Transition Pathways towards Design Principles of Self-Sovereign Identity

Completed Research Paper

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 to identify physical endpoints and the associated organizations (Tobin and Reed, 2016). End-users experience this design every day when they interact with the servers of digital service providers using an https connection (Preukschat and Reed, 2021). Servers identify themselves with public-private key pairs and SSL certificates, i.e., documents that are electronically signed by one of a few dozens of global "certificate authorities" (Soltani et al., 2021). The resulting public key infrastructure (PKI) can be considered the Internet's equivalent of a public "address book" or "telephone book" listing reputed organizations (Adams and Lloyd, 2003). Through its integration in browsers and mobile and web applications, it constitutes today's backbone of 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 NHS 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 user name or an e-mail address, and a credential. A credential is a mechanism for identification, i.e., to prove an identity to a system (Bosworth et al., 2005). This can be, for instance, a password, a smartcard, or an electronic identity (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 to simplify future verification. However, manual registration and the secure management of credentials – especially passwords – for sometimes even hundreds of digital services presents a substantial challenge and inconvenience to end-users (Bonneau et al., 2012). Related efforts for companies and governments lie in maintaining security, supporting operations, and 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). IdPs can be companies like Google and Microsoft or government agencies like the Unique Identification Authority of India (Srinivasan et al., 2018). Similarly to the siloed approach, these providers store (and to some extent verify) their user's identity attributes. However, IdPs 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 more efficient and convenient for users, it is often criticized for its centralized storage of large amounts of identity data and corresponding cyber-security and surveillance risks and for monetizing their users' identity and usage data (Srinivasan et al., 2018; van Bokkem et al., 2019; Zuboff, 2015), taking powerful market positions. Federated identity management also does not address the lack of digital representations of core identity-related documents such as passports, driver's licences, 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; OECD, 2011; Weigl et al., 2022). 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 also played a critical role in the development of federated identity standards (Preukschat and Reed, 2021). Subsequently, Allen (2016), who was a crucial figure in incubating SSI, coined the term as a principle-based framework for a decentralized system of user-centric digital identities (Weigl et al., 2022). These principles, in combination with an overlap of the SSI and blockchain communities, have created various research, industry, and public sector projects that explore and evaluate the implementation and adoption of SSI (Čučko and Turkanović, 2021; Soltani et al., 2021).

Allen (2016)'s 10 principles provide the first definition of SSI as a then mostly theoretical construct. At that time, there were no relevant reference standards or practical experiences with the large-scale deployment of SSI 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 business and public services, SSI has considerably evolved and embraced new components and perspectives. For instance, Allen's principles 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. One example are the different "levels of assurance" formulated in the European electronic Identification, Authentication and Trust Services (eIDAS) regulation (Schellinger et al., 2022). These changes, as part of a continuous innovation and evolution process within the SSI community, highlight that digital identity management approaches cannot be viewed merely from a techno-centric perspective. Further, the concepts of "sovereignty" and "decentralization" in the context of identity are contested (Sedlmeir et al., 2021) and subject to different interpretations according to actors' social and institutional context (Weigl et al., 2022). Indeed, the concept of SSIs for natural persons implicitly signifies a shift in social arrangements and requires an investigation that extends beyond the "epistemic script" (Grover and Lyytinen, 2015, p. 274). Therefore, SSI-solutions should be understood and analyzed as innovations with "political-economic dimensions" (Dijck and Jacobs, 2020).

The objective of this paper is to drive these developments by supporting research and practice in the development and design of SSI solutions through the creation of design principles for SSI-based identity management. To derive these principles, we analyse SSI as a concept that initially emerged from an incubated niche, diverging from existing digital identity management regimes. More specifically, using the multilevel perspective (MLP) by Geels and Schot (2007) as a theoretical lens, we retrace the *transition pathway* of SSI from a technological niche towards a mainstream concept. Through this theoretical lens, we derive the design principles following a design science research (DSR) study (Hevner et al., 2004; Peffers et al., 2007). We first 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 that illustrate the complexity of technical foundations and paths involved, and the need for multi-faceted research to formally structure and map these developments (Whitley et al., 2014). Next, we present the steps of our DSR, which involves a systematic literature review to develop the initial version of design principles for SSI and four subsequent iterative refinement and evaluation cycles in which we interviewed 15 experts from academia and businesses on SSI after respective workshops. We then discuss the goals and general relevance of the developed design principles for the area of SSI, especially in the context of Allen's 10 principles, and describe tensions that we observed in SSI's pathway from 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

