Analyzing Terms of Use Adoption in SSI Digital Wallets: A Review of Current Implementations

Stefano Bistarelli[1], Chiara Luchini[1,2,*] and Francesco Santini[1]

[1]Department of Mathematics and Computer Science, University of Perugia, Via Vanvitelli 1, 06123 Perugia (PG), Italy
[2]Department of Mathematics and Computer Science "Ulisse Dini", University of Florence, Viale Giovanni Battista Morgagni 67/a, 50134 Florence (FI), Italy

Abstract

The landscape of digital identity is undergoing a profound transformation, shifting from centralized architectures to user-centric and decentralized models such as *Self-Sovereign Identity* (*SSI*). SSI has demonstrated its applicability in domains such as healthcare and education, offering enhanced autonomy and data protection through technologies such as *Verifiable Credentials* (*VCs*). In parallel, regulatory frameworks such as the European Union's eIDAS 2.0 have accelerated the development of interoperable digital identity solutions, notably the *European Digital Identity Wallet* (*EUDIW*), aligning with the principles of SSI. Despite this progress, most existing SSI wallet implementations remain focused on individual users, lacking essential features for organizational contexts. In this study, we address this gap by conducting a systematic secondary review of the current landscape of industrial digital wallets, assessing their implementation of the *Terms of Use* (*ToU*) field. Our paper aims to inform the development of digital wallets tailored to enterprises and governments in SSI ecosystems.

Keywords

Digital Wallet, Terms of Use, Self-Sovereign Identity

1. Introduction

The digital identity landscape is undergoing a profound transformation, shifting from centralized models toward user-centric approaches aligned with contemporary security and privacy demands. This shift is exemplified by the growing adoption of *Self-Sovereign Identity* (*SSI*) systems, which place individuals in control of their digital identities and have found practical applications in sectors such as healthcare and education. For instance, the *UK National Health Service* (*NHS*) deployed a digital staff passport in the form of a VC during the COVID-19 pandemic [1], while the *European Blockchain Services Infrastructure* (*EBSI*) has been used for cross-border credential verification in higher education [2].

This technological evolution is paralleled by regulatory advancements, most notably the European Union's eIDAS 2.0 regulation. eIDAS 2.0 aims to standardize and secure digital identity across the EU by mandating the adoption of *European Digital Identity Wallet* (*EUDIW*) [3, 4] by 2026. These wallets allow individuals and organizations to manage a variety of credentials, ranging from *electronic identification* (*eID*) to cryptographic materials for digital signatures. National initiatives, such as the *Italian Digital Wallet System* (*IT-Wallet System*) [5], reflect the growing institutional momentum behind digital wallet deployment.

However, most existing SSI digital wallet implementations focus primarily on individual users rather than organizational or enterprise-level scenarios [6]. This highlights a gap in the current ecosystem, suggesting the need for further research and development of SSI-based wallets tailored to institutional requirements. Among the key features required by government and industrial entities adopting SSI systems as IAM is the inclusion of the *Terms of Use* (*ToU*) field within Verifiable Credentials [6].

DLT2025: 7th Distributed Ledger Technology Workshop, June, 12-14 2025 - Pizzo, Italy

[*] Corresponding author.

stefano.bistarelli@unipg.it (S. Bistarelli); chiara.luchini@collaboratori.unipg.it (C. Luchini); francesco.santini@unipg.it (F. Santini)
https://bista.sites.dmi.unipg.it/ (S. Bistarelli); https://francescosantini.sites.dmi.unipg.it/ (F. Santini)
0000-0001-7411-9678 (S. Bistarelli); 0009-0001-6846-0922 (C. Luchini); 0000-0002-3935-4696 (F. Santini)

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2025-11-24

The ToU property, as defined in the Verifiable Credentials Data Model v2.0 [7] by the *World Wide Web Consortium* (*W3C*), offers a standardized mechanism for specifying the legal and operational conditions under which a verifiable credential or presentation is issued. This functionality can be particularly relevant in contexts where the transferability of credentials, such as employee information, must be restricted or governed by specific policies. Consequently, the ToU property is considered a requirement for digital wallets designed to support organizational use cases. However, due to the relatively recent redefinition of the ToU specification and the limited awareness surrounding its practical implications, many existing wallet implementations do not yet support or prioritize this feature.

This paper reviews the current state of industrial digital identity wallets, focusing on their implementation of the ToU property to support the development of SSI solutions for companies and governments. Using a secondary systematic review of academic and gray literature, the study identifies and analyzes a representative set of wallets for ToU support. The paper is organized as follows: Section 2 introduces the SSI architecture and the role of digital wallets; Section 3 details the research methodology, and Section 5 reviews existing literature. Finally, Section 6 presents the findings and outlines future research direction.

2. Digital wallets and SSI

This section introduces the concept of SSI, emphasizing its architecture, core components, and the role of digital wallets. SSI represents a shift in digital identity management by placing individuals at the center of control, in contrast to the traditional client-server model that has long positioned users as passive recipients of services managed by centralized authorities. In response, SSI proposes a user-centric approach grounded in ten foundational principles outlined by Christopher Allen [8], which promote privacy, transparency, user consent, and interoperability.

At the heart of the SSI ecosystem are three key actors: the identity holder (typically the user), the issuer (a trusted authority that issues credentials), and the verifier (an entity that requests and checks those credentials). These interactions may be enhanced by decentralized technologies like blockchain, which provide a trust layer without relying on centralized control. Digital identities in SSI are managed through *Verifiable Credentials* (*VCs*) [7], which are digitally signed claims about a subject that include metadata, attributes, and cryptographic proofs of authenticity. These credentials can be aggregated into *Verifiable Presentations* (*VPs*), which allow users to share selected information with verifiers. Both VCs and VPs can include ToU that define how, when, and by whom the information may be used, providing an additional layer of legal and contextual control, particularly valuable in sensitive or regulated environments.

