Electronic Markets (2026) 36:17
https://doi.org/10.1007/s12525-025-00867-8

FUNDAMENTALS

Self-sovereign identity: A conceptual framework and research agenda

Daniel Richter[1] · **Jürgen Anke**[1]

Received: 5 November 2024 / Accepted: 11 December 2025

Abstract
Self-sovereign identity (SSI) is a novel approach to digital identity management, which is controversially discussed in technological communities and academia and lately also in the political space. Positions in the debate range from touting SSI as introducing a paradigm shift in internet identity and user privacy, while others dismiss the concept as libertarian hyperbole. SSI aims to give individuals an independent digital existence and control over their digital identities. Technically, this is achieved by providing individuals with digital identity wallet applications, which allow them to store and present digitally verifiable credentials. Despite its transformative potential, SSI is not comprehensively conceptualized in information system research. Therefore, in this Fundamentals article, we offer the following contributions: First, based on existing information systems research, we provide a consolidated definition and a conceptual framework of SSI structured along five analytic levels: (1) foundational principles, (2) credential exchange, (3) technical building blocks, (4) applications, and (5) governance. Second, we present an information systems research agenda on SSI, including concrete research questions and promising theoretical directions.

Keywords Identity management · Self-sovereign identity · Digital wallets · Verifiable credentials · Data sovereignty · Information systems

JEL Classification L86 · O14 · O33 · D80

Introduction

"On the internet, nobody knows you're a dog."

Amid the digital transformation of society, Peter Steiner's iconic 1993 cartoon resonates to this day, as secure and usable identity management (IDM) has become a fundamental requirement for building trust in today's electronic markets. Before transacting with digital service providers, consumers are typically required to create user accounts, which involve identity checks and proving other characteristics relevant to the business relationship. To minimize onboarding costs and offer a streamlined customer experience, service providers often allow their customers to reuse existing digital identities registered with large platform providers. However, this widely used practice—a form of so-called federated IDM—exhibits several weaknesses. For service providers, it increases platform lock-in, creating a strategic dependency for customer relationship management. More critically for individuals, the centralization of large amounts of data with platform providers also increases the risk of data breaches, leading to the misuse of personal information and diminishing personal welfare (Bachura et al., 2022; Pang & Vance, 2025). The traditional alternative is that service providers independently employ and secure separate IDM systems, an approach known as fragmented IDM (Rieger et al., 2024). However, this approach is costly and complex, especially in implementing multi-organizational digital services, requiring the definition of dedicated interfaces between stakeholders (Smith & McKeen, 2011). Also, it raises as many questions about data sovereignty for consumers: Users of federated and fragmented IDM systems are dependent on

Responsible Editor: Maximilian Schreieck

✉ Daniel Richter
daniel.richter@htw-dresden.de

Jürgen Anke
juergen.anke@htw-dresden.de

[1] Digital Service Systems Group, Faculty of Computer Science/Mathematics, HTW Dresden, Friedrich-List-Platz 1, 01069 Dresden, Germany

third parties to manage and provide proof of their personal information, with inherent limits on consent and control (Bazarhanova & Smolander, 2020).

A growing dissatisfaction with this status quo led to the development of *self-sovereign identity* (SSI) and, ultimately, to a paradigm shift in IDM. The term SSI was first publicly explicated in a seminal blog post by Allen (2016), wherein he proposes ten principles as a foundation for the development of IDM systems, which "ensure the user control that's at the heart of self-sovereign identity." An overview of these foundational principles is given in Table 1. The basic premise of SSI is that users must have a digital *existence* independent from the digital services and systems they interact with. Consequently, they must be able to exert *control* over their digital identities and the exchange of attributes, so that disclosure is *minimized*. *Portability* and *interoperability* of digital identities across service contexts ensure a loosely-coupled architecture. These principles stand in stark contrast to contemporary IDM approaches and motivated the development of many concurrent novel technologies in the realization of Allen's principles (Kuperberg, 2019).

Resulting from these development efforts, electronic business applications of *digital identity wallets* for managing and sharing personal data are among the most discussed topics in recent information systems (IS) research. Exemplary application areas explored in IS journal articles include mobility-as-a-service (Hoess et al., 2024), taxation (Guggenberger et al., 2023), event ticketing (Feulner et al., 2022), and know-your-customer procedures (Schlatt et al., 2021). A recent Electronic Markets Fundamentals article by Babel et al. (2025) consolidates this application-oriented research by introducing a comprehensive overview of SSI's value propositions. These include improved data control and usability for wallet holders as well as more efficient and compliant data processing on the side of organizations (Babel et al., 2025).

Table 1 Original principles of self-sovereign identity proposed by Allen (2016)

Principle	Short description
Existence	Users must have an independent existence.
Control	Users must control their identities.
Access	Users must have access to their own data.
Transparency	Systems and algorithms must be transparent.
Persistence	Identities must be long-lived.
Portability	Information and services about identity must be transportable.
Interoperability	Identities should be as widely usable as possible.
Consent	Users must agree to the use of their identity.
Minimalization	Disclosure of claims must be minimized.
Protection	The rights of users must be protected.

While the potential benefits of applying SSI in practice are well understood, several challenges impede its adoption. One of these impediments is the conceptual ambiguity surrounding SSI, which is reflected in the diverse definitions proposed by IS scholars: SSI is seen as, e.g., "a decentralized and automated approach for issuing, holding and verifying credentials" (Lacity & Carmel, 2022, p. 1), "an artifact" (Weigl et al., 2023, p. 2), "a new paradigm […] for end-users' digital identity management" (Feulner et al., 2022, p. 1760), and "a design philosophy" (Kim & Kokuryo, 2024, p. 5). IS scholars such as Laatikainen et al. (2021a) and Weigl et al. (2023) consider such conceptual diversity an inhibitor in implementation projects and a hindrance to furthering precise inquiry on SSI and its partial aspects. Besides applications, this encompasses ethical and design principles (Kim & Kokuryo, 2024; Sedlmeir et al., 2022a), organizational requirements (Bochnia et al., 2024; Glöckler et al., 2023; Rieger et al., 2024; Sedlmeir et al., 2022b), and governance mechanisms (Amard et al., 2024; Degen & Teubner, 2024; Kölbel et al., 2022; Richter et al., 2023).

We argue that the SSI value propositions by Babel et al. (2025) can only be realized in electronic markets if IS research contributes to an understanding of how these different aspects of SSI interrelate. Therefore, in this Fundamentals article, we answer the call by Babel et al. (2025) for a unified and comprehensive IS conceptualization of SSI. To serve as a common foundation for our argument in this article, we introduce basic IDM terminology in the "Basic terminology" section. Then, based on an analysis of the definitions and themes in the available IS literature on SSI, we provide two main contributions: First, in the "Conceptualizing self-sovereign identity" section, we introduce *a consolidated definition and conceptual framework of SSI*, explain the rationale behind its structure, and discuss its relationship to existing contributions from IS literature. Second, based on this discussion, we introduce an *IS research agenda*, including research questions and theoretical avenues in the "Research opportunities" section. Finally, in the "Summary" section, we conclude this Fundamentals article by reiterating the most important SSI research opportunities in light of our conceptual framework and its application to current trends in practice.

Basic terminology

Discussions of IDM often involve quite technical terms with syntactic similarities but varying meanings. This includes the central concept of *identity*, which features many different dimensions, including psychological, organizational, cultural, and technological. *IDM* consists of organizational and technical processes, which aim to answer three basic questions about users trying to access an online service, which

are (1) Identification: "Who are you?", (2) Authentication: "How do I know it's you?", and (3) Authorization: "What are you allowed to do or see?" (Smith & McKeen, 2011).

During these processes, IDM systems create, store, and use *digital identities*, which are collections of *attributes* that represent a subject, i.e., an individual in the real world (Windley, 2023, p. 9). Attributes may be structured as *claims* stated about a subject, e.g., "Example University claims that Alice has a degree in computer science." Claims are often bundled and represented as *credentials* (Richter et al., 2023). Credentials are defined as documents containing claims and status information, the presentation of which enables their holders to exercise certain powers (Richter et al., 2023; Smith et al., 2020). For example, presenting valid flight tickets at an airport gate enables passengers to board a plane. Credentials can be used in all three IDM processes, i.e., to prove specific attributes, detect recurring users, and decide about authorizations (Clauß & Köhntopp, 2001). Besides attributes, a digital identity is denoted by a contextually unique *identifier*, such as a username, and bound to the subject using authentication factors, such as a password (Anke & Richter, 2023).

Conceptualizing self-sovereign identity

This section answers the simple but fundamental question: "What exactly is self-sovereign identity?" As shown in the introduction, IS research has proposed a variety of definitions, nuancing different partial aspects of the concept. Two aspects in particular are commonly highlighted in conundrum: technical artifacts and user empowerment. SSI is often described as an approach to or a paradigm of IDM in which "a user controls all their data" (Schlatt et al., 2021), leveraging technologies such as digital identity wallets, verifiable credentials, and blockchain. However, the principles guiding the use of these technologies are rarely explicitly spelled out, including "user security, privacy, individual autonomy and self-empowerment" (Giannopoulou & Wang, 2021) and "personal digital sovereignty" (Sedlmeir et al., 2022a). Rather, the focus of many IS research works on SSI is less on the realization of SSI's fundamental principles and more on exploring solutions to business problems with novel technical artifacts. Examples include design-oriented studies on more efficient taxation of online retailers (Guggenberger et al., 2023), gaining market control in event ticketing (Feulner et al., 2022), and enabling coopetitive mobility-as-a-service (Hoess et al., 2024).

As a result, we observe a conceptual conflation of SSI with the technical artifacts, which were developed as tools to realize the SSI principles (Glöckler et al., 2023; Kudra et al., 2025). An instance of this techno-centricity in the conceptualization of SSI is the common reference to the so-called "trust triangle" (Babel et al., 2025; Ehrlich et al., 2021; Lacity & Carmel, 2022), which is an interaction model taken from the technical specification of verifiable credentials, commonly used to implement SSI-enabled applications (Sporny et al., 2022). Similarly, we can observe that SSI is reduced to the application of digital identity wallets (Kudra et al., 2025; Weigl et al., 2023). These technical building blocks are undeniably important in the pursuit of SSI, but neither is their use required by SSI's foundational principles, nor does it guarantee that they will be fulfilled (Álvarez et al., 2025; Doege et al., 2024). However, the SSI principles do prescribe a decoupling of personal information from service providers, which we will introduce as the social mechanism of credential exchange in the corresponding section. Nonetheless, sidelining SSI's fundamental principles for technical architectures creates two problems visible in IS research:

First, an insufficient delineation of the SSI principles and their technical implementation leads to semantic ambiguity. The goal of these principles is to shift the balance of power in personal data processing from organizations to individuals. While there are numerous benefits for organizations to use SSI-related technologies (Babel et al., 2025), there is no *SSI for organizations* per se (cf. Bochnia et al., 2024; Guggenberger et al., 2023; Sedlmeir et al., 2022b). We argue that using SSI-related technologies exclusively for business reasons is not SSI. Such a framing downplays the importance of the principles, which are inherently not applicable to organizations, lacking an independent existence and privacy rights. Further, SSI's inherent focus on benefitting individuals limits adequately identifying the organizational problem space for SSI-related technologies, creating unnecessary theoretical boundaries to other IS research areas, such as data ecosystems (Möller et al., 2024; Schäfer et al., 2023) and organizational data sovereignty (von Scherenberg et al., 2024).