Multi-level perspective on technological transitions

Digital identity management models can be viewed as socio-technical constructs undergoing a process of innovation (Seltsikas and O'Keefe, 2010; Smith and McKeen, 2011; Whitley et al., 2014). This process, which embeds the corresponding innovation into identity management, consists of a sequence of interactions and stages. The MLP has been introduced as part of the socio-technical systems (STS) theory and dissects the in-

novation process in terms of 'technological niches", the established "socio-technical regime", and the larger "exogenous landscape" (Geels, 2004). Using the MLP as a theoretical lens, we aim to consolidate and contextualize the phenomenon of SSI-based identity management. Moreover, our research intends to contribute to the stream of information systems (IS) research that explores the 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).

From the perspective of STS, questions pertaining to technology development build on theories of technological entrenchment and strategies to incubate or sustain novel technologies. Technological 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, p. 11). 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). Many researchers have analyzed this phenomenon in the context of technological innovations over the past 40 years (e.g., Callon, 1986; Collingridge, 1980; Hughes, 1983; Rip and Kemp, 1998; Russell and Williams, 2002). They assume that innovation takes place in protected niches, where builders safely develop and improve their technology, which – over time – "stabilizes as the outcome of successive learning processes" to form new regimes (Geels, 2004, p. 913).

Taking these collective understandings, Geels (2004) proposes a multilevel perspective (MLP), which was revised in Geels and Schot (2007). The framework consists of overall three levels: the micro-, meso-, and macro-level. At all levels, different selection factors apply, which form the technology and drive innovation. Technological niches construct the framework's micro-level. 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" for niche innovations to break through (Geels, 2004; Geels and Schot, 2007) .

A Brief History of Self-Sovereign Identity

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, Shamir, and Adleman resulted in an instantiation of the eponymous RSA cryptosystem (Rivest et al., 1978). 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 interactively with a "mathematical trick". This one-way mathematical connection between the secret key as credential and the public key as identifier opens up unique 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 "issuing" entity – 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 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, a service provider. The latter can cryptographically check the integrity of this digital certificate and, accordingly, rely on the attested attributes, provided that the verifying party trusts the issuer. In the context of institutions and their services, this has evolved into today's hierarchical 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.

Among cypherpunks – libertarian and privacy-oriented communities that make use of cryptographic tools to pursue their ideals (Narayanan, 2013) – there were also early attempts to use cryptographic keypairs and digital certificates issued by end-users for end-users to create a "Web of Trust" (Zimmermann, 1995), for instance, with implementations like Pretty Good Privacy (PGP). In the early 2000s, attempts were made to base this construction on institutional instead of social trust. These efforts aimed to push adop-