Importantly, SSI is not limited to managing the identities of individuals [9, 10]. It extends to organizations, devices, and even non-human entities, allowing for a broad and adaptable application of identity management. Credentials are stored securely in digital wallets—user-managed applications that function as personal identity managers.

Digital wallets are central to the implementation of SSI. More than just secure storage tools, they empower users to manage, share, and control their credentials across different domains, such as healthcare, education, finance, and public services. As highlighted in recent studies [11], digital wallets offer notable benefits, such as improved efficiency, enhanced security, and stronger privacy, that serve both individuals and organizations. Furthermore, digital wallets play a key role in achieving interoperability between different identity systems. Through standardized data formats and communication protocols, such as the W3C Verifiable Credentials and DID specifications, wallets may support credential exchange in various domains, including public services, healthcare, education, finance, and more. This flexibility supports the development of a unified digital identity experience, reducing the dependence on centralized authorities.

3. Research Method

This study investigates current implementations of digital wallets within SSI systems that incorporate the ToU field as a mechanism to restrict the use of VCs or VPs. Given the limited awareness and adoption of this feature, primarily due to criticisms that it was “insufficiently specified” [12], we anticipate identifying only a small number of technologies that use it. In particular, in response to these concerns, the specification of the ToU field has been revised and updated in subsequent documentation [13].

To identify the most relevant studies and minimize research bias, it is essential to establish a well-defined review protocol. This includes the formulation of our research questions, which were guided by the *Population, Intervention, Comparison, Outcome, Context* (*PICOC*) framework [14, 15], adapted to the specific focus of our study. The “Population” includes digital wallets within SSI systems, while the “Intervention” refers to tools or methods that enhance these wallets, specifically those implementing the ToU field. The “Comparison” component is not applicable, as traditional (non-SSI) wallets are not considered. The “Outcomes” aims to identify and quantify SSI wallets that support the ToU field for regulating VCs and VPs. The “Context” spans academic and industry literature, including systematic reviews, technical reports, and white papers. Based on these criteria, we derive the following research questions (RQs): “What are the current digital wallet technologies that support SSI systems regarding their technical architecture and user privacy features?” (**RQ1**) and “Which digital wallets implement the ToU field as defined in the Verifiable Credential Data Model specification?” (**RQ2**).

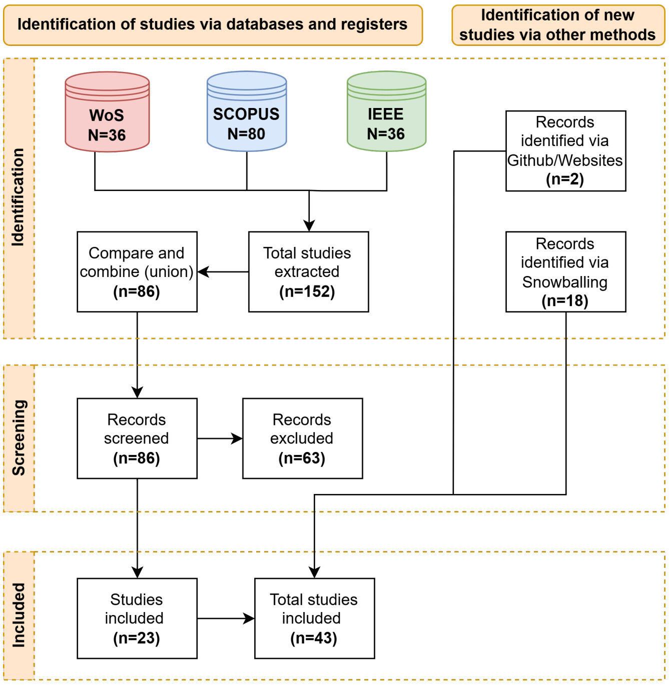
Following the formulation of the RQs, we identified the data sources to be considered for our systematic review. Figure 1a shows the research flow process following the PRISMA framework[1]. According to Brereton et al. [16], the most relevant digital libraries for Software Engineering research include: *IEEE Xplore*, *ACM Digital Library*, *Google Scholar*, *CiteSeer Library*, *Inspec*, *ScienceDirect*, and *EI Compendex*. Based on this guidance, we selected IEEE Xplore, Scopus, and Web of Science (WoS). For each selected source, we define an advanced search query built around a standard search string, adapted to the specific syntax of each platform. The general search expression used was the following:“(“self sovereign identity” OR “Self Sovereign Identity” OR ssi) AND identity AND wallet)” (**Q**). For the inclusion criteria, we restricted the results to English-language (**I1**) publications from 2020 to 2025 (**I2**) within the fields of computer science or engineering (**I3**). Table 1b shows the number of results based on the search process considering the query and the inclusion criteria.

The screening phase involved manual inspection of titles, abstracts, keywords, and conclusions, excluding non-peer-reviewed and narrowly focused studies. Preference was given to surveys and reviews of literature discussing digital identity wallets, particularly those that addressed design, privacy, and usability. This yielded 23 primary studies for analysis. The initial search results were consolidated and de-duplicated, revealing Scopus as the most comprehensive source. In contrast, IEEE Xplore and Web of Science contributed only a limited number of unique entries, as illustrated in Figure 1c. To broaden the dataset, the study employed a Snowballing method [17], utilizing both *Backward* and *Forward Snowballing* to identify additional 18 relevant papers through iterative citation tracking. Two more sources were manually included: the Gimly GitHub repository [18] and the European Blockchain Association’s website [19]. This process culminated in a final dataset of 43 documents for in-depth examination.

