Transition Pathways towards Design Principles of Self-Sovereign Identity

Completed Research Paper

Johannes Sedlmeir
FIM Research Center
Bayreuth, Germany
johannes.sedlmeir@fim-rc.de

Jasmin Huber
University of Bayreuth
Bayreuth, Germany
jasmin.huber@uni-bayreuth.de

Tom Barbereau
Linda Weigl
Tamara Roth
SnT, University of Luxembourg
Luxembourg, Luxembourg
{tom.barbereau, linda.weigl,
tamara.roth}@uni.lu

Abstract

Society's accelerating digital transformation during the COVID-19 pandemic highlighted clearly that the Internet lacks a secure, efficient, and privacy-oriented model for identity. Self-sovereign identity (SSI) aims to address core weaknesses of siloed and federated approaches to digital identity management from both users' and service providers' perspectives. SSI emerged as a niche concept in libertarian communities, and was initially strongly associated with blockchain technology. Later, when businesses and governments began to invest, it quickly evolved towards a mainstream concept. To investigate this evolution and its effects on SSI, we conduct design science research rooted in the theory of technological transition pathways. Our study identifies nine core design principles of SSI as deployed in relevant applications, and discusses associated competing political and socio-technical forces in this space. Our results shed light on SSI's key characteristics, its development pathway, and tensions in the transition between regimes of digital identity management.

Keywords: Certificate, digital wallet, distributed ledger, innovation, public key infrastructure, verifiable credential

Introduction

According to Kim Cameron, Microsoft's former Chief Architecture of Identity, "the Internet was built without a way to know who and what [people] are connecting to" (Cameron, 2005). It typically only allows the identification of physical endpoints and the associated organizations (Tobin and Reed, 2016). End-users experience this design daily when they interact with the servers of digital service providers using an https connection (Preukschat and Reed, 2021). Servers identify themselves with cryptographic key pairs and SSL certificates, i.e., documents that are electronically signed by one of a few dozen global "certificate authorities" (Soltani et al., 2021). The resulting public key infrastructure (PKI) can thus be considered the Internet's equivalent of a public "address book" or "telephone book" for public entities, maintained by a list of reputed organizations (Adams and Lloyd, 2003). Through its integration into web browsers and mobile applications, it provides the backbone of today's trusted interactions via the Internet (Jøsang, 2014).

Despite the apparent success of digital certificates, they are rarely extended to end-users. One of the few examples include the European Union's Digital COVID certificates (Rieger et al., 2021) and the introduction of staff passports for the United Kingdom's national health service during the pandemic (Lacity and Carmel, 2022). Instead, end-user identities are typically managed through *siloed* and *federated* systems (El Maliki and Seigneur, 2007). In the siloed approach, users need to register a new account for each digital service that they interact with. Oftentimes, these accounts are just a combination of an identifier, such as a username or an e-mail address, and a credential to prove control over the identifier, such as a password or a smartcard (Whitley et al., 2014). Registering or maintaining an account may also involve filling in registration forms and visiting a company branch or government office that verifies claims such as the possession of a valid driver's license (Sedlmeir et al., 2021). Resulting records can be verified by the digital service provider and stored on its servers, so simplifying future verification processes. However, manual registration and the secure management of passwords for sometimes hundreds of digital services presents a substantial challenge and inconvenience to end-users (Bonneau et al., 2012). Related challenges for companies and governments lie in maintaining security, supporting operations, and manually verifying users' attributes (Schlatt et al., 2021; Smith and McKeen, 2011).

To address these downsides, dedicated identity providers (IdPs) entered the market (Maler and Reed, 2008). Examples for IdPs are companies like Google and Microsoft and government agencies like the Unique Identification Authority of India (Sedlmeir et al., 2021). As in the siloed approach, IdPs store (and to some extent verify) their users' identity attributes. Additionally, they enable users to authenticate with other service providers that connect with the IdP using their IdP account. Technically, when logging in to a digital service, users are redirected to their IdP, where they sign in with their corresponding credential. The IdP then forwards an attestation of the required identity attributes to the service provider (Madsen et al., 2005; Maler and Reed, 2008). As the resulting network of IdPs and digital service providers resembles a federation, this identity paradigm is called federated identity management (Maler and Reed, 2008). While the "single sign-on" experience of the federated approach is efficient and convenient for users, it is often criticized for the centralized storage of identity data and corresponding cyber-security risks and surveillance risks. Moreover, IdPs often monetize their users' identity and usage data (van Bokkem et al., 2019; Zuboff, 2015), taking powerful market positions. Federated identity management also has not yet addressed the lack of machine-verifiable digital representations of core identity-related documents such as passports, driver's licenses, or diplomas (Sedlmeir et al., 2021).

The shortcomings of the siloed and federated approaches have led to growing interest in a *user-centric* and *decentralized* digital identity paradigm (El Maliki and Seigneur, 2007; Kubach et al., 2020; OECD, 2011). Attempts to implement this paradigm in the context of e-commerce and enterprise IT systems date back to the early 2000s (Backes et al., 2005; Chadwick et al., 2003). These endeavors have ultimately led to the concept of self-sovereign identity (SSI) – an expression of personal digital sovereignty. It emerged as a "technological niche" (Geels, 2004) among digital identity communities, most notably, the Internet Identity Workshops (IIWs), which previously played a major role in the development of federated identity standards (Preukschat and Reed, 2021). Subsequently, Allen (2016), who was a leading figure in incubating SSI, coined the term as a principle-based framework for a decentralized system of user-centric digital identities. His "10 principles of SSI" provide the first definition of SSI. At that time, there were no relevant reference standards or practical experiences with the large-scale deployment of SSI-based systems and their interaction with the regulatory, technical, and economic environment. Since then, through inter- and intra-organizational proofs of concept and pilot projects in businesses and public services, SSI has evolved considerably (Schellinger et al., 2022). Different technological components of SSI and various identification and authentication scenarios were explored (Sedlmeir et al., 2021; Soltani et al., 2021). However, the development of guidelines and design considerations for SSI system implementation or evaluation has stalled or, at best, evolved in heterogeneous directions based on no or weak scientific evidence. For instance, Allen's principles stem from a blog post and mainly focus on libertarian values like autonomy and privacy; yet, applications of SSI in industry and e-government also require specific authenticity and accountability guarantees (Kubach et al., 2020). Moreover, regulatory aspects like the different "levels of assurance" formulated in the European electronic Identification, Authentication and Trust Services (eIDAS) regulation impact practical SSI implementations (Schellinger et al., 2022; Schwalm et al., 2022). The continuous innovation and evolution process within the SSI community hence cannot be viewed merely from a techno-centric per-

spective. Indeed, the concepts of "sovereignty" and "decentralization" in the context of digital identity are contested (Sedlmeir et al., 2021) and subject to different interpretations according to actors' social and institutional context (Weigl et al., 2022). Consequently, SSI-solutions should be understood and analyzed as innovations with "political-economic dimensions" (Dijck and Jacobs, 2020).

Related research on SSI is scarce and has not captured this context thus far. As a result, "SSI is still only loosely defined" (Mühle et al., 2018) and there seems to be no updated definition of SSI that includes both practitioners' and researchers' perspectives. The academic debate on SSI is also fuzzy: while initially scholarship emphasized the role of blockchain as an essential technological building block (e.g., Koens and Meijer, 2018; Mühle et al., 2018), more recent research suggests a smaller role for blockchain (Schlatt et al., 2021). In the last years, there has been a noticeable trend towards, among others, a stronger focus on applications in regulated domains, user experience, privacy-oriented implementations, and the bundling of attestations (Feulner et al., 2022; Sartor et al., 2022; Schwalm et al., 2022; Soltani et al., 2021). Harmonized design principles (DPs) are required for research and practice, e.g., to evaluate identity management concepts and solutions consistently and not only from a techno-centric and deductive perspective (e.g., see Koens and Meijer (2018)). Considering the diversity of technical niche innovations, socio-technical developments, and the influence of an exogenous landscape which impacted the adoption of SSI, we believe that a rigorous and timely assessment of the key characteristics of SSI is required. We provide an updated model in the form of DPs for SSI that supplements the libertarian concept as introduced by Allen (2016) with influences of the technical environment as well as regulatory and business requirements in terms of accountability, authenticity, and trust structures.