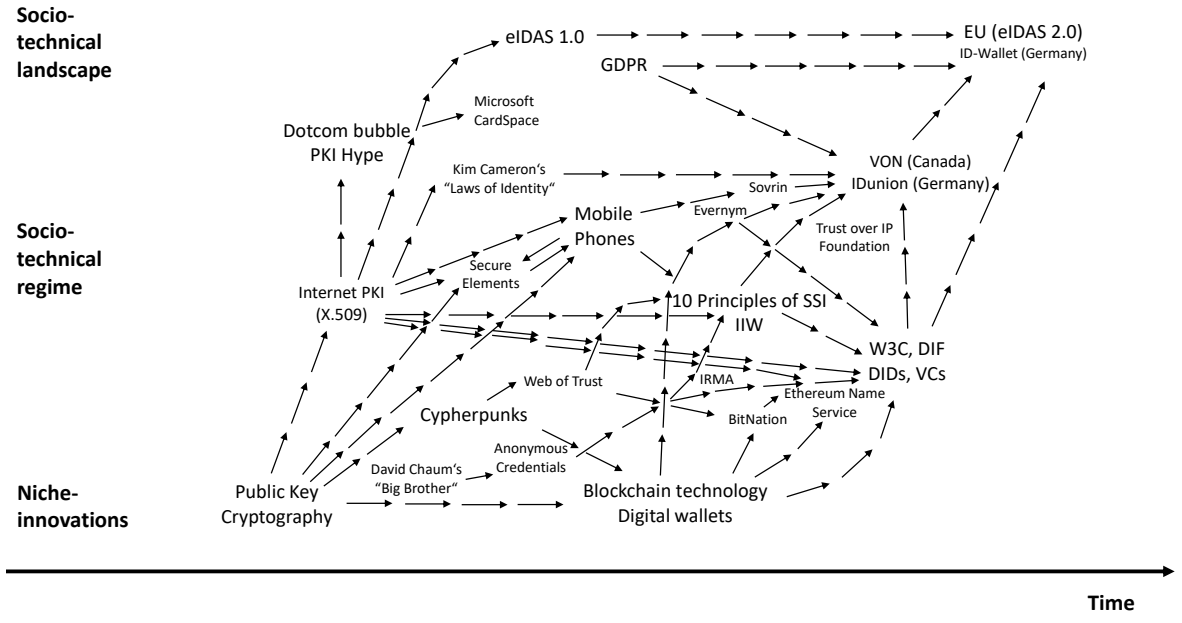

Figure 1. Multilevel perspective on selected key events and their interdependencies in identity management that are relevant for SSI.

tion, for instance, in e-commerce or enterprise identity and access management by extending the Internet's PKI for organizations and their servers to humans. They did so by using, 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 cryptography-oriented approach failed to gain large-scale traction, it prevailed for some time in niche communities. This mostly includes computer scientists and cypherpunks who took Chaum's warnings of surveillance threats on the Internet and corresponding spillover effects on society seriously (Chaum, 1985) and explored cryptographic tools to minimize information exposure during a verifiable presentation. In cryptography research, this led to innovative enhancements: In contrast to established digital certificates, anonymous credentials use zero-knowledge proofs (ZKPs) to derive evidence on the ownership of a digital certificate and to verify only a subset of attributes. That is, it attests a claim without revealing an associated unique identifier, such as the binding public key or the value of the issuer's digital signature on the certificate (Backes et al., 2005; Camenisch and Lysyanskaya, 2001). IRMA, for instance, offers an implementation 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. In the context of PKI, these are mainly "certificate authorities" responsible for mapping organizations to their public keys (Nakamoto, 2008). After Bitcoin and blockchain technologies more broadly gained foothold, libertarian forces saw opportunities to establish a registry for identities through mapping humans 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 and the Ethereum Name Service (ENS). In addition, the popularity of tools to manage cryptocurrencies made citizens and decision-makers in industry and politics aware of the opportunities of a digital wallet – maintained on abundant smartphones – for digital identity (Jørgensen and Beck, 2022; Sartor et al., 2022).

In 2016, the name SSI was coined by Allen (2016) and the concept has since become the focal topic far beyond the half-yearly IIW conferences. While gathering "internal momentum" (Geels and Schot, 2007, p. 400), the principles stipulated within this group soon became reference points for SSI solutions. In parallel, 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 (DIF). Arguably, the two most important standards in the context of SSI are decentralised identifiers (DIDs) – public keys enriched with meta-data – and verifiable credentials (VCs) as a generalization of digital certificates that offers a higher flexibility with regard to semantics, to include meta-data, and to incorporate features of anonymous credentials. 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, p. 411) that are continuously reconfigured and converge into a solution. The heterogeneity in configurations manifests in the use of blockchain as a component – in particular, with later configurations. The realization that pseudonymous public keys or DIDs do not provide privacy, 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 SSI implementations. In more recent projects, end-users' DIDs and VCs are now entirely stored in digital wallets on their devices, and a blockchain only hosts the PKI for public institutions and revocation registries (Lacity, 2022; Schlatt et al., 2021; Sedlmeir et al., 2021). This can be seen in projects like Canada's Verifiable Organizations Network (VON), Germany's IDunion, and recent modifications in the European Self-Sovereign Identity Framework's technical approach.

