hilfe der Wallet als Kommunikationsmittel austauschen und das Teilen von Kontaktdaten (wie Email oder Telefonnummer) somit nicht mehr länger notwendig ist.

Bei der Erarbeitung des erweiterten Funktionsumfangs wurden zunächst weder technische noch rechtliche Anforderungen berücksichtigt, sondern der Fokus allein auf die Perspektive der Nutzenden und deren Anforderungen an eine Wallet gerichtet. Dabei wurden sowohl die aktuellen Hürden von Dienstleistungen als auch die Usability-Probleme existierender Wallets berücksichtigt.

Die Zukunft des vorgestellten Konzepts einer nutzungsfreundlicheren Wallet könnte darin liegen, dass zunächst eine Übergangslösung zur aktuellen Situation gesucht wird. So wäre es denkbar, dass Nutzende sich mittels ihrer Wallet bei ihren Accounts anmelden können oder über ihre Wallet automatisiert Änderungen in den Datensätzen bei den Dienstleistern anstoßen. Durch letzteres wird gleichzeitig verhindert, dass sämtliche Daten manuell angepasst werden müssen als auch, dass

die Nutzenden Dienste übersehen, welche die aktualisierten Daten benötigen. Dabei sollte die Datenänderung nur nach Zustimmung der Nutzenden erfolgen.

Da im Rahmen dieses Beitrags noch keine Validierung der Funktionen zusammen mit Nutzenden stattgefunden hat, soll dies in einer Folgeuntersuchung erarbeitet werden. Dabei soll unter anderem der Fokus auf dem Gebiet der Usable Security liegen. Denkbar wäre ebenso eine Untersuchung hinsichtlich einer visuellen Darstellung oder der Nutzung geeigneter Icons.

Mit Hilfe dieses Beitrags soll ebenso deutlich gemacht werden, dass es wichtig ist Nutzende frühzeitig einzubinden zur Ermittlung ihres Vorwissens sowie ihrer Anforderungen an die Anwendung. Zum anderen sollte die gesamte Entwicklung der Anwendung aus der Sicht der Nutzenden begleitet werden, z. B. mit Hilfe von User-Experience-Methoden. Das schließt ebenso ein, dass bei solchen sicherheitsrelevanten Anwendungen nicht nur der Fokus auf der Sicherheit liegen sollte, sondern die Anwendung so ausgearbeitet werden sollte, dass sie gleichzeitig sicher und stets nutzungsfreundlich bleibt. Dies ermöglicht die Entwicklung einer nutzungszentrierten Wallet.

Funding Das dieser Veröffentlichung zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Wirtschaft und Klimaschutz unter den Förderkennzeichen 01MN21001A und 01MN21003F gefördert.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Bhargav-Spantzel A, Camenisch J, Gross T, Sommer D (2006) User centricity: a taxonomy and open issues. Proceedings of the second ACM workshop on Digital identity management (DIM '06). Association for Computing Machinery, New York, S 1–10 https://doi.org/10.1145/1179529.1179531

Blockchain HELIX (2020) helix id Wallet. https://helixid.io/. Zugegriffen: 31. Jan. 2023

Budiu R (2015) Mobile user experience: limitations and strengths. Nielsen Norman group. https://www.nngroup.com/articles/mobile-ux/. Zugegriffen: 29. Jan. 2023

Bundesamt für Justiz (2017) Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG). http://www.gesetze-im-internet.de/ozg/__1.html. Zugegriffen: 15. Jan. 2023

Bundesministerium der Justiz (2009) Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz – PAuswG) – §14. https://www.gesetze-im-internet.de/pauswg/BJNR134610009.html. Zugegriffen: 29. Jan. 2023

Bundesministerium des Inneren und Heimat (2023) Der Online-Ausweis. https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/online-ausweisen/online-ausweisen-node.html. Zugegriffen: 15. Jan. 2023

Bundesministerium für Arbeit und Soziales (2019) Verordnung zur Änderung der Barrierefreie-Informationstechnik-Verordnung und der Behindertengleichstellungsschlichtungsverordnung. https://www.bmas.de/DE/Service/Gesetze-und-Gesetzesvorhaben/verordnung-aenderung-der-bitv.html. Zugegriffen: 30. Sept. 2022