To derive these principles, we use the multi-level perspective (MLP) by Geels and Schot (2007) as a theoretical lens to retrace the *transition pathway* of SSI from a technological niche towards a mainstream concept. Through this theoretical lens, we derive the DPs following a design science research (DSR) study (Hevner et al., 2004; Peffers et al., 2007). We introduce Geels and Schot's MLP and use it to give a first, informal overview of different SSI-related historical milestones and evolutions in identity management. They illustrate the complexity of technical foundations and paths involved, and highlight the need for multi-faceted research to formally structure and map these developments (Whitley et al., 2014). Next, we present our DSR, which involves a systematic literature review (SLR) to develop the initial version of DPs for SSI and four subsequent iterative refinement and evaluation cycles in which we interview 15 experts from academia and businesses on SSI. We then discuss the implications of the developed DPs for the area of SSI, especially in the context of Allen's principles. We also point to related tensions that we observed in SSI's transition from being principally a libertarian theoretical construct to a practical identity management paradigm. Finally, we summarize our findings and outline the need for further developments and research in the area of SSI.

Background

Digital identity management models can be viewed as socio-technical constructs undergoing a permanent process of innovation (Seltsikas and O'Keefe, 2010; Smith and McKeen, 2011; Whitley et al., 2014). Leaning on Science and Technology Studies (STS), questions pertaining to technology development build on theories of technological entrenchment and strategies to incubate or sustain novel technologies. The concept of entrenchment stems from the idea that "when change is easy, the need for it cannot be foreseen; [though] when the need for change is apparent, change has become expensive, difficult, and time-consuming" (Collingridge, 1980). That is, the convenience of an established solution, called the "entrenched" solution, makes change difficult to achieve as neither social nor economic or political drivers for change exist (Geels, 2002). Over the past 40 years, numerous researchers have analyzed this phenomenon in the context of technological innovations (e.g., Callon, 1986; Hughes, 1983). They assume innovation takes place in protected niches where technologists safely develop and improve their technology, which – over time – "stabilizes as the outcome of successive learning processes" to form new regimes (Geels, 2004).

The multi-level perspective (MLP) was introduced as part of STS and dissects the innovation process in terms of 'technological niches", the established "socio-technical regime", and the larger "exogenous landscape" (Geels, 2004). Respectively, the framework consists of three levels –- the micro, meso, and macro

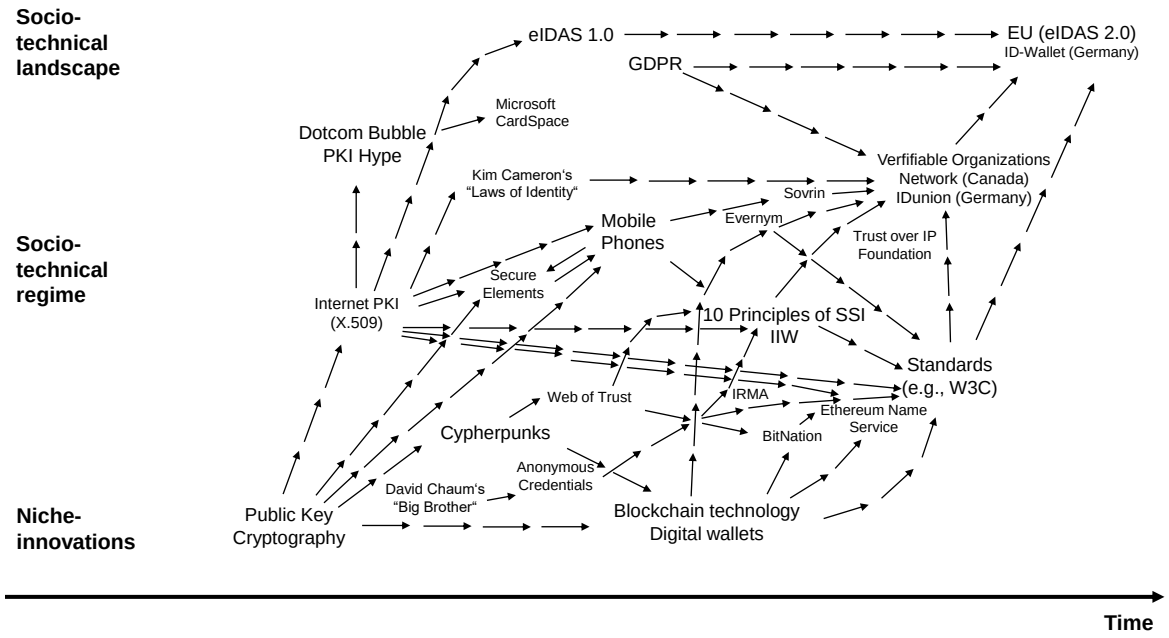

Figure 1. Multilevel perspective on selected key events and their interdependencies in identity management.

level – upon which different selection factors apply to drive innovation and shape technology development. Technological niches construct the framework's micro-level. At this level, radical novelties emerge, that is, innovations deviating considerably from the existing regime. Established regimes reside at the meso level and are often characterized by lock-in and path-dependent mechanisms of economic, social, organizational, or political nature (Geels, 2002). Lastly, the macro level contains the wider exogenous landscape in terms of the socio-political and economic conditions that may change and create "windows of opportunity" through which niche innovations can emerge (Geels, 2004; Geels and Schot, 2007). We aim to use the MLP as a theoretical lens to consolidate and contextualize the phenomenon of SSI-based identity management. Moreover, our work contributes to the stream of Information Systems research that explores technical opportunities and policy recommendations as well as more general managerial and societal questions associated with the development of identification technologies (Sedlmeir et al., 2021; Whitley et al., 2014). Prior to doing so, the development of SSI ought to be contextualized within past regimes. Hence, by adopting the MLP, Figure 1 structures the key events and their influences on the evolution of SSI that we present in the following.

Public key cryptography can be considered the most foundational part of both the existing trust layer on the Internet and implementations of SSI. While originally invented by Ellis and Cocks in 1973/74, the first publication by Rivest et al. (1978) resulted in an instantiation of the eponymous RSA cryptosystem. Public key cryptography uses one-way functions to derive a public key – typically a large number that can be considered a non-human-readable identifier – from a randomly generated secret key. The ownership of the key pair, i.e., knowledge of the secret key, can be proven mathematically without disclosing the secret key itself. The mathematical connection between the secret key as credential and the public key as identifier also opens up new opportunities for digital identity management beyond mere authentication. When it comes to presenting identity attributes for the purpose of identification or authorization, these can be verifiably claimed through digital certificates. That is, an "issuer" – either a reputed person or an organization known by its public key – uses its own secret key to electronically sign a document that lists the subject's public "binding" key along with its other identity attributes. An identity subject can then send this digital certificate and a proof of ownership of the binding key in a *verifiable presentation* directly to a relying ("verifying") party, for

instance, to a service provider. The latter can cryptographically check the integrity of this digital certificate based on the issuer's digital signature. Provided that the verifying party trusts the issuer, it can then rely on the attested attributes. In the context of institutions and their digital services, this has evolved into today's system of X.509 certificates for servers and the Internet's PKI (Chadwick et al., 2003). Within the MLP, we understand PKI standards and related infrastructural components as a socio-technical regime that received significant adoption with the Dotcom bubble, became stable, and remained widespread through its crucial role for https-based communication.

"Cypherpunks" is the name given to libertarian and privacy-oriented communities that make use of cryptographic tools to pursue their goals (Narayanan, 2013). Some of these groups made early attempts to create a "Web of Trust" using cryptographic key pairs and digital certificates, issued by end-users for end-users (Zimmermann, 1995). An example of this is the implementation of "Pretty Good Privacy". In the early 2000s, attempts were made to base these efforts on institutional trust instead of social trust. A key goal was to improve digital identity management in areas such as e-commerce or enterprise IT by extending the Internet's PKI for organizations and their servers to use by individuals. They used, for instance, smartcards that securely store key pairs and certificates issued by the users' employers (Chadwick et al., 2003). While the vision to extend this user-centric and cryptography-oriented approach failed to gain large-scale traction, it prevailed for some time in niche communities. This mostly included computer scientists and cypherpunks who took seriously Chaum's warnings of surveillance threats on the Internet and corresponding spillover effects on society (Chaum, 1985, "Big Brother"). They explored cryptographic tools to minimize information exposure during a verifiable presentation. In cryptography research, this led to innovative solutions. In contrast to established digital certificates, anonymous credentials (also called attribute-based credentials) facilitate zero-knowledge proofs to provide data-minimal evidence on the ownership of a digital certificate and required attributes. That is, an anonymous credential allows to derive verifiable presentations without revealing all the attributes that it attests. It also allows to avoid the disclosure of an associated unique identifier, such as the binding public key or the value of the issuer's digital signature (Backes et al., 2005; Camenisch and Lysyanskaya, 2001). IRMA ("I Reveal My Attributes") was one of the first practical implementations of these anonymous credentials (Alpár and Jacobs, 2013). Besides privacy, niche innovations also emerged in communities of cryptographers and cypherpunks who sought to minimize the involvement of trusted third parties like certificate authorities. After Bitcoin and blockchain technologies gained a broader foothold, actors driven by libertarian values saw opportunities to establish a registry for digital identities by mapping individuals to their public keys on a transnational digital infrastructure. This rekindled interest in using public key cryptography for end-users' identity management resulted in projects like BitNation (Kuperberg, 2019). In addition, the popularity of tools to manage cryptocurrencies made citizens and decision-makers in industry and politics aware of the opportunities of identity management via digital wallets applications on smartphones (Jørgensen and Beck, 2022; Sartor et al., 2022).