4. Digital Wallets Analysis

From the final set of 43 documents, digital wallets mentioned or used for comparison were extracted. The analysis focused solely on the currently implemented solutions, explicitly excluding academic proposals or prototypes. As a result, only identity wallets developed by companies or organizations were selected. More than 30 industrial wallets were identified, although only a subset of the most frequently cited implementations is presented. It should be noted that several documents did not

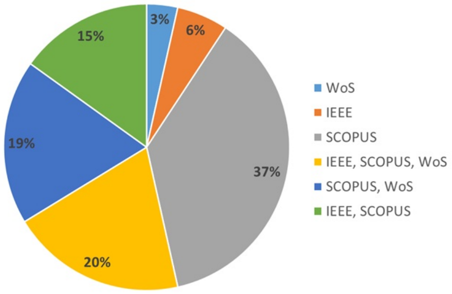
[1] PRISMA flow diagram: https://www.prisma-statement.org/prisma-2020-flow-diagram.


Identification of studies via databases and registers
Identification of new studies via other methods
Identification
WoS N=36
SCOPUS N=80
IEEE N=36
Records identified via Github/Websites (n=2)
Compare and combine (union) (n=86)
Total studies extracted (n=152)
Records identified via Snowballing (n=18)
Screening
Records screened (n=86)
Records excluded (n=63)
Included
Studies included (n=23)
Total studies included (n=43)

(a) Research process flow based on PRISMA framework [20].

Database	Q	I1	I2	I3	Final N°
IEEE Xplore	37	-	36	-	36
Web of Science	49	48	46	36	36
SCOPUS	90	-	88	80	80
Total					152

(b) Results of search process with inclusion criteria.



(c) Percentage of documents by file combination.

Figure 1: Summary of research process results.

reference industrial wallets, instead focusing on experimental or academic models. Figure 2 highlights the most frequently mentioned industrial implementations from the past five years.

Although these wallets generally adhere to the principles and concepts of SSI, they exhibit notable differences in terms of functionality and technical implementation, which present challenges in interoperability [21]. Furthermore, several digital wallets are no longer commercially available, and the majority remain in an early or relatively immature stage of development [22, 23]. For example, Jolocom, a Berlin-based SSI pioneer, ceased operations due to bankruptcy. Its SmartWallet, last updated in mid-2023, shows no signs of ongoing development, and both its website and whitepaper are no longer available. ShoCard was discontinued following its acquisition by Ping Identity in 2019. The uPort project was officially split into Veramo and Serto in 2021. Although the archived uPort Mobile app remains accessible, it has not been updated since 2019. Consequently, the Veramo framework stands in place of uPort, being regarded as its functional successor.

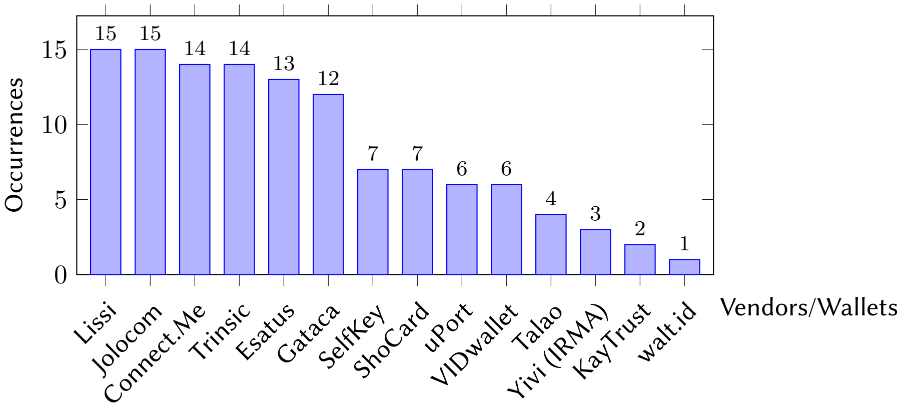


Figure 2: Most cited vendors and digital wallets.

As mentioned above, [6] identifies key requirements for enterprise-oriented SSI solutions. The authors analyzed six digital wallets from different vendors, namely Jolocom, Lissi, Esatus, Trinsic, CARO, and the Business Partner Agent by Bosch, highlighting that none of them satisfied the ToU requirement as of 2024. In this work, we revisit some of those implementations to verify whether they have been updated to support this feature. In addition, our analysis includes a broader set of digital wallets, as illustrated in Figure 2. This analysis re-examines some of those implementations to assess any recent updates and expands the scope to include a broader range of digital wallets, as shown in Figure 2.

According to [24], wallets such as Lissi, Connect.me, Gataca, and SelfKey are not designed for enterprise use. Moreover, most of the surveyed wallets are open source; proprietary exceptions include Gataca and VIDwallet. The source code for esatus, Lissi, Gataca, and VIDwallet could not be retrieved, so these wallets are only briefly described. We present an overview of the selected open-source digital wallets and assess their current ToU implementation status:

- **Lissi**: Lissi Wallet (Let's Initiate Self-Sovereign Identity) [25] is a digital identity wallet developed by Neosfer GmbH in partnership with Commerzbank AG and launched in 2019. Lissi plays a central role in European projects like IDunion [26], which aims to build an interoperable, DLT-based identity infrastructure across Europe. In line with evolving EU regulations, Lissi has introduced the EUDI-Wallet Connector to ensure seamless integration with all official EUDI-Wallets across the EU, maintaining adaptability to future standards.
- **Connect.me**: Connect.Me [27] is a mobile SSI wallet developed by Evernym and one of the first to be built on the Sovrin network. It enables users to collect, manage, and share verifiable digital credentials while maintaining full control over their digital identity. Built on Hyperledger Indy and using Hyperledger Ursa for cryptography, the wallet enables secure pairwise connections, credential storage, and the selective disclosure of information. However, based on an analysis of the publicly available source code on GitHub, there is no evidence of native support for the ToU property in the current implementation.
- **Trinsic**: Trinsic [28] is a U.S.-based company founded in 2019 that focuses on digital identity solutions. After selling its decentralized identity platform to Dentity in December 2024, Trinsic shifted its focus to the Identity Acceptance Network, a system designed to streamline identity verification by accepting pre-verified digital IDs from over 100 million users. Trinsic offers developer-friendly tools, including SDKs in various programming languages and APIs for handling VCs and DIDs. While the platform promotes open standards and interoperability, it currently lacks native support for the ToU field.
- **Jolocom**: Jolocom [29] was a Berlin-based company focused on decentralized digital identity solutions in line with SSI principles. Although the company has ceased operations, its open-source tools remain available to the public. Key offerings include the Jolocom SDK, which supports the development and verification of digital identities, and the SmartWallet, a mobile app for managing credentials and performing SSI-related actions, such as selective disclosure. Based on the current state of the GitHub repositories and the absence of updates since 2023, we confirm the observation made in [6] that the ToU property is not implemented in Jolocom's current toolset.
- **esatus**: esatus AG [30] is a German IT service provider with over 35 years of experience, specializing in information security, identity and access governance, and digital identity management. Since 2015, the company has been actively engaged in the development of SSI technologies and contributes to major European initiatives such as IDunion. Its flagship product, esatus SOWL, offers a comprehensive SSI solution designed for seamless integration into existing IT infrastructures. It features a modern, container-based architecture and supports various authentication and authorization protocols, enabling secure and efficient identity management.
- **Gataca**: Gataca [31] founded in 2017 as an academic research initiative at MIT, with the mission of tackling cybersecurity threats and identity fraud in conducting business online. Today, it has evolved into a leading European player in the SSI space, offering advanced decentralized identity solutions. Gataca Wallet is a mobile application that provides unlimited, encrypted storage for

identity credentials, including national identification cards, driver's licenses, insurance cards, and academic diplomas.

- **SelfKey**: SelfKey [32] is a blockchain-based decentralized autonomous organization (DAO) dedicated to developing an SSI platform. Central to its ecosystem is the open-source SelfKey Identity Wallet, which allows users to manage digital identities, securely store personal documents, and handle cryptocurrencies such as ETH and KEY—the platform's native ERC-20 utility token. The token facilitates staking, service access, and incentivization of trusted behavior. Based on an analysis of its GitHub repository, the wallet lacks support for the W3C-defined ToU property in Verifiable Credentials. While a term class exists, it is limited to displaying the wallet's own terms or managing KYC agreements, rather than embedding ToU metadata within credentials.
- **PingOne Neo (ex ShoCard)**: ShoCard was a blockchain-based IdM system designed to allow users to securely store and manage their digital identities [33]. Following its acquisition by Ping Identity in 2020 [34], ShoCard's foundational concepts were integrated into PingOne Neo [35], a decentralized identity platform grounded in SSI principles. Key components of the platform include PingOne Verify, which uses official documentation and biometric verification for high-trust identity validation, and PingOne Credential, which supports customizable credential formats. Additionally, the PingOne Neo SDK facilitates the integration of digital identity features into mobile applications, providing developers with a flexible and secure infrastructure for building decentralized identity solutions. Although the platform does not natively implement the ToU field, its design allows for the incorporation of such a field.
- **VIDwallet**: VIDwallet [36], developed by Validated ID, is a mobile-based digital identity wallet designed to replace traditional physical wallets. It is the first digital wallet to achieve full compliance with the EBSI across all supported use cases. VIDwallet enables users to securely store and present personal credentials, including driver's licenses, passports, and vaccination records, for both in-person and online authentication scenarios. The wallet is ledger-agnostic, supporting a range of distributed ledger technologies (DLTs), including EBSI, Ethereum, and Velocity. It also works independently of distributed networks by employing the DID key method. While VIDwallet refers specifically to the mobile application, it is integrated into the broader VIDidentity ecosystem, which encompasses complementary services such as VIDcredentials Studio, VIDissuer, and VIDconnect.
- **Veramo**: Veramo [37] is a JavaScript framework designed for managing verifiable data, emphasizing flexibility, modularity, and cross-platform operability. It enables developers to build identity agents and deploy decentralized identity solutions across various environments, including Node.js, web browsers, and React Native, through a unified and consistent API. In 2023, the project was officially transferred to the Decentralized Identity Foundation (DIF) and is now maintained by the Veramo User Group. While Veramo does not natively support the ToU property in VCs or VPs, its extensible design allows for the creation of custom plugins to implement such functionality.
- **Talao**: Talao [38] is a French mobile identity wallet developed by the European startup Talao, specifically designed to align with the European Self-Sovereign Identity Framework (ESSIF). According to the official documentation and the publicly available source code on GitHub, the ToU field is not natively implemented. However, the TALAO project is based on two foundational components developed by SpruceID: DIDKit and SSI. The SpruceID VC syntax includes native support for the ToU field, which is therefore available at the infrastructure level, although it is not yet used by default in the wallet implementation.
- **Yivi (IRMA)**: Yivi [39], formerly known as IRMA, is a privacy-centric, open-source authentication system developed by the Privacy by Design Foundation. It implements the Idemix attribute-based credential scheme, enabling users to manage digitally signed personal attributes issued by trusted entities. These credentials are stored locally on the mobile app and can be selectively shared with verifiers, who validate them using the issuer's public key. Each credential follows a specific type that defines its structure and authorized issuers. The official documentation and the source code available in the GitHub repository do not discuss any ToU field.