Second, governance becomes subordinate to technical designs. The SSI principles are demands toward the configuration of *both* the technical artifacts *and* the governance of the social structures in which these artifacts are used. After all, how can power peacefully shift to individuals without institutional backing? However, governance, seen as a vital component for SSI adoption, remains underrepresented in IS research, undermining the applicability of socio-technical designs (cf. Feulner et al., 2022; Guggenberger et al., 2023; Hoess et al., 2024; Schlatt et al., 2021).

To allow for a more nuanced discussion of SSI in IS, we propose a consolidated conceptual framework (Fig. 1). The framework unpacks SSI's most important aspects and explains their interrelations. The design of our conceptual framework builds on similar proposals, such as the "Trust Over IP Model" (Huitema et al., 2021) and the "SSI reference model" (Yildiz et al., 2023). We adopt the layered

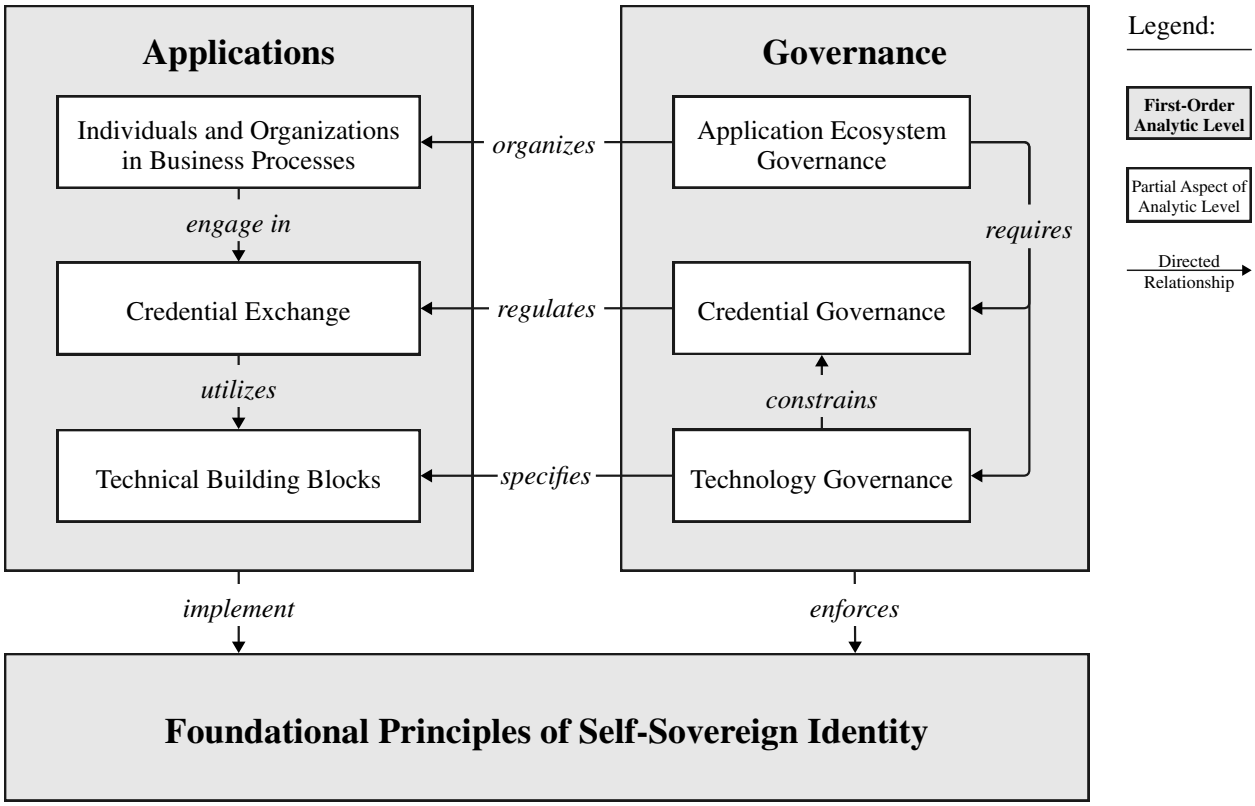

Fig. 1 Conceptual framework for SSI

structure of important SSI concepts common to these proposals, including technology, credential exchange, applications, and governance. However, both frameworks focus primarily on configuring technical building blocks and interoperable architectures. Also, foundational principles are lacking altogether, which is *the* defining normative element of SSI as an approach to IDM. In contrast, our framework is grounded in IS research and offers a more holistic, socio-technical perspective on SSI. Along with the commonly discussed technical building blocks, we elevate SSI's foundational principles and governance to first-order concepts, which enables an explanation of how the principles influence the design of artifacts and how governance is necessary to uphold the principles. Our conceptual framework is structured along these three first-order analytic levels and its partial aspects, represented by grey and white boxes in Fig. 1, respectively. These analytic levels are discussed in the following subsections:

1. *Foundational principles*: At the heart of SSI are its eponymous principles, providing ethical values and ensuring the focus on benefiting individuals in socio-technical designs.
2. *Credential exchange*: Although the principles do not endorse specific technical standards, they prescribe an interaction pattern analogous to the handling of physical documents, known as credential exchange.
3. *Technical building blocks*: These are the various artifacts that were developed following the formulation of SSI's foundational principles and are commonly used to implement SSI-based applications.
4. *Applications*: At this level, we situate the configuration of SSI's technical building blocks to enable organization-to-individual transactions according to the foundational principles.
5. *Governance*: As the adoption of SSI hinges on effective governance mechanisms, we introduce this cross-cutting component into the conceptual framework, enabling and constraining SSI's other partial aspects.

Based on our conceptual framework of SSI, we propose the following definition:

Self-sovereign identity (SSI) is an identity management (IDM) approach based on foundational principles and multi-level governance, ensuring individuals' control over their digital identities. SSI-based applications leverage the credential exchange mechanism implemented by technical building blocks to enable decentralized identity data ecosystems.

Foundational principles

Undeniably, at the foundation of SSI lay its principles, first formulated by Allen (2016). Allen's principles can be seen as a development of the so-called "Laws of Identity" by Cameron (2005), who, in the face of "rapidly proliferating episodes of theft and deception," argued that IDM should prioritize user control and consent. This focus on control aligns with established conceptualizations of data sovereignty (von Scherenberg et al., 2024). In this light, the vision behind the SSI principles can be interpreted as achieving personal data sovereignty for individuals. However, as Abbas et al. (2024) rightfully criticize, control alone is not sufficient to achieve this goal. Rather, a central facet is the protection of data ownership and privacy, which need to be safeguarded by control, security, and compliance (Abbas et al., 2024). These facets are reflected in the principles of *protection*, *access*, and *minimalization* (Allen, 2016).

Taken together, Allen's original principles create a framework for a "21st-century digital identity system" (Allen, 2016), advancing the vision of an "identity layer for the Internet" (Cameron, 2005, p. 2). The fundamental requirement for such an "identity metasystem" (Cameron, 2005, p. 3) is laid out in Allen's first principle of *existence*, necessitating digital identities to be long-lived and managed in strict separation from their usage contexts. To enable this separation, Allen draws on the concept of *claims* as subsets of digital identities, which are to be controlled and shared by users autonomously. Beyond claims, Allen (2016) did not propose a specific implementation approach for IDM systems based on his principles, leading to a wave of technological innovation and standards development.

Following the development of various artifacts claiming to realize the original principles, a discourse on the principles themselves emerged, first in technological niches (Cucko et al., 2022; Ferdous et al., 2019), later also in a socio-political context (Sedlmeir et al., 2022a; Weigl et al., 2023). The ongoing process of technology development and the socio-technical negotiation of values highlights tensions between specific principles, e.g., between the verifiability and reliability of attributes vis-à-vis user expectations such as control and privacy (Sedlmeir et al., 2022a).

The original SSI principles embody libertarian values such as autonomy and privacy (Sedlmeir et al., 2022a). The priority of these values depends greatly on the dominant worldview and political system, wherein the principles are discussed (Sedlmeir et al., 2021; Weigl et al., 2023). In 2024, the European Parliament and the Council of the European Union adopted regulation 2024/1183 as regards establishing the European Digital Identity Framework, also known as eIDAS 2.0 (Regulation 2024/1183). In article 5a, the regulation stipulates the provisioning of digital identity wallets to all individuals in the European Union, putting personal information processing "under the sole control of the user" (Regulation 2024/1183). This is in line with the rights to privacy and individual control over data laid out in the European Declaration on Digital Rights and Principles for the Digital Decade (2022). While at the surface, this allows for SSI-based IDM, data sovereignty is not explicitly mentioned in the regulation at all. Further, the primary design choices in the regulation's normative technical specification, which include static identifiers for individuals, systematically undermine privacy principles (Álvarez et al., 2025).

While pragmatism is necessary to move toward personal data sovereignty, Allen (2025), referencing eIDAS 2.0 and the current geopolitical climate, warned against an "erosion of foundational principles." Concerning the applicability of SSI in societal mainstream, we agree that "updates to its core principles are indispensable" (Sedlmeir et al., 2022a, p. 14), but only to the extent that socio-technical developments advance greater personal data sovereignty for individuals. In this light, we follow Khosrawi-Rad et al. (2025) in their argument for more transparency in the visions pursued in IS research. Because of their impact on technical, political, and academic spheres, we build on Allen's foundational principles in this Fundamentals article on SSI.

Credential exchange

As outlined in the previous section, the original SSI principles heavily draw on the concept of claims and explain the rationale for their handling in a user-centric way (Allen, 2016). By drawing on an analogy from the interaction pattern of IDM in the physical world, the discussion of claims eventually shifted toward the concept of *credentials.* This shift is also reflected in the latest iterations of the SSI principles, such as the *verifiability* and *authenticity* principles proposed by Sedlmeir et al. (2022a), explicitly mentioning credentials rather than claims, unlike, e.g., Allen (2016) and Ferdous et al. (2019).