The term SSI was coined by Allen (2016) in a blog post. His "principles of SSI" encompass users' independent *existence* (1); the *control* (2) they must have over their identities; the *access* (3) users are granted to their own data; the *transparency* (4) of related systems and algorithms' implementation; the *persistence* (5) of identities for as long as users wish; the *portability* (6) of attestations tied to users' identities; *interoperability* (7); *consent*-based (8) sharing of users' identity data; privacy through disclosure *minimalization* (9); and, finally, users' rights *protection* (10). The concept has since become a focal topic far beyond the relatively narrow focus of the half-yearly IIW conferences (Čučko and Turkanović, 2021; Soltani et al., 2021). While gathering "internal momentum" (Geels and Schot, 2007), the principles stipulated within this group soon became reference points for SSI solutions. In parallel, the first blockchain-based implementations of SSI appeared, such as Evernym's solution based on what later became Hyperledger Indy and Aries. Their efforts significantly influenced technical and non-technical standards, which were refined from a governance perspective, for instance, by Sovrin and the Trust over IP foundation and from a technical perspective by the World Wide Web Consortium (W3C) and the Decentralized Identity Foundation. Arguably, the two most important standards in the context of SSI are "decentralized identifiers" – public keys enriched with meta-data – and "verifiable credentials" – digitally signed attestations that offer higher flexibility with regard to semantics and that enable them to incorporate meta-data and features of anonymous credentials (Sedlmeir et al., 2021). Within these smaller regimes, respective socio-technical configurations for SSI were established.

The configurations in individual regimes, however, are not homogeneous. Instead, they can be considered "sequences of multiple component-innovations" (Geels and Schot, 2007) that are continuously reconfigured and converge into a solution. The heterogeneity in configurations manifests itself, for instance, in the contested use of blockchain as a component. The realization that pseudonymous public keys do not provide sufficient privacy (Sedlmeir et al., 2022), and that the immutability of a blockchain is not required for digital attestations signed by an issuer (Schlatt et al., 2021), diminished the role of blockchain in more recent SSI implementations. In many projects, end-users' identifiers, endpoints, and attestations are now exclusively stored in digital wallets on their devices. A blockchain then at most hosts the PKI for public institutions as well as revocation registries (Lacity, 2022; Schlatt et al., 2021). This can be seen, for instance, in Canada's Verifiable Organizations Network, the European cooperative society IDunion, and the European Self-Sovereign Identity Framework's technical approaches. SSI projects are often tied to dynamics in the socio-technical landscape. Ongoing political initiatives, like the revision of the European eIDAS regulation and the desire to establish a German ID Wallet, manifest the attention SSI has obtained from the regulatory domain. The development of SSI for identity management hence reflects the interplay of the MLP's different levels and the corresponding technical, socio-economical, and political selection factors. SSI is often hailed as a revolutionary innovation, yet its implementations are not considerably different from early proposals of using PKI and anonymous credentials stored on end users' portable computing devices (Backes et al., 2005; Chadwick et al., 2003). Arguably, public key cryptography alone contributes significantly to more secure and efficient identity management (Bonneau et al., 2012). Blockchain technology, which is still a component of many instantiations of SSI, only plays a minor role from a technical perspective (Schlatt et al., 2021). Yet, it appears to have contributed to its initial broad-based hype, as previous moderate attempts to lobby for the adoption of public key cryptography and digital certificates by end-users in research (e.g., Rannenberg et al., 2015) and policy (e.g., eIDAS) have not received the anticipated widespread adoption (Kubach et al., 2020). This mirrors Geels (2004)'s proposition that despite technical superiority over the incumbent technical solution, other factors beyond the technological regime influence successful adoption of a new regime. Since SSI connected with blockchain technology, there has been somewhat unprecedented support from political decision makers (Weigl et al., 2022).

Research Approach

For our DSR approach, we first identified the problem space to obtain descriptive knowledge on SSI solutions that researchers currently discuss through an initial SLR (Gregor and Hevner, 2013; vom Brocke et al., 2020). We then gathered qualitative data from the SLR and subsequent 15 expert interviews (Sonnenberg and vom Brocke, 2012). During data collection, we challenged, validated, and refined our tentative results against current practices and discussion in IT development and industry in iterative rephrase-and-evaluate loops (Gregor and Hevner, 2013; Hevner et al., 2004; Peffers et al., 2007). In this process, the MLP allowed us to contextualize our findings from the SLR on the various characteristics of SSI and the trajectories of its technical constituents. To integrate existent design knowledge into our endeavor to create additional, generalizable design knowledge (vom Brocke et al., 2020), we focused on the present solution space of SSI. More specifically, we reviewed and consolidated existing DPs from literature and SSI projects in a DSR study to derive DPs for SSI as a form of decentralized digital identity management. As related developments are driven by both theory and practice (Allen, 2016; Camenisch and Lysyanskaya, 2001; Preukschat and Reed, 2021; Whitley et al., 2014), DSR allowed us to consolidate observations from either perspective. A first set of DPs typically builds on Ω-knowledge or descriptive knowledge, which conveys an understanding of the laws and regularities of an observed phenomenon. Subsequent evaluation and sense-making processes then help derive a finite set of DPs, commonly referred to as Λ-knowledge or prescriptive knowledge (Gregor and Hevner, 2013; vom Brocke et al., 2020). According to the knowledge contribution framework, our DSR approach follows the precept of *exaptation*. Exaptation requires the extension of a known solution to new problems (Gregor and Hevner, 2013). Digital identity management is a well-known research topic (Smith and McKeen, 2011; Whitley et al., 2014) and often makes use of cryptographic components. Yet, the challenges we identified in the Introduction section have necessitated a paradigm shift. Current design knowledge, however, is often too unspecific and applications too versatile to derive generally accepted DPs for SSI (Preukschat and Reed, 2021). To address this problem, we consolidate existing and extend current design knowledge in generalizable and actionable DPs (Gregor and Hevner, 2013).

In line with Webster and Watson (2002) and Fink (2005), we extracted 2,504 publications from 14 databases, including ACM DL, IEEE Xplore, ScienceDirect, Scopus, Springer Link, Web of science, and Google scholar for our SLR. We started with two initial search strings, "self-sovereign identity" and "self-sovereignty", to get an overview of current research on SSI. We used the initial results to extract additional relevant keywords that had not yet been included in our search string. Owing to the close connection between blockchain and SSI communities as discussed in the Background section, our final search string then comprised keywords from the identity and blockchain realm: "self-sovereign identity" OR self-sovereignty OR (identity AND (blockchain OR decentrali*ed)). The term "decentralized", as influenced by Kuperberg (2019), seems an essential characteristic of SSI and inextricably linked to the concept, also through its strong link to blockchain communities (Weigl et al., 2022). In a title screening, we identified 84 publications as potentially being relevant. After a detailed full-text analysis of these contributions and applying inclusion (detailed discussion or use of design or evaluation criteria for SSI systems) and exclusion criteria (no English language, article not accessible, purely cryptographic content), 14 publications remained. A subsequent forward and backward search (Fink, 2005; Webster and Watson, 2002) yielded another 8 publications, seven of which are gray literature, technical standards (e.g., by the W3C), or laws (the EU's General Data Protection Regulation (GDPR)). Yet, two of the most popular contributions on SSI (Allen (2016) and Cameron (2005)) could not be extracted with our SLR, as they represent blog posts that are typically not listed in academic databases. We included these two contributions in our knowledge base since they contain essential definitions of SSI and discussions about key requirements.

