Electronic Markets (2025) 35:28
https://doi.org/10.1007/s12525-025-00772-0

FUNDAMENTALS

# Self-sovereign identity and digital wallets

**Matthias Babel[1] · Lukas Willburger[2] · Jonathan Lautenschlager[1] · Fabiane Völter[3] · Tobias Guggenberger[3] · Marc-Fabian Körner[3] · Johannes Sedlmeir[4] · Jens Strüker[3] · Nils Urbach[5]**

Received: 17 April 2024 / Accepted: 17 February 2025 / Published online: 2 April 2025


**Abstract**
Current approaches to managing digital identities struggle to meet the demands of ongoing digital transformation. They either create fragmented identities tied to specific online services, making it difficult for users to manage, or they raise concerns about being locked into corporate identity providers and data protection issues. Additionally, they provide limited support for machine-verifiable identity attributes. This reliance on third parties for managing machine identities can put companies at a market disadvantage. Therefore, there is a pressing need for a unified identity management solution that allows for the portable and interoperable use of verifiable identity data across services. The recently announced European Digital Identity Wallet marks a significant step forward in digital identity management. This initiative aims to provide EU citizens with a unified, secure, and convenient way to access both public and private online services, thereby enhancing the efficiency and security of digital interactions and prioritizing user needs. Self-sovereign identity (SSI) forms the basis for such a wallet-based identity ecosystem that supports electronic market growth. However, as a relatively new concept, SSI still lacks a unified theoretical analysis and a thorough exploration of its value propositions for digital ecosystems and networked businesses.

**Keywords** DID · eIDAS · Identity ecosystem · Privacy · User centricity · Verifiable credential · Zero-knowledge proof

**JEL Classification** O14

## Abbreviations

| | |
|---|---|
| DLT | Distributed ledger technology |
| eIDAS | Electronic Identification, Authentication and Trust Services |
| EUDIW | European Digital Identity Wallet |
| FIM | Federated identity management |
| GDPR | General Data Protection Regulation |
| IdP | Identity provider |
| NFT | Non-fungible token |
| SSI | Self-sovereign identity |
| SSO | Single sign-on |
| ZKP | Zero-knowledge proof |
| IdM | Identity management |

Responsible Editor: Ulrike E. Lechner

Extended author information available on the last page of the article

## Introduction

Digital identity ecosystems, which include users, organizations, and services, have grown increasingly complex and segmented. Stakeholders commonly create *partial identities* for each service they use in networked businesses, leading to isolated user accounts that are difficult to harmonize due to a lack of interoperability and portability (Pfitzmann & Hansen, 2010; Sedlmeir et al., 2021). As the use of digital services expands, it becomes more challenging to manage these partial identities and the associated identity attributes for every stakeholder involved. However, despite their growing complexity, current solutions for identity management (IdM) across various services fail to meet user expectations (Franz & Benlian, 2022; Bonneau et al., 2012).

Today, big tech companies provide federated identity management (FIM) solutions that make users dependent on those identity service offerings. Although one can also transfer these identity services to other services, the data sovereignty

of these federated services remains with the big tech companies. Thus, there is a lack of self-determination over the user's own data (Vapen et al., 2016). This problem will also become more significant for service providers in the future machine-to-machine economy, which will feature the identity management for billions of smart, connected machines performing economic business-to-business transactions automatically. These transactions will be vital in sectors like energy transition and the automotive industry, underscoring the need to identify and assign unique identities to people, organizations, and machines (Schweizer et al., 2020; Jöhnk et al., 2021; Körner et al., 2022; Babel et al., 2022; Braud et al., 2021).

In such a scenario, it is crucial for companies to participate actively in a neutral identity ecosystem, as relying on third parties for the data sovereignty of their machine identities could place them at a market disadvantage. Consequently, there is an urgent requirement for a unified IdM solution that facilitates the portable and interoperable use of verifiable identity data across services. This solution must address the fragmentation of IdM processes and create a trusted infrastructure capable of supporting verifiable transactions in diverse contexts (Allen, 2016; Preukschat & Reed, 2021; Windley, 2020; Pfitzmann & Hansen, 2010).

To address the patchwork of digital IdM, the European Commission has adopted the *eIDAS 2.0* regulation, which envisions a secure and interoperable framework for digital identities across the European Union. The introduction of the *European Digital Identity Wallet* (EUDIW) represents a significant opportunity for improving digital identity management (Degen & Teubner, 2024). This initiative aims to give EU citizens a unified, secure, and convenient method to access both public and private online services, improving the efficiency and security of digital interactions and focusing on user needs in the near future (Bochnia et al., 2023), while at the same time leveling the playing field and ensuring "sovereignty" in its single digital market (Ernstberger et al., 2023; Codagnone & Weigl, 2023; Rieger et al., 2022).

The revision of the eIDAS regulation introduces significant implications for a diverse set of stakeholders, including EU public organizations, big tech platform providers, and financial institutions. These groups will be directly influenced by new mandates requiring support for digital wallet log-in capabilities and the implementation of strong authentication measures via the EUDIW (Rieger et al., 2024). Additionally, the ability of users to generate qualified electronic signatures through their digital wallets is expected to be particularly valuable, especially for organizations aiming to digitize processes that have traditionally depended on physical signatures, seals, or in-person verification. Furthermore, digital wallets promise several advantages in terms of efficiency, security, and privacy, which are beneficial to both users and organizations. These benefits remain compelling even for entities not yet legally required to adopt the EUDIW, demonstrating the broader potential of digital wallets in the context of digital transformation.

Digital wallets prioritize individuals' control over their identity data use, ensuring that users can decide when to disclose their personal information and enabling them to reuse it across applications and services. In this environment, several countries and organizations are actively developing frameworks to support expanding and regulating what has been coined "self-sovereign" or "decentralized" IdM solutions. Self-sovereign identity (SSI) lays the groundwork for establishing such a wallet-based, viable identity ecosystem that promotes the growth of electronic markets (Soltani et al., 2021; Schwalm et al., 2022; Weigl et al., 2022; Bochnia et al., 2023). However, SSI, as a relatively new concept, still faces a lack of unified theoretical analysis and comprehensive exploration of its role in digital ecosystems and networked businesses (Sedlmeir et al., 2022a). Accordingly, we strive to lay the foundation for SSI by outlining the value propositions of wallet-based identity management and explaining its impact from the perspectives of both businesses and individuals.

## Foundations of SSI

### Earlier approaches to IdM

During the initial registration process, service providers typically store users' identity attributes associated with an account in their own databases. One common approach to user *authentication*, i.e., to claiming ownership of such a previously generated account, is the combination of usernames and passwords (Novakouski, 2013). More generally, *credentials* are used to prove ownership of such an account (Bosworth et al., 2005), for instance, by providing something the user knows (e.g., a password), possesses (e.g., a special piece of hardware), or is (e.g., certain biometric properties). Secure authentication through username and password combinations is often a challenge for users, as it requires them to remember or securely store the password for each service provider they use (Novakouski, 2013). As identity data is stored in a service provider's individual data silo, it is also commonly not portable across different domains (Sedlmeir et al., 2021; Wang & De Filippi, 2020). Considering the need to interact with multiple service providers within this fragmented approach, the existing patchwork of identity silos leads to a low degree of interoperability and, consequently, low security as well as a cumbersome user

experience (Sedlmeir et al., 2021; Jøsang et al., 2015).

To streamline and simplify registration processes, major technology companies like Apple, Google, or Meta have devised federated identity management approaches (Maler & Reed, 2008; Vapen et al., 2016). While federated identity management can support single sign-on (SSO) services by allowing users to authenticate once and gain access to multiple related services across different organizations, not all SSO implementations are based on federated identity management. For example, SSO solutions like Kerberos operate within a *single* domain, allowing users to access multiple internal services without federated identity across multiple external platforms (Neuman & Ts'o, 1994). In the context of federated identity management, these technologies enable users to log into their accounts at connected service providers through their identity provider (IdP) and reuse their identity attributes across different platforms.