The mechanism of credential exchange is central to the realization of the SSI principles. To fulfill their function in allowing (or denying) holders to exercise powers at varying times and places, credentials need to be stored in a portable environment with holder control (Smith et al., 2020). Both the existence of credentials and the availability of accessible means to store, carry, and present them enable an interaction model known as the *trust triangle* (Bochnia et al., 2024; Reed et al., 2021, p. 25; Yildiz et al., 2023). The trust triangle depicted in Fig. 2 shows two interactions between three roles, conceptually separated in time and place:

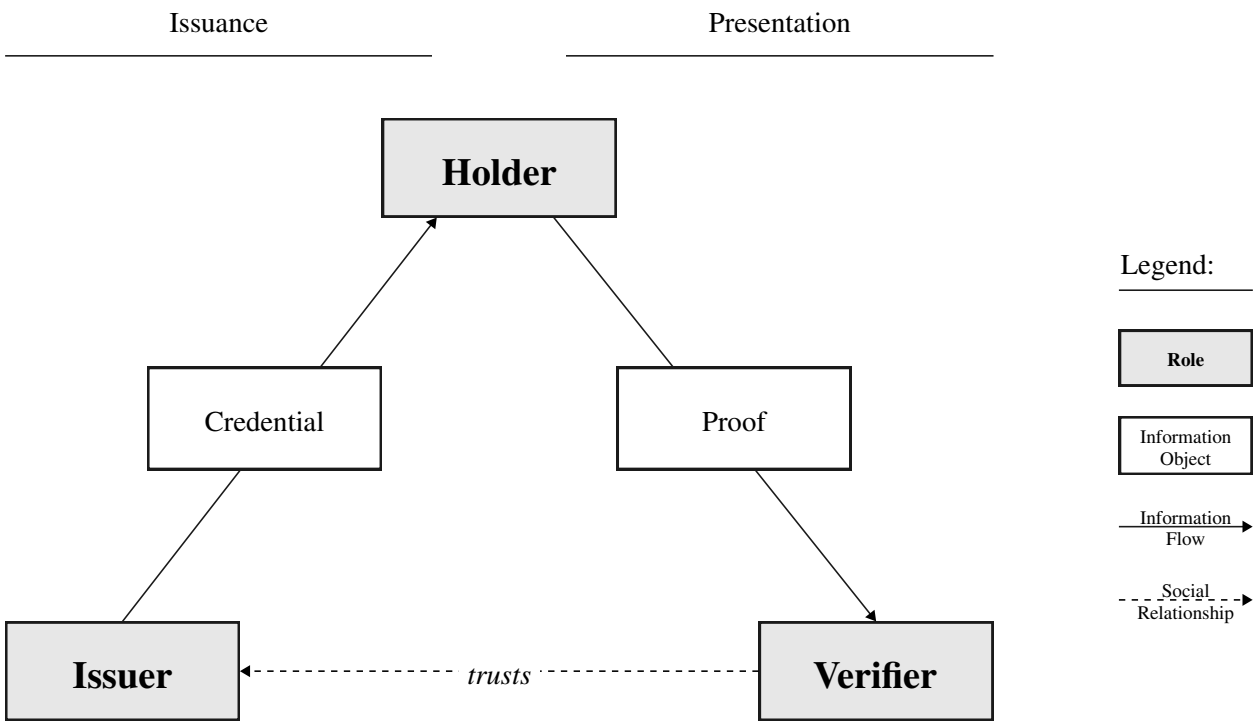

Fig. 2 Role model of credential exchange, adapted from Reed et al. (2021)

1. Issuance: First, an *issuer* makes claims about a subject and provides the corresponding credential to a *holder*.
2. Presentation: Second, when confronted with the necessity to prove claims about the credential subject, a holder presents a proof based on the required set of claims from one or more credentials to a *verifier*.

The triangle is completed by a trust relationship from the verifier toward the issuer of a credential. This relationship is an important factor for the verifier's acceptance of the credential as an authentic proof of the required claims. For verifiers, other decision-relevant factors include structural integrity and validity, i.e., that the credential has not been tampered with, and that it has not expired or been revoked, respectively (Reed et al., 2021). As the issuer can be explicitly denoted in the credential or implicitly known using a protected credential format, direct data exchange between the verifier and the issuer becomes unnecessary. Thus, when the holder of a credential presents proof to a verifier, the issuer does not gain information about this interaction. This contrasts with federated IDM, which typically requires direct requests for attributes from a third party, thereby revealing contextual information and invading user privacy.

Although the relationship between the verifier and issuer is the most important in enabling user control, further trust relationships can be considered. First, the holder needs to trust the issuer that the claims made are correct, so they can prove attributes as they exist in reality. Second, the holder also needs to trust the verifier that they use the shared claims diligently. This shows the importance of governance mechanisms, such as verifier audits, in ensuring that credential exchange fulfills the SSI principles.

Finally, it is worth noting that credential exchange roles are not fixed to specific actors (cf. Babel et al., 2025) but are centered on specific credentials. For example, an individual may be the issuer of a product review, the holder of a driving license, and the verifier of an online shop quality seal. The relationship between the roles at the analytic levels of credential exchange and business processes is discussed in more detail in the "Applications" section.

Technical building blocks

The role of credential exchange in SSI is to enable IDM according to its foundational principles, which are primarily designed to empower and protect individuals. The mechanism of credential exchange determines a decentralized technical architecture for SSI, as verifiable credentials—constituting digital identities—are distributed across individual holders. Since organizations need interfaces to interact with holders, either to issue or verify credentials, this highlights additionally required technical capabilities, which go far beyond the widely discussed artifact of a digital identity wallet (Bochnia et al., 2024). Especially, the question of trust

establishment, as specified in the trust triangle, remains the subject of many discussions at the technical (Jeyakumar et al., 2022), organizational (Rieger et al., 2024), and political levels (Degen & Teubner, 2024).

In the early days of SSI development, blockchain and other distributed ledger technologies played a prominent role in establishing trust relationships in a decentralized way (Cucko & Turkanovic, 2021; Liu et al., 2020; Mühle et al., 2018). Today, this role is less pronounced (Hoess et al., 2022) and has given way to the broader concept of verifiable data registries (Sporny et al., 2022), allowing for more technological diversity and varying degrees of centralization. Even though SSI prompted the development of several new technologies and specifications, there is no standard for the technical architecture of SSI implementations. However, some fundamental technical building blocks, such as verifiable credentials and digital wallets, are particularly important for realizing credential-exchange-based IDM in line with SSI principles (Mühle et al., 2018; Sedlmeir et al., 2022a; Weigl et al., 2023). We present these building blocks in the following sections along a structure inspired by Davie et al. (2019) and Yildiz et al. (2023).

Verifiable credentials

Verifiable credentials are the most important building block of SSI systems. Narrowly defined, verifiable credentials are digital credentials that implement the eponymous World Wide Web Consortium (W3C) data model specification (Sporny et al., 2022). The development of verifiable credentials takes inspiration from the handling of physical credentials and is augmented by modern cryptography for privacy protection, information reliability, and authenticity (Sedlmeir et al., 2021, 2022a). W3C verifiable credentials consist of three parts: (1) metadata, such as credential type and issuer, (2) claims about a subject, and (3) cryptographic proofs, such as digital signatures by the issuer. Verifiable credentials thus not only allow for the transmission of claims but also provide proof of their provenance, which is an important information quality characteristic (Gharib & Giorgini, 2019). Additionally, verifiable credentials can be used to create *verifiable presentations*, enabling the recombination of discrete claims from one or more credentials that are required in a specific context. Such so-called *selective disclosure* contributes to the SSI principle of data minimalization.

In a broader sense, verifiable credentials can be viewed as a more general concept of digital credentials, not necessarily built on the W3C data model (Sedlmeir et al., 2021). For example, ISO-compliant digital driving licenses (ISO, 2021) and "open badges" (1EdTech Consortium, 2025) can be considered verifiable credentials. It should be noted, however, that a benefit of using the W3C data model is its support for the SSI principle of interoperability (Yildiz et al., 2023). W3C verifiable credentials can represent any claim about any subject, including organizations and objects (Sporny et al., 2022). As a result, the standard influenced digital transformation projects, which go beyond SSI's goal of empowering individuals, e.g., cross-border trade (UN/CEFACT, 2022) and legal entity identification (GLEIF, 2023).

Digital identity wallets and agents

As verifiable credentials are inspired by physical credentials, *digital identity wallets* (wallets) are analogous to the physical wallets used to organize and transport credentials in daily life. Wallets are applications that individuals can use to store and present proof of verifiable credentials (Weigl et al., 2023). To process incoming credential offers and proof requests, wallets need to implement interoperable protocols (Davie et al., 2019), which are often subsumed as *agent* functionalities (O'Donnell, 2021). Issuance and verification of verifiable credentials are out of the scope of most available wallet applications, limiting the agency of individuals (O'Donnell, 2021). Still, wallets are an important tool for realizing several SSI principles, providing an independent digital existence as well as facilitating access to and control over credentials, identifiers, and associated cryptographic keys. While it can be argued to what degree they fulfill the SSI principles (Doege et al., 2024), the wallets currently under development by European Union member states are an important initiative to provide many individuals with the means to manage their digital identities and credentials autonomously.

Verifiable data registries

Not all information necessary to verify the authenticity, validity, and integrity of verifiable credentials can be found in the credentials themselves (Biele et al., 2025). The loose coupling of issuers, holders, and verifiers in SSI systems is mediated by *verifiable data registries*. These serve to provide a common source of truth for information, such as credential revocation status, contextually applicable credential schemas, and trusted issuers for specific credential types (Hoess et al., 2024; Sporny et al., 2022). Such information is not merely technical but is strongly connected to the governance in a given application domain (Reed, 2021). At the beginning of SSI's development, blockchain and other distributed ledger technologies were favored for reliably providing such information in a decentralized governance model (Mühle et al., 2018; Wang & Filippi, 2020). The fashion around blockchain supported the early diffusion of SSI in organizational settings (Hoess et al., 2023), but it also led to conceptual derivations and ambiguities (Weigl et al., 2023)

of SSI with a focus not necessarily on the SSI principles but on the use of blockchain, e.g., (Kuperberg, 2019; Liu et al., 2020; Yan et al., 2024). However, blockchain is not necessary to provide verifiable data registries in SSI and should be used cautiously, e.g., for sensitive data on-chain or for payments (Hoess et al., 2022). For example, Jeyakumar et al. (2022) propose using the Domain Name Service to register trusted credential issuers. While the dominance of blockchain-based approaches has been attenuated, the discussion on which type of registry to use for which information and in which use case is still ongoing and driven by SSI practice (O'Donnell et al., 2025) and design-oriented research (Feulner et al., 2022; Guggenberger et al., 2023; Hoess et al., 2024; Schlatt et al., 2021).

Decentralized public key management

A common misconception about using blockchain in SSI applications is that individuals' digital identities are stored on a public ledger (Schellinger et al., 2022). Fundamentally, this misconception stems from the confusion between digital identities and *decentralized identifiers (DIDs)*, another W3C specification inspired by the SSI principles (Reed et al., 2022). Fundamentally, DIDs provide a namespace for globally unique identifiers (Cucko et al., 2022). More importantly, the specification allows the standardized resolution of these identifiers to public keys stored in verifiable data registries (Mühle et al., 2018). In other words, they are a tool for *decentralized public key management* (Smith, 2021). This enables individuals in control of the corresponding private keys—stored in their digital identity wallet—to prove their binding to the identifiers. Thus, when presenting proof of a credential, they can authenticate themselves as rightful holders and/or subjects without relying on third parties (Wang & Filippi, 2020). In this way, decentralized public key management aims to realize the SSI principles of existence, control, and persistence.

DIDs can be implemented and managed in various ways, resulting in several different so-called *DID methods*. Some of these methods rely on blockchain to store public keys, which is the source of the misconception mentioned above (Sporny & Sabadello, 2025). However, these keys do not allow for correlation if not reused across relationships (Satybaldy et al., 2024). DIDs are a source of discussion in the SSI community as different DID methods allow for varying degrees of independence from external systems (Smith, 2021; Yildiz et al., 2023). Whether DIDs need to be used at all, or whether more centralized public key infrastructures are sufficient for realizing the SSI principles, is an ongoing debate (Smethurst, 2023).

Applications

In recent years, the ongoing consolidation of SSI's core technical building blocks along standardization paths has enabled more focused research on the application of SSI in various domains. Mobility (Hoess et al., 2022, 2024; Richter & Anke, 2021), commerce (Feulner et al., 2022; Guggenberger et al., 2023), finance (Gramlich et al., 2024; Schlatt et al., 2021), and healthcare (Göppinger et al., 2024; Houtan et al., 2020; Lacity & Carmel, 2022) are some exemplary domains of recent IS publications with design or exploratory orientations. These studies show how the generic roles of credential exchange are instantiated and enacted in concrete business processes.

