Government Information Quarterly 40 (2023) 101873

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

The construction of self-sovereign identity: Extending the interpretive flexibility of technology towards institutions

Linda Weigl [a,b,*], Tom Barbereau [b], Gilbert Fridgen [b]

[a] Institute for Information Law, University of Amsterdam, Amsterdam, Netherlands
[b] SnT – Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg City, Luxembourg

ARTICLE INFO

Keywords:
Electronic identification
Digital identity
Self-sovereign identity
Interpretive flexibility
Social construction of technology
Blockchain

ABSTRACT

Ever-growing concerns over 'Big Brother' continue driving individuals towards user-centric identity management systems. Nascent innovations are framed as offering *Self-Sovereign Identity* (SSI). Because of the association with value-laden ideals and technical components like blockchain, SSI is caught up with both hype and idiosyncrasy. Competing interpretations of SSI damage the public discourse and risk misrepresenting affordances these systems might offer. Based on a qualitative inductive interview study and document analysis, this article extrapolates a constructivist theoretical frame – the Extended Model of Interpretive Flexibility – which combines insights from the Social Construction of Technology and the Structurational Model of Technology. The Extended Model of Interpretive Flexibility highlights malleability in the technical implementations and social representations, which in turn is affected by and influences institutional properties around SSI. This research further offers implications for practice around the implementation of SSI, in particular regarding policy, management, and design. For theory on public sector information systems, the proposed model has generalizable potential for the analysis of socio-technical systems and offers future research directions.

1. Introduction

Digital identity management systems are susceptible to substantial, but also controversial developments in the technological design and the underlying socio-political promises they ought to deliver (Cheesman, 2020; Giannopoulou, 2023; Halpin, 2020). For digital public services, many countries deploy electronic identification systems that citizens rely on for a wide array of services (OECD, 2011). For these services, citizens' electronic identification (eID) attributes are stored in centralized silos – an architecture vulnerable to cyber-attacks, potentially resulting in identity theft and misuse (Bélanger & Carter, 2008). For commercial purposes, Internet users make use of *federated* identity management systems offered by private companies (Sedlmeir et al., 2021). Users typically register and login with Google, Meta, or other providers. These allow them to conveniently verify their identity via single sign-on (SSO) authentication through the platform where their accounts are registered (Chadwick et al., 2019). In this model, user convenience comes at a cost. Centralized platforms enable the aggregation and exploitation of personal data, thus igniting privacy and security concerns (Maler & Reed, 2008). Recent breaches of Yahoo (Weinberger, 2016), LinkedIn (Canales, 2021), and Meta (then Facebook) (Holmes, 2021) underscore the undeniable reality that the violation of digital security is affecting everyone who is part of the network at some point in time.

In response, *user-centric* identity management models have gained momentum in order to confer "users greater control over their personal information" (OECD, 2011: 162). Storing identity data in a decentralized registry has emerged as a viable solution to address security concerns (Sedlmeir et al., 2021). Here, models based on cryptography such as distributed ledger technology (DLT), have become a rising trend amid digital identity communities of developers (Ferdous et al., 2019; Mühle et al., 2018). Members of these communities have begun promoting a user-centric, decentralized model under the heading of Self-Sovereign Identity (SSI) (Allen, 2016; Preukschat & Reed, 2021). SSI promises users[1] the power to "own" their identities (Tobin & Reed, 2017) by providing new means to manage and control personal data and

* Corresponding author.
E-mail addresses: l.weigl@uva.nl (L. Weigl), tom.barbereau@uni.lu (T. Barbereau), gilbert.fridgen@uni.lu (G. Fridgen).

[1] The use of SSI is not restricted to the digital identification of individuals by public authorities. Digital identity can express identity attributes of citizens, organizations, and even objects of the Internet of Things (IoT). This study, however, focuses on the use of SSI by governmental agencies in the context of identifying individuals.

https://doi.org/10.1016/j.giq.2023.101873
Received 12 April 2022; Received in revised form 28 September 2023; Accepted 19 October 2023
Available online 27 October 2023

eliminate traditionally centralized models.