- **KayTrust**: KayTrust [40] is a mobile wallet by NTT Data to manage digital credentials in various use cases, such as diplomas and vaccination certificates. It ensures data integrity and trust through real-time verification via the LACChain Ethereum network. The platform offers technical resources, including reference implementations, SDKs for Java and JavaScript/NodeJS, and deployable apps such as KayTrust Wallet and KayTrust Provider. According to the official documentation and publicly available source code on GitHub, the KayTrust ecosystem does not currently implement the ToU field as part of its verifiable credential schema.
- **walt.id**: walt.id [41] is a leading provider of open-source digital identity and wallet infrastructure, founded in 2021. It enables developers, public institutions, and private enterprises to design and deploy secure, scalable, and interoperable identity solutions across a broad spectrum of industries. The platform offers a wide suite of tools, including cross-platform libraries, RESTful APIs, and customizable white-label applications. According to both the official documentation and source code on GitHub, walt.id currently supports the use of the ToU field in VCs.

Wallet	Vendor	ToU	License	Reference
Connect.Me	Evernym	No	Apache 2.0	[42, 43, 24, 44, 22, 45, 46, 47, 48, 49, 18, 50, 51, 52]
Trinsic	Trinsic Technologies Inc	No	MIT	[42, 53, 54, 24, 44, 22, 45, 49, 18, 50, 51, 52, 6, 19]
Jolocom SmartWallet/Jolocom SDK	Jolocom	No	AA2-SDK of Governikus GmbH/Apache 2.0	[42, 55, 24, 44, 46, 43, 18, 49, 50, 51, 56, 6, 19]
SelfKey Identity Wallet	SelfKey	No	MIT	[42, 24, 49, 18, 51, 57]
PingOne Neo SDK (Shocard)	PingOne Identity	No	Apache 2.0	[42, 49, 50, 51, 58, 59]
Veramo (uPort)	DIF/Veramo User Group	No	Apache 2.0	[46, 43, 49, 50, 56, 58]
Talao Wallet	Talao	No	Apache 2.0	[24, 18, 44]
Yivi (IRMA)	Privacy by Design Foundation	No	GPLv3	[24, 18, 51]
KayTrust SDK	NTT DATA	No	Apache 2.0	[24, 18]
walt.id	walt.id	Yes	Apache 2.0	[24]

Table 1
Summary of open-source digital wallets and licenses.

Table 1 provides a comparative overview of several open-source digital wallets, detailing their respective vendors, the extent to which the ToU field is implemented, and the software licenses governing their distribution. The final column cites the sources from which each wallet has been referenced and extracted. A notable trend across the majority of these wallets is the lack of explicit support for the ToU field within their VC implementations.

5. Related Work

Several studies have examined the evolving role and requirements of identity wallets in the digital age, each contributing unique insights into their development, use, and governance. One such study by Podgorelec et al. [60] provides a systematic review of the academic literature on digital wallets used for identity management. The authors analyze 26 peer-reviewed papers to clarify definitions, functionalities, and capabilities of identity wallets, aiming to shed light on the motivations behind their adoption and the features they offer. Our research draws from both scholarly and non-academic sources, with a specific emphasis on identity wallets built around SSI principles. Ansaroudi et al. [24] offer a more technical perspective by proposing a classification system for identity wallets based on two main criteria: mechanisms for establishing trust and strategies for controlling the sharing of credentials. Their analysis builds on the Trust over IP (ToIP) layered framework, highlighting technologies that support tamper-proof credentials and secure, selective disclosure. Our study complements this by evaluating digital wallets through the lens of organizational and governmental requirements, particularly regarding the ToU feature. Bochnia et al. [6] contribute to the discussion by outlining a comprehensive set of requirements for SSI systems within organizational contexts. These include technical, operational, and relational aspects of credential management and inter-organizational identity. Their work also identifies gaps between current SSI solutions and the needs of enterprise environments. Building on their findings, we revisit several of the wallets they reviewed and expand the analysis to include additional industrial solutions. Zhang et al. [59] explore the broader theme of data sovereignty within the Web 3.0 landscape, positioning SSI as a key enabler of user-centric digital identity. Their study outlines major challenges in the field, such as key management, scalability, and interoperability, and also addresses unresolved issues like managing dynamic attributes, user personas, and attribute ownership—critical hurdles for current SSI architectures. Samir et al. [61] introduce Decentralized Trustworthy Self-Sovereign Identity Management (DT-SSIM), a decentralized identity management framework that uses Shamir's Secret Sharing, blockchain, and smart contracts to enhance privacy and security. The authors present a comparative analysis of existing solutions like ShoCard, SelfKey, Sovrin, and uPort, emphasizing DT-SSIM's innovative architecture. Finally, Rota's Master's thesis [62] presents the development of a standalone SSI framework based on blockchain and MetaMask, which was later integrated into the Data Cellar project by the Links Foundation. The thesis also includes a preliminary evaluation of existing SSI-based identity management systems such as ShoCard, Sovrin, and uPort.

6. Conclusion

The digital identity space is shifting toward more user-centric and privacy-preserving models through the adoption of SSI architectures. This paper examines whether industrial digital identity wallets support the ToU property. Based on a structured review of academic and gray literature, a representative set of wallets was analyzed for ToU compliance. The results show limited adoption of the ToU feature, despite its potential, particularly among enterprise-oriented wallets.

Future research should broaden the scope to include wallets aligned with EUDIW or integrated into EBSI and implement the ToU property in practice. Such work would demonstrate the benefits of ToU for legal traceability, data governance, and interoperability, advancing SSI adoption in the enterprise and government sectors.