For example, Hoess et al. (2024) implemented SSI's technical building blocks in an artifact for a mobility-as-a-service system. Figure 3 exemplifies how SSI enables inter-organizational data exchange along the business processes of travel booking and inspection during a journey. As a result of the booking process, the mobility service provider issues a travel ticket, which serves as proof of a valid booking later during an inspection by a ticket inspector. This data exchange is necessary based on the business requirement to detect fare dodgers. In the SSI-enabled application,

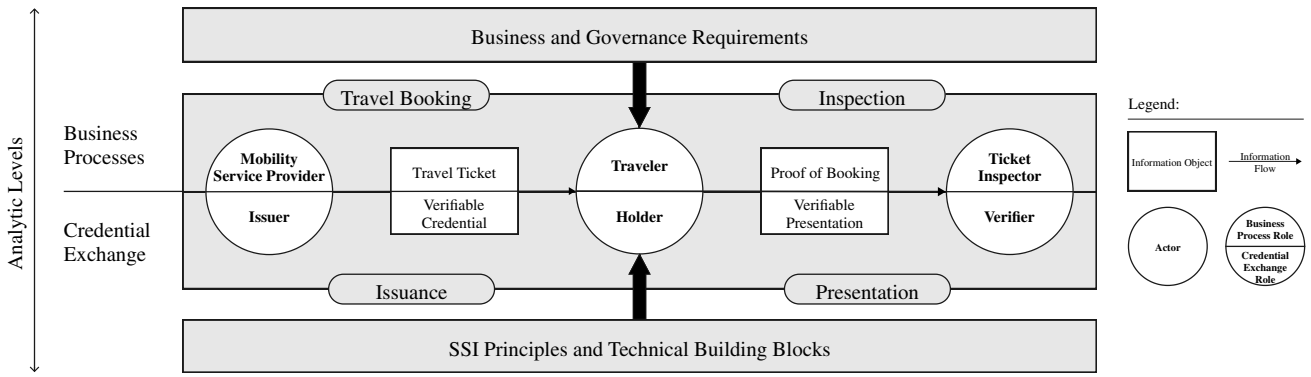

Fig. 3 Instantiated credential exchange based on the case study by Hoess et al. (2024)

a tension between legitimate business interests in data exchange (Glöckler et al., 2023) and the SSI principles' goal of protecting individuals' (in this case, the traveler's) privacy becomes apparent (Sedlmeir et al., 2022a). Hoess et al. (2024) mediate this tension by allowing the selective disclosure of only necessary attributes in the form of a verifiable presentation based on the travel ticket, thereby supporting the data minimalization principle.

Whereas the studies mentioned above focus more on architectural principles from an organizational perspective, another, albeit smaller, IS research stream is engaged with user perceptions of instantiated wallet applications. While the evaluated wallets were found to be useful tools for personal data control, the general concept of SSI, including technical terms such as "credentials" remains difficult for users to understand (Ostern & Cabinakova, 2019; Sartor et al., 2022). First proposals for wallet design principles have been established, but they still need to be evaluated with a large and diverse set of users in actual business processes (Krauß et al., 2023; Sellung & Kubach, 2023), potentially using novel user acceptance frameworks (Guggenberger et al., 2022).

Although SSI is an IDM approach focusing on data sovereignty for individuals, its adoption also depends on benefiting the interests of organizations. In their Fundamentals article, Babel et al. (2025) systematize the potential benefits of SSI into seven value propositions, applicable to both individuals and organizations. According to Babel et al. (2025), the value propositions of SSI are efficiency, risk reduction, data control, usability, verifiability, cost reduction, and compliance. The mobility example above illustrates how these propositions might materialize, e.g., by introducing automated ticket issuance and privacy-preserving inspections.

Despite these benefits, SSI adoption in practice is still limited. This is due to several challenges, identified by Laatikainen et al. (2021a) across the technology, business, governance, regulatory, and societal spheres. For example, SSI's technical building blocks remain novel artifacts that require further standardization and integration into existing IDM systems and business processes (Babel et al., 2025; Bazarhanova & Smolander, 2020; Kudra et al., 2025; Laatikainen et al., 2021a). This includes providing components with infrastructure characteristics, such as verifiable data registries, which are often taken for granted but are hardly established in practice (Degen & Teubner, 2024). Similarly, the assumption that market-based business models for providers of SSI's technical building blocks exist (Bazarhanova & Smolander, 2020) might not hold in practice (Kubach & Sellung, 2021; Laatikainen et al., 2021a). Hence, governance solutions, such as the public provisioning of essential technical building blocks within the scope of eIDAS 2.0, are required to enable the adoption of SSI—beyond isolated business processes—in application ecosystems (Laatikainen et al., 2021b; Weigl et al., 2023).

Governance

The notion of governance is an important subject of discussion in the SSI community. While not part of Allen's original principles, early in SSI's development, governance was identified as necessary to implement the organizational trust between credential verifiers and issuers (Davie et al., 2019). However, this is just one aspect of SSI governance, which is commonly conceptualized as operating on different levels (Davie et al., 2019; Laatikainen et al., 2021b; Satybaldy et al., 2024). We follow this multi-level view of SSI governance and apply it to the three previously introduced analytic levels: (1) credential exchange, (2) technical building blocks, and (3) applications, and explain how they are interrelated.

To implement the trust relationships between the standard roles operating on the level of credential exchange, a fourth role of *governance authority* was proposed (Reed, 2021). Its purpose is to create and manage a binding regulatory document for actors wishing to participate in the exchange of a defined set of credentials in an application ecosystem. The rules set out in these *credential governance frameworks* aim to enable and constrain the use of credentials (Richter et al., 2023). Besides regulating their use, these frameworks are constitutive for credential exchange as they define the structure and validity conditions of credentials (Richter et al., 2023; Smith et al., 2020). The German Act on Identity Cards and Electronic Identification ("PAuswG") is an example of a credential governance framework that regulates the German national identification card, passport, and similar credentials. However, to automate trust decisions in SSI-enabled applications, credential governance frameworks need to be machine-readable by wallets and agents and readily accessible in verifiable data registries. SSI practice has come up with proposals for *machine-readable governance*, e.g., in the scope of the eIDAS Architecture and Reference Framework (European Commission, 2025), EBSI VC Framework (EBSI, 2024), TRAIN (Chadwick et al., 2023; Jeyakumar et al., 2022; Kubach & Roßnagel, 2021), or Credential Trust Establishment (Decentralized Identity Foundation, 2022). Nevertheless, these proposals still lack large-scale practical trials, and the relationships among them are still poorly understood due to differing scopes (Biele et al., 2025).

On a technology level, governance regulates the desired properties and use of SSI's technical building blocks. A good example of such a *technology governance* process can be taken from the ongoing development of European Union Digital Identity Wallets. Various consultation processes and public discourse led to the definition of supported verifiable credential formats, exchange protocols, identifiers, verifiable

data registries, and certification of components (European Commission, 2025).

As SSI-enabled applications are built and interact across multiple business processes in various domains, they form and are embedded into application ecosystems. Hence, credential governance and technology governance are also part of a higher-level structure: *application ecosystem governance* (Satybaldy et al., 2024). On the level of application ecosystems, governance deals with the definition of applicable value-creating mechanisms for SSI-enabled applications and the orchestration of actors towards these. This includes balancing the interests of public, private, and individual actors participating in these ecosystems as well as ensuring the financing of technology provisioning (Degen & Teubner, 2024; Richter & Anke, 2024). Due to a lack of SSI projects with the necessary maturity, the relationship between application ecosystem governance and domain-specific institutions is still poorly understood. For example, which modes of governance to choose, i.e., market-based (Kubach & Roßnagel, 2024), regulatory (Degen & Teubner, 2024), and cooperative (Kölbel et al., 2022), and in which contexts is still an open research frontier (Amard et al., 2024).

Research opportunities

While our previous remarks synthesize the current state of IS research on SSI, we now apply our conceptual framework to highlight promising research avenues along the central components of (1) foundational principles, (2) credential exchange, (3) technical building blocks, (4) applications, and (5) governance. As a result, we present the IS research agenda on SSI depicted in Table 2. With this agenda, we provide a structured overview of SSI research questions and propose a set of conceptual foundations we deem as promising to their pursuit. These include theories, models, frameworks, concepts, and methods used in IS research, which may serve as sources for crafting theoretical lenses suitable to the respective research avenues (cf. Niederman & Salvatore, 2019). Thereby, we aim to guide future SSI research toward a better integration with the IS body of knowledge.

Opportunities for research on foundational principles

As shown above, SSI is driven by a set of principles that reflect underlying human values. However, such values differ between cultural contexts, so implementing SSI might not be feasible in every country. Additionally, the expected availability of verified identity information that is easy to share might incentivize organizations to gather such data to learn more about their customers. This creates privacy tensions between the data demands of organizations and the desire to protect the privacy of individuals. These issues open the following research avenues:

Underlying values of SSI principles

The values of technology providers influence the properties of the artifacts they create (Spiekermann et al., 2022). It is, therefore, essential to negotiate these values with stakeholders of SSI-enabled applications and clearly define goals and principles for their development and proliferation. SSI's initial development was influenced by libertarian values, such as skepticism towards centralized states, leading to a strong focus on decentralization (Allen, 2016; Sedlmeir et al., 2021). The prevalence of these values is a societal matter, shaped by cultural history and political climate. Consequently, the principles for designing digital identity systems need to be analyzed with a greater focus on the cultural dimension and political priorities (Weigl et al., 2023). This could help avoid degenerative outcomes, such as excluding marginalized groups (Masiero & Arvidsson, 2021).

Actionable compliance with SSI principles

Many users are skeptical about sharing personal information (Beduschi, 2021). Advanced cryptographic techniques for data minimization, such as zero-knowledge proofs, need to be more extensively applied and tested in productive scenarios to allow for more insights into the behavioral implications of their use and further develop standards for their adoption by coercive parties (Glöckler et al., 2023). Regulation could address this issue by providing technical and organizational measures to reduce coercion, e.g., requiring relying parties to be approved by a governance authority before they can request data from individuals (Quach et al., 2022). This, however, might interfere with the individual's freedom to share data. Another approach is to require verifiers to declare what data they may request for what purpose in a machine-readable form. This way, wallet apps could provide contextual information to let individuals make an informed decision (Ebert et al., 2023). Future research should investigate the effectiveness and acceptance of such measures to ensure compliance with the SSI principles.