SSO often employs Open Authorization (OAuth), a standardized protocol that securely grants third parties access to services via a token, eliminating the need to directly share the owners's credentials (Hardt, 2012). Building on OAuth, OpenID Connect (OIDC) adds an authentication layer that can provide identity attributes in the form of an ID token (Sakimura et al., 2014). This allows users to log in and share data (that might even be verified by the IdP), such as address and payment information, using credentials from providers like Google or Amazon. Although this approach offers convenience at no cost to users, it raises privacy concerns (Maler & Reed, 2008; Beck et al., 2018) and comes with strong lock-in effects for connected users and services. In the role of centralized IdPs, service provider of FIMs exercise control over their customers' data, gaining insights into their interactions with connected third-party services. This could result in the creation of a comprehensive user identity, encompassing not only master data but also transactional meta-data reflecting users' actual behavior within digital ecosystems (Zuboff, 2015; van Bokkem et al., 2019).

Moreover, service providers or digital platforms integrating SSO may lose direct access to customer information, jeopardizing their business models by rendering them dependent on the IdP (Hermes et al., 2020; Rieger et al., 2022). Additionally, current identity solutions predominantly cater to individuals, leaving businesses and machines without access functionalities for managing their own identities (Sedlmeir et al., 2021; Fedrecheski et al., 2020).

## Background on SSI

Pertinent research considers SSI as a paradigm shift in digital IdM (Cameron, 2005; Allen, 2016), rooted in the concept of digital wallets (Lacity & Carmel, 2022; Weigl et al., 2022). A digital wallet is an application that runs on one or multiple of a user's edge devices, typically including a mobile phone (Naik & Jenkins, 2020a), and empowers them to manage attestations of their digital identity attributes. In this context, digital signatures facilitated by asymmetric cryptographic keys allow to make identity attributes machine-verifiable (Wang & De Filippi, 2020; Jørgensen & Beck, 2022; Sartor et al., 2022). Thus, a digital wallet is very similar to its physical counterpart, which is usually kept directly by its owner and holds various types of attestations, such as an employee badge, a driver's license, or a membership card (Naik & Jenkins, 2020b; Schlatt et al., 2022a).

Leveraging this concept, SSI aims to establish an open ecosystem for authentication and the exchange of machine-verifiable identity information in which users have full control over the disclosure of their identity-related data (Sedlmeir et al., 2022a). The discourse of this paradigm among researchers and practitioners, as well as regulation at the national and international level, has set the guidelines for the design and implementation of corresponding protocols, software, and hardware, which can be summarized as SSI technology (Lacity & Carmel, 2022).

Fundamentally, an SSI-based solution incorporates three key roles: issuers, holders, and verifiers (Davie et al., 2019; Čučko & Turkanović, 2021). Holders interact directly and bilaterally with both issuers and verifiers. Verifiers maintain only an indirect trust relationship with issuers. This results in what is called the "trust triangle" (see Fig. 1) (Mühle et al., 2018). Issuers create digital attestations, called verifiable credentials, and send them to holders. Verifiable credentials entail claims, which are statements about an entity's identity attributes; for instance, master data (e.g., name, age), relationships (e.g., mother, daughter), or entitlements (e.g., memberships, legal status, access authorizations) that are cryptographically attested by the issuer through a digital signature (Preukschat & Reed, 2021; Sporny et al., 2022a).

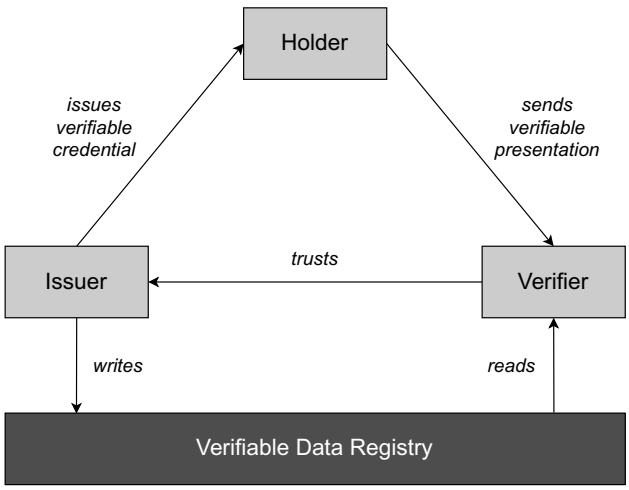


**Fig. 1** Trust triangle in the context of SSI-based interactions (adapted from Davie et al., 2019)

Holders store and manage their verifiable credentials that they received from different issuers in their digital wallet apps (Preukschat & Reed, 2021; Sporny et al., 2022a; Sartor et al., 2022). In this way, issuers enable holders to make provable claims about their identity attributes when bilaterally interacting with verifiers in what is called a verifiable presentation: Upon request, holders can use their verifiable credentials to disclose selected identity attributes in a machine-verifiable way to a relying party that acts as a verifier, without the need to interact with the issuer (Soltani et al., 2021; Čučko & Turkanović, 2021).

The underlying verifiable credentials are not restricted to representing identity attributes corresponding to natural persons (Bartolomeu et al., 2019; Kulabukhova et al., 2019). They can also refer to organizations or machines as subjects. Furthermore, the person holding a credential may not always be the same as the subject represented in the verifiable credential. For example, a credential could pertain to a machine, but its holder could be the owner of that machine, or it could relate to a company, with a legal representative holding the credential.

Owing to the distinct separation of stakeholders' roles and interactions and the corresponding decentralized management of identity attributes, it is essential that the different actors within the trust triangle can establish trusted connections when exchanging verifiable credentials or verifiable presentations. For instance, verifiers must associate the digital signatures on a verifiable credential with an organization they trust; and holders must be protected against malicious verifiers that do not have a legal basis for processing data obtained in a verifiable presentation. For this purpose, SSI makes use of publicly accessible and trusted infrastructure to publish data, including cryptographic keys, associated with issuers and verifiers, such as public institutions. As such, verifiable data registries form the foundation for associating a verifiable credential with a particular issuer and, thus, create trust within the trust triangle (Schmidt et al., 2021).

## The current state of SSI

Current research efforts on SSI primarily focus on conceptual and technical considerations of this paradigm. Specifically, studies have delved into the detailed architectural requirement and design-related aspects of SSI-based systems (Mühle et al., 2018; Bochnia et al., 2023; Satybaldy et al., 2024), encompassing core technical components (Čučko et al., 2022a), as well as the engineering process of implementations of SSI within business processes. For instance, Mühle et al. (2018) proposed technical components essential for SSI-based systems, including identification and authentication mechanisms, the exchange of verifiable identity attributes, and methods for public and private data storage. Various researchers have deliberated on the advantages of distributed ledger technology (DLT) for storing data that is supposed to be publicly available in SSI-based systems, emphasizing decentralization, auditability, and transparency in verifiable data registries (Ghaffari et al., 2022; Drăgnoiu, 2021). However, discussions have also emerged regarding limitations that restrict these elements' potential roles (Schlatt et al., 2022a).

Moreover, researchers have addressed specific socio-technical challenges within SSI-based systems (Satybaldy et al., 2024), such as interoperability (Fedrecheski et al., 2020), key recovery (Singh et al., 2021; Soltani et al., 2019), and revocation (Abraham et al., 2020, 2021). Several scholars propose different approaches of conceptualizing IT architectures for those systems (Liu et al., 2020; Schlatt et al., 2022a; Feulner et al., 2022). These proposals predominantly focus on particular domains and use cases, such as know-your-customer processes in the financial sector (Schlatt et al., 2022a; Cho et al., 2021), electronic prescriptions in healthcare (Fotopoulos et al., 2020; Schlatt et al., 2022b), fraud prevention in event or mobility ticketing systems (Feulner et al., 2022; Hoess et al., 2024), implementation of COVID-19 vaccination passports (Abid et al., 2022; Shuaib et al., 2021; Rieger et al., 2021), as well as use cases within the mobility sector (Stockburger et al., 2021; Hoess et al., 2024) and supply chain management (Cocco et al., 2021). These endeavors aim to evaluate the advantages of SSI for IdM within digital ecosystems. Research is also exploring the emerging ecosystem involved in designing and implementing IdM solutions that follow the SSI paradigm (Schmidt et al., 2021; Pöhn et al., 2021).