Acknowledgments

Stefano Bistarelli and Chiara Luchini are members of the INdAM Research group GNCS, and all three authors are members of Consorzio CINI. This work has been partially supported by: GNCS-INdAM, CUP_E53C23001670001; MUR PNRR project SERICS (PE00000014 AQuSDIT: CUP_H73C22000880001, COVERT: CUP_J93C23002310006), funded by the European Union – Next Generation EU; EU MUR PNRR project VITALITY (J97G22000170005), funded by the European Union – Next Generation EU; University of Perugia - Fondo Ricerca di Ateneo (2020, 2022) – Projects BLOCKCHAIN4FOODCHAIN, FICO, RATIONALISTS, "Civil Safety and Security for Society".

Declaration on Generative AI

During the preparation of this work, the author(s) utilized ChatGPT and Grammarly to perform the following tasks: grammar and spelling checks, paraphrasing and rewording, and enhancing writing style. After using these tools and services, the author(s) reviewed and edited the content as needed and took full responsibility for the content of the publication.

References

[1] M. Lacity, E. Carmel, Implementing self-sovereign identity (ssi) for a digital staff passport at uk nhs, University of Arkansas (2022).

[2] E. Tan, E. Lerouge, J. Du Caju, D. Du Seuil, Verification of education credentials on european blockchain services infrastructure (ebsi): Action research in a cross-border use case between belgium and italy, Big Data and Cognitive Computing 7 (2023). doi:10.3390/bdcc7020079.

[3] European Commission, The European Digital Identity Wallet Architecture and Reference Framework | Shaping Europe's Digital Future., Technical Report, European Commission, 2023. https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework.

[4] European Commission, Eu digital identity wallet, 2025. https://tinyurl.com/2rzfvt3c.

[5] Dipartimento per la trasformazione digitale, It-wallet: three digital documents available for all italian citizens and residents, 2024. https://tinyurl.com/yc6bc6ud.

[6] R. Bochnia, D. Richter, J. Anke, Self-sovereign identity for organizations: Requirements for enterprise software, IEEE Access 12 (2024) 7637–7660. doi:10.1109/ACCESS.2023.3349095.

[7] M. Sporny, D. Longley, D. Chadwick, O. Steele, Verifiable Credentials Data Model v2.0, Technical Report, World Wide Web Consortium (W3C), 2024.

[8] C. Allen, The path to self-sovereign identity, 2016. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

[9] P. C. Bartolomeu, E. Vieira, S. M. Hosseini, J. Ferreira, Self-sovereign identity: Use-cases, technologies, and challenges for industrial iot, in: 24th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA 2019, Zaragoza, Spain, September 10-13, 2019, IEEE, 2019, pp. 1173–1180. doi:10.1109/ETFA.2019.8869262.

[10] N. V. Kulabukhova, A. Ivashchenko, I. Tipikin, I. Minin, Self-sovereign identity for iot devices, in: S. Misra, O. Gervasi, B. Murgante, E. N. Stankova, V. Korkhov, C. M. Torre, A. M. A. C. Rocha, D. Taniar, B. O. Apduhan, E. Tarantino (Eds.), Computational Science and Its Applications - ICCSA 2019 - 19th International Conference, Saint Petersburg, Russia, July 1-4, 2019, Proceedings, Part II, volume 11620 of *Lecture Notes in Computer Science*, Springer, 2019, pp. 472–484. doi:10.1007/978-3-030-24296-1_37.

[11] M. Babel, L. Willburger, J. Lautenschlager, F. Völter, T. Guggenberger, M. Körner, J. Sedlmeir, J. Strüker, N. Urbach, Self-sovereign identity and digital wallets, Electron. Mark. 35 (2025) 28. doi:10.1007/S12525-025-00772-0.

[12] World Wide Web Consortium (W3C), termsofuse is insufficiently specified, https://github.com/w3c/vc-data-model/issues/1010, 2023.

[13] World Wide Web Consortium (W3C), Update to terms of use description, https://github.com/w3c/vc-data-model/pull/1295, 2023.

[14] M. Petticrew, H. Roberts, Systematic Reviews in the Social Sciences: A Practical Guide, volume 11, Blackwell Publishing, 2006. doi:10.1002/9780470754887.

[15] B. Kitchenham, S. Charters, Guidelines for performing systematic literature reviews in software engineering 2 (2007).

[16] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, M. Khalil, Lessons from applying the systematic literature review process within the software engineering domain, Journal of Systems and Software 80 (2007) 571–583. doi:https://doi.org/10.1016/j.jss.2006.07.009, software Performance.

[17] C. Wohlin, Guidelines for snowballing in systematic literature studies and a replication in software engineering, in: M. J. Shepperd, T. Hall, I. Myrtveit (Eds.), 18th International Conference on Evaluation and Assessment in Software Engineering, EASE '14, London, England, United Kingdom, May 13-14, 2014, ACM, 2014, pp. 38:1–38:10. doi:10.1145/2601248.2601268.

[18] Gimly, Ssi wallets, 2022. https://github.com/Gimly-Blockchain/ssi-wallets.

[19] European Blockchain Association, Ssi wallets, 2025. https://europeanblockchainassociation.org/ssi-wallets/.

[20] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw, A. Hróbjartsson, M. M. Lalu, T. Li, E. W. Loder, E. Mayo-Wilson, S. McDonald, L. A. McGuinness, L. A. Stewart, J. Thomas, A. C. Tricco, V. A. Welch, P. Whiting, D. Moher, The prisma 2020 statement: an updated guideline for reporting systematic reviews, BMJ 372 (2021). doi:10.1136/bmj.n71. arXiv:https://www.bmj.com/content/372/bmj.n71.full.pdf.

[21] D. O'Donnell, 2023 wallet report update: Emerging trust layer, trust registries & interoperability, https://www.continuumloop.com/2023-wallet-report-update/, 2023.

[22] S. Cucko, V. Kersic, M. Turkanovic, Towards a catalogue of self-sovereign identity design patterns, Applied Sciences 13 (2023). doi:10.3390/app13095395.