Our approach towards DPs for SSI-based digital identity management follows the two modes of "kernel theory to design entity grounding" and "design entity to design theory grounding" to enrich the current knowledge base (vom Brocke et al., 2020). The evaluation of various approaches to implement SSI based on our SLR in combination with information retrieved from the basket of literature and projects on identity management referenced in the Introduction and Background sections helped us to derive design requirements. These served as solution fitness criteria for the challenges of digital identity management from the perspective of end-users, businesses, and regulators. Evaluations of existing approaches additionally delivered design features that we included in the development of a first set of DPs (Gregor and Hevner, 2013; vom Brocke et al., 2020). To increase their projectability, we evaluated and complemented them in four iterative evaluation cycles. The outcome was a nascent design theory in the form of a consolidated set of DPs (Hevner et al., 2004; Peffers et al., 2007; vom Brocke et al., 2020). Throughout this iterative process, we followed the suggested procedure of Hevner et al. (2004) to refine the DPs in 15 evaluation interviews with six researchers and nine industry experts, who are all highly esteemed in the field of SSI design and implementation. The practitioners represent relevant organizations and projects from niche innovations and the socio-technical regime (some have multiple of the following roles): Five interviewees have been regular attendees and presenters at last years' IIWs, and eight of them are actively involved in SSI-related standardization bodies like Sovrin, the Trust over IP foundation, and the W3C. Two interviewees are among the four editors of the W3C decentralized identifiers standard, which is also co-authored by Christopher Allen. Five interviewees are in leading positions for the implementation of the Verifiable Organizations Network or the IDunion project within their company, and four of them represent businesses that develop cloud and edge SSI wallets in Europe and North America. Moreover, we communicated our findings beyond exchanging ideas in the expert interviews as recommended for the DSR (Hevner et al., 2004). This included presentations of our work at the IIW, where it served as a discussion basis for the Principles of SSI, which were later – including adjustments – published by the Sovrin Foundation (2021). This work also considerably influenced a related compilation by the Trust over IP Foundation (2021). The aim of the interviews was to ensure the parsimony of our DPs for the creation of SSI-based solutions. To achieve parsimony, we controlled for the completeness, usefulness, and understandability of our DPs throughout the interviews. Interviewees were each encouraged to review the entire list of DPs and to provide (1) additions to the list, (2) reframing of existing DPs, and (3) changes to the definition of DPs. We also discussed openly the current state of decentralized digital identity management as well as the technical and social foundations, opportunities, and challenges of these approaches as perceived by the interviewees. The semi-structured interviews hence allowed the interviewees to elaborate on their professional perspective of SSI. We conducted each interview remotely. The interviews lasted between 30 and 60 minutes and were audio-recorded and transcribed afterwards. We refrained from scheduling new interviews once we reached a point where the interviewees provided us with

almost identical feedback and did not suggest any further additions (Myers and Newman, 2007). For both the coding of selected literature and the interviews, we performed a two-stage process of inductive and deductive coding, as recommended by Miles et al. (2018). That is, two authors first separately analyzed the data, assigning codes to identify factors relevant to the design of SSI applications. They then abstracted these codes into higher-level concepts, i.e., our first tentative DPs from literature (deductive coding) and their refinement during the analysis of the interviews (inductive coding). After the literature coding and every fifth interview, the independent authors compared and discussed their results where diverging (Miles et al., 2018).

We connected the DPs with our kernel theory, the MLP, by discussing them against the backdrop of SSI's trajectory through the socio-political landscape and its interaction with legacy systems. This should ensure the relevance of our DPs (Hevner et al., 2004; Peffers et al., 2018) and, moreover, demonstrate that SSI as a form of decentralized digital identity management has developed from a radical niche to an acknowledged design (Geels, 2004; Geels and Schot, 2007) in private- and public-sector applications (Schlatt et al., 2021; Soltani et al., 2021). That is, our nascent design theory can be categorized as a design relevant explanatory or predictive theory. Our DPs enrich theories that have been relevant to initial design choices (Kuechler and Vaishnavi, 2012) such as those defined by Allen (2016). Our discussion of the resulting DPs through the lens of MLP additionally epitomizes the ascendance of technologies into broad-based adoption and provides an outlook for how SSI could further develop (Geels, 2004; Geels and Schot, 2007).

Findings

In the SLR coding process, we focused on identifying design requirements and design features for SSI management systems. While both design requirements and design features are often broad, they provide the basis for the formulation of DPs (Hevner et al., 2004; vom Brocke et al., 2020). Some requirements within the literature are already formulated as DPs (e.g., Allen (2016) and Tobin and Reed (2016)) but – dependent on their definition and relative position in the history of SSI development – may only cover a fraction of what may be relevant to date. We clustered these design requirements and features into a first set of nine DPs. In the following evaluation rounds, we added and removed one DP and adapted the remaining DPs until we reached a point where three subsequent interviews did not propose any meaningful changes. We first present the tentative DPs compiled on the basis of the SLR, and subsequently describe the changes implemented during the refinement cycles.

From Design Requirements and Features to Tentative Design Principles

DP1: Human Replicate. To account for the target group of SSI-based digital identities, the design requirements "human integration" (Cameron, 2005) and "human requirements [in the form of] privacy [and] empowerment" (Goodell and Aste, 2019) as well as the design feature "biometric interfaces" (Koens and Meijer, 2018) show a clear focus of SSI on natural persons, who seek to play a more active role in the management of their identity-related data. The features "reliable credential management" (Grüner et al., 2019), "data ownership", "data control", "consent to data processing" (Ferdous et al., 2019), and "portability of data" (Tobin and Reed, 2016) further emphasize the purpose of SSI as a collection of attributes related to a natural person. These can be kept for a person's entire life and, upon display, be used to disclose identity attributes. Thus, SSI enables increased agency and independence for natural persons, who wish to manage access to and distribution of their personal data. An identity considered as "self-sovereign" hence needs to be understood as collection of attributes of a real existing human being, but only of the parts they are willing to show – also called partial identities (Clauß and Köhntopp, 2001). Moreover, Abdullah et al. (2019) emphasize the concept of guardianship to give all individuals equal access to using an SSI.

DP2: Control. The design requirement of "deciding on the displayed information" (Ferdous et al., 2019) grants users of SSI "data control" (e.g., Alsayed Kassem et al., 2019; Whitley, 2009; Windley, 2019). How and when their data is being used warrants their explicit "consent to data processing" (Allen, 2016; Alsayed Kassem et al., 2019; Cameron, 2005; Ferdous et al., 2019). Controlling hence limits "what personal data is made available to others" (Whitley, 2009). This also includes the design feature of "updateability" and "revocability of consent" (Moe and Thwe, 2019) and is directly linked to the proposed identity life cycle

of Koens and Meijer (2018), which contains the design features "create, attest, show, prove, renew, delete, and revoke". As such, SSI involves not only consent and control when sharing identity-related information but also "availability", i.e., the identity subject's ability to access and share verifiable information anywhere and at any time (Ferdous et al., 2019). Yet, in the context of verifiability, this does not mean that users should be able to modify all their identity information according to their liking.

DP3: Flexibility. To share their data anywhere and at any time, user-centric applications of SSI need to consider the design features "standardization" and "interoperability" (Allen, 2016; Ferdous et al., 2019; Tobin and Reed, 2016) among the different digital identity management solutions. The feature "pluralism of operators and technologies" (Cameron, 2005) should not hamper the feature "integration" (Kuperberg, 2019) of the various approaches to fulfill the design requirement of a "consistent experience across contexts" (Cameron, 2005). This also includes the design feature "portability of data" (Abraham, 2017; Allen, 2016; Ferdous et al., 2019; Tobin and Reed, 2016) in the form of identity attributes and corresponding attestations to other providers. That is, users should be able to decide which implementation to build upon – including a choice of their digital wallet. They should be empowered to consider their needs, independent of providers, and should be guaranteed interoperability with underlying technical and semantic standards.

DP4: Security. Aside from interoperability and standards, SSI-based solutions must also guarantee for the design requirement "confidentiality" which – besides availability and integrity – constitutes security. It not only entails the design features of "protection" from data accumulation, data fraud, and more powerful entities (Allen, 2016; Tobin and Reed, 2016) but also the limitation of storage and use of information for non-specified purposes as demanded by the GDPR. Overall, users should be protected from unwittingly or mistakenly sharing information with third parties, thus providing "end-to-end security" (Cavoukian, 2009). This includes also purely bilateral communication, end-to-end encryption (Goodell and Aste, 2019), and the verification of the involved verifying party's identity in a verifiable presentation to avoid man-in-the-middle attacks (Toth and Anderson-Priddy, 2019).