Bundesministerium für Wirtschaft und Klimaschutz (2020) Schaufenster Sichere Digitale Identitäten. https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html. Zugegriffen: 20. Sept. 2022

Cameron A, Grewe O (2022) An overview of the digital identity lifecycle (v2). IDPro Body Knowl. https://doi.org/10.55621/idpro.31

Der U, Jähnichen S, Sürmeli J (2017) Self-sovereign identity—opportunities and challenges for the digital revolution. arXiv. https://doi.org/10.48550/arxiv.1712.01767

Deutsches Institut für Normung e. V. (2018) Ergonomie der Mensch-System-Interaktion – Teil 11: Gebrauchstauglichkeit: Begriffe und Konzepte (DIN EN ISO 9241-11:2018-11). Beuth Verlag GmbH. https://doi.org/10.31030/2757945

Deutsches Institut für Normung e. V. (2020) Ergonomie der Mensch-System-Interaktion – Teil 110: Interaktionsprinzipien (DIN EN ISO 9241-110:2020-10). Beuth Verlag GmbH. https://doi.org/10.31030/3147467

eco – Verband der Internetwirtschaft e. V., techconsult (2022) Security & digitale Identiäten in einer digitalisieren Welt. https://www.eco.de/themen/eco-studien-und-whitepaper/studie-security-digitale-identitaeten-in-einer-digitalisierten-welt/#download. Zugegriffen: 10. Jan. 2023

Ehrlich T, Richter D, Meisel M, Anke J (2021) Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. HMD 58:247–270. https://doi.org/10.1365/s40702-021-00711-5

Europäische Kommission (2021) Vorschlag für eine Verordnung des Europäschen Parlament und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäsche digitale Identität. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52021PC0281. Zugegriffen: 31. Jan. 2023

Europäisches Parlament und Rat (2016) Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Amtsblatt der Europäischen Union. [Online] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L:2016:119:TOC [Gesehen 21. Januar 2023].

European Commission (2022) Digital economy and society index (DESI) 2022. https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022. Zugegriffen: 30. Jan. 2023

European Data Protection Supervisor (2022) The EU digital identity wallet: episode 1—an overview. https://edps.europa.eu/press-publications/publications/podcasts/eu-digital-identity-wallet-episode-1-overview_en. Zugegriffen: 21. Sept. 2022

Evernym Inc., An Avast Company (2022) Connect.Me. https://www.evernym.com/connectme/. Zugegriffen: 30. Jan. 2023

forsa Politik- und Sozialforschung (2020) Digitalisierungsmonitor 2020 – Ergebnisse einer repräsentativen Bevölkerungsbefragung im Auftrag der Fraktion der Freien Demokraten im Deutschen Bundestag. https://www.fdpbt.de/sites/default/files/2020-10/Digitalisierungsmonitor-2020-forsa-Studie.pdf. Zugegriffen: 31. Jan. 2023

Garfinkel S (2005) Design principles and patterns for computer systems that are simultaneously secure and usable. Thesis (Ph. D.), Massachusetts Institute of Technology, Dept. of Electrical Engineering and Computer Science.

Hassenzahl M (2008) User experience (UX): Towards an experiential perspective on product quality. In: Proceedings of the 20th Conference on l'Interaction Homme-Machine (IHM '08). Association for Computing Machinery, New York, S 11–15 https://doi.org/10.1145/1512714.1512717

Hevner AR, March ST, Park J, Ram S (2004) Design science in information systems research. MISQ 28(1):75–105. https://doi.org/10.2307/25148625

Hoepner P, Welzel C, Wulff M (2019) Identifizierung und Authentifizierung leicht gemacht – die Nutzer ins Zentrum stellen, Nationales E-Government Kompetenzzentrum e. V. https://negz.org/wp-content/uploads/2022/12/6_Kurzstudie-Identifizierung-und-Authentifizierung-2020.pdf. Zugegriffen: 28. Jan. 2023