Opportunities for research on credential exchange

Credential exchange builds on trust relationships, which in practice need to be secured by appropriate governance mechanisms, such as auditing and verifying trusted actors (Richter et al., 2023). To profit from efficiency gains by digitally transforming credential exchange, while also safeguarding institutional integrity, these governance mechanisms need to be automatable (Biele et al., 2025). As credential exchange coordinates transacting individuals and

Table 2 IS research agenda on SSI

Research avenue	Exemplary research questions	Potential conceptual foundations
Foundational principles		
Underlying values of SSI principles	- What are the most important values underlying the SSI principles? - How do SSI applications differ depending on the political and cultural context? - How can tensions between SSI principles be mediated?	Theory of basic human values Tensions Paradox Multi-level perspective
Actionable compliance to SSI principles	- How can compliance to SSI principles be ensured in socio-technical designs? - Which measures can effectively mitigate privacy tensions between individuals and organizations in SSI?	Value-based engineering Algorithmic governance Tensions Paradox
Credential exchange		
Institutional embeddedness of credential exchange	- What are the key aspects of trust frameworks that need to be described in machine-readable form to automate trust decisions? - How can the lifecycle of machine-readable governance information be organized in a secure and reliable manner?	Social ontology Institutionalization Social network theory
Economics of credential exchange	- How can the monetary value of verifiable credentials be determined? - How can protocols be designed to enable individuals to monetize their data?	Information value Peer-to-peer payment protocols
Technical building blocks		
Wallet user experience	- Which design heuristics can be applied to create a seamless user experience in multi-device SSI applications? - How can interactions in wallets be designed to empower the individual to make informed data-sharing decisions? - What factors drive the adoption of SSI's technical building blocks?	Human-centered design Usable security Technology acceptance model
Enterprise capabilities	- Which functionalities are needed to enable organizations to handle credentials as issuer, verifier and holder? - How can enterprise SSI components be integrated into existing business applications and workflow automation?	Enterprise architecture Distributed systems
Trust management infrastructure	- What are the characteristics of decentralized trust management approaches for open SSI ecosystems? - How can interoperability between different trust management approaches be achieved?	Trust models Public-key cryptography Digital infrastructure
Applications		
Verifiable credentials as universal data containers	- What are the conceptual boundaries of SSI? - What is the impact of utilizing verifiable credentials in e-business, e.g., on transaction cost?	Social construction of technology
Service system transformation	- How does SSI improve the value co-creation in service systems? - What methods and practices are required to transform service systems to utilize SSI systematically?	Service-dominant logic Disintermediation
Business process management	- How does credential exchange impact business process design? - What business process pattern can be identified to support the integration of credential exchange into business processes?	Work system theory

Table 2 (continued)

Research avenue	Exemplary research questions	Potential conceptual foundations
Governance		
Multi-level ecosystem governance	- How can the objectives of different stakeholder groups be balanced to create a thriving identity data ecosystem? - How can governance be adapted to changing conditions? - What are viable forms of governance for SSI-based digital identity infrastructure?	Service-dominant logic Institutionalization Institutional work Collective action theory Network governance
Business models	- What is the impact of SSI on existing information-based business models? - What business model innovation opportunities arise for organizations that maintain sources of reusable data, which could be issued as verifiable credentials?	Business model innovation Data-driven business models Information quality
Impact of SSI	- What is the impact of SSI on individuals, organizations, and society on an economical, ecological, and social level? - What are the adverse effects of SSI, and how can they be mitigated?	Sustainability reporting Degenerative outcomes Transaction cost theory

organizations by enacting the relevant institutional arrangements, more research is also needed in analyzing the role and forms of data exchange in electronic markets, which fall into the problem space of technology for digital credential exchange (Smith et al., 2020). This opens the following research avenues:

Institutional embeddedness of credential exchange

In the "Credential exchange" section, we build on social ontology to conceptualize credential exchange as a basic social mechanism, which is independent from the various media used for its implementation (Richter et al., 2023; Smith et al., 2020). This perspective enables identifying diverse potential applications for SSI based on the instances of credential exchange found in practice. Proposals for SSI implementations abound (see the "Applications" section), from the perspective of social ontology, we can observe a lack of research on the institutional arrangements into which credential exchange is embedded. Because credentials enable or constrain their holders to exercise a diverse set of powers, such as participating in an election or deducting money from a bank account, implementing SSI warrants a more detailed understanding of the relationships between the actors involved and the context of various credential exchange instances. Research in this direction could move beyond the concept of trust and focus on actors' authority, legitimacy, and the power dynamics, which are institutionalized by credential exchange. Such research could uncover the types of institutional environments that foster or inhibit the adoption of SSI.

Economics of credential exchange

The standardized exchange of verifiable digital credentials can lead to innovation potentials and new revenue streams in data economies. Some examples are authenticity credentials for products (Heeß et al., 2024) and platform-independent reputation management (Hesse & Teubner, 2020). Also, actors in data ecosystems are subject to several digital identity problems, from onboarding to verifying exchange partners and data authenticity (Möller et al., 2024). Determining and capturing the value of the identity information encapsulated in credentials might serve as the basis for business models in SSI-enabled application ecosystems. This includes opportunities for individuals to monetize data and negotiate usage conditions with verifiers, e.g., in customer loyalty programs. Further research at the intersection of IS, marketing, and economics could address this issue.

Opportunities for research on technical building blocks

While the basic technical building blocks for SSI are available, technical maturity remains a challenge for implementation projects (Laatikainen et al., 2021a). Specifically, fragmentary standardization of advanced functions such as zero-knowledge proofs is in conflict with the security requirements of implementing organizations and regulation (Kudra et al., 2025). As a result, in the scope of the European Union Digital Identity Wallets, such functions have been excluded from the initial release schedule. Further, digital identity technologies need to be easily usable,

enabling individuals to exercise their rights to privacy and informational self-determination effectively (Guggenberger et al., 2022). At the same time, they must be provided with capabilities to detect actors with malicious or opportunistic intent, such as providers of fake shops.

For organizations, handling verifiable credentials is more complex than for individuals (Bochnia et al., 2024). Concepts and implementations of organizational wallets and SSI-based organizational identities are experiencing dynamic developments. It is understood that SSI will only be successful if organizations obtain enterprise-grade capabilities to act not only as issuers and verifiers of digital credentials but also as holders. Similarly, digital infrastructure for trust establishment during credential exchange is still fragmented and its feature set is insufficiently specified to enable credential exchange across ecosystem boundaries (Biele et al., 2025). In detail, these issues can be addressed as follows.

Wallet user experience

As digital identity wallets are still a novel concept for most individuals, the interactions with these artifacts need to be designed with a high degree of usability and with an appropriate amount of information, allowing users to understand the important implications of their technology use (Sartor et al., 2022). Concepts and patterns of *usable security* need to be more systematically applied to digital wallets, allowing them to make more informed choices about, e.g., whom to share their attributes with (Ebert et al., 2023, 2024). Future research should contribute design knowledge on wallets that provide users with an environment where they can confidently exchange credentials with third parties. This requires the consideration of the complete user journey into which wallet interactions are embedded.

According to the privacy calculus model, individuals balance the costs and benefits of sharing personal data (Klopfer & Rubenstein, 1977; Laufer & Wolfe, 1977; Pavlou, 2011). Therefore, SSI adoption also depends on whether its technical building blocks provide tangible benefits to users. Technology acceptance models applied to digital identity could help to prioritize further acceptance factors during design and market introduction, e.g., value propositions, usability, and usage intentions (Guggenberger et al., 2022).

Enterprise capabilities

As wallets and verifiable credentials constitute important technical building blocks for SSI applications on the side of individuals, organizations also need to integrate technical capabilities for credential management into their existing enterprise system architectures and business processes (Glöckler et al., 2023; Guggenberger et al., 2023). While there are providers specifically targeting organizational users, there are no established software categories yet. This hampers the design and development of interoperable components, which can be flexibly combined to support different degrees of SSI readiness in organizations (Bochnia et al., 2023). Therefore, future research should translate organizational requirements for SSI software into sets of conceptually clearly defined components and interfaces (Bochnia et al., 2024).

Trust management infrastructure

Verifiable data registries are a fundamental technical building block supporting trust decisions of actors in credential exchange. These decisions regard, e.g., trustworthy issuers and verifiers, legitimate authorities as well as credential status, validity, and integrity (Biele et al., 2025). The implementation approaches and scope of these systems are very diverse across both design-oriented research and practice. However, as SSI is increasingly adopted and VCs are exchanged across more organizational and ecosystem boundaries, a more streamlined approach to process such trust-relevant information – trust management – is necessary to avoid complex system architectures and growing integration costs. Adopting an infrastructural perspective on automated trust decisions in SSI-based credential exchange highlights technical building blocks, which are still underdeveloped or missing in most architectural considerations. This includes standardized trust policy languages, which describe the rules for credential exchange generated by governance authorities and actor-specific requirements, and trust protocols, which query the diversely implemented verifiable data registries (Alber et al., 2021; Yildiz et al., 2023).

Future research should focus on a scalable and maintainable approach to trust management, which utilizes verifiable data registries. Due to the specifics of domains and jurisdictions, it is unlikely that only a single approach will prevail. Therefore, cross-domain trust establishment and trust management system interoperability are further research frontiers. Part of this research avenue is to validate these proposals from practice regarding their scope and expressiveness for real-world applications in different domains.

Opportunities for applications research

As shown in the "Foundational principles" section, the key driver for the inception and development of SSI is achieving individual data sovereignty. However, verifiable credentials, as a key technical building block of SSI, have proven to be much more versatile than just representing individuals' digital identities. As research on organizational applications of verifiable credentials shows, they can express a wide range of facts that might need to be verified in digital interactions (Guggenberger et al., 2023). This includes identities of organizations and objects, relationships, and guardianship (Babel

et al., 2025; Reed & Preukschat, 2021). Furthermore, transaction data like receipts for groceries, supply chain information, and digital product passports are already designed as verifiable credentials in practice. Therefore, verifiable credentials can be considered a universal container for verifiable data.

Verifiable credentials as universal data containers

The application of verifiable credentials has shown that the exchange of verifiable information using standard protocols is transformative for electronic business. This goes beyond SSI, as handling verifiable credentials requires other technical components, especially for organizations. At the same time, SSI principles that are centered around individuals do not fit in such scenarios. Furthermore, the original idea of SSI deals with credentials whose claims include the individual or their associated entities as the subject. It is easy to understand that using a verifiable credential to prove the successful transfer of bulk material between two companies is beneficial. However, it is hard to justify why this is considered part of a self-sovereign digital identity. As we discussed in the "Conceptualizing self-sovereign identity" and "Foundational principles" sections, we acknowledge the danger of watering down the importance of the SSI principles in conceptualizing SSI as an IDM approach *for organizations*. However, departing from the individual-centric SSI concept, IS research is presented with new opportunities to explore the organizational application of SSI's technical building blocks in what might be called *verifiable data ecosystems*. Exemplary domains for investigation could be digital product passports (Heeß et al., 2024), secondary markets (Engelmann & Schwabe, 2024), and circular economies (Hoppe et al., 2025).

In these emerging verifiable data ecosystems, public and private organizations can satisfy compliance demands, requiring a high degree of information quality, by using verifiable credentials. They can transform and optimize their cross-organizational business processes and service offerings using credential exchange within the boundaries specified by ecosystem governance. Especially in industrial ecosystems, data spaces are used as infrastructure to establish data ecosystems for peer-to-peer data exchange based on domain governance and contractual relationships (Möller et al., 2024). Recent developments in data spaces have started integrating verifiable credential exchange as a foundational building block, indicating an upcoming convergence of these digital transformation efforts (Data Spaces Support Centre, 2025). The integration of SSI's technical building blocks into domain-specific application ecosystems is embedded in a larger trend of organizational digital transformation, necessitating process innovations and a transformation of service models and systems, for which suitable methods and models are needed. This can be augmented by empirically validating the positive and negative impacts of SSI's technical building blocks in various domains. Hence, we can identify the following research avenues:

Service system transformation

SSI-based solutions have been proposed for various information quality problems in different domains, such as finance (Schlatt et al., 2021), commerce (Feulner et al., 2022; Guggenberger et al., 2023), and mobility (Hoess et al., 2024; Richter & Anke, 2021). However, there is still a lack of knowledge on the systematic transformation of service systems towards adopting digital wallets and verifiable credentials. Methods and tools could help practitioners to systematically evaluate the potential benefits of SSI and identify promising application areas within the use cases they manage. Another area of future research lies in the identification and more detailed conceptualization of information quality and identity problems from a business perspective, which is needed to better understand the capabilities of SSI applications (Engelmann & Schwabe, 2024). Future research should focus on application ecosystems as the analytic level in which multiple actors have to coordinate their joint value creation. A better conceptualization of domain-specific ecosystems is needed to understand how credential exchange can improve actor coordination.