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 privacy-oriented proposals of using attribute-based PKI in combination with portable computing devices (Backes et al., 2005; Chadwick et al., 2003). In fact, public key cryptography alone arguably contributes to more secure and efficient identity management as compared to passwords (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 success, 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., European Commission, 2014) 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. In the case of SSI, there has been somewhat unprecedented support from the political regime since SSI connected with blockchain technology (Weigl et al., 2022), arguably culminating in the decisive role of SSI for multiple German pilots coordinated by the Chancellery and the revision of the European eIDAS regulation, which aim to provide German and European citizens with interoperable attestations stored in digital wallets, in line with the SSI concept.

Figure 1 features the described key events and their influences on the evolution of SSI through the lens of MLP. Considering the diversity of technical niche innovations, socio-technical developments, and the influence of regulation and businesses, which impacted the development of SSI, we believe that a rigorous and timely assessment of the key characteristics of SSI in the context of these novel influences is required. We aim to describe this updated model of SSI, which 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.

Research Approach

In addition to illustrating pathways and influences in the three STS' key layers on the development of SSI, we use the MLP as a theoretical lens for a DSR study to derive the core characteristics of the SSI concept in the form of design principles. The MLP allows us to contextualize findings from a systematic literature review (SLR) on the various characteristics of SSI and its technical constituents' trajectories. To integrate existent design knowledge in 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 consoli-

dated existing design principles from literature and SSI projects in a DSR study to develop design principless (DPs) for decentralized digital identity management. As developments in digital identity management 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 design principles 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 design principles, commonly referred to as Λ-knowledge or prescriptive knowledge (Gregor and Hevner, 2013; vom Brocke et al., 2020).

In line with Webster and Watson (2002) and Fink (2005), we extracted 2504 academic contributions, out of which 84 were considered directly relevant. 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. This led to keywords that combined "Identity" – as in "Identity Management", "Identity Management System", "Identity Access Management", or "Digital Identity" – AND "Blockchain", as well as "Identity" AND "Decentralized". While blockchain is not a prerequisite for SSI (Preukschat and Reed, 2021; Sedlmeir et al., 2021), as pointed out in the Background section, there is a strong historical connection between blockchain and SSI, and most SSI instantiations anchor at least their PKI on this technology (Sartor et al., 2022; Sedlmeir et al., 2021). In contrast, the term "decentralized", as influenced by Kuperberg et al. (2019), seems an essential characteristic of SSI and inextricably linked to the concept (Weigl et al., 2022).

After a detailed full-text reading of the selected 84 contributions, 14 papers remained. An additional forward-backward reference search (Fink, 2005; Webster and Watson, 2002), based on our preliminary selection, yielded 7 more highly relevant papers. 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 databases. We included these two contributions in our academic knowledge base, as they contain essential definitions of SSI and discussions about key requirements. They even provided first design principles for digital identity management systems (Allen, 2016; Cameron, 2005).

Our approach towards design principles for decentralized 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, p. 13). Evaluation of various existing decentralized digital identity approaches 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 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 design principles (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 design principles (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 design principles in 15 evaluation interviews with six researchers and nine industry experts in the field of SSI. 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 standardization bodies like Sovrin, the Trust over IP foundation, and the W3C. Two interviewees are among the four editors of the W3C DID standard, which is also co-authored by Christopher Allen. Five interviewees are in leading positions for the implementation of Canada's VON or Germany's IDunion projects 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).