While existing research offers guidance regarding technical aspects and architectural development, limited attention has been directed towards examining the organizational impact resulting from SSI adoption or providing critical evaluations. For instance, Laatikainen et al. (2021) and Rieger et al. (2024) touch upon organizational benefits stemming from SSI implementation, yet primarily focus on organizational decision-making strategies. Similarly, Lacity and Carmel (2022) discuss the advantages of verifiable credentials for staff members in the UK's National Health Service, emphasizing cost reduction and fraud mitigation. However, the current body of research lacks a comprehensive understanding of the potential benefits associated with establishing an ecosystem of portable and interoperable personal, organizational, and machine identities for networked businesses and organizations. We postulate that an overarching approach facilitating the seamless and verifiable exchange of digital identity information is necessary to drive the digitization and digitalization of processes across many sectors. SSI may provide the missing link necessary to implement holistic electronic business-to-customer (B2C) and business-to-business (B2B) markets and advance the digital transformation.

The topic of digital wallets is also gaining momentum in practice. A growing number of industry- and government-backed organizations and consortia, such as the *Verifiable Organizations Network (VON)*[1] or *IDunion*[2] are working on establishing SSI within a practical environment. From a political point of view, the European Union has already made the first attempts to bring these explorations into line with its agreement on the revision of the eIDAS regulation and to support the ongoing digital transformation of the European economy and society (Schwalm et al., 2022). In particular, each member state of the European Union (EU) must offer its citizens at least one digital wallet application supporting verifiable credentials following a common toolbox implementation within the next few years (European Commission, 2023a, b; Council of the European Union, 2023). These efforts are accompanied by SSI-based showcase projects, such as the *European Self-Sovereign Identity Framework (ESSIF)*[3] or the *EU Digital Wallet Consortium (EWC)*[4] that already employ digital wallets to practically implement business-related case studies based on the technical and organizational specifications of *eIDAS 2.0*.[5] As a result, the *potential* of SSI-based solutions also appears to be growing rapidly in practice (Smith, 2020; Soltani et al., 2021; Weigl et al., 2022). That said, it should be kept in mind that any identity system as a component facilitating electronic markets must always be understood in a larger context. Not only the underlying technology of IdM itself is relevant, but also its embedding and usage in the system landscape and the creation or integration of digital ecosystems.

These projects represent just a small part of the exploration of SSI, with many tied to governmental initiatives aimed at equipping citizens with digital identities. Yet, privately led SSI projects remain relatively scarce. Notwithstanding this situation, the potential of SSI and its value propositions are becoming increasingly evident, promising transformative impacts across numerous sectors. As the landscape of digital identity continues to evolve, the involvement of both the public and private sectors will be crucial in realizing the full spectrum of SSI's capabilities. The collaborative efforts between governmental agencies, industries, and academia in pioneering and advancing SSI projects not only pave the way for a more interconnected and efficient digital world but also highlight the collective commitment to harnessing technology for greater societal benefit.

[1] https://vonx.io/

[2] https://idunion.org/

[3] https://decentralized-id.com/government/europe/eSSIF/

[4] https://eudiwalletconsortium.org/

[5] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651

## Value propositions of SSI

In this section, we will explore the practical benefits of SSI in electronic markets for the core stakeholders as outlined in the trust triangle, i.e., issuer, holders, and verifiers (see Fig. 1). These value propositions do not exclusively belong to a single stakeholder group but can create added value from various perspectives. Yet, we have categorized them based on where their added value appears most significant. By examining how SSI empowers individuals, enhances trust, security, and efficiency for verifiers, and streamlines processes for issuers in IdM, we can better understand this novel paradigm's potential impact on electronic markets. Please refer to the Appendix for further details on our process and how we arrived at the value propositions, which Table 1 summarizes.

### Issuers

Although the role of issuers is not always clearly defined in today's identity ecosystem, they still play an essential role, often as a part of a digital service that engages in both identity provisioning and verification. If they maintain their operations in a wallet-based system, they could smoothly transition into an SSI identity ecosystem. This move allows them to benefit from advantages on both the issuer and verifier sides. SSI provides two primary benefits for identity issuers: It increases efficiency and reduces the risk associated with issuing identity information. These advantages not only enhance the issuer's role but also solidify their position in digital IdM.

**Efficiency** SSI aims to streamline the verification process by directly issuing verifiable credentials—which can be verified cryptographically without further interaction with the issuer—to holders. This approach eliminates the need for issuers to repeatedly engage with verifiers for each instance of a verification (Sedlmeir et al., 2021; Preukschat & Reed, 2021). Once issued, holders can independently and verifiably present their verifiable credentials to various verifiers via verifiable presentations, promoting the creation of interoperable identity ecosystems (Mühle et al., 2018; Satybaldy et al., 2024). Such ecosystems reduce the need to re-attest the same identity information across different applications (Lacity & Carmel, 2022).

Central to these ecosystems are publicly accessible verifiable data registries. These registries offer crucial information for verifying identity presentations, including the public keys and potentially further public information about issuers (Satybaldy et al., 2024) or verifiers (Schlatt et al., 2022b). Consequently, they support a more decentralized and flexible governance model for IdM, facilitating easier integration for new market entrants (Mühle et al., 2018; Koens & Meijer, 2018). This model contrasts sharply with the restricted

**Table 1** Value propositions of SSI

| Role | Value proposition | Description |
|---|---|---|
| Issuers | Efficiency | SSI streamlines the verification process by issuing verifiable credentials, which can be cryptographically verified without requiring further interaction with the issuer. This reduces the need for repeated verification and creates interoperable identity ecosystems |
| Issuers | Risk reduction | SSI reduces the risk of identity theft or misuse by relying on secure wallets for holders and strong holder binding in verifiable credentials. The paradigm allows issuers to reduce the risks associated with data breaches and distributing personal data |
| Holders | Data control | SSI empowers holders by giving them full control over which identity attributes they share. Selective disclosure and support for unlinkability ensure data minimization, reducing unnecessary data exposure and improving privacy |
| Holders | Usability | SSI focuses on a user-centric design with simplified interfaces for connecting to services while maintaining high standards of security and data control. It seeks to improve user experience by reducing barriers to adoption |
| Verifiers | Verifiability | SSI enhances the verifiability of identity information by relying on machine-verifiable credentials, which confirm both the authenticity and integrity of the data. This reduces risks associated with self-attested data or manual identity checks |
| Verifiers | Cost reduction | SSI lowers costs by automating identity verification processes through machine-verifiable attestations, reducing the need for paperwork and manual checks and the risk of associated errors while improving security and compliance |
| Verifier | Compliance | SSI emphasizes user control over data, aligning well with data protection laws. By minimizing data processing, SSI helps verifiers reduce compliance risks and supports a privacy-by-design approach. |

data access in SSO systems, where the IdP closely controls the availability and potential costs of verifiable data. Verifiable data registries can also be used to manage the revocation states of verifiable credentials, further reducing the need for direct interaction between issuers and verifiers (Ehrlich et al., 2021). In this context, SSI enables the immediate revocation of verifiable credentials, providing real-time control over their validity and addressing fraud effectively (Schlatt et al., 2022a; Hoess et al., 2022).

**Risk reduction** To minimize the risk of issuing verifiable data to unauthorized parties, issuers can rely on previous identification and authentication via existing verifiable credentials (Sporny et al., 2022b; Preukschat & Reed, 2021; Satybaldy et al., 2024). Thus, SSI facilitates a direct and secure on-demand exchange of verifiable identity data, significantly lowering the risk of data breaches. Moreover, SSI aims to reduce the risk of identity theft or misuse. To this end, the paradigm focuses on providing secure wallets for holders, further minimizing potential attack vectors on these edge devices (European Commission, 2023a). By implementing verifiable credentials with strong (e.g., hardware-based) holder binding, the risk of fraudulent activities is supposed to be lowered (Sporny et al., 2022a; Camenisch & Lysyanskaya, 2004; Feulner et al., 2022). Such activities that need to be avoided include the unauthorized sharing of verifiable credentials or the reuse of presented credentials by verifiers, like replay attacks (German Federal Office for Information Security, 2019). Recent developments, such as the Architecture and Reference Framework corresponding to the EUDIW, foresee lists of trusted verifiers in order to secure interactions based on different levels of assurance (European Commission, 2023a; Martinez Jurado et al., 2021). Furthermore, technical solutions like designated verifier proofs, which provide cryptographic assurances that limit data exposure to authorized parties only, can help to ensure trust (Baum et al., 2022; Babel & Sedlmeir, 2023). Consequently, these measures ensure the proper use of issued verifiable information, aligning with the interests of the issuers as it supports maintaining the integrity of their issued credentials and protects the holder from phishing or oversharing their identity information.