[23] D. Reed, D. O'Donnell, Digital wallet report 2021 update, http://continuumloop.com/digital-wallet-report-update/, 2021.

[24] Z. E. Ansaroudi, R. Carbone, G. Sciarretta, S. Ranise, Control is nothing without trust a first look into digital identity wallet trends, in: V. Atluri, A. L. Ferrara (Eds.), Data and Applications Security and Privacy XXXVII - 37th Annual IFIP WG 11.3 Conference, DBSec 2023, Sophia-Antipolis, France, July 19-21, 2023, Proceedings, volume 13942 of *Lecture Notes in Computer Science*, Springer, 2023, pp. 113–132. doi:10.1007/978-3-031-37586-6_7.

[25] Neosfer GmbH, Lissi, 2025. Lissi: https://www.lissi.id/.

[26] IDunion, Idunion ermglicht selbstbestimmte identten., 2025. https://idunion.org/.

[27] Evernym, Connect.me, 2023. Connect.Me: https://github.com/evernym/ConnectMe, Evernym: https://www.evernym.com/.

[28] Trinsic Technologies Inc, Trinsic, 2025. Trinsic: https://trinsic.id/, Trinsic SDK: https://github.com/trinsic-id/sdk.

[29] Jolocom, Jocolom, 2022. Jolocom SDK: https://github.com/jolocom/jolocom-sdk, Jolocom SmartWallet: https://github.com/jolocom/smartwallet-app.

[30] esatus AG, esatus, 2025. Esatus SOWL:https://esatus.com/en/digital-identity/.

[31] Gataca, Gataca, 2025. Gataca: https://gataca.io/, Gataca Wallet: https://gataca.io/products/wallet/.

[32] SelfKey, Selfkey foundation, 2024. SelfKey: https://selfkey.org/, SelfKey Identity Wallet: https://github.com/SelfKeyFoundation/Identity-Wallet.

[33] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, K. R. Choo, Blockchain-based identity management systems: A review, J. Netw. Comput. Appl. 166 (2020) 102731. doi:10.1016/J.JNCA.2020.102731.

[34] P. Identity, Ping identity acquires personal identity leader shocard to revolutionize privacy, streamline customer interactions and put users in control of their identity, 2020. https://tinyurl.com/mrcmejpb.

[35] Ping Identity, Pingone neo, 2025. PingOne Neo: https://tinyurl.com/ya379t5j, PingOne Credential: https://tinyurl.com/39f969we, PingOne Neo Native SDKs: https://github.com/pingidentity/pingone-neo-mobile-sdk.

[36] Validated ID, Vidwallet, 2025. VIDWallet: https://www.validatedid.com/en/identity/vidwallet.

[37] Decentralized Identity Foundation (DIF) - Veramo User Group, Veramo, 2025. Veramo: https://veramo.io/, Veramo User Group: https://blog.identity.foundation/veramo-user-group/.

[38] Talao, Talao, 2025. Talao: https://talao.io/, Talao Verifiable Credentials: https://doc.wallet-provider.io/vc_type, Talao Wallet: https://github.com/TalaoDAO/AltMe/tree/TALAO, SpruceID: https://spruceid.com/, DIDKit - SpruceID: https://github.com/spruceid/didkit, SSI - SpruceID: https://github.com/spruceid/ssi.

[39] Privacy by Design Foundation, Yivi, 2025. Yivi: https://www.yivi.app/en/., Yivi GitHub: https://github.com/privacybydesign/irmamobile.

[40] NTT Data, Kaytrust, 2025. KayTrust: https://www.kaytrust.id/, KayTrust Documentation: https://developer.kaytrust.id/, KayTrust Github: https://github.com/KayTrust.

[41] walt.id, walt.id, 2025. Walt.id: https://walt.id/, walt.id GitHub: https://github.com/walt-id/waltid-identity.

[42] R. Sellung, M. Kubach, Research on user experience for digital identitywallets: state-of-the-art and

recommendations, in: Open Identity Summit 2023, Gesellschaft für Informatik eV, 2023, pp. 39–50.

[43] A. Khayretdinova, M. Kubach, R. Sellung, H. Roßnagel, Conducting a usability evaluation of decentralized identity management solutions, in: M. Friedewald, M. Kreutzer, M. Hansen (Eds.), Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg, DuD-Fachbeiträge, Springer Fachmedien Wiesbaden, 2022, pp. 389–406. URL: https://doi.org/10.1007/978-3-658-33306-5_19. doi:10.1007/978-3-658-33306-5_19.

[44] S. Cucko, B. Sumak, M. Turkanovic, Identification and analysis of self-sovereign identity user interface and user experience design patterns, in: IEEE International Conference on Decentralized Applications and Infrastructures, DAPPS 2023, Athens, Greece, July 17-20, 2023, IEEE, 2023, pp. 166–173. URL: https://doi.org/10.1109/DAPPS57946.2023.00030. doi:10.1109/DAPPS57946.2023.00030.

[45] V. Kersic, U. Vidovic, A. Vrecko, M. Domajnko, M. Turkanovic, Orchestrating digital wallets for on- and off-chain decentralized identity management, IEEE Access 11 (2023) 78135–78151. URL: https://doi.org/10.1109/ACCESS.2023.3299047. doi:10.1109/ACCESS.2023.3299047.

[46] S. Kostic, M. Poikela, Do users want to use digital identities? a study of a concept of an identity wallet, in: Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022). USENIX Association, Boston, MA, 2022, pp. 195–211.

[47] J. Sedlmeir, J. Huber, T. J. Barbereau, L. Weigl, T. Roth, Transition pathways towards design principles of self-sovereign identity, in: Proceedings of the 43rd International Conference on Information Systems (ICIS), 2022.