We connected the design principles 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 design principles (Hevner et al., 2004; Peffers et al., 2018) and, moreover, demonstrate that decentralized digital identity management has developed from a radical niche to a now dominant design (Geels, 2004; Geels and Schot, 2007) in private- and public-sector applications (European Commission, 2021; 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. That is, our design principles 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 design principles through the lens of MLP additionally epitomizes the ascendance of technologies into broad-based adoption and provides an outlook of how decentralized digital identity management could further develop (Geels, 2004; Geels and Schot, 2007).

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 actionable design principles to digital identity management (Preukschat and Reed, 2021; Sporny et al., 2019). To address this problem, we consolidate existing and extend current design knowledge in generalizable and actionable design principles (Gregor and Hevner, 2013).

For both literature and interview analysis, we performed a qualitative evaluation (Sonnenberg and vom Brocke, 2012). In line with recommendations of Myers and Newman (2007), we used semi-structured interviews based on an interview guideline. In our 15 evaluation interviews, we first openly discussed the current state of decentralized digital identity management as well as the technical and social foundations of these approaches. Thereafter, we presented and reviewed the first version of our consolidated design principles for decentralized digital identity management. The interviews took between 45 and 60 minutes and were audio-recorded as well as transcribed for further analysis. For data analysis, we followed the recommendations by Miles et al. (2014) and performed a two-step coding process based on inductive and deductive coding. Based on this structured data, we continuously reviewed and refined our consolidated design principles in iterative rephrase-and-evaluate loops (Hevner et al., 2004; Peffers et al., 2007).

Findings

Following our SLR on key publications in the field of SSI and the subsequent two-step coding of the relevant literature, we identified several 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 design principles (Hevner et al., 2004; vom Brocke et al., 2020). Some requirements within the literature are already formulated as design principles (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 design principles. In the following evaluation rounds, we added and removed one design principle and adapted the principles until we reached a point where three subsequent interviews did not propose any meaningful changes. We first present the tentative design principles 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 per-

son. 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 the context of privacy hence limits "what personal data is made available to others" (Whitley, 2009). This also includes the design feature of "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 of sharing identity-related information but also its "availability", i.e., the identity subject's ability to access and share verifiable information anywhere and at any time (Ferdous et al., 2019). Yet, this does not mean that users should be able to modify 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 on – 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 solution must also guarantee for the design requirement "confidentiality" (European Commission, 2016) 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) and Tobin and Reed (2016) but also the limitation of storage and use of information for non-specified purposes (European Commission, 2016). Overall, users should be protected from unwittingly or mistakenly sharing information with third parties. This includes the verification of the involved entities' identities, purely bilateral communication, and end-to-end encryption (Goodell and Aste, 2019).

DP5: Privacy. Closely related to security is user privacy. In the context of SSI, it generally refers to the minimal disclosure of information, including a control over the degree of anonymity in interactions based on unique pairwise pseudonyms for each individual private connection. Relevant design requirements and design features either directly demand "privacy by design and per default" with "end-to-end security" (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 "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).

DP6: Credibility. Despite the goal of privacy protection, information should be authenticated and revoked in the case of error, changes of attributes, or expiration of an attestation. This 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). Thus, changes to personal information need to be adjusted in due time, so that invalid or lost attributes can be revoked using a revocation registry. This enables the checking of the validity of credentials.

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 a 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, 2020). If transactions break general laws or credentials are used in an unauthorized way, global or local anonymity revocation may be useful (**youtube**; Cavoukian et al., 2007; 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. Moreover, approaches should consider the different needs of users.

DP9: Future orientation. In addition, the "end-user experience" (Kuperberg et al., 2019) largely depends on how well the SSI-based digital identity management approach fits the surrounding environment. 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 heavily rely 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" and "minimal disclosure" (Cameron, 2005; Ferdous et al., 2019; Windley, 2019) of information. 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 DP1 as according to Expert 2, also smart devices and organizations can leverage an SSI. Regarding DP2, Experts 1 and 2 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 DP3. This was also closely linked to criticism on DP6 and DP7, 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" and the issuer's trustworthiness (Expert 2). Experts 1 and 2 generally regarded "performance [to be] a subtopic of usability" (DP8) and both as non-functional requirements instead of a DP. Regarding DP9, Expert 2 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, DP4 and DP5 were highlighted as particularly relevant (Experts 4, 6), while the adjusted DP8 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 considered DP9 as important, yet more of a requirement than a principle. It would indirectly already be represented in several other DPs, such as DP2 and DP3. For DP6, 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 DP1 to *Representation*, as the term *Replicate* may be uncommon and difficult to understand.