Business process management

As business processes are used to describe and analyze coordinated cooperative service exchange, organizations need tools and languages to model policy-based trust decisions therein. This goes beyond a traditional authorization approach as digital identities represent more attributes that impact business decisions, and not just access to specific systems. Examples of work in this direction include the development of trust policy languages formally describing informational demands for digital identities (Alber et al., 2021; Mödersheim et al., 2019) and the integration of the concepts of trust and uncertainty in business process modeling (Müller et al., 2020, 2021).

Opportunities for governance research

The technological and organizational capabilities discussed above enable the establishment of SSI-based digital identity infrastructures. Such infrastructures depend not only on the availability of technical artifacts but also on their adoption by individuals and organizations. To drive the development, operation, and adoption of SSI's technical building blocks and trigger network effects that make it attractive for additional actors to use SSI, regulatory incentives are required. Regulation presents the institutional framework for SSI's application in electronic markets. It balances economically

driven information requirements and potential efficiency gains with societally negotiated values such as informational self-determination, privacy, and inclusivity. Value creation opportunities arise, for example, from the provision of technology as well as the provisioning and utilization of verifiable credentials. Again, regulation determines how market participants can capture these values, e.g., by defining market entry conditions for technology providers and permissible business models, e.g., regarding data monetization.

Multi-level ecosystem governance

Numerous societal actors are participating in developing, provisioning, and using SSI for value co-creation in digital transactions. Service ecosystems allow an analysis of this inter-actor collaboration and the institutions and institutional arrangements that guide them (Vargo & Lusch, 2016). Depending on the focal object (Guggenberger et al., 2020), different ecosystem types and governance constellations can be identified for SSI. For example, the focus on digital wallets and their underlying infrastructures allows for analyzing governance requirements for monetization and the role of the state in orchestrating a digital identity infrastructure (Degen & Teubner, 2024). Introducing official digital identity wallets in European Union member states is an important development toward more standardization and consolidation in technical implementation approaches to SSI (Kudra et al., 2025). With a strong focus on providing the means to manage and exchange official documents with public authorities, the applicability of these wallets in a universal sense and their acceptance by private actors depend on the specific demands for verified information and the cost of alternative provisioning technologies (Kubach & Roßnagel, 2024). Digital wallets and associated components might develop to be part of other applications and operating systems rather than a singular point to manage all identity-related attributes (Degen & Teubner, 2024). Similarly, technology providers might offer wallet provisioning models with less data sovereignty but higher comfort, such as cloud-based wallets (Sule et al., 2021). This technical view contrasts the governance perspective for singular credential types, which gives a framework for the structure and usage of credentials, such as public transport tickets and government identification means (Richter et al., 2023). Finally, the perspective of the use of SSI for satisfying information requirements in digital transactions enables an impact assessment of technology choice (Richter & Anke, 2024). Future research could analyze how governance of technology and credentials should be designed to support the domain-specific requirements of various application ecosystems. This includes both structural features of governance mechanisms as well as suitable methodologies for their design, such as modelling techniques (Sroor et al., 2022).

Business models

Decentralizing digital identities through verifiable credentials induces a new dynamic in personal data markets. Actors like credit bureaus constructed their business models by directly selling verified information, such as credit ratings, to relying parties. In the future, banks might supply their customers with corresponding verifiable credentials, allowing relying parties to circumvent such services (Metz, 2014). Such a shift has general implications for personal data markets, where millions of user profiles are auctioned and traded (Spiekermann et al., 2015a, 2015b). These markets operate largely out of the public sphere and, more importantly, out of the attention of individuals whose personal data is being traded (Agogo, 2021). As a result, negotiation in these markets is skewed towards market providers. Spiekermann and Korunovska (2017) found that awareness of market participation and control over personal data are important mechanisms in these markets, as they heavily shift the balance towards individuals. As the introduction of the European Union General Data Protection Regulation has not fundamentally changed personal data markets (Agogo, 2021), it becomes clear that this control needs to be actionable. Spiekermann et al., (2015a, 2015b) argue for the introduction of technology that supports individuals in managing and commodifying their personal data in a sovereign way—a call that SSI might finally fulfill by providing individuals with digital wallets to control their verifiable credentials. Whether personal data markets will be disintermediated by the introduction of SSI also hinges on whether businesses follow strategic advice to engage in real negotiation with data subjects and focus on data minimization by default (Roeber et al., 2015). Similarly, disintermediation effects can be seen in other domains, such as electric mobility (Richter & Anke, 2021), prompting further research into the dependency of business models on verified information and digital identities. The question of business models is also connected to providers of technical building blocks, such as wallets. With regulation mandating the provisioning of European Union citizens with digital identity wallets free of charge and a generally low willingness to pay for identity services, the question of the economic viability and bundling of digital identity technologies needs further research (Kubach & Roßnagel, 2024).

Impact of SSI

The application of SSI promises benefits for individuals, organizations, and society as a whole, which have been derived through qualitative arguments based on the features of SSI (Babel et al., 2025; Reed & Preukschat, 2021). Future research needs to empirically validate whether these benefits exist, determine under which conditions they materialize, and

quantify them. Sustainability might be a suitable perspective that covers economic, ecological, and social effects. An important social aspect is to endow people in the Global South with identities if they face unstable institutions in their nations or cannot prove their identity because they fled from their home countries. This is a key prerequisite for social participation, as for travel, visa applications, and access to basic support services, a provable identity is required. In this research direction, Garazha et al. (2024) propose design principles for creating an identity system for Ukrainian refugees.

Besides investigating benefits, adverse impacts of SSI also need to be considered. While SSI can potentially enable greater inclusion, it can also lead to erroneous inclusion and even digital exclusion, leaving individuals unable to access essential services (Masiero & Arvidsson, 2021). Further, implementing standardized digital identity infrastructure based on SSI-related technology without strong governance risks the abuse of power to coerce users into oversharing more easily accessible personal data. This risks twisting the principled intention of SSI toward more individual data sovereignty into unwanted surveillance outcomes (Masiero, 2023). These are just exemplary of the "dark sides" of SSI, which currently are not researched extensively. Besides identifying more concrete risks, future research could also develop appropriate countermeasures.

Summary

This Fundamentals article introduces a conceptual foundation of the phenomenon of self-sovereign identity. While traditional approaches to digital identity have been discussed under the concept of identity and access management, the emergence of SSI as a new IDM approach has sparked new interest in the IS research community. SSI and exchanging verifiable credentials in real-world applications as a socio-technical mechanism can be investigated from various angles. We clustered potential research topics along the core elements of our proposed conceptual framework of SSI into the categories of (1) foundational principles, (2) credential exchange, (3) technical building blocks, (4) applications, and (5) governance. In each perspective, research opportunities can be found that connect SSI to other established topics in IS and adjacent disciplines.

Future research could be organized into two overarching research themes: (a) fulfilling SSI principles through user-centered IDM and (b) utilizing SSI's technical building blocks for trustworthy digital interactions between individuals, organizations, and objects in service ecosystems.

(a) Pursuing SSI principles will empower users to control their identity data, which in turn puts the responsibility of thoughtful handling of this data upon the user. This leads to questions on technology acceptance, which is also driven by digital literacy, e.g., having the required skills to make informed decisions about what data to share with whom. Proliferation of wallets and their use for the direct exchange of verifiable data between users and online service providers weakens the position of federated IDM, as used in social logins provided by Google, Apple, Microsoft, and Meta. This shift might become a threat to existing business models of these companies, e.g., personalized advertising. Solving these issues is key for a successful adoption of SSI-based IDM solutions, e.g., the European Union Digital Identity Wallet.

(b) Beyond the focus of SSI on the individual, it has also led to the development of technical building blocks with a much broader application scope than IDM for individuals. In particular, verifiable credentials and their associated protocols offer a standardized mechanism to exchange a wide array of verifiable facts about entities like persons, organizations, and objects between interaction partners. This might lead to improved privacy, process automation, and higher information quality in digital interactions. Overall, SSI's technical building blocks have the potential to fundamentally transform the design of inter-organizational coordination in ecosystems through the exchange of automatically verifiable data. While the potential benefits are well understood, there is still a lack of empirically grounded design knowledge on how to put it into practice.

SSI and its related technologies have the transformative power to redesign the way we establish trust in digital interactions, both in the digital and physical spheres. However, negative impacts ("dark sides") must not be overlooked and need to be mitigated through the responsible design of technology and its governance. The socio-technical approach of IS as a discipline is ideally suited to investigate these phenomena and design useful artifacts that serve the interests of individuals, organizations, and society alike.

Funding Open Access funding enabled and organized by Projekt DEAL.

References

1EdTech Consortium. (2025). *Open Badges Specification*. https://www.imsglobal.org/spec/ob/v3p0

Abbas, A. E., van Velzen, T., Ofe, H., van de Kaa, G., Zuiderwijk, A., & Reuver, M. (2024). Beyond control over data: Conceptualizing data sovereignty from a social contract perspective. *Electronic Markets, 34*, 20.https://doi.org/10.1007/s12525-024-00695-2

Agogo, D. (2021). Invisible market for online personal data: An examination. *Electronic Markets, 31*(4), 989–1010. https://doi.org/10.1007/s12525-020-00437-0

Alber, L., More, S., Mödersheim, S., & Schlichtkrull, A. (2021). Adapting the TPL trust policy language for a self-sovereign identity world. In H. Roßnagel, C. H. Schunck, & S. Mödersheim (Eds.), *Open Identity Summit 2021* (pp. 107–118). Gesellschaft für Informatik e.V. https://dl.gi.de/handle/20.500.12116/36506

Allen, C. (2016). *The path to Self-Sovereign Identity*. https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/

Allen, C. (2025). *Musings of a trust architect: when technical standards meet geopolitical reality: Digital identity, sovereignty, and the erosion of foundational principles*. https://www.blockchaincommons.com/musings/gdc25/

Álvarez, I. A., Hölzmer, P., & Sedlmeir, J. (2025). Privacy evaluation of the European Digital Identity Wallet's architecture and reference framework. *Computers & Security*, 104707. https://doi.org/10.1016/j.cose.2025.104707

Amard, A., Hartwich, E., Hoess, A., Rieger, A., Roth, T., & Fridgen Gilbert (2024). Designing digital identity infrastructure: A taxonomy of strategic governance choices. In T. X. Bui (Chair), *Hawaii International Conference on System Sciences,* Honolulu, HI. https://hdl.handle.net/10125/107396

Anke, J., & Richter, D. (2023). Digitale Identitäten. *HMD Praxis der Wirtschaftsinformatik, 60*(2), 261–282. https://doi.org/10.1365/s40702-023-00965-1

Babel, M., Willburger, L., Lautenschlager, J., Völter, F., Guggenberger, T., Körner, M.-F., Sedlmeir, J., Strüker, J., & Urbach, N. (2025). Self-sovereign identity and digital wallets. *Electronic Markets, 35*, 28. https://doi.org/10.1007/s12525-025-00772-0

Bachura, E., Valecha, R., Chen, R., & Rao, H. R. (2022). The OPM data breach: An investigation of shared emotional reactions on Twitter. *MIS Quarterly, 46*(2), 881–910. https://doi.org/10.25300/MISQ/2022/15596

Bazarhanova, A., & Smolander, K. (2020). The review of non-technical assumptions in digital identity architectures. In T. X. Bui (Chair), *Hawaii International Conference on System Sciences,* Honolulu, HI. http://hdl.handle.net/10125/63576

Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. *Data & Policy*. https://doi.org/10.1017/dap.2021.15

Biele, E., Richter, D., Bochnia, R., & Anke, J. (2025). Supporting trust decisions of holders and verifiers: A unified model of trust management in SSI. In H. Roßnagel (Ed.), *Open Identity Summit. Open Identity Summit 2025* (pp. 113–126). Gesellschaft für Informatik e.V. https://doi.org/10.18420/oid2025_08

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

Bochnia, R., Richter, D., & Anke, J. (2023). Lifting the veil of credential usage in organizations: A taxonomy. In H. Roßnagel, C. H. Schunck, & J. Günther (Eds.), *Open Identity Summit 2023* (pp. 27–38). Gesellschaft für Informatik e.V. https://doi.org/10.18420/OID2023_02

Cameron, K. (2005). *The Laws of Identity: Kim Cameron's Identity Weblog*. https://www.identityblog.com/?p=352

Chadwick, D. W., Kubach, M., Sette, I., & Johnson Jeyakumar, I. H. (2023). Establishing Trust in SSI Verifiers. In H. Roßnagel, C. H. Schunck, & J. Günther (Eds.), *Open Identity Summit 2023.* Gesellschaft für Informatik e.V. https://doi.org/10.18420/OID2023_01

Clauß, S., & Köhntopp, M. (2001). Identity management and its support of multilateral security. *Computer Networks, 37*, 205–219. https://doi.org/10.1016/S1389-1286(01)00217-1

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

Cucko, S., Becirovic, S., Kamisalic, A., Mrdovic, S., & Turkanovic, M. (2022). Towards the classification of self-sovereign identity properties. *IEEE Access, 10*, 88306–88329. https://doi.org/10.1109/ACCESS.2022.3199414

Data Spaces Support Centre (Ed.). (2025). *Data sovereignty and trust - Blueprint v2.0*. https://dssc.eu/space/BVE2/1071255699/Data+Sovereignty+and+Trust

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

Decentralized Identity Foundation. (2022). *Credential trust establishment 1.0.* Decentralized Identity Foundation. https://identity.foundation/credential-trust-establishment/

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

Doege, D., Bochnia, R., & Anke, J. (2024). Fulfilling principles of self-sovereign identity: Towards a conformity assessment approach for human wallets. In H. Roßnagel, C. H. Schunck, & F. Sousa (Eds.), *Open Identity Summit* (pp. 177–182). Gesellschaft für Informatik e.V. https://dl.gi.de/items/334c718b-5fa7-46f9-ab6f-7d5ad0c3391b

Ebert, S., Krauß, A.-M., & Anke, J. (2023). Towards informed choices: A decision model for adaptive warnings in self-sovereign identity. In *Mensch und Computer 2023*.

Ebert, S., Krauß, A.-M., Biedermann, B., Jürgenssen, O., & Anke, J. (2024). *Nutzungsqualität im Fokus: Ergebnisse einer Fokusgruppe zur Wahrnehmung der Nutzungsqualität einer SSI-Anwendung mit Dongle.* https://doi.org/10.18420/RVI2024-06

EBSI. (2024). *EBSI W3C VCs and VPs*. https://hub.ebsi.eu/vc-framework/ebsi-w3c-vc-vp

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

Engelmann, A., & Schwabe, G. (2024). Certified data chats for future used car markets. *Electronic Markets, 34*, 45. https://doi.org/10.1007/s12525-024-00725-z

European Commission. (2022). *European Declaration on Digital Rights and Principles for the Digital Decade*. https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

European Commission. (2025). *Architecture and Reference Framework*. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/

Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. *IEEE Access, 7*, 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173

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

Garazha, A., Merz, C., Schwabe, G., & Zavolokina, L. (2024). Resilience in times of crisis: Empowering refugees with self-sovereign identity. *International Conference on Information Systems*. https://aisel.aisnet.org/icis2024/general_is/general_is/2

Gharib, M., & Giorgini, P. (2019). Information quality requirements engineering with STS-IQ. *Information and Software Technology, 107*, 83–100. https://doi.org/10.1016/j.infsof.2018.11.002

Giannopoulou, A., & Wang, F. (2021). Self-sovereign identity. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1550

GLEIF. (2023). *Introducing the verifiable LEI (vLEI) - vLEI – GLEIF*. https://www.gleif.org/en/vlei/introducing-the-verifiable-lei-vlei

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

Göppinger, S. M. M., Meier, A., Elshan, E., Malekan, O., & Leimeister, J. M. (2024). Beyond trial and error: Strategic assessment of decentralized identity in US healthcare. *International Conference on Information Systems*. https://aisel.aisnet.org/icis2024/ishealthcare/ishealthcare/14

Gramlich, V., Guggenberger, T., Principato, M., Schellinger, B., Duda, S., & Stoetzer, J.-C. (2024). In decentralized finance nobody knows you are a dog. In T. X. Bui (Chair), *Hawaii International Conference on System Sciences,* Honolulu, HI. https://hdl.handle.net/10125/107396

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

Guggenberger, T., Möller, F., Haarhaus, T., Gür, I., & Otto, B. (2020). Ecosystem types in information systems. *Twenty-Eigth European Conference on Information Systems: Liberty, Equality, and Fraternity in a Digitizing World.* Association for Information Systems. https://aisel.aisnet.org/ecis2020_rp/45

Guggenberger, T., Neubauer, L., Stramm, J., & Völter, F. (2022). Accept me as I am or see me go: A qualitative analysis of user acceptance of self-sovereign identity applications. In T. Bui (Chair), *Proceedings of the 56th Hawaii International Conference on System Sciences (HICSS)* (pp. 6560–6569).

Heeß, P., Rockstuhl, J., Körner, M.-F., & Strüker, J. (2024). Enhancing trust in global supply chains: Conceptualizing digital product passports for a low-carbon hydrogen market. *Electronic Markets, 34*, 10. https://doi.org/10.1007/s12525-024-00690-7

Hesse, M., & Teubner, T. (2020). Takeaway trust: A market data perspective on reputation portability in electronic commerce. In T. Bui (Ed.), *Proceedings of the Annual Hawaii International Conference on System Sciences, Proceedings of the 53rd Hawaii International Conference on System Sciences* (pp. 5119–5128). Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2020.629

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

Hoess, A., Roth, T., Sedlmeir, J., Fridgen, G., & Rieger, A. (2022). With or without blockchain? Towards a decentralized, SSI-based eRoaming Architecture. In T. Bui (Chair), *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS)*. https://doi.org/10.24251/HICSS.2022.562

Hoess, A., Rieger, A., Roth, T., Fridgen, G., & Young, A. G. (2023). Managing fashionable organizing visions: Evidence from the European blockchain services infrastructure. In *European Conference on Information Systems*. https://aisel.aisnet.org/ecis2023_rp/337

Hoppe, C., Schoormann, T., Winkelmann, S., & Möller, F. (2025). Tensions in implementing a circular economy – Empirical insights from the automotive industry. *Computers & Industrial Engineering, 204*, Article 111090. https://doi.org/10.1016/j.cie.2025.111090

Houtan, B., Hafid, A. S., & Makrakis, D. (2020). A survey on blockchain-based self-sovereign patient identity in healthcare. *IEEE Access, 8*, 90478–90494. https://doi.org/10.1109/ACCESS.2020.2994090

Huitema, C., Bachenheimer, D., O'Donnell, D., Reed, D., Fleenor, J., Young, K., Hand, K., Kneiss, K., Jordan, J., Bendixsen, L., Subrahmanyam, P. A., Mukhopadhyay, S., Perry, S., Syntez, V., Malhotra, V., & Chu, W. (2021). *Introduction to Trust Over IP: Version 2.0.* Trust Over IP Foundation. https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf

ISO (2021–09). *Personal identification — ISO-compliant driving licence:* Part 5: Mobile driving licence (mDL) application (ISO/IEC 18013–5:2021). International Organization for Standardization. https://www.iso.org/standard/69084.html

Jeyakumar, I. H. J., Chadwick, D. W., & Kubach, M. (2022). A novel approach to establish trust in verifiable credential issuers in self-sovereign identity ecosystems using TRAIN. In H. Roßnagel, C. H. Schunck, & S. Mödersheim (Eds.), *Open Identity Summit 2022* (pp. 27–38). Gesellschaft für Informatik e.V. https://doi.org/10.18420/OID2022_02

Khosrawi-Rad, B., Robra-Bissantz, S., Strohmann, T., & Vom Brocke, J. (2025). On the role of vision in design science research. In S. Chatterjee, J. Vom Brocke, & R. Anderson (Eds), *Local Solutions for Global Challenges. DESRIST 2025. Lecture Notes in Computer Science* (Vol. 15703). Springer. https://doi.org/10.1007/978-3-031-93976-1_4

Kim, D., & Kokuryo, J. (2024). Establishing altruistic ethics to use technology for social welfare—How Japan manages Web3 and self-sovereign identity in local communities. *Electronic Markets, 34*, 6. https://doi.org/10.1007/s12525-023-00684-x

Klopfer, P. H., & Rubenstein, D. I. (1977). The concept privacy and its biological basis. *Journal of Social Issues, 33*(3), 52–65. https://doi.org/10.1111/j.1540-4560.1977.tb01882.x

Kölbel, T., Gawlitza, T., & Weinhardt, C. (2022). Shaping governance in self-sovereign identity ecosystems: Towards a cooperative business model. *Internationale Tagung Wirtschaftsinformatik*. https://aisel.aisnet.org/wi2022/it_for_development/it_for_development/18

Krauß, A.-M., Kostic, S., & Sellung, R. A. (2023). A more user-friendly digital wallet? User scenarios of a future wallet. In H. Roßnagel, C. H. Schunck, & J. Günther (Eds.), *Open Identity Summit 2023* (pp. 73–84). Gesellschaft für Informatik e.V. https://doi.org/10.18420/OID2023_06

Kubach, M., & Roßnagel, A. (2021). A lightweight trust management infrastructure for self-sovereign identity. In H. Roßnagel, C. H. Schunck, & S. Mödersheim (Eds.), *Open Identity Summit 2021* (pp. 155–166). Gesellschaft für Informatik e.V. Regular Research Papers.

Kubach, M., & Roßnagel, H. (2024). Economically viable identity ecosystems: Value capture and market strategies. In H. Roßnagel, C. H. Schunck, & F. Sousa (Eds.), *Open Identity Summit* (pp. 27–38). Gesellschaft für Informatik e.V. https://dl.gi.de/items/1e80debf-ddd1-4876-ab9b-c4b13be2bc64

Kubach, M., & Sellung, R. (2021). On the market for self-sovereign identity: Structure and stakeholders. In A. Roßnagel, C. H. Schunck, & S. Mödersheim (Chairs), *Open Identity Summit 2021* (pp. 143–154). Gesellschaft für Informatik e.V. Regular Research Papers.