DP5: Privacy. Closely related to security is user privacy. In the context of SSI, it generally refers to the minimal disclosure of information, which provides users control over the degree of anonymity in interactions based on the support for unique pairwise pseudonyms for each individual private connection. Relevant design requirements and design features either directly demand "privacy by design and by default" (Cavoukian, 2009) and a high level of "pseudonymity" via pairwise unique digital identities and public keys as well as "private agents" with no storage of private data on the underlying ledger (Alsayed Kassem et al., 2019; Moe and Thwe, 2019; Windley, 2019). This allows to ensure the "unobservability" and "unlikability" (Moe and Thwe, 2019) of user information, if required. Moreover, "selective disclosure" serves as a design feature to reveal only the identity attributes relevant for a specific interaction and purpose (Cameron, 2005; Ferdous et al., 2019; Windley, 2019). Anonymous credentials (Soltani et al., 2018) and zero-knowledge proofs (Stokkink and Pouwelse, 2018; van Bokkem et al., 2019) are often mentioned as technical backbone for such enhanced privacy design features.

DP6: Credibility. Despite the goal of privacy protection, information should be authentic and verifiable also regarding timeliness. This includes the opportunity to revoke attestations from the side of the user in the case of loss or theft of the digital wallet, or or from issuers' side to account for changes of attributes and authorizations (Mühle et al., 2018). One way of implementing these design features without the need to interact with the issuer in a verifiable presentation is through the support for expiration dates and the use of revocation registries (Mühle et al., 2018). Credibility also reflects the design requirements of "transparency" (Abraham, 2017; Allen, 2016; Tobin and Reed, 2016) as well as the design features of "disclosure" (Ferdous et al., 2019), "identity assurance" and "identity verification" (Toth and Anderson-Priddy, 2019).

DP7: Authenticity. Only the respective subject should be able to pass on their data to requesting third parties. Pseudonym or credential sharing among different users, or the creation of new credentials by combining ones that do not belong to a single individual, should not be possible. Such systems exhibit "consistency of credentials", which can, for instance, be achieved through biometric interfaces and hardware-bound link secrets or be disincentivized by corresponding PKI-assured economic bonds or all-or-nothing non-transferability (Camenisch and Lysyanskaya, 2001; Hardman, 2019). If transactions break general

laws or credentials are used in an unauthorized way, global or local anonymity revocation may be useful (Camenisch and Lysyanskaya, 2001; Koens and Meijer, 2018).

DP8: Usability and Performance. Aside from verification and authentication mechanisms as the very core of SSI-based solutions, general concepts of usability must be considered to fulfil the design requirement of "user empowerment" (Abraham, 2017; Alsayed Kassem et al., 2019; Goodell and Aste, 2019). A related requirement, "positive end-user experience" (Kuperberg et al., 2019), plays a major role in delivering other requirements, such as "user trust" – which is essential for acceptance (Seltsikas and O'Keefe, 2010) – and "self-sovereign digital identity management" (Yan et al., 2017). While the "positive end-user experience" mainly complements the design feature of "user-friendly interfaces", it may also concern features such as "scalability" (Koens and Meijer, 2018), "minimum downtime", and "efficient performance" (Camenisch and Lysyanskaya, 2001; Kuperberg et al., 2019). Thus, SSI-based digital identity management approaches require intuitive and easy access personal data, as well as the streamlined and quick sharing of information.

DP9: Future orientation. In addition, the success of SSI largely depends on how well it fits the surrounding environment (Kuperberg et al., 2019). To enable such a fit, there are a number of economic design requirements, including the "prevention of monopolization" as well as "empowerment of businesses" (Goodell and Aste, 2019) and "manageable costs" (Ferdous et al., 2019). These requirements rely heavily on design requirements such as "efficient protocols" (Camenisch and Lysyanskaya, 2001), "organizational flexibility" and "local storage" (Abraham, 2017) as well as design features such as "decentralized governance" (Ferdous et al., 2019; Windley, 2019). Thus, we conclude that SSI-based digital identity management approaches need an innovative environment that allows structural changes to implement SSI, including adaptations of governance and agile management.

Design Iterations

From the first to the second design iteration, we removed the specification of "Human" before the first tentative principle Human Replicate (TDP1). We did this because according to Expert 2 (Practitioner), smart devices and organizations can also use an SSI. Regarding Control (TDP2; DP2), Experts 1 (Researcher) and 2(P) detected potential tensions between increased control (i.e., user empowerment) and an undesirable amount of responsibility that "people now are not used to having". Open-source licensing agreements and legal compliance may be additional determining factors of Flexibility (TDP3; DP3). This was also closely linked to criticism on Credibility (TDP6) and Authenticity (TDP7), which would currently neglect the "rules of trust and basically Web of Trust, where you have to make sure the data coming from the issuer is credible" (Expert 2(P)). Experts 1(R) and 2(P) generally regarded "performance [to be] a subtopic of usability" (TDP8) and both as non-functional requirements instead of a DP, so we adjusted our TDP8 on Usability and Performance accordingly. Regarding Future orientation (TDP9), Expert 2(P) missed "bridging the gap between self-sovereign identity and the existing world of authentication and authorization" to create functional SSI.

From the second to the third design iteration, Security (TDP4; DP5) and Privacy (TDP5; DP5) were highlighted as particularly relevant (Experts 4(P), 6(R)), while the adjusted Usability (TDP8) still appeared to be deficient, neglecting other "important usability factors", such as "ease of use" and literacy, as well as the simplicity of information access. Expert 4(P) considered Future orientation (TDP9) as important, yet more of a requirement than a principle. It would indirectly already be represented in several other DPs, such as Control (TDP2) and Flexibility (TDP3). For Credibility (TDP6), the focus on revocability of consent was too narrow ("revoke the credential if it is a fake passport or whatever"), which is why we took the more general term "revocability" to also account for revocation due to incorrect data. Moreover, we renamed the previously iterated TDP1 Replicate to Representation (DP1), as the term Replicate may be uncommon and difficult to understand.

From the third to the fourth design iteration, we eliminated Future orientation (TDP9). This is because the experts considered an environment with both innovative and legacy features to be more a basic requirement than a DP specific for the implementation of SSI. As the interviewees considered the term of DP1 to be a subset of the principle alongside authentication – "because it is everything, like identification, authentication, and that you exist" (Expert 6(R)) – we renamed and redefined the DP. Regarding Flexibility

Principle	Description (Key features)
DP1: Representation	SSI can represent any entity digitally – human, legal, or technical. (Attributes, authentication, existence, identification, partial identities, persistence)
DP2: Control	Only the actual controller has decision-making power over their digital identity. (Access, manage, ownership, right to be forgotten, single source of truth, update)
DP3: Flexibility	No vendor lock-in: low switching costs, focus on interoperable standards, and open-source projects. (Documentation, integration, no monopoly, portability, standards, transparency)
DP4: Security	State-of-the-art cryptographic tools and authenticated, end-to-end encrypted interactions. (Identification of relying party, key management, protection, secure communication, tamper-proofness)
DP5: Privacy	In each interaction, only the data that is essential for its purpose is revealed. (Bilateral by default, consent, minimized correlation, need to know, selective disclosure)
DP6: Verifiability	The validity and timeliness of credentials can be checked efficiently. (Certificate chain, credential management, machine readability, provability, revocability)
DP7: Authenticity	Credentials are bonded to their initial bearers. (Binding, consistency of credentials, identity fraud protection, limited transferability, risk-based authentication)
DP8: Reliability	There is guidance that helps verifiers to decide which issuers they can trust in a highly dependable infrastructure. (Decentralization, governance, guidance, no single point of failure, public registration, scalability, Web of Trust)
DP9: Usability	Success and durability factors. (Efficiency, end-user experience, minimum downtime, multiple access points, performance, recovery, simplicity, support)

Table 1. Final design principles and their definitions, including key features for implementation.

(TDP3), Experts 5(P) and 11(P) suggested renaming it "openness". We refrained from doing so as it would neglect other essential properties of the principle such as interoperability and portability. In accordance with interview feedback, which offered criticism that it was "too specific" and did not include "more general points" (Expert 9(R)), we redefined Privacy (TDP5). Experts 2(P), 5(P), and 6(R) also suggested redefining Credibility (DP6), as they considered it to be too focused on technological building blocks that yet have to be established. We refrained from adding "decentralization" as a separate DP as it is a basic "prerequisite of the infrastructure" (Expert 5(P)) but added it to Future orientation (TDP9). Moreover, we renamed Credibility (TDP6) to Verifiability (DP6) and redefined Authenticity (DP7).