Empowering holders to present their identity information directly significantly shifts the traditional approach of identity verification. This eliminates the need for issuers to be involved in sharing identity data with third parties. Thereby, the risk of accidentally leaking sensitive identity information greatly decreases. This reduces the burden on issuers, freeing them from the complexities and liabilities linked to distributing personal identity data. Moreover, with identity

data stored on the holder's side, issuers are relieved from the need to continuously provide this data, further reducing their data storage requirements and lowering the risk of vulnerabilities in the event of cyber attacks (Rieger et al., 2024).

## Holders

Individuals (but also organizations), as holders of their SSI wallets, experience upfront control and usability of their identity data as value propositions that empower them and enhance their interactions within electronic markets.

**Data control** SSI puts holders in full control of identity attributes attested by verifiable credentials, marking data sovereignty as a core value proposition. Under these circumstances, digital wallets empower their holders to be at the core of the IdM system, instead of the edge as in federated or siloed approaches (Weigl et al., 2022; Sartor et al., 2022). In the case of individuals, holders tend to go against their personal preferences by sharing more information on online platforms than they feel comfortable with. Researchers call this contradiction the privacy paradox, and studies like those by Gimpel et al. (2018) and Norberg et al. (2007) have thoroughly documented this tension. When users present verifiable information through scans of analog documents or established digital formats (e.g., PDF Advanced Electronic Signatures), it is required to share all the included identity attributes, mostly due to technical restrictions. This leads to the disclosure of unnecessary information for the dedicated context.

SSI proposes to mitigate such oversharing by implementing selective disclosure mechanisms or even more sophisticated data minimization techniques such as zero-knowledge proofs (ZKPs) (Babel & Sedlmeir, 2023). The paradigm distinguishes between attestations issued by the issuer that remain with the holder (verifiable credentials) and the data that the holder eventually presents to the verifier (in the verifiable presentations), also see the "Foundations of SSI" section. Verifiable presentations are supposed to support the *selective disclosure* of verifiable credential claims, meaning that holders can control which specific identity attributes they want to share. Often, it is not even relevant for the verifier to learn about the attribute itself, but only about a *predicate* inferred from it. For example, the exact age of a person is rarely needed; rather, a classification into an interval, such as being over the age of 21, is sufficient (Glöckler et al., 2023). SSI also applies ZKPs to avoid the sharing of unique identifiers in the cryptographic meta-data, restricting linkability to the attributes that need to be revealed according to the verifier's requirements by utilizing specialized digital signature creation and verification methods (Looker et al., 2022; Camenisch & Lysyanskaya, 2002).

In the end, holders should be empowered to decide with whom they share what data at what time. This approach significantly enhances their degree of data control and decreases personal data exposure, thereby reducing the risk of identity theft and improving privacy and security.

**Usability** Engaging in IdM rarely holds an inherent value, leading users to choose the path of least resistance when they have different means of IdM at hand. Usability, therefore, is not just an added advantage but a crucial element that drives the societal acceptance and security of such systems (Jøsang & Pope, 2005; Guggenberger et al., 2023a). SSI seeks to merge the user-friendly aspects of SSO services with the highest standards of data control and security. By focusing on a user-centric design and incorporating cryptographic components in the form of (hardware-bound) cryptographic keypairs, verifiable credentials, and verifiable presentations, it makes digital identities both accessible and secure (Preukschat & Reed, 2021). The eIDAS regulation highlights this opportunity and requires member states of the EU to offer digital identity wallets to their citizens, emphasizing usability as a crucial prerequisite for widespread adoption (European Commission, 2023a). Modern digital wallets are designed to simplify connections to services without burdening users with complex details (Sartor et al., 2022). This strategy, similar to the functioning of Internet browsers, may be able to strike a balance between offering broad functionality and alerting users to security concerns, such as the dangers of interacting with unauthorized verifiers (Teuschel et al., 2023), thereby protecting their digital identities from threats and misuse.

The open architecture of SSI systems welcomes credentials from a wide range of issuers, lowering entry barriers and fostering a decentralized, public trust infrastructure akin to the Web's public key infrastructure (PKI) (Lacity & Carmel, 2022; Grindal et al., 2024). This inclusiveness in verifiable credential acceptance showcases the system's flexibility and user-focused design, making digital IdM a smoother experience for users. In SSI, managing an identity does not depend on a single credential and is not restricted to a single business domain or application. Instead, it includes various identity parts from multiple domains (Pfitzmann & Hansen, 2010). An SSI wallet effectively gathers these pieces, simplifying the management of identity data for users and serving as a single wallet for all applications. This approach may not only enhance user experience but also reduce the risk of vendor lock-in in electronic markets.

### Verifiers

SSI offers verifiers reliable, efficient, and data-minimized information about holders, enhancing trust and reducing costs in the verification process.

**Verifiability** Self-attested identity data, such as information provided through contact forms, often carries significant risks related to fraud and poor data quality. Traditional remote identity verification methods, on the other hand, involve substantial paperwork, manual checks that can be unreliable, and the storage of sensitive user information, leading to considerable costs and inefficiencies (Sedlmeir et al., 2021; Lacity & Carmel, 2022). Consequently, stakeholders in electronic markets frequently face a dilemma: either they need to rely on unverified data, which can cause numerous issues in business processes, or they need to invest in expensive (third-party) identity verification services, like video identification. To address these challenges, SSI offers a compelling value proposition by fostering an open ecosystem built on trust relationships between issuers and verifiers (Mühle et al., 2018), as depicted in Fig. 1. This ecosystem facilitates the widespread use of verifiable credentials, which are crucial for ensuring the authenticity of the data's source and the integrity of the data itself. By leveraging these machine-verifiable credentials, SSI enhances the verifiability of identity information, confirming both its genuineness and its consistency over time. Moreover, by adopting an open-access model, SSI strategically reduces financial barriers for verifiers, particularly by minimizing the high upfront costs associated with identity verification during onboarding processes. This approach not only improves the efficiency of verification but also supports the broader goal of encouraging widespread user adoption (Schlatt et al., 2022a). Through this model, verifiers can be confident in the authenticity and integrity of the data they receive, reducing the risks associated with relying on unverified information.

In this framework, verifiability means being able to confirm the integrity of the content and the authenticity of both the issuer and presenter of a verifiable credential. Additionally, validity checks—including expiration and revocation—are necessary (Sedlmeir et al., 2021; Preukschat & Reed, 2021). Typically, verifiable credentials come with a digital signature ensuring integrity and authenticity. Verifiable data registries facilitate a secure cryptographic link between the issuer's public key, used as a pseudonym, and the actual entity, potentially including information beyond the domain name included in traditional digital certificates improving authenticity. For instance, organizations in the EU can obtain specific extended validation certificates—called Qualified Website Authentication Certificates (QWACs)—that include their registration number in the commercial register and are anchored in European legislation (Martius et al., 2024).

Verifiable data registries can also help make it easier for verifiers to decide which issuers to trust in a growing identity ecosystem. Many SSI initiatives adopt decentralized verifiable data registries to reduce reliance on any single authority. Initial efforts to create a universal registry led to using DLT for its neutral platform capabilities (Mühle et al., 2018; Koens & Meijer, 2018). However, as decentralization can also come from an ecosystem of various verifiable data registries, the focus on this technology might decrease in the future.