Interestingly, considering SSI's ambition to weaken state responsibility through a decentralized design (Giannopoulou, 2023), SSI models are now not only on the agenda of private organizations (Microsoft, 2018), but also governments (Bundesregierung, 2021; Finnish Government, 2021). Because some SSI models rely on DLTs (Mühle et al., 2018), SSI is often described as a "blockchain-based identity" (Kubach et al., 2020: 37). Due to its association with such value-laden technologies (Ølnes & Jansen, 2017), SSI is caught up with similar technology hype and idiosyncratic visions of decentralization (Cheesman, 2020; Ferdous et al., 2019; Giannopoulou, 2023). Moreover, the pursuit of concepts like "self-sovereignty" and "data sovereignty" is increasingly perceived as a "type of unease manifest in cyberspace" based on the presumed ongoing failure of centralized institutions (Herian, 2020: 157). The competing value appropriation and social embedding of SSI results in a range of different interpretations among stakeholder groups.

The heterogeneity of SSI's technical operationalization (Kuperberg, 2020) and its social ambiguity (Giannopoulou & Wang, 2021; Ishmaev, 2020), make SSI implementations malleable to the flexible interests of key actors involved in the design process. This can be both a blessing and a curse. As a developing technical niche innovation (Sedlmeir et al., 2022), the concept of SSI is susceptible to modifications and iterations to improve its design and better reflect the needs of holders, issuers or verifiers. From a public policy perspective, innovative ideas that are loosely defined allow policy issues to be presented in a way that can either promote or prevent them from appearing on the political agenda (Weigl et al., 2022). However, undefined and value-laden discourses can also damage public understandings and affect democratic decision-making (Jones, 1994). With the eID innovation being a "co-constructed process of policy-making and technology" (Wihlborg, 2013: 143), misleading information is particularly perceptible. Considering citizens' low trust in online security, Otjacques et al. (2007) emphasize the importance of public awareness strategies to foster a better public understanding of the concepts of digital identity, and caution against otherwise large-scale acceptance problems of e-government solutions. Chaum (1985: 1044) highlights that "the initial choice [for the architecture] will gather economic and societal momentum, making reversals increasingly less likely". Further, Chaum (1985) writes that "[w]hichever approach prevails, it will likely have a profound and enduring impact on economic freedom, democracy, and our informational rights." In response to these pleas, we analyze the construction of SSI by addressing the following research question: *How do stakeholder interests and institutional properties shape the social embedding of self-sovereign electronic identification systems?*

To answer this research question, in Section 2 we highlight SSIs ambiguity in both social as well as technical terms. Then, in Section 3 we introduce our theoretical lens – Social Construction of Technology (SCOT) – and the concept of *interpretive flexibility* (Pinch & Bijker, 1984; Sahay & Robey, 1996). We develop our contribution by means of a qualitative study into SSI, an artifact "in development" (Sedlmeir et al., 2021) that we systematically analyze based on coded interview transcripts and whitepapers (Myers & Newman, 2007) described in Section 4. In Section 5, we present the findings of our study in terms of the technical, social, and institutional domain. In Section 6, based on these three domains, we establish the Extended Model of Interpretive Flexibility (EMIF). The EMIF is a constructivist model that builds on the work of both, Orlikowski's Structurational Model of Technology (1992) and Doherty et al.'s re-conceptualization of interpretive flexibility (2006). We derive implications for research in the technical, social and institutional domain. Furthermore, we draw several policy, managerial, and design implications for SSI from our findings.