During the fourth design iteration – which yielded the final and consolidated set of DPs – we received positive feedback from our Experts 13(P), 14(R), and 15(R). In accordance with their feedback, we summarized the current definitions within the most relevant and generalizable core statement and exchanged the order of Usability (TDP8) and Reliability (TDP9) to Usability (DP9) and Reliability (DP8) in line with their perceived importance. Table 1 features the final DPs, including a subset of terms often used in related work and by the interviewees. The DPs characterize SSI as a user-centric "identification infrastructure" (Whitley et al., 2014) based on cryptographically verifiable attestations not only for organizations and their servers but also for end-users, maintained and controlled in digital wallets on their mobile devices (Sedlmeir et al., 2021; Soltani et al., 2021).

Discussion

The derivation of DPs delivered theoretical insights into how to develop design knowledge from such broad-based technological innovations using DSR. At first glance, our derived DPs are similar to the "Ten Principles of SSI" by Allen (2016). When Allen conceived these, SSI was mainly a theoretical concept and a formulation of key characteristics of an identity management that neither had a foundation for technical implementation, nor a history of real-world use. Yet, our SLR has revealed other seminal papers that propose practical design and evaluation criteria for SSI implementations that may be more actionable. Our interviews with practitioners, who work on the adoption of SSI in the public and private sector, allowed us to incorporate their experiences into our assessment.

Using the lens provided by the MLP, a key insight from our iterative DSR evaluation was that different types of regimes apply selection criteria at different velocities. Instead of continuously stabilizing the outcome of successive learning processes to turn innovation into a new regime, the policy regime forced a breakthrough in the implementation of SSI by taking advantage of a perceived "window of opportunity" (Geels, 2004; Geels and Schot, 2007). In the meantime, both the socio-cultural regime and technological regime are still at the stage of negotiation, not yet having produced a dominant design (Sedlmeir et al., 2021; Weigl et al., 2022). This was reflected in our interviews, where several interviewees emphasized that their recommendation on how to best implement SSI-based digital identity management solutions relies on their learning from ongoing IT-projects. Specifically, this involved integration into legacy identity and access management solutions and regulatory constraints. Knowing that SSI is still in a trial phase, and that its long-term success is dependent on negotiation with selection factors of the incumbent socio-technical regime, the interviewees appreciated the overall structure of our nine DPs. Yet, they also indicated that the definitions may require adaption over time as this space becomes increasingly mature.

Our study thus contributes to various levels of the current research discussions. Theoretically, it presents a novel way of combining a constructivist theoretical lens from STS with the design science paradigm. Thereby, it adds to the epistemological diversity in the Information Systems field. As a result, our study does not only address the gap of a missing theory or framework on identity management, it also introduces a new theoretical perspective of kernel theory development. It does this through critical reflection about the materiality and non-materiality of the observed construct, thus bypassing the positivist and techno-centric presumptions that often form the basis of DSR (McKay and Marshall, 2005; Niehaves, 2007). Practical implications, on the other hand, can be drawn from the iterative refinement of our DPs with the interview partners. They provide a common denominator for research on SSI and the development and evaluation of corresponding identity management systems in practice. The final DPs also allow us to identify several tensions that may be relevant for both researchers and practitioners. These tensions not only pertain to the novelty of SSI but also to the selection environment created by the incumbent regime and the larger exogenous socio-technical landscape of the MLP (Geels, 2004; Geels and Schot, 2007). The tensions also reflect and align with the findings of Weigl et al. (2022), who studied the interpretive flexibility of SSI. Hence, we believe that these tensions represent promising research directions.

Firstly, we observed a tension between selection factors of the policy regime and the socio-cultural regime. The establishment of Data Privacy (DP5) and User Control (DP2) in SSI-based digital identity management solutions may compromise its Applicability (DP6, DP7): For example, aspects such as the theft or sharing of mobile devices were often not sufficiently considered by the originators of this concept. These originators tended to be libertarians and cryptographers whose focus was often on ensuring control and in particular minimal disclosure and anonymity. The result was a lack of unique identifiers for processes that organizations need to consider in practical applications (Allen, 2016; Camenisch and Lysyanskaya, 2001; Cameron, 2005). To mitigate the risk of identity-related fraud with stolen mobile devices or credentials, Tobin (2017) and Koens and Meijer (2018) suggest revocation and escrow mechanisms if credentials are used in an unlawful way or if they contradict the user-specific consistency of credentials (Camenisch and Lysyanskaya, 2001). To retain a high level of privacy, zero-knowledge proofs enable minimum disclosure while compliant with regulation that requires the verification and authentication of a certain amount of user data (Sedlmeir et al., 2021). Yet, the tools currently available for zero-knowledge proofs are difficult to integrate into existing secure elements that facilitate hardware-binding (Schellinger et al., 2022). This currently still leads to

a trade-off between privacy and authenticity that – despite the availability of technical solutions (Delignat-Lavaud et al., 2016; Rosenberg et al., 2022) – has not yet been resolved in practical implementations.

A second tension arises from the conflicting selection forces of the policy regime and the socio-cultural regime. The challenge pertains to the requirement to balance Verifiability (DP6) and Reliability (DP8) against end-user expectations like Control (DP2) and Privacy (DP5). This tension has its roots in the libertarian ideals of minimal disclosure, anonymity support, and full control of users over displayed data – ideals that are commonly associated with SSI (Allen, 2016; Preukschat and Reed, 2021; Weigl et al., 2022). While a milder version of these ideals forms the core of SSI, the verifiable credentials stored in the users' wallets require a trustworthy issuer and a proof of this originator. Trust registries and qualified electronic signatures, as, for instance, implemented in the context of eIDAS, may mediate this tension in the practical implementation of SSI (Schwalm et al., 2022). Should an organization issue an incorrect attestation – whether intentionally or not – the option for revocation must be available (Interviewee 10). It should also be possible to remove an unreliable issuer from certain trust registries. As a result, abandoning information silos is only practical in the cross-domain sense: While issuers are no more involved in verifiable presentations, they still need to store some of the attestation-related information to facilitate potential future revocation.

A third tension emerges from selection factors of the socio-cultural and the technological regimes. This tension pertains to the balance between the desire for maximum flexibility and the functional requirements of Interoperability (DP3). With an initially strong focus on libertarian values (Allen, 2016), the conceptual version of SSI emphasized a high degree of freedom and personalization of the technological application for users (Preukschat and Reed, 2021). This, however, makes interoperability between solutions cumbersome and impairs the desired flexibility to choose a solution that fits individual needs. Consequently, one currently "cannot copy credentials from wallet to wallet [...] and if you want to switch your identity to a different network, that requires reissuing the credentials on the other network" (Interviewee 10). A more "mainstream" version of SSI, thus, would have to mediate between flexibility and interoperability by enforcing some degree of standardization, yet without hampering the portability of digital wallets that hold the cryptographic keys and credentials to avoid vendor lock-in (Allen, 2016; Ferdous et al., 2019; Koens and Meijer, 2018; Yan et al., 2017).

Our DSR study contextualizes the current development and discusses factors that helped develop SSI as a new regime of identity management from a broad, transnational perspective. Yet, we cannot guarantee that we incorporated all relevant events and practical implementations of SSI in this study. We aimed to ensure a comprehensive perspective via using broad search strings, many databases, and forward and backwards searches in our SLR. During the interviews that guided the refinement of DPs, we made inquiries about other interviewees or projects that may be of relevance. Nevertheless, it should be noted that, with the exception of one Asian researcher, all our interview partners were European and North American. Moreover, the interviews were distributed only over 6 months. A more longitudinal study that rigorously analyzes discussions from events (such as the latest IIWs) or amendments in regulatory documents) may be required to consolidate the chronology of changes. Our DPs form a snapshot of the current design knowledge on SSI and a perspective on its pathway through regimes of identity management. Yet, they may be subject to change, not least, from advances in knowledge gained from successful or failed applications of SSI. We will seek better retracing of the selection factors of each regime by conducting further interviews with experts in the respective regimes. In addition, to grasp the considerations of the socio-cultural regime and that of end-users, future research may add a survey-based evaluation.