**Cost reduction** SSI can significantly reduce costs for verifiers by streamlining identity verification processes. By leveraging machine-verifiable attestations, it eliminates the need for manual checks and the handling of extensive paperwork (Bernabe et al., 2020; Lacity & Carmel, 2022). This approach not only speeds up the verification process but also avoids human errors and reduces the resources required for these tasks (Abid et al., 2022; Feulner et al., 2022). Furthermore, SSI introduces an efficient way to manage and verify identities across different domains through a unified approach to corresponding protocols. This uniformity in processing reduces the technological and operational complexity, leading to lower operational costs. Additionally, the trust inherent in SSI reduces the risk of fraud, further decreasing potential costs associated with security breaches and data inaccuracies (Sedlmeir et al., 2021). Overall, SSI proposes to offer a cost-effective solution for verifiers by automating and securing the identity verification process (Guggenberger et al., 2023b).

**Compliance** At the core of SSI is the principle of data control, which is one of its key value propositions. Consequently, SSI is inherently aligned with data protection laws (Weigl et al., 2023). By adopting SSI, verifiers can more easily adhere to these regulations, as they can minimize the amount of information they process (Ra et al., 2021). This reduction in data handling lowers the risk of non-compliance penalties and helps protect their reputation. Implementing SSI solutions embodies a privacy-by-design approach, significantly reducing risks associated with data management (Čučko et al., 2022a).

## SSI in electronic markets

Despite significant conceptual and practical progress in SSI (Brands, 2000; Backes et al., 2005; Satybaldy et al., 2024; Sedlmeir et al., 2021) and its anticipated future role following the revision of the European eIDAS regulation (European Commission, 2023a), its practical adoption to date still remains limited. It is crucial for research to not only advance the theoretical framework but also to provide practical guid-

ance that underscores the unique value propositions of SSI for stakeholders in real-world applications.

While numerous private and government-supported initiatives have embarked on SSI projects across various sectors, efforts to integrate these projects into broader system landscapes are still in their infancy. Legacy systems based on conventional digital certificates, despite their limitations in scaling digital identity, remain relevant in research and practical web security applications (Sedlmeir et al., 2022a). SSI, along with its core technical components, will rarely operate in isolation; rather, it will complement existing IT solutions, such as identity and access management protocols, eID smart cards, and X.509 certificates (Kuperberg & Klemens, 2022; Delignat-Lavaud et al., 2016; Babel & Sedlmeir, 2023). For SSI solutions to be competitive, they must align with regulatory standards and meet the demands of enterprise software (Bochnia et al., 2023).

The fluctuating technology hype surrounding SSI, reminiscent of and connected to blockchain technology (Sedlmeir et al., 2022a; Hoess et al., 2023), serves as a lesson for practitioners to critically assess the opportunities and challenges of new paradigms and tailor them to specific use cases (Satybaldy et al., 2024). While the integration of SSI into digital identity solutions is essential for digital innovation and transformation, it does not automatically solve all security and disclosure control-related concerns (Sedlmeir et al., 2022b). However, with proper design, it can significantly enhance the efficiency and control of verifiable data disclosure. This shift also facilitates the examination of technology interactions and the identification of potential weaknesses within SSI, such as ongoing challenges related to user support and the economic costs associated with wallet-based, non-proprietary IdM systems (Anderson, 2011). Moreover, any emerging system must comply with legal constraints, such as level of assurance (LoA) requirements posed by eIDAS, and meet safeguards that established systems already address through maturity.

Related work identifies several challenges that SSI is currently facing and must overcome to achieve large-scale adoption. Key technical issues include the standardization of protocols and cryptographic building blocks such as credential formats, issuance and presentation protocols, and privacy-enhancing technologies like ZKP (Laatikainen et al., 2021; Čučko et al., 2022b; Yildiz et al., 2023; Babel & Sedlmeir, 2023). Additionally, bringing mobile phone manufacturers into the fold is essential to leverage modern devices' NFC interfaces and hardware for secure key management. On the organizational side, challenges include ensuring a fair distribution of economic incentives, which currently seem to favor relying parties and disadvantage issuers (Lacity & Carmel, 2022), as well as establishing governance frameworks for trusted lists of relying parties entitled to request identity attributes from digital wallets. Another significant hurdle is crossing the chasm toward a regime where strong network effects drive the widespread adoption of digital wallets (Schlatt et al., 2022a). Consequently, future research could focus on developing methods to quantify cost reductions by categorizing use cases, analyzing verification requirements, and assessing the potential savings across different scenarios. Furthermore, related research indicates that improving user experience is critical for successful adoption (Sartor et al., 2022; Guggenberger et al., 2023a). Finally, an important avenue for future research is to explore where, when, and how SSI will fundamentally transform business processes across various industries, marking a significant step in the ongoing evolution of digital identity management.

In electronic markets, the interplay of socio-technical factors is crucial in redefining trust and transactional relationships. SSI offers stakeholders unparalleled control over the verifiable disclosure of digital identity data, facilitating secure, private, and efficient participation in electronic interactions. This paradigm shift reallocates trust from centralized authorities to decentralized networks and cryptographic safeguards. Furthermore, SSI introduces socio-economic shifts, potentially redistributing power between users and SSO service providers to reduce the lock-in effects of big tech companies and level the playing field for smaller service providers in the digital market (Rieger et al., 2022). Yet, this transformation is not without challenges, as concerns related to usability, interoperability, and data minimization remain. Overcoming these hurdles requires collaborative efforts among technologists, social scientists, policymakers, and industry leaders to align SSI implementations with societal norms, legal standards, and user expectations. A thorough understanding of SSI's socio-technical aspects is vital for building trust, ensuring transparency, and promoting inclusivity in digital commerce ecosystems.

## Conclusion

This article lays the foundation for understanding SSI from an organizational perspective by merging insights from both academic research and practical applications. We highlight the core value propositions SSI offers to its key stakeholders—issuers, holders, and verifiers—through its fundamental components: verifiable credentials, digital wallets, and verifiable data registries. This perspective underscores SSI's current capabilities and its significance for networked businesses, positioning it as a cornerstone for the evolution of digital identity management systems.

Ultimately, this article presents the SSI paradigm as a promising concept in today's complex field of IdM systems. It argues that SSI can provide stakeholders with a higher degree of control and effective use of their (verifiable) iden-

tity data, thereby improving on previous trade-offs inherent in fragmented account management and SSO services.

**Supplementary Information** The online version contains supplementary material available at https://doi.org/10.1007/s12525-025-00772-0.

**Funding** Open Access funding enabled and organized by Projekt DEAL. We gratefully acknowledge the financial support of the project "ID-Ideal" (Grant-Number: 01MN21001l) by the Federal Ministry for Economic Affairs and Climate Action (BMWK) and the project supervision by the project management organization DLR.
We gratefully acknowledge the support and cooperation of the Future Energy Lab of the German Energy Agency within the "BMIL" and "DIVE" project.
We gratefully acknowledge the Bavarian State Ministry of Digital Affairs and the Bavarian State Taxation Office for their support of the project "SSI@LfSt."
We gratefully acknowledge the Bavarian Ministry of Economic Affairs, Regional Development and Energy for their support of the project "Fraunhofer Blockchain Center (20-3066-2-6-14)."
We gratefully acknowledge the Luxembourg National Research Fund (FNR) in the "PABLO" (grant reference 16326754) project and Luxembourg's Ministry for Digitalisation.