IDnow (2023) IDnow Digital Identity Index 2023 Deutschland – Eine Studie zur Zukunft der digitalen Identität in Deutschland. https://www.idnow.io/de/portfolio/digital-identity-index-2023-deutschland/. Zugegriffen: 23. Jan. 2023

Initiative D21 e. V. (2022) D21-Digital-Index 2021/2022 Wie digital ist Deutschland? Jährliches Lagebild zur Digitalen Gesellschaft. https://initiatived21.de/app/uploads/2022/02/d21-digital-index-2021_2022.pdf. Zugegriffen: 15. Jan. 2023

Initiative D21 e. V., TU München (2022) eGovernment Monitor 2022 Nutzen und akzeptieren Bürger*innen die digitale Verwaltung? Die deutschen Bundesländer, Deutschland, Österreich und die Schweiz im Vergleich. https://initiatived21.de/app/uploads/2022/10/egovernment_monitor_2022.pdf. Zugegriffen: 23. Jan. 2023

Jaferian P, Hawkey K, Sotirakopoulos A, Velez-Rojas M, Beznosov K (2011) Heuristics for evaluating IT security management tools. In: Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS '11). Article 7. Association for Computing Machinery, New York, S 1–20 https://doi.org/10.1145/2078827.2078837

Jolocom (2023) Jolocom. https://jolocom.io/. Zugegriffen: 30. Jan. 2023

Khayretdinova A, Kubach M, Sellung R, Roßnagel H (2022) Conducting a usability evaluation of decentralized identity management solutions. In: Friedewald M, Kreutzer M, Hansen M (Hrsg) Selbstbestimmung, Privatheit und Datenschutz. Springer Vieweg, Wiesbaden https://doi.org/10.1007/978-3-658-33306-5_19

Kohler T (2022) Psychology for UX: study guide. Nielsen Norman group. https://www.nngroup.com/articles/psychology-study-guide/. Zugegriffen: 31. Jan. 2023

Korir M, Parkin S, Dunphy P (2022) An empirical study of a decentralized identity wallet: usability, security, and perspectives on user control. In: Eighteenth symposium on usable privacy and security (SOUPS 2022). USENIX Association, Boston, S 195–211

Linux Foundation T (2022) Linux foundation announces an intent to form the openwallet foundation. https://www.linuxfoundation.org/press/linux-foundation-announces-an-intent-to-form-the-openwallet-foundation. Zugegriffen: 21. Sept. 2022

Markus ML, Majchrzak A, Gasser L (2002) A design theory for systems that support emergent knowledge processes. MISQ 26(3):179–212 (http://www.jstor.org/stable/4132330)

Moran K (2016) How chunking helps content processing. Nielsen Norman group. https://www.nngroup.com/articles/chunking/. Zugegriffen: 31. Jan. 2023

Neosfer (2023) The Lissi wallet. https://www.lissi.id/for-users. Zugegriffen: 30. Jan. 2023

Nguyen K (2022) EUid: digital identity in an electronic wallet. Bundesdruckerei. https://www.bundesdruckerei.de/en/innovation-hub/euid-digital-identity-electronic-wallet. Zugegriffen: 15. Jan. 2023

Nielsen J (2012) Usability 101: introduction to usability. Nielsen Norman group. https://www.nngroup.com/articles/usability-101-introduction-to-usability/. Zugegriffen: 18. Jan. 2023

Podgorelec B, Alber L, Zefferer T (2022) What is a (digital) identity wallet? A systematic literature review. 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), S 809–818 https://doi.org/10.1109/COMPSAC54236.2022.00131

Privacy by Design Foundation (2023) IRMA. https://irma.app/. Zugegriffen: 30. Jan. 2023

Reposito (2013) Studie: Kunden wollen Kundenkarten – aber nicht im Geldbeutel. UNITED NEWS NETWORK. https://www.pressebox.de/inaktiv/reposito-gmbh/Studie-Kunden-wollen-Kundenkarten-aber-nicht-im-Geldbeutel/boxid/591644. Zugegriffen: 29. Jan. 2023

Sartor S, Sedlmeir J, Rieger A, Roth T (2022) Love at first sight? A user experience study of self-sovereign identity wallets. ECIS 2022 research papers, 46. https://aisel.aisnet.org/ecis2022_rp/46. Zugegriffen: 21. Sept. 2022