[48] S. Sartor, J. Sedlmeir, A. Rieger, T. Roth, Love at first sight? A user experience study of self-sovereign identity wallets, in: R. Beck, D. Petcu, M. Fotache, S. Matook, R. Helms, M. Wiener, L. Rusu, T. Tuunanen (Eds.), 30th European Conference on Information Systems - New Horizons in Digitally United Societies, ECIS 2022, Timisoara, Romania, June 18-24, 2022, 2022. URL: https://aisel.aisnet.org/ecis2022_rp/46.

[49] M. Kuperberg, R. Klemens, Integration of self-sovereign identity into conventional software using established IAM protocols: A survey, in: H. Roßnagel, C. H. Schunck, S. Mödersheim (Eds.), Open Identity Summit 2022, Copenhagen, Denmark, July 7-8, 2022, volume P-325 of *LNI*, Gesellschaft für Informatik e.V., 2022, pp. 51–62. URL: https://doi.org/10.18420/OID2022_04. doi:10.18420/OID2022_04.

[50] R. N. Zaeem, M. Khalil, M. Lamison, S. Pandey, K. Barber, On the usability of self sovereign identity solutions, University of Texas at Austin Center for Identity, UTCID (2021) 21–02.

[51] R. N. Zaeem, K. C. Chang, T. Huang, D. Liau, W. Song, A. Tyagi, M. M. Khalil, M. R. Lamison, S. Pandey, K. S. Barber, Blockchain-based self-sovereign identity: Survey, requirements, use-cases, and comparative study, in: J. He, R. Unland, E. S. Jr., X. Tao, H. Purohit, W. van den Heuvel, J. Yearwood, J. Cao (Eds.), WI-IAT '21: IEEE/WIC/ACM International Conference on Web Intelligence, Melbourne VIC Australia, December 14 - 17, 2021, ACM, 2021, pp. 128–135. URL: https://doi.org/10.1145/3486622.3493917. doi:10.1145/3486622.3493917.

[52] J. Sedlmeir, R. Smethurst, A. Rieger, G. Fridgen, Digital identities and verifiable credentials, Bus. Inf. Syst. Eng. 63 (2021) 603–613. URL: https://doi.org/10.1007/s12599-021-00722-y. doi:10.1007/S12599-021-00722-Y.

[53] J. Glöckler, J. Sedlmeir, M. Frank, G. Fridgen, A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity, Bus. Inf. Syst. Eng. 66 (2024) 421–440. URL: https://doi.org/10.1007/s12599-023-00830-x. doi:10.1007/S12599-023-00830-X.

[54] S. Chuhan, V. Wojnas, Designing and evaluating a resident-centric digital wallet experience, in: A. Moallem (Ed.), HCI for Cybersecurity, Privacy and Trust - 5th International Conference, HCI-CPT 2023, Held as Part of the 25th HCI International Conference, HCII 2023, Copenhagen, Denmark, July 23-28, 2023, Proceedings, volume 14045 of *Lecture Notes in Computer Science*, Springer, 2023, pp. 591–609. URL: https://doi.org/10.1007/978-3-031-35822-7_38. doi:10.1007/978-3-031-35822-7_38.

[55] M. Teuschel, D. Pöhn, M. Grabatin, F. Dietz, W. Hommel, F. Alt, 'don't annoy me with

privacy decisions!' - designing privacy-preserving user interfaces for SSI wallets on smartphones, IEEE Access 11 (2023) 131814–131835. URL: https://doi.org/10.1109/ACCESS.2023.3334908. doi:10.1109/ACCESS.2023.3334908.

[56] Y. Liu, Q. Lu, H. Paik, X. Xu, Design patterns for blockchain-based self-sovereign identity, in: EuroPLoP '20: European Conference on Pattern Languages of Programs 2020, Virtual Event, Germany, 1-4 July, 2020, ACM, 2020, pp. 16:1–16:14. URL: https://doi.org/10.1145/3424771.3424802. doi:10.1145/3424771.3424802.

[57] F. Ghaffari, K. Gilani, E. Bertin, N. Crespi, Identity and access management using distributed ledger technology: A survey, Int. J. Netw. Manag. 32 (2022). URL: https://doi.org/10.1002/nem.2180. doi:10.1002/NEM.2180.

[58] A. Bazarhanova, K. Smolander, The review of non-technical assumptions in digital identity architectures, in: 53rd Hawaii International Conference on System Sciences, HICSS 2020, Maui, Hawaii, USA, January 7-10, 2020, ScholarSpace, 2020, pp. 1–10. URL: https://hdl.handle.net/10125/64527.

[59] K. L. Tan, C.-H. Chi, K.-Y. Lam, Survey on digital sovereignty and identity: From digitization to digitalization, ACM Comput. Surv. 56 (2023). doi:10.1145/3616400.

[60] B. Podgorelec, L. Alber, T. Zefferer, What is a (digital) identity wallet? A systematic literature review, in: H. V. Leong, S. S. Sarvestani, Y. Teranishi, A. Cuzzocrea, H. Kashiwazaki, D. Towey, J. Yang, H. Shahriar (Eds.), 46th IEEE Annual Computers, Software, and Applications Conferenc, COMPSAC 2022, Los Alamitos, CA, USA, June 27 - July 1, 2022, IEEE, 2022, pp. 809–818. doi:10.1109/COMPSAC54236.2022.00131.

[61] E. Samir, H. Wu, M. Azab, C. Xin, Q. Zhang, Dt-ssim: A decentralized trustworthy self-sovereign identity management framework, IEEE Internet of Things Journal 9 (2022) 7972–7988. doi:10.1109/JIOT.2021.3112537.

[62] L. Rota, Decentralized Identity Management: Building and Integrating a Self-Sovereign Identity Framework, Master's thesis, Politecnico di Torino, 2024. http://webthesis.biblio.polito.it/id/eprint/30910.