## Declarations

**Conflict of interest** The authors declare no competing interests.



## References

Abid, A., Cheikhrouhou, S., Kallel, S., & Jmaiel, M. (2022). NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. *Software: Practice and Experience, 52*(4), 841–867. https://doi.org/10.1002/spe.2983

Abraham, A., Koch, K., More, S., Ramacher, S., & Stopar, M. (2021). Privacy-preserving eID derivation to self-sovereign identity systems with offline revocation. In *Ieee 20th international conference on trust, security and privacy in computing and communications* (pp. 506–513). https://doi.org/10.1109/TrustCom53373.2021.00080

Abraham, A., More, S., Rabensteiner, C., & Hörandner, F. (2020). Revocable and offline-verifiable self-sovereign identities. In *Ieee 19th international conference on trust, security and privacy in computing and communications* (pp. 1020–1027). https://doi.org/10.1109/TrustCom50675.2020.00136

Allen, C. (2016). The path to self-sovereign identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

Anderson, R. (2011). Can we fix the security economics of federated authentication? In *Proceedings of the 19th international workshop on security protocols* (pp. 25–32). https://doi.org/10.1007/978-3-642-25867-1_4

Babel, M., & Sedlmeir, J. (2023). *Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs*. https://arxiv.org/abs/2301.00823

Babel, M., Gramlich, V., Körner, M.-F., Sedlmeir, J., Strüker, J., & Zwede, T. (2022). Enabling end-to-end digital carbon emission tracing with shielded NFTs. *Energy Informatics, 5*(1)https://doi.org/10.1186/s42162-022-00199-3

Backes, M., Camenisch, J., & Sommer, D. (2005). Anonymous yet accountable access control. In *Proceedings of the workshop on privacy in the electronic society* (pp. 40–46). https://doi.org/10.1145/1102199.1102208

Bartolomeu, P. C., Vieira, E., Hosseini, S. M., & Ferreira, J. (2019). Self-sovereign identity: Use-cases, technologies, and challenges for industrial IoT. In *24th ieee international conference on emerging technologies and factory automation* (pp. 1173–1180). https://doi.org/10.1109/ETFA.2019.8869262

Baum, C., Jadoul, R., Orsini, E., Scholl, P., & Smart, N. P. (2022). Feta: Efficient threshold designated-verifier zero-knowledge proofs. In *Proceedings of the 2022 acm sigsac conference on computer and communications security*. https://doi.org/10.1145/3548606.3559354

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems, 19*, 1020–1034. https://doi.org/10.17705/1jais.00518

Bernabe, J. B., David, M., Moreno, R. T., Cordero, J. P., Bahloul, S., & Skarmeta, A. (2020). Aries: Evaluation of a reliable and privacy-preserving European identity management framework. *Future Generation Computer Systems, 102*, 409–425. https://doi.org/10.1016/j.future.2019.08.017

Bochnia, R., Richter, D., & Anke, J. (2023). Self-sovereign identity for organizations: Requirements for enterprise software. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3349095

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Ieee symposium on security and privacy* (pp. 553–567). https://doi.org/10.1109/SP.2012.44

Bosworth, K., Lee, M. G., Jaweed, S., & Wright, T. (2005). Entities, identities, identifiers and credentials - What does it all mean? *BT Technology Journal, 23*, 25–36. https://doi.org/10.1007/s10550-006-0004-2

Brands, S. (2000). *Rethinking public key infrastructures and digital certificates: Building in privacy*. MIT Press.

Braud, A., Fromentoux, G., Radier, B., & Grand, O. L. (2021). The road to European digital sovereignty with Gaia-X and IDSA. *IEEE Network, 35*(2), 4–5. https://doi.org/10.1109/MNET.2021.9387709

Camenisch, J., & Lysyanskaya, A. (2002). A signature scheme with efficient protocols. In *International conference on security in communication networks* (pp. 268–289). Springer. https://doi.org/10.1007/3-540-36413-7_20

Camenisch, J., & Lysyanskaya, A. (2004). Signature schemes and anonymous credentials from bilinear maps. In *Annual international cryptology conference* (pp. 56–72). Springerhttps://doi.org/10.1007/978-3-540-28628-8_4

Cameron, K. (2005). The laws of identity. http://myinstantid.com/laws.pdf

Cho, K. W., Jeong, B.-G., & Shin, S. U. (2021). Verifiable credential proof generation and verification model for decentralized SSI-

based credit scoring data. *IEICE Transactions on Information and Systems, E104.D*(11), 1857–1868https://doi.org/10.1587/transinf.2021NGP0006

Cocco, L., Tonelli, R., & Marchesi, M. (2021). Blockchain and self sovereign identity to support quality in the food supply chain. *Future Internet, 13*(12). https://doi.org/10.3390/fi13120301

Codagnone, C., & Weigl, L. (2023). Leading the charge on digital regulation: The more, the better, or policy bubble? *Digital Society, 2*(1), 4. https://doi.org/10.1007/s44206-023-00033-7

Council of the European Union. (2023). *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity - General approach*. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/DV/2023/02-09/05_CA_eIDAS_EN.pdf

Čučko, Š, Bećirović, Š, Kamišalić, A., Mrdović, S., & Turkanović, M. (2022). Towards the classification of self-sovereign identity properties. *IEEE Access, 10*, 88306–88329. https://doi.org/10.1109/ACCESS.2022.3199414

Čučko, Š, Bećirović, Š, Kamišalić, A., Mrdović, S., & Turkanović, M. (2022). Towards the classification of self-sovereign identity properties. *IEEE access, 10*, 88306–88329. https://doi.org/10.1109/ACCESS.2022.3199414

Čučko, Š, & Turkanović, M. (2021). Decentralized and self-sovereign identity: Systematic mapping study. *IEEE Access, 9*, 139009–139027. https://doi.org/10.1109/ACCESS.2021.3117588

Davie, M., Gisolfi, D., Hardman, D., Jordan, J., O'Donnell, D., & Reed, D. (2019). The trust over IP stack. *IEEE Communications Standards Magazine, 3*(4), 46–51. https://doi.org/10.1109/MCOMSTD.001.1900029

Degen, K., & Teubner, T. (2024). Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. *Electronic Markets, 34*, 50. https://doi.org/10.1007/s12525-024-00731-1

Delignat-Lavaud, A., Fournet, C., Kohlweiss, M., & Parno, B. (2016). Cinderella: Turning shabby x.509 certificates into elegant anonymous credentials with the magic of verifiable computation. *IEEE Symposium on Security and Privacy,* 235–254. https://doi.org/10.1109/SP.2016.22

Drăgnoiu, A.-E. (2021). Using blockchain technology for software identity maintenance. In *Proceedings of the 22nd international middleware conference: Doctoral symposium* (pp. 25-28). https://doi.org/10.1145/3491087.3493682

Dubé, L., & Paré, G. (2003). Rigor in information systems positivist case research: Current practices, trends, and recommendations. *MIS Quarterly, 27*(4), 597–636. https://doi.org/10.2307/30036550

Ehrlich, T., Richter, D., Meisel, M., & Anke, J. (2021). Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. *HMD Praxis der Wirtschaftsinformatik, 58*(2), 247–270. https://doi.org/10.1365/s40702-021-00711-5

Ernstberger, J., Lauinger, J., Elsheimy, F., Zhou, L., Steinhorst, S., Canetti, R., ... Song, D. (2023). SoK: Data sovereignty. In *8th european symposium on security and privacy* (pp. 122–143). IEEE. https://doi.org/10.1109/EuroSP57164.2023.00017

European Commission (2023a). *Regulation of the European Parliament and ofthe Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/DV/2023/02-09/05_CA_eIDAS_EN.pdf

European Commission. (2023b). *The common union toolbox for a coordinated approach towards a European digital identity framework*. https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

Fedrecheski, G., Rabaey, J. M., Costa, L. C. P., Calcina Ccori, P. C., Pereira, W. T., & Zuffo, M. K. (2020). Self-sovereign identity for IoT environments: A perspective. *In Global internet of things summit*. https://doi.org/10.1109/GIOTS49054.2020.9119664

Feulner, S., Sedlmeir, J., Schlatt, V., & Urbach, N. (2022). Exploring the use of self-sovereign identity for event ticketing systems. *Electronic Markets, 32*(3), 1759–1777. https://doi.org/10.1007/s12525-022-00573-9

Fotopoulos, F., Malamas, V., Dasaklis, T. K., Kotzanikolaou, P., & Douligeris, C. (2020). A blockchain-enabled architecture for IoMT device authentication. In *Ieee eurasia conference on iot, communication and engineering* (Vol. 32, pp. 1759–1777). https://doi.org/10.1109/ECICE50847.2020.9301913

Franz, A., & Benlian, A. (2022). Exploring interdependent privacy - Empirical insights into users' protection of others' privacy on online platforms. *Electronic Markets, 32*(4), 2293–2309. https://doi.org/10.1007/s12525-022-00566-8

German Federal Office for Information Security. (2019). *Technical guideline TR-03159 mobile identities*. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03159/TR-03159-1.pdf?_blob=publicationFile&v=1

Ghaffari, F., Gilani, K., Bertin, E., & Crespi, N. (2022). Identity and access management using distributed ledger technology: A survey. *International Journal of Network Management, 32*(2). https://doi.org/10.1002/nem.2180