From the third to the fourth design iteration, we eliminated DP9, as the experts considered an environment with both innovative and legacy features more as a basic requirement than a DP specific to the implemen-

Principle	Description
Representation	SSI can represent any entity, whether it is human, legal, or technical, in a digital way. (Attributes, authentication, existence, identification, partial identities, persistence)
Control	Only the actual controller has maximised decision-making power over their digital identity. (Access, manage, ownership, right to be forgotten, single source of truth, update)
Flexibility	No vendor lock-in: low switching costs, focus on interoperable standards, and open-source projects. (Documentation, integration, no monopoly, portability, standards, transparency)
Security	State-of-the-art cryptographic tools and end-to-end encryption for all interactions. (Key management, protection, secure communication, tamper-proofness)
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)
Verifiability	The validity and timeliness of credentials can be checked efficiently. (Certificate chain, credential management, machine readability, provability, revocability)
Authenticity	Credentials are bonded to their initial bearers. (Binding, consistency of credentials, identity fraud protection, limited transferability, risk-based authentication)
Reliability	There is guidance that helps verifiers to decide which issuers to trust in a dependable infrastructure. (Decentralization, governance, guidance, no single point of failure, public registration, scalability, Web of Trust)
Usability	Success and durability factors in the interest of the subjects. (Efficiency, end-user experience, minimum downtime, multiple access points, performance, recovery, simplicity, support)

Table 1. Final design principles and their short definitions including key features for implementation after the fourth iteration of interviews in our DSR.

tation 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) – we renamed and redefined the DP. Regarding DP3, Experts 5 and 11 suggested renaming it to "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 criticized that it was "too specific" and did not include "more general points" (Expert 9), we redefined DP5. Experts 2, 5, and 6 also suggested redefining DP6, as they considered it too focused on not yet established technological building blocks. We refrained from adding "decentralization" as a separate DP as it is a basic "prerequisite of the infrastructure" (Expert 5) but added it to DP9. Moreover, we redefined DP6 and DP7 and renamed DP8.

During the fourth design iteration – which yielded the final and consolidated set of design principles – we received positive feedback from our Interviewees 13 to 15. In accordance with their feedback, we summarized the current definitions to the most relevant and generalizable core statement and changed the order of DP8 and DP9 in line with their perceived importance. Table 1 features the final design principles, including a subset of terms that related work and the interviewees often used. The design principles characterize SSI

as a user-centric "identification infrastructure" (Whitley et al., 2014) based on cryptocraphically verifiable attestations not only for organizations and their servers but also for end-users, maintained and controlled in digital wallets on their mobile phones (Weigl et al., 2022).

Discussion

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

Taking the lens of the MLP, a key insight that our iterative evaluation produced 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 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 recommendations on how to best implement SSI-based digital identity management solutions rely on their learnings from ongoing IT-projects and specifically the integration in legacy identity and access management solutions and regulatory constraints. Knowing that SSI is still in its trialing phase and its long-term success dependent on negotiation with selection factors of the incumbent socio-technical regime, the interviewees appreciated the overall structure of our nine design principles. Yet, they also indicated that the definitions may have to be adapted over time with increasing maturity.

Throughout the iterative refinement of our design principles with the interview partners, we identified several tensions. 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 reflect and align with the findings of Weigl et al. (2022), who studied the interpretive flexibility of SSI. Thus, 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): The often strong focus on minimal disclosure and anonymity support caused by the libertarian and cryptography-affectionate origins did not sufficiently consider incidents, such as theft or sharing of mobile devices, and the consequences of lacking 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 Hardman (2021) 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 still retain a high level of privacy, ZKPs enable minimum disclosure while being compliant with regulation that requires the verification and authentication of certain user data (Hardman, 2020; Sedlmeir et al., 2021). Yet, the tools currently available for ZKPs are difficult to integrate with existing secure elements that facilitate hardware-binding, leading to a trade-off between privacy and authenticity that – despite technical solutions have been conceptualized (Delignat-Lavaud et al., 2016) – has not yet been resolved in practice (Schellinger et al., 2022).