Sawers P (2022) Linux Foundation announces the OpenWallet Foundation to develop interoperable digital wallets. TechCrunch. https://techcrunch.com/2022/09/13/linux-foundation-announces-the-openwallet-foundation-to-develop-interoperable-digital-wallets/. Zugegriffen: 21. Sept. 2022

Schade A (2016) Customization vs. Personalization in the user experience. Nielsen Norman group. https://www.nngroup.com/articles/customization-personalization/. Zugegriffen: 30. Jan. 2023

Schnepf S, Pagel D, Störk S (2021) PwC-Studie Der Online-Ausweis auf dem Smartphone und die digitale Brieftasche. PwC. https://www.pwc.de/de/branchen-und-markte/oeffentlicher-sektor/pwc-studie-der-online-ausweis-auf-dem-smartphone-und-die-digitale-brieftasche.pdf. Zugegriffen: 31. Jan. 2023

Schwab C, Kuhlmann S, Bogumil J, Gerber S (2019) Digitalisierung der Bürgeramter in Deutschland. Hans-Böckler-Stiftung, Düsseldorf. https://www.boeckler.de/pdf/p_study_hbs_427.pdf. Zugegriffen: 10. Jan. 2023

Sellung R, Hölscher M, Burgstaller-Hochenwarter L (2022) Good practices of user experience and design research for mobile and electronic governmental services in. In: Kö A, Francesconi E, Kotsis G, Tjoa AM, Khalil I (Hrsg) Electronic government and the information systems perspective. EGOVIS 2022. Lecture Notes in Computer Science, Bd. 13429. Springer, Cham https://doi.org/10.1007/978-3-031-12673-4_10

Sherwin K (2016) Hierarchy of trust: the 5 experiential levels of commitment. Nielsen Norman group. https://www.nngroup.com/articles/commitment-levels/. Zugegriffen: 15. Jan. 2023

Software USUAG (2020) Wie Behörden mit Online-Bürgerservices überzeugen Was Kommunen können und Nutzer*innen wollen. Repräsentative Bürger*innenbefragung zur Digitalisierung von Verwaltungsleistungen. https://media.usu.com/de-de/infocenter/studie-ozg-studie#usu_header. Zugegriffen: 21. Sept. 2022

Son YJ, Park MJ, Park JS (2021) Self-sovereign identity (SSI): structured literature reviews with socio-technical perspective. J Inf Syst 30(4):119–152. https://doi.org/10.5859/KAIS.2021.30.4.119

Sovrin Foundation (2023) Principles Of SSI V3. https://sovrin.org/principles-of-ssi/. Zugegriffen: 28. Jan. 2023

Sporny M, Longley D, Chadwick D (2022) Verifiable credentials data model v1.1. W3C. https://www.w3.org/TR/vc-data-model/. Zugegriffen: 21. Sept. 2022

Trinsic Technologies Inc (2022) Identity wallets. https://trinsic.id/identity-wallets/. Zugegriffen: 30. Jan. 2023

W3C (2018) Web Content Accessibility Guidelines (WCAG) 2.1. https://www.w3.org/TR/WCAG21/. Zugegriffen: 30. Sept. 2022

Watts S, Shankaranarayanan G, Even A (2009) Data quality assessment in context: a cognitive perspective. Decis Support Syst 48(1):202–211. https://doi.org/10.1016/j.dss.2009.07.012

Whitten A, Tygar JD (1999) Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In: Proceedings of the 8th conference on USENIX Security Symposium. SSYM'99, Bd. 8. USENIX Association, USA, S 14

Wohlgemuth S, Jendricke U, Markotten GTD, Domer F, Müller G (2003) Sicherheit und Benutzbarkeit durch Identitätsmanagement. Aktuelle Trends in der Softwareforschung-Tagungsband zum doITForschungstag, Stuttgart, S 241–260

Yee K-P (2004) Aligning security and usability. IEEE Secur Privacy 2(5):48–55. https://doi.org/10.1109/MSP.2004.64