Gimpel, H., Kleindienst, D., & Waldmann, D. (2018). The disclosure of private data: Measuring the privacy paradox in digital services. *Electronic Markets, 28*(4), 475–490. https://doi.org/10.1007/s12525-018-0303-8

Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2023). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Business & Information Systems Engineering*. https://doi.org/10.1007/s12599-023-00830-x

Grindal, K., Mueller, M., & Srivastava, V. (2024). Non-governmental governance of trust on the Internet: WebPKI as public good. In *Workshop on the Economics of Information Security*. https://bpb-us-e2.wpmucdn.com/sites.utdallas.edu/dist/e/1380/files/2024/03/Grindal-et-al-WEIS-2024-0836cad1909f1424.pdf

Guggenberger, T., Neubauer, L., Stramm, J., Völter, F., & Zwede, T. (2023b). Accept me as I am or see me go: A qualitative analysis of user acceptance of self-sovereign identity applications. In *Proceedings of the 56th hawaii international conference on system sciences* (pp. 6560–6569). https://scholarspace.manoa.hawaii.edu/items/5c28d83b-fa5d-4357-add8-ea3f2afca398

Guggenberger, T., Kühne, D., Schlatt, V., & Urbach, N. (2023). Designing a cross-organizational identity management system: Utilizing SSI for the certification of retailer attributes. *Electronic Markets, 33*, 3. https://doi.org/10.1007/s12525-023-00620-z

Hardt, D. (2012). *The OAuth 2.0 authorization framework*. https://www.rfc-editor.org/info/rfc6749

Hermes, S., Kaufmann-Ludwig, J., & Schreieck, M. (2020). A taxonomy of platform envelopment: Revealing patterns and particularities. *Proceedings of the 26th americas conference on information systems*. https://aisel.aisnet.org/amcis2020/strategic_uses_it/strategic_uses_it/17

Hoess, A., Lautenschlager, J., Sedlmeir, J., Fridgen, G., Schlatt, V., & Urbach, N. (2024). Toward seamless mobility-as-a-service: Providing multimodal mobility through digital wallets. *Business & Information Systems Engineering*. https://doi.org/10.1007/s12599-024-00856-9

Hoess, A., Rieger, A., Roth, T., Fridgen, G., & Young, A. G. (2023). Managing fashionable organizing visions: Evidence from the European blockchain services infrastructure. *Proceedings of the 44th international conference on information systems*. AIS. https://aisel.aisnet.org/ecis2023_rp/337

Hoess, A., Roth, T., Sedlmeir, J., Fridgen, G., & Rieger, A. (2022). With or without blockchain? Towards a decentralized, SSI-based

eRoaming architecture. In *Proceedings of the 55th hawaii international conference on system sciences* (pp. 4621–4630). https://doi.org/10.24251/HICSS.2022.562

Jöhnk, J., Albrecht, T., Arnold, L., Guggenberger, T. M., Lämmermann, L., Schweizer, A., & Urbach, N. (2021). The rise of the machines: Conceptualizing the machine economy. *Proceedings of the 25th pacific asia conference on information systems*. https://aisel.aisnet.org/pacis2021/54

Jørgensen, K. P., & Beck, R. (2022). Universal wallets. *Business & Information Systems Engineering, 64*(1), 115–125. https://doi.org/10.1007/s12599-021-00736-6

Jøsang, A., & Pope, S. (2005). User centric identity management. In *Auscert asia pacific information technology security conference* (Vol. 22, p. 2005). Citeseer.

Jøsang, A., Rosenberger, C., Miralabé, L., Klevjer, H., Varmedal, K. A., Daveau, J., ... Taugbøl, P. (2015). Local user-centric identity management. *Journal of Trust Management, 2*(1). https://doi.org/10.1186/s40493-014-0009-6

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University, 33*(2004), 1–26.

Koens, T., & Meijer, S. (2018). *Matching identity management solutions to self-sovereign identity principles*. https://www.slideshare.net/TommyKoens/matching-identity-managementsolutions-to-selfsovereign-identity-principles/1

Körner, M.-F., Sedlmeir, J., Weibelzahl, M., Fridgen, G., Heine, M., & Neumann, C. (2022). Systemic risks in electricity systems: A perspective on the potential of digital technologies. *Energy Policy, 164*, 112901. https://doi.org/10.1016/j.enpol.2022.112901

Kulabukhova, N., Ivashchenko, A., Tipikin, I., & Minin, I. (2019). Selfsovereign identity for IoT devices. In *International conference on computational science and its applications* (pp. 472–484). Springer. https://doi.org/10.1007/978-3-030-24296-1_37

Kuperberg, M., & Klemens, R. (2022). Integration of self-sovereign identity into conventional software using established IAM protocols: A survey. In *Open identity summit*https://doi.org/10.18420/OID2022_04

Laatikainen, G., Kolehmainen, T., & Abrahamsson, P. (2021). Self-sovereign identity ecosystems: Benefits and challenges. *Proceedings of the 12th scandinavian conference on information systems*. Association for Information Systems. https://aisel.aisnet.org/scis2021/10

Lacity, M., & Carmel, E. (2022). Self-sovereign identity and verifiable credentials in your digital wallet. *MIS Quarterly Executive, 21*(3). https://aisel.aisnet.org/misqe/vol21/iss3/6

Liu, Y., Lu, Q., Paik, H.-Y., Xu, X., Chen, S., & Zhu, L. (2020). Design pattern as a service for blockchain-based self-sovereign identity. *IEEE Software, 37*(5), 30–36. https://doi.org/10.1109/MS.2020.2992783

Looker, T., Kalos, V., Whitehead, A., & Lodder, M. (2022). *The BBS signature scheme*. https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html

Maler, E., & Reed, D. (2008). The Venn of identity: Options and issues in federated identity management. *IEEE Security & Privacy Magazine, 6*(2), 16–23. https://doi.org/10.1109/MSP.2008.50

Martinez Jurado, V., Vila, X., Kubach, M., Jeyakumar, Henderson Johnson, & I., Solana, A., & Marangoni, M. (2021). Applying assurance levels when issuing and verifying credentials using trust frameworks. *Open identity summit 2021* (pp. 167–178). Gesellschaft für Informatik e.V: Bonn.

Martius, K., Hühnlein, T., Hühnlein, D., & Wich, T. (2024). Trustworthy QWACs – fact or fiction? In *Open identity summit* (pp. 189–194). https://doi.org/10.18420/OID2024_18

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review, 30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Naik, N., & Jenkins, P. (2020a). Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology. In *8th ieee international conference on mobile cloud computing, services, and engineering* (pp. 90–95). IEEE. https://doi.org/10.1109/MobileCloud48802.2020.00021

Naik, N., & Jenkins, P. (2020b). Your identity is yours: Take back control of your identity using GDPR compatible self-sovereign identity. In *7th international conference on behavioural and social computing*. https://doi.org/10.1109/BESC51023.2020.9348298

Neuman, B., & Ts'o, T. (1994). Kerberos: an authentication service for computer networks. *IEEE Communications Magazine, 32*(9), 33–38. https://doi.org/10.1109/35.312841

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Novakouski, M. (2013). User-centric identity management: A future vision for IdM. *CrossTalk: The Journal of Defense Software Engineering, 26*, 21–26.

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

Pfitzmann, A., & Hansen, M. (2010). *A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management*. Dresden, Germany. http://www.maroki.de/pub/dphistory/2010_Anon_Terminology_v0.34.pdf

Pöhn, D., Grabatin, M., & Hommel, W. (2021). Eid and self-sovereign identity usage: An overview. *Electronics, 10*(22), 2811. https://doi.org/10.3390/electronics10222811

Preukschat, A., & Reed, D. (2021). *Self-sovereign identity: Decentralized digital identity and verifiable credentials*. Shelter Island: Manning.