A second tension arises from the conflicting selection forces of the policy regime and socio-cultural regime. The challenge pertains to balancing reliability (DP6, DP8) against end-user expectations (DP2, DP5) and also 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 proof that they actually originate from there and have not changed since. Trust registries and qualified electronic signatures, as, for instance, implemented in the context of eIDAS, may mediate this tension in practical implementations of SSI. Should an organization issue an incorrect VC – whether on purpose or not – the option for revocation must be given (Interviewee 10), and/or the issuer must even be removed from certain trust registries or policies. As a result, abandoning information silos is only practical in the cross-domain sense: While the issuer's involvement in verifiable presentations is not required and, therefore, cannot track end users' interactions, they need to store some of the master data related to the certificates that they issue to have sufficient information available to provide or revoke VCs.

A third tension emerges between selection factors of the socio-cultural and the technological regime. This tension pertains to the balancing of a maximum of flexibility against functional requirements of interoperability (DP3). With an initially strong focus on libertarian values (Allen, 2016), the more "radical" 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 ultimately 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 focusing on 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). The strong involvement of governments with establising these infrastructure and their support with implementing digital wallets may prove highly valuable in this context.

A fourth tension involves selection forces between the policy regime, the technological regime, and – up to a certain degree –- also of the socio-cultural regime. That is, users prefer convenience over security and privacy (Cabinakova et al., 2019; Ostern and Cabinakova, 2019; Satchell et al., 2011), which puts pressure on the technology developers to still retain the legally required security standards while improving or sustaining the current level of usability or convenience. With regard to SSI, this could, for instance, result in the retention of ways to securely storing data or warrant larger data wallets to store additional personal data such as pictures or videos. Data storage in the from of verifiable credentials may however not be necessary at all. Regardless of the dominant design, negotiations between the selection forces of the technological, political and socio-cultural regime have to settle for the "path of least resistance", which simultaneously ought to be the "secure path" (Dhamija and Dusseault, 2008).

Our study contextualizes the current development and discusses factors that helped develop SSI as a new regime of identity management and aims at a broad, transnational perspective. Yet, we cannot guarantee that we incorporated all relevant events and practical implementations of SSI. We aimed to ensure a comprehensive perspective through our DSR approach, as we used broad search strings and many databases in our systematic literature review. During the interviews that guided the refinement of design principles, we inquired for other interviewees or projects that may be of relevance. Still, 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, and a more longitudinal study that rigorously analyzes discussions from events like the latest IIWs or amendments in regulatory documents may be required to consolidate the chronology of changes in the SSI concept. Thus, while our DPs consolidate a snapshot of the current design knowledge on SSI and a perspective on its pathway through regimes of identity management, they may be subject to change – not least, from learnings on successful or failed applications of SSI. To better retrace the selection factors of each regime, we plan to conduct further interviews with experts in the respective regimes for a further development of this study. 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 retraced and contextualized the historical development of SSI using the MLP as a theoretical lens. Our systematic literature review in combination with DSR delivered a set of nine DPs that consolidate

existing design knowledge on the concept of SSI. We refined and extended this consolidated knowledge in four iterations with 15 experts from industry and academia and used the MLP as a frame to understand the development of SSI from a radical niche to a popular concept that is now considered, for instance, in national and industry consortia in North America and Europe as well as the eIDAS 2.0 regulation for large-scale productive use. This may help to better understand SSI in the context 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 them. In this context, we elaborated on the difficulties that different velocities of regime negotiation could have on prudent use of windows of opportunity.