Conclusion

Our study retraces the historical development of SSI using the MLP as a theoretical lens. Our SLR in combination with DSR delivered a set of nine DPs that consolidate existing design knowledge of the SSI concept. We refined and extended this consolidated knowledge in four iterations with 15 experts from industry and academia. We used the MLP as a frame to help us to better understand the development of the concept of SSI. It was originally introduced mainly by a radical niche, but is now widely taken into account by states and industy consortia. Use currently seems focused in North America and Europe, including the eIDAS 2.0 regulation designed for large-scale productive use. Our work may help to better understand SSI in the con-

text of business and regulated domains and to communicate its key characteristics and technical building blocks to decision makers and end-users. We also discovered tensions between the different negotiating regimes and suggested ways to mediate these. In this context, we elaborated on the difficulties that different velocities of regime negotiation could have on the prudent use of windows of opportunity. The relevance of our research comes from the close interaction with stakeholders who take part in projects in the SSI ecosystem. Aside from direct experience, our research also draws on observations from crucial requirements and real-life failures, as illustrated, for instance, by the German government's digital driver's license. While the knowledge gained from this, and changes to the concept may initially seem to considerably impair SSI's key goal of giving users more control, it also contributed to establishing an open ecosystem of verifiable digital interaction. We learned that if SSI aims to embrace digital identity management in practice, updates to its core principles are indispensable. By establishing consensus on an updated model of SSI that is integrated in regulatory and institutional requirements, our findings also suggest that a perception of SSI as a concept driven by anti-democratic forces owing to its name may be a minor issue (Sedlmeir et al., 2021). Consequently, our contribution indicates that research that consolidates historical influences on SSI may help to mediate tensions and contribute to achieving a feasible identity management solution beyond authentication (Bonneau et al., 2012). Our DPs also aim to provide a common basis for future research on design choices and trends within decentralized digital identity systems. Based on such a common understanding, researchers may tackle some of the remaining open questions concerning the design of SSI-based solutions. This involves, among others, further studying user experience requirements and corresponding success factors (Sartor et al., 2022), investigating the necessity of improved anonymous credential implementations with extended privacy capabilities (Rosenberg et al., 2022), and studying the fitness of technical tools like blockchain for decentralized governance, enhanced availability, or social recovery (Benchaya Gans et al., 2022).

References

Abdullah, A., Breeijen, S. d., Cooper, K., Corning, M., Coutts, O., Cranston, R., Dahl, H., Hardman, D., Hickman, N., and Neubauer, N. (2019). *On Guardianship in Self-Sovereign Identity*.

Abraham, A. (2017). *Whitepaper About the Concept of Self-Sovereign Identity Including its Potential*.

Adams, C. and Lloyd, S. (2003). *Understanding PKI: Concepts, Standards, and Deployment Considerations,* Addison-Wesley Professional.

Allen, C. (2016). *The Path to Self-Sovereign Identity*.

Alpár, G. and Jacobs, B. (2013). "Towards Practical Attribute-Based Identity Management: The IRMA Trajectory," in *IFIP Working Conference on Policies and Research in Identity Management,* Springer.

Alsayed Kassem, J., Sayeed, S., Marco-Gisbert, H., Pervez, Z., and Dahal, K. (2019). "DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network," *Applied Sciences* (9:15).

Backes, M., Camenisch, J., and Sommer, D. (2005). "Anonymous yet Accountable Access Control," in *Proceedings of the ACM Workshop on Privacy in the Electronic Society,* pp. 40–46.

Benchaya Gans, R., Ubacht, J., and Janssen, M. (2022). "Governance and Societal Impact of Blockchain-Based Self-Sovereign Identities," *Policy and Society* (41:3), pp. 402–413.

Bonneau, J., Herley, C., Van Oorschot, P. C., and Stajano, F. (2012). "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," in *Symposium on Security and Privacy,* IEEE, pp. 553–567.

Callon, M. (1986). "The Sociology of an Actor-Network: The Case of the Electric Vehicle," in *Mapping the Dynamics of Science and Technology,* M. Callon, J. Law, and A. Rip (eds.). Palgrave, pp. 19–34.

Camenisch, J. and Lysyanskaya, A. (2001). "An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation," in *International Conference on the Theory and Applications of Cryptographic Techniques,* Springer, pp. 93–118.

Cameron, K. (2005). *The Laws of Identity*. Microsoft.

Cavoukian, A. (2009). *Privacy by Design… Take the Challenge,* Information and Privacy Commissioner.

Chadwick, D., Otenko, A., and Ball, E. (2003). "Role-Based Access Control with X.509 Attribute Certificates," *IEEE Internet Computing* (7:2), pp. 62–69.

Chaum, D. (1985). "Security without Identification: Transaction Systems to Make Big Brother Obsolete," *Communications of the ACM* (28:10), pp. 1030–1044.

Clauß, S. and Köhntopp, M. (2001). "Identity Management and its Support of Multilateral Security," *Computer Networks* (37:2), pp. 205–219.
Collingridge, D. (1980). *The Social Control of Technology,* Open University Press.
Čučko, Š. and Turkanović, M. (2021). "Decentralized and Self-Sovereign Identity: Systematic Mapping Study," *IEEE Access* (9), pp. 139009–139027.
Delignat-Lavaud, A., Fournet, C., Kohlweiss, M., and Parno, B. (2016). "Cinderella: Turning Shabby X.509 Certificates into Elegant Anonymous Credentials with the Magic of Verifiable Computation," in *Symposium on Security and Privacy,* IEEE, pp. 235–254.
Dijck, J. van and Jacobs, B. (2020). "Electronic Identity Services as Sociotechnical and Political-Economic Constructs," *New Media & Society* (22:5), pp. 896–914.
El Maliki, T. and Seigneur, J.-M. (2007). "A Survey of User-Centric Identity Management Technologies," in *International Conference on Emerging Security Information, Systems, and Technologies,* IEEE, pp. 12–17.
Ferdous, M. S., Chowdhury, F., and Alassafi, M. O. (2019). "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," *IEEE Access* (7), pp. 103059–103079.
Feulner, S., Sedlmeir, J., Schlatt, V., and Urbach, N. (2022). "Exploring the Use of Self-Sovereign Identity for Event Ticketing Systems," *Electronic Markets*.
Fink, A. (2005). *Conducting Research Literature Reviews: From the Internet to Paper,* SAGE.
Geels, F. W. (2002). "Technological Transitions as Evolutionary Reconfiguration Processes: A Multi-Level Perspective and a Case-Study," *Research Policy* (31:8-9), pp. 1257–1274.
Geels, F. W. (2004). "From Sectoral Systems of Innovation to Socio-Technical Systems," *Research Policy* (33:6–7), pp. 897–920.
Geels, F. W. and Schot, J. (2007). "Typology of Sociotechnical Transition Pathways," *Research Policy* (36:3), pp. 399–417.
Goodell, G. and Aste, T. (2019). "A Decentralized Digital Identity Architecture," *Frontiers in Blockchain* (2).
Gregor, S. and Hevner, A. R. (2013). "Positioning and Presenting Design Science Research for Maximum Impact," *MIS Quarterly* (37:2), pp. 337–355.
Grüner, A., Mühle, A., Gayvoronskaya, T., and Meinel, C. (2019). "A Comparative Analysis of Trust Requirements in Decentralized Identity Management," in *International Conference on Advanced Information Networking and Applications,* Springer, pp. 200–213.
Hardman, D. (2019). *What If Someone Steals My Phone?* Available at: https://sovrin.org/wp-content/uploads/2019/03/What-if-someone-steals-my-phone-110319.pdf [Accessed: September 29, 2022].
Hevner, A. R., March, S. T., Park, J., and Ram, S. (2004). "Design Science in Information Systems Research," *MIS Quarterly* (28:1), pp. 75–105.
Hughes, T. P. (1983). *Networks of Power: Electrification in Western Society, 1880-1930,* John Hopkins University Press.
Jørgensen, K. P. and Beck, R. (2022). "Universal Wallets," *Business & Information Systems Engineering* (64), pp. 115–125.
Jøsang, A. (2014). "Identity Management and Trusted Interaction in Internet and Mobile Computing," *IET Information Security* (8:2), pp. 67–79.
Koens, T. and Meijer, S. (2018). *Matching Identity Management Solutions to Self-Sovereign Identity Principles*.
Kubach, M., Schunck, C. H., Sellung, R., and Roßnagel, H. (2020). "Self-Sovereign and Decentralized Identity as the Future of Identity Management?," in *Open Identity Summit 2020,* Gesellschaft für Informatik eV, pp. 35–47.
Kuechler, W. and Vaishnavi, V. (2012). "A Framework for Theory Development in Design Science Research: Multiple Perspectives," *Journal of the Association for Information Systems* (13:6), pp. 395–423.
Kuperberg, M. (2019). "Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective," *IEEE Transactions on Engineering Management* (63:4), pp. 1008–1027.
Kuperberg, M., Kemper, S., and Durak, C. (2019). "Blockchain Usage for Government-Issued Electronic IDs: A Survey," in *International Conference on Advanced Information Systems Engineering,* Springer, pp. 155–167.
Lacity, M. and Carmel, E. (2022). *Implementing Self-Sovereign Identity (SSI) for a Digital Staff Passport at UK NHS*.