Kudra, A., Rieger, A., Sedlmeir, J., Roth, T., Fridgen, G., & Young, A. (2025). Digital identity wallets: A guide to the EU' s new identity model. *Information Systems Journal*, Article isj.70009. Advance online publication. https://doi.org/10.1111/isj.70009

Kuperberg, M. (2019). Blockchain-based identity management: A survey from the enterprise and ecosystem perspective. *IEEE Transactions on Engineering Management*, 1–20. https://doi.org/10.1109/TEM.2019.2926471

Laatikainen, G., Kolehmainen, T., & Abrahamsson, P. (2021a). Self-sovereign identity Ecosystems: Benefits and Challenges. *12th Scandinavian Conference on Information Systems: Living in a digital world?*. Association for Information Systems. https://aisel.aisnet.org/scis2021/10/

Laatikainen, G., Kolehmainen, T., Li, M., Hautala, M., & Kettunen, A. (2021b). Towards a trustful digital world: Exploring self-sovereign identity ecosystems. *Twenty-fifth Pacific Asia Conference on Information Systems*. Association for Information Systems. https://aisel.aisnet.org/pacis2021/19

Lacity, M., & Carmel, E. (2022). Self-sovereign identity and verifiable credentials in your digital wallet. *MIS Quarterly Executive, 21*(3), Article 6.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Raymond Choo, K.-K. (2020). Blockchain-based identity management systems: A review. *Journal of Network and Computer Applications, 166*, Article 102731. https://doi.org/10.1016/j.jnca.2020.102731

Masiero, S. (2023). Digital identity as platform-mediated surveillance. *Big Data & Society, 10*(1), 205395172211351. https://doi.org/10.1177/20539517221135176

Masiero, S., & Arvidsson, V. (2021). Degenerative outcomes of digital identity platforms for development. *Information Systems Journal, 31*(6), 903–928. https://doi.org/10.1111/isj.12351

Metz, R. (2014). Credit Scoring: Will our digital identity replace the real person? In K. Purnhagen & H. Micklitz (Eds.), *Studies in European Economic Law and Regulation. Varieties of European Economic Law and Regulation: Liber Amicorum for Hans Micklitz* (1st ed., pp. 635–650). Springer.

Mödersheim, S., Schlichtkrull, A., Wagner, G., More, S., & Alber, L. (2019). TPL: A trust policy language. In W. Meng, P. Cofta, C. D. Jensen, & T. Grandison (Eds.), *IFIP Advances in Information and Communication Technology. Trust Management XIII* (Vol. 563, pp. 209–223). Springer International Publishing. https://doi.org/10.1007/978-3-030-33716-2_16

Möller, F., Jussen, I., Springer, V., Gieß, A., Schweihoff, J. C., Gelhaar, J., Guggenberger, T., & Otto, B. (2024). Industrial data ecosystems and data spaces. *Electronic Markets, 34*, 41. https://doi.org/10.1007/s12525-024-00724-0

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

Müller, M., Garzon, S. R., Rosemann, M., & Kupper, A. (2020). Towards trust-aware collaborative business processes: An approach to identify uncertainty. *IEEE Internet Computing, 24*(6), 17–25. https://doi.org/10.1109/MIC.2020.3023180

Müller, M., Ostern, N., Koljada, D., Grunert, K., Rosemann, M., & Küpper, A. (2021). Trust mining: Analyzing trust in collaborative business processes. *IEEE Access, 9*, 65044–65065. https://doi.org/10.1109/ACCESS.2021.3075568

Niederman, F., & Salvatore, M. (2019). The "theoretical lens" concept: We all know what it means, but do we all know the same thing? *Communications of the Association for Information Systems, 44*, 1–33. https://doi.org/10.17705/1CAIS.04401

O'Donnell, D. (2021). Digital wallets and digital agents. In A. Preukschat & D. Reed (Eds.), *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials* (pp. 189–219). Manning Publications.

O'Donnell, D., Reed, D., Seltzer, W., Kesselman, A., & Poltorak, D. (2025). *The ecosystem-of-ecosystems model for decentralised digital trust infrastructure: A white paper from the Ayra Association*. Version 3.0. Ayra Association. https://ayra.forum/wp-content/uploads/2025/01/The-Ecosystem-of-Ecosystems-Model-V3.pdf

Ostern, N., & Cabinakova, J. (2019). Pre-prototype testing: Empirical insights on the expected usefulness of decentralized identity management systems. In T. X. Bui (Chair), *Hawaii International Conference on System Sciences*. https://scholarspace.manoa.hawaii.edu/handle/10125/59440

Pang, M.-S., & Vance, A. (2025). Breached and denied: The cost of data breaches on individuals as mortgage application denials. *MIS Quarterly, 49*(2), 465–494. https://doi.org/10.25300/MISQ/2024/18787

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly, 35*(4), 977–988. https://doi.org/10.2307/41409969

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science, 50*(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Reed, D. (2021). SSI governance frameworks. In A. Preukschat & D. Reed (Eds.), *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials* (pp. 248–273). Manning Publications.

Reed, D., & Preukschat, A. (2021). SSI Scorecard: Major features and benefits of SSI. In A. Preukschat & D. Reed (Eds.), *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials* (pp. 58–84). Manning Publications.

Reed, D., Joosten, R., & van Deventer, O. (2021). The basic building blocks of SSI. In A. Preukschat & D. Reed (Eds.), *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials* (pp. 21–38). Manning Publications.

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., Sabadello, M., & Holt, J. (2022). *Decentralized Identifiers (DIDs) v1.0: W3C Recommendation.* W3C. https://www.w3.org/TR/did-1.0/

Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (2024). https://eur-lex.europa.eu/eli/reg/2024/1183/oj

Richter, D., & Anke, J. (2021). Exploring potential impacts of self-sovereign identity on smart service systems. *Business Information Systems*, 105–116. https://doi.org/10.52825/bis.v1i.68

Richter, D., & Anke, J. (2024). Getting to know your customer: Onboarding in an urban mobility ecosystem. *19th International Conference on Wirtschaftsinformatik,* Würzburg, Germany. https://aisel.aisnet.org/wi2024/76

Richter, D., Praas, C. R., & Anke, J. (2023). Beyond paper and plastic: A meta-model for credential use and governance. *European Conference on Information Systems.* Symposium conducted at the meeting of Association for Information Systems, Kristiansand, Norway. https://aisel.aisnet.org/ecis2023_rp/371/

Rieger, A., Roth, T., Sedlmeir, J., Fridgen, G., & Young, A. (2024). Organizational identity management policies. *Journal of the Association for Information Systems, 25*(3), 522–527. https://doi.org/10.17705/1jais.00887

Roeber, B., Rehse, O., Knorrek, R., & Thomsen, B. (2015). Personal data: How context shapes consumers' data sharing with organizations from various sectors. *Electronic Markets, 25*(2), 95–108. https://doi.org/10.1007/s12525-015-0183-0

Sartor, S., Sedlmeir, J., Rieger, A., & Roth, T. (2022). Love at first sight? A user experience study of self-sovereign identity wallets.

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, 12*, 16151–16177. https://doi.org/10.1109/ACCESS.2024.3357940

Schäfer, F., Rosen, J., Zimmermann, C., & Wortmann, F. (2023). Unleashing the potential of data ecosystems: Establishing digital trust through trust-enhancing technologies. *European Conference on Information Systems,* Kristiansand, Norway. https://aisel.aisnet.org/ecis2023_rp/325

Schellinger, B., Sedlmeir, J., Willburger, L., Strüker, J., & Urbach, N. (2022). *Mythbusting Self-Sovereign Identity (SSI): Diskussionspapier zu selbstbestimmten digitalen Identitäten.* Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT. https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1426/wi-1426_deutsch.pdf

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2021). Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. *Information & Management*, 103553. https://doi.org/10.1016/j.im.2021.103553

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

Sedlmeir, J., Barbereau, T., Huber, J., Weigl, L., & Roth, T. (2022a). Transition pathways towards design principles of self-sovereign identity. *International Conference on Information Systems*. https://aisel.aisnet.org/icis2022/is_implement/is_implement/4

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

Sellung, R., & Kubach, M. (2023). Research on user experience for digital identity wallets: state-of-the-art and recommendations. *Open Identity Summit 2023*, *volume P-335*, 39-. https://dl.gi.de/items/ff98be0e-ab17-4993-89dc-abebefaecf64

Smethurst, R. (2023). Digital identity wallets and their semantic contradictions. *European Conference on Information Systems*. https://aisel.aisnet.org/ecis2023_rp/288

Smith, S. M. (2021). Decentralized key management. In A. Preukschat & D. Reed (Eds.), *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials* (pp. 220–247). Manning Publications.

Smith, B., Loddo, O. G., & Lorini, G. (2020). On credentials. *Journal of Social Ontology, 6*(1), 47–67. https://doi.org/10.1515/jso-2019-0034

Smith, H. A., & McKeen, J. D. (2011). The identity management challenge. *Communications of the Association for Information Systems*, *28.* https://doi.org/10.17705/1CAIS.02811

Spiekermann, S., & Korunovska, J. (2017). Towards a value theory for personal data. *Journal of Information Technology, 32*(1), 62–84. https://doi.org/10.1057/jit.2016.4

Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K.-L. (2015a). The challenges of personal data markets and privacy. *Electronic Markets, 25*(2), 161–167. https://doi.org/10.1007/s12525-015-0191-0

Spiekermann, S., Böhme, R., Acquisti, A., & Hui, K.-L. (2015b). Personal data markets. *Electronic Markets, 25*(2), 91–93. https://doi.org/10.1007/s12525-015-0190-1

Spiekermann, S., Krasnova, H., Hinz, O., Baumann, A., Benlian, A., Gimpel, H., Heimbach, I., Köster, A., Maedche, A., Niehaves, B., Risius, M., & Trenz, M. (2022). Values and ethics in information systems. *Business & Information Systems Engineering, 64*(2), 247–264. https://doi.org/10.1007/s12599-021-00734-8

Sporny, M., & Sabadello, M. (2025). *DID Methods: Known DID Methods in the Decentralized Identifier Ecosystem.* W3C. https://www.w3.org/TR/did-extensions-methods/

Sporny, M., Longley, D., & Chadwick, D. W. (2022). *Verifiable credentials data model v1.1: W3C Recommendation.* W3C. https://www.w3.org/TR/vc-data-model/

Sroor, M., Hickman, N., Kolehmainen, T., Laatikainen, G., & Abrahamsson, P. (2022). How modeling helps in developing self-sovereign identity governance framework: An experience report. *Procedia Computer Science, 204*, 267–277. https://doi.org/10.1016/j.procs.2022.08.032

Sule, M.-J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: Issues and trends. *Technology in Society, 67*, Article 101734. https://doi.org/10.1016/j.techsoc.2021.101734

UN/CEFACT (2022). *White Paper: eDATA Verifiable Credentials for Cross Border Trade*. https://unece.org/sites/default/files/2023-10/WhitePaper_VerifiableCredentials-CrossBorderTrade.pdf

Vargo, S. L., & Lusch, R. F. (2016). Institutions and axioms: An extension and update of service-dominant logic. *Journal of the Academy of Marketing Science, 44*(1), 5–23. https://doi.org/10.1007/s11747-015-0456-3

von Scherenberg, F., Hellmeier, M., & Otto, B. (2024). Data sovereignty in information systems. *Electronic Markets, 34*, 15. https://doi.org/10.1007/s12525-024-00693-4

Wang, F., & Filippi, P. (2020). Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. *Frontiers in Blockchain, 2*, Article 28. https://doi.org/10.3389/fbloc.2019.00028

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), Article 101873. https://doi.org/10.1016/j.giq.2023.101873

Windley, P. J. (2023). *Learning Digital Identity*. O'Reilly Media, Inc. https://learning.oreilly.com/library/view/learning-digital-identity/9781098117689/

Yan, Z., Zhao, X., Liu, Y., & Luo, X. (2024). Blockchain-driven decentralized identity management: An interdisciplinary review and research agenda. *Information and Management, 61*(7), 104026. https://doi.org/10.1016/j.im.2024.104026

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