The relevance of our research comes from the close interaction with stakeholders as part of projects in the SSI ecosystem. This has already led to contributions to documents like Sovrin's Principles of SSI (Sovrin Foundation, 2021). Aside from direct experiences, our research also draws on observations from crucial requirements and failures, as illustrated, for instance, by the German government's digital driver's licence. While corresponding learnings and turns in the concept may at first seem to considerably impair SSI's key goal of giving user more control and establishing an open ecosystem of verifiable digital interaction, we learned that if SSI aims to embrace digital identity management in practice, the updates are indispensable. Consequently, our contribution highlights that research that consolidates historical influences on SSI can help to mediate tensions and to achieve a feasible identity management solution beyond authentication (Bonneau et al., 2012). Our design principles thus provide a common basis for future research on design choices and trends within decentralized digital identity systems.

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.

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.

Bosworth, K., Gonzalez Lee, M., Jaweed, S., and Wright, T. (2005). "Entities, Identities, Identifiers and Credentials – What Does it All Mean?," *BT Technology Journal* (23:4), pp. 25–36.

Cabinakova, J., Ostern, N., and Krönung, J. (2019). "Understanding Preprototype User Acceptance of Centralised and Decentralised Identity Management Systems," in *Proceedings of the 27th European Conference on Information Systems,* AIS.

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 Macmillan, 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*.

Cavoukian, A., Stoianov, A., and Carter, F. (2007). "Biometric Encryption," *Biometric Technology Today* (15:3), p. 11.

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.
Dhamija, R. and Dusseault, L. (2008). "The Seven Flaws of Identity Management: Usability and Security Challenges," *IEEE Security & Privacy* (6:2), pp. 24–29.
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.
European Commission (2014). *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC.*
European Commission (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC.*
European Commission (2021). *Commission Proposes a Trusted and Secure Digital Identity for All Europeans.*
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.
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," en. *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.
Grover, V. and Lyytinen, K. (2015). "New State of Play in Information Systems research," *MIS Quarterly* (39:2), pp. 271–296.
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. (2020). *Webinar on ZKP-Oriented Credentials.*
Hardman, D. (2021). *Indy Hype 0011: Credential Revocation.*
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* (online first).
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* (online first).

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.

Miles, M. B., Huberman, A. M., and Saldaña, J. (2014). *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.

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

Nakamoto, S. (2008). *A Peer-to-Peer Electronic Cash System*.

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

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

Ostern, N. and Cabinakova, J. (2019). "Pre-Prototype Testing: Empirical Insights on the Expected Usefulness of Decentralized Identity Management Systems," in *Proceedings of the 52nd Hawaii International Conference on System Sciences,* pp. 1834–1843.

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.

Rip, A. and Kemp, R. (1998). "Technological Change," in *Human Choice and Climate Change,* vol. II. Battelle Press.

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.

Russell, S. and Williams, R. (2002). "Social Shaping of Technology: Frameworks, Findings and Implications for Policy," in *Shaping Technology, Guiding Policy: Concepts, Spaces, and Tools,*

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

Satchell, C., Shanks, G., Howard, S., and Murphy, J. (2011). "Identity Crisis: User Perspectives on Multiplicity and Control in Federated Identity Management," *Behaviour & Information Technology* (30:1), pp. 51–62.

Schellinger, B., Sedlmeir, J., Willburger, L., Strüker, J., and Urbach, N. (2022). *Mythbusting Self-Sovereign Identity (SSI): Diskussionspapier zu selbstbestimmten digitalen Identitäten*. Whitepaper.

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* (online first), p. 103553.

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. (2021). "A Survey of Self-Sovereign Identity Ecosystem," *Security and Communication Networks* (2021).

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*.

Sporny, M., Longley, D., and Chadwick, D. (2019). *Verifiable Credentials Data Model 1.0*. W3C.

Srinivasan, J., Bailur, S., Schoemaker, E., and Seshagiri, S. (2018). "The Poverty of Privacy: Understanding Privacy Trade-Offs from Identity Infrastructure Users in India," *International Journal of Communication* (12), pp. 1228–1247.

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.