Lacity, M. C. (2022). "Blockchain: From Bitcoin to the Internet of Value and Beyond," *Journal of Information Technology*.

Madsen, P., Koga, Y., and Takahashi, K. (2005). "Federated Identity Management for Protecting Users from ID Theft," in *Proceedings of the 2005 Workshop on Digital Identity Management,* pp. 77–83.

Maler, E. and Reed, D. (2008). "The Venn of Identity: Options and Issues in Federated Identity Management," *IEEE Security & Privacy* (6:2), pp. 16–23.

McKay, J. and Marshall, P. (2005). "A Review of Design Science in Information Systems," in *Proceedings of the 16th Australasian Conference on Information Systems,* AIS.

Miles, M. B., Huberman, A. M., and Saldaña, J. (2018). *Qualitative Data Analysis: A Methods Sourcebook,* 4th ed. SAGE.

Moe, K. S. and Thwe, M. (2019). "Investigation of Blockchain Based Identity System for Privacy Preserving University Identity Management System," *International Journal of Trend in Scientific Research and Development* (3:6), pp. 336–341.

Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C. (2018). "A Survey on Essential Components of a Self-Sovereign identity," *Computer Science Review* (30), pp. 80–86.

Myers, M. D. and Newman, M. (2007). "The Qualitative Interview in IS Research: Examining the Craft," *Information and Organization* (17:1), pp. 2–26.

Narayanan, A. (2013). "What Happened to the Crypto Dream?, Part 1," *IEEE Security & Privacy* (11:2), pp. 75–76.

Niehaves, B. (2007). "On Epistemological Diversity in Design Science: New Vistas for a Design-Oriented IS Research?," in *Proceedings of the 28th International Conference on Information Systems,* AIS.

OECD (2011). *Digital Identity Management: Enabling Innovation and Trust in the Internet Economy*.

Peffers, K., Tuunanen, T., and Niehaves, B. (2018). "Design Science Research Genres: Introduction to the Special Issue on Exemplars and Criteria for Applicable Design Science Research," *European Journal of Information Systems* (27:2), pp. 129–139.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. (2007). "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems* (24:3), pp. 45–77.

Preukschat, A. and Reed, D. (2021). *Decentralized Digital Identity and Verifiable Credentials: Self-Sovereign Identity,* Manning.

Rannenberg, K., Camenisch, J., and Sabouri, A. (2015). "Attribute-Based Credentials for Trust," *Identity in the Information Society, Springer*.

Rieger, A., Roth, T., Sedlmeir, J., and Fridgen, G. (2021). "The Privacy Challenge in the Race for Digital Vaccination Certificates," *Med* (2:6), pp. 633–634.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* (21:2), pp. 120–126.

Rosenberg, M., White, J., Garman, C., and Miers, I. (2022). *zk-creds: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure*.

Sartor, S., Sedlmeir, J., Rieger, A., and Roth, T. (2022). "Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets," in *Proceedings of the 30th European Conference on Information Systems,* AIS.

Schellinger, B., Sedlmeir, J., Willburger, L., Strüker, J., and Urbach, N. (2022). *Mythbusting Self-Sovereign Identity (SSI): Discussion Paper on User-Centric Identities*.

Schlatt, V., Sedlmeir, J., Feulner, S., and Urbach, N. (2021). "Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity," *Information & Management*, p. 103553.

Schwalm, S., Albrecht, D., and Alamillo, I. (2022). "eIDAS 2.0: Challenges, Perspectives and Proposals to Avoid Contradictions between eIDAS 2.0 and SSI," in *Open Identity Summit 2022,* Gesellschaft für Informatik eV, pp. 63–74.

Sedlmeir, J., Lautenschlager, J., Fridgen, G., and Urbach, N. (2022). "The Transparency Challenge of Blockchain in Organizations," *Electronic Markets*.

Sedlmeir, J., Smethurst, R., Rieger, A., and Fridgen, G. (2021). "Digital Identities and Verifiable Credentials," *Business & Information Systems Engineering* (63:5), pp. 603–613.

Seltsikas, P. and O'Keefe, R. M. (2010). "Expectations and Outcomes in Electronic Identity Management: The Role of Trust and Public Value," *European Journal of Information Systems* (19:1), pp. 93–103.

Smith, H. A. and McKeen, J. D. (2011). "The Identity Management Challenge," *Communications of the Association for Information Systems* (28:1), pp. 169–180.
Soltani, R., Nguyen, U. T., and An, A. (2018). "A New Approach to Client Onboarding Using Self-Sovereign Identity and Distributed Ledger," in *IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data,* IEEE, pp. 1129–1136.
Soltani, R., Nguyen, U. T., and An, A. (2021). "A Survey of Self-Sovereign Identity Ecosystem," *Security and Communication Networks*.
Sonnenberg, C. and vom Brocke, J. (2012). "Evaluations in the Science of the Artificial – Reconsidering the Build-Evaluate Pattern in Design Science Research," in *International Conference on Design Science Research in Information Systems,* Springer, pp. 381–397.
Sovrin Foundation (2021). *Principles of SSI V2*.
Stokkink, Q. and Pouwelse, J. (2018). "Deployment of a Blockchain-Based Self-Sovereign Identity," in *International Conference on Internet of Things and Green Computing and Communications and Cyber, Physical and Social Computing and Smart Data,* IEEE, pp. 1336–1342.
Tobin, A. (2017). *Sovrin: What Goes on the Ledger?*
Tobin, A. and Reed, D. (2016). *The Inevitable Rise of Self-Sovereign Identity*. The Sovrin Foundation.
Toth, K. C. and Anderson-Priddy, A. (2019). "Self-Sovereign Digital Identity: A Paradigm Shift for Identity," *IEEE Security & Privacy* (17:3), pp. 17–27.
Trust over IP Foundation (2021). *Principles of SSI*.
van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., and Zarin, N. (2019). *Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology*.
vom Brocke, J., Winter, R., Hevner, A., and Maedche, A. (2020). "Special Issue Editorial – Accumulation and Evolution of Design Knowledge in Design Science Research: A Journey through Time and Space," *Journal of the Association for Information Systems* (21:3), pp. 520–544.
Webster, J. and Watson, R. T. (2002). "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), pp. 13–26.
Weigl, L., Barbereau, T. J., Rieger, A., and Fridgen, G. (2022). "The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility," in *Proceedings of the 55th Hawaii International Conference on System Sciences,* pp. 2543–2552.
Whitley, E. A. (2009). "Informational Privacy, Consent and the "Control" of Personal Data," *Information Security Technical Report* (14:3), pp. 154–159.
Whitley, E. A., Gal, U., and Kjaergaard, A. (2014). "Who Do You Think You Are? A Review of the Complex Interplay between Information Systems, Identification and Identity," *European Journal of Information Systems* (23:1), pp. 17–35.
Windley, P. J. (2019). "Multisource Digital Identity," *IEEE Internet Computing* (23:5), pp. 8–17.
Yan, Z., Gan, G., and Riad, K. (2017). "BC-PDS: Protecting Privacy and Self-Sovereignty through BlockChains for OpenPDS," in *Symposium on Service-Oriented System Engineering,* IEEE, pp. 138–144.
Zimmermann, P. R. (1995). *The Official PGP User's Guide,* MIT Press.
Zuboff, S. (2015). "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* (30:1), pp. 75–89.

Acknowledgements

We thank our interview partners for their time and dedication and their valuable insights. Further, we want to express our gratitude to Alexander Rieger and the anonymous reviewers for their constructive feedback. This work was supported by PayPal and the Luxembourg National Research Fund FNR (P17/IS/13342933/PayPal-FNR/Chair in DFS/Gilbert Fridgen). Moreover, we would like to acknowledge the support of the European Union (EU) within its Horizon 2020 programme, project MDOT (Medical Device Obligations Taskforce), Grant agreement 814654.