Ra, G., Kim, T., & Lee, I. (2021). Vaim: verifiable anonymous identity management for human-centric security and privacy in the internet of things. *IEEE Access, 9*, 75945–75960. https://doi.org/10.1109/ACCESS.2021.3080329

Rieger, A., Roth, T., Sedlmeir, J., & Fridgen, G. (2021). The privacy challenge in the race for digital vaccination certificates. *Med, 2*(6), 633–634. https://doi.org/10.1016/j.medj.2021.04.018

Rieger, A., Roth, T., Sedlmeir, J., Fridgen, G., & Young, A. G. (2024). Organizational identity management policies. *Journal of the Association for Information Systems, 25*, 522–527. https://doi.org/10.17705/1jais.00887

Rieger, A., Roth, T., Sedlmeir, J., Weigl, L., & Fridgen, G. (2022). Not yet another digital identity. *Nature Human Behaviour, 6*, 3–3. https://doi.org/10.1038/s41562-021-01243-0

Sakimura, N., Bradley, J., Jones, M., De Medeiros, B., & Mortimore, C. (2014). OpenID connect core 1.0. *The OpenID Foundation*.

Sartor, S., Sedlmeir, J., Rieger, A., & Roth, T. (2022). Love at first sight? A user experience study of self-sovereign identity wallets. In *Proceedings of the 30th european conference on information systems*. https://aisel.aisnet.org/ecis2022_rp/46

Satybaldy, A., Ferdous, M. S., & Nowostawski, M. (2024). A taxonomy of challenges for self-sovereign identity systems. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3357940

Schlatt, V., Sedlmeir, J., Traue, J., & Völter, F. (2022). *Harmonizing sensitive data exchange and double-spending prevention through blockchain and digital wallets: The case of e-prescription management*. Distributed Ledger Technologies: Research and Practice. https://doi.org/10.1145/3571509

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2022). Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. *Information & Management, 59*, 103553. https://doi.org/10.1016/j.im.2021.103553

Schmidt, K., Mühle, A., Grüner, A., & Meinel, C. (2021). Clear the fog: Towards a taxonomy of self-sovereign identity ecosystem members. In *18th international conference on privacy, security and trust*. IEEE. https://doi.org/10.1109/PST52912.2021.9647797

Schwalm, S., Albrecht, D., & Alamillo, I. (2022). eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI. In *Open identity summit*. https://doi.org/10.18420/OID2022_05

Schweizer, A., Knoll, P., Urbach, N., von der Gracht, H. A., & Hardjono, T. (2020). To what extent will blockchain drive the machine economy? Perspectives from a prospective study. *IEEE Transactions on Engineering Management, 67*(4), 1169–1183. https://doi.org/10.1109/TEM.2020.2979286

Sedlmeir, J., Huber, J., Barbereau, T. J., Weigl, L., & Roth, T. (2022a). Transition pathways towards design principles of self-sovereign identity. *Proceedings of the 43rd international conference on information systems*. Copenhagen. https://aisel.aisnet.org/icis2022/is_implement/is_implement/4

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets, 32*(3), 1779–1794. https://doi.org/10.1007/s12525-022-00536-0

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering, 63*(5), 603–613. https://doi.org/10.1007/s12599-021-00722-y

Shuaib, M., Alam, S., Nasir, M. S., & Alam, M. S. (2021). Immunity credentials using self-sovereign identity for combating COVID-19 pandemic. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.03.096

Singh, H. P., Stefanidis, K., & Kirstein, F. (2021). A private key recovery scheme using partial knowledge. In *11th ifip international conference on new technologies, mobility and security* (pp. 1–5). https://doi.org/10.1109/NTMS49979.2021.9432642

Smith, S. S. (2020). *Blockchain, self-sovereign identity, and the future of data privacy*. https://www.forbes.com/sites/seansteinsmith/2020/09/09/blockchain-self-sovereign-identity-and-the-future-of-data-privacy/?sh=183ea31aea7d

Soltani, R., Nguyen, U. T., & An, A. (2019). Practical key recovery model for self-sovereign identity based digital wallets. In *IEEE international conference on dependable, autonomic and secure computing, international conference on pervasive intelligence and computing, international conference on cloud and big data computing, international conference on cyber science and technology congress* (pp. 320–325). https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00066

Soltani, R., Nguyen, U. T., & An, A. (2021). A survey of self-sovereign identity ecosystem. *Security and Communication Networks, 2021*,. https://doi.org/10.1155/2021/8873429

Sporny, M., Longley, D., & Chadwick, D. (2022a). Verifiable Credentials data model v1.1. World Wide Web Consortium (W3C). https://www.w3.org/TR/did-core/

Sporny, M., Longley, D., Sabadello, M., Reed, D., Steele, O., & Allen, C. (2022b). *Decentralized identifiers (DIDs) v1.0 – core architecture, data model, and representations. W3C Recommendation*. https://www.w3.org/TR/did-core/

Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. *Blockchain: Research and Applications, 2*(2), 100014. https://doi.org/10.1016/j.bcra.2021.100014

Teuschel, M., Pöhn, D., Grabatin, M., Dietz, F., Hommel, W., & Alt, F. (2023). 'don't annoy me with privacy decisions!'-Designing privacy-preserving user interfaces for SSI wallets on smartphones. *IEEE Access, 11*, 131814–131835. https://doi.org/10.1109/ACCESS.2023.3334908

Toth, K. C., & Anderson-Priddy, A. (2019). Self-sovereign digital identity: A paradigm shift for identity. *IEEE Security & Privacy, 17*(3), 17–27. https://doi.org/10.1109/msec.2018.2888782

van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. (2019). *Self-sovereign identity solutions: The necessity of blockchain technology*. https://arxiv.org/pdf/1904.12816.pdf

Vapen, A., Carlsson, N., Mahanti, A., & Shahmehri, N. (2016). A look at the third-party identity management landscape. *IEEE Internet Computing, 20*, 18–25. https://doi.org/10.1109/MIC.2016.38

Wang, F., & De Filippi, P. (2020). Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. *Frontiers in Blockchain, 2*,. https://doi.org/10.3389/fbloc.2019.00028

Webster, J., & Watson, R. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), 13–23.

Weigl, L., Barbereau, T. J., Rieger, A., & Fridgen, G. (2022). The social construction of self-sovereign identity: An extended model of interpretive flexibility. *Proceedings of the 55th hawaii international conference on system sciences*. https://scholarspace.manoa.hawaii.edu/items/17d400d6-5230-4fc8-a569-7b30b0ef3e82

Weigl, L., Barbereau, T., & Fridgen, G. (2023). The construction of self-sovereign identity: Extending the interpretive flexibility of technology towards institutions. *Government Information Quarterly, 40*(4), 101873. https://doi.org/10.1016/j.giq.2023.101873

Windley, P. (2020). *The Sovrin SSI stack*. https://www.windley.com/archives/2020/03/the_sovrin_ssi_stack.shtml

Yildiz, H., Küpper, A., Thatmann, D., Göndör, S., & Herbke, P. (2023). Towards interoperable self-sovereign identities. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3313723

Yin, R. (2014). *Case study research: Design and methods* (5th ed). Sage Publications.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*, 75–89. https://doi.org/10.1057/jit.2015.5

## Authors and Affiliations

**Matthias Babel[1] · Lukas Willburger[2] · Jonathan Lautenschlager[1] · Fabiane Völter[3] · Tobias Guggenberger[3] · Marc-Fabian Körner[3] · Johannes Sedlmeir[4] · Jens Strüker[3] · Nils Urbach[5]**

✉ Matthias Babel
matthias.babel@fit.fraunhofer.de

Lukas Willburger
lukas.willburger@fit.fraunhofer.de

Jonathan Lautenschlager
jonathan.lautenschlager@fit.fraunhofer.de

Fabiane Völter
fabiane.voelter@fim-rc.de

Tobias Guggenberger
tobias.guggenberger@fim-rc.de

Marc-Fabian Körner
marc.koerner@fim-rc.de

Johannes Sedlmeir
johannes.sedlmeir@uni.lu

Jens Strüker
jens.strueker@fim-rc.de

Nils Urbach
nils.urbach@fb3.fra-uas.de

1 Branch Business & Information Systems Engineering of the Fraunhofer FIT, Bayreuth, Germany

2 Branch Business & Information Systems Engineering of the Fraunhofer FIT, Augsburg, Germany

3 FIM Research Center, University of Bayreuth, Bayreuth, Germany

4 Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Esch-sur-Alzette, Luxembourg

5 Frankfurt University of Applied Sciences, Frankfurt, Germany