2. Background

2.1. Electronic identification systems

The management of public service interactions between citizens and public administrations essentially relies on citizens' identity information, such as name, date of birth, address or nationality (Lips et al., 2009). Since citizens' identity information is rooted in the confirmation of an individual's citizenship, most forms of personal identification lie within the purview of government (Wihlborg, 2013). One example of an established tool for identification of citizenship are passports: as government-issued and internationally recognized documents, they enable citizens to prove their identity at international borders, making it easier to travel freely (Van Dijck & Jacobs, 2020). Official governmental identity documents are also a trust anchor for administrations and other service providers. Although subliminal, personal identification using government-issued documents is crucial in people's life when they need to interact with public administrations to, for instance, pay taxes, change address, or when making use of services offered by commercial providers (e.g., opening a bank account) (Wihlborg, 2013).

Identity proofing with physical documents always carries the risk of security breaches, identity theft, or a loss of privacy (Van Dijck & Jacobs, 2020). On the one hand, the deployment of passports, allows border control agencies to monitor international movements. On the other hand, the registration of international movements also enables some degree of surveillance (ibid.). This has been evident in the United States, where in its campaign to combat terrorism following the 2001 Twin Tower attacks, significant efforts were made to plan and organize "policing and identification functions well before the traveler arrives at the border, but also, in certain cases, after they arrive on American soil" (Walters, 2006).

With the establishment of the Internet, governments embraced electronic means of transacting with their citizens (Layne & Lee, 2001). The remote interaction emphasized the importance of strong requirements for governments to mitigate cybercrimes (Van Dijck & Jacobs, 2020) and to protect users' privacy. For governments, the introduction of electronic identification (eID) systems also represents a step towards a more transparent, trustworthy and legitimate information society (Wihlborg, 2013). With these advantages and opportunities in mind, over the past decade, governments gradually transitioned from paper-based to electronic means of identification (Gascó, 2003; Thomas & Streib, 2003). In the process, some often turn to the private sector for the resources and expertise needed to implement new systems (Dawes & Pardo, 2002; West, 2007). In fact, these dynamics and systems challenge the traditional perception of identity management as a prerogative preserved for state authorities. eID models now take various forms, most of which store identity attributes in central servers of a few digital platforms who act as third-party gatekeepers (Jin, 2015). This federated identity model comprises Big Tech firms like Meta and Google, offering single sign-on (SSO) solutions, and state-owned online platforms such as Chinese companies like Baidu and Tencent. An exception to these developments is the 'financial identification society' (e.g., Sweden) (Husz, 2018: 391) where the digital BankID is used for a variety of transactions in most Scandinavian countries.

2.2. From centralized to decentralized electronic identification

For public administrations, the authentication of citizens in online settings comes with challenges regarding security, privacy and confidentiality (Layne & Lee, 2001; Seltsikas & O'Keefe, 2010). As illustrated with the example of the 'ordinary' passport, the increasing cooperation of government agencies through a connected web of databases, relies on the exchange of sensitive data (Otjacques et al., 2007). This process of *datafication* or, the transformation of human life into quantified data (Mayer-Schönberger, 2013), led to the establishment of a two-sided paradigm: the gradually normalized means to access people's data on

the one side, and the exploitative monetization of data as a "regular currency for citizens to pay for their communication services and security" on the other (Van Dijck, 2014: 197). In fact, data collection, cross-referencing (aggregation), and the hidden amassment of metadata enables monitoring and real-time tracking, which can result in the (unintended) surveillance by both, governments and third parties (Cap & Maibaum, 2002; Hiller & Belanger, 2001; Newell, 2014; Walters, 2006; Zuboff, 2015, 2019). This results in a paradoxical situation where eID models seek to enhance security and efficiency on the one hand, but compromise users' privacy on the other (Backhouse & Halperin, 2008; Mir et al., 2020).

The development and use of cryptographic protocols and decentralized technologies represent efforts to address this contradiction. With DLT, new paradigms of decentralized, user-centric identity or Self-Sovereign Identity (SSI) arose in niche spaces of identity management (Ferdous et al., 2019; Mühle et al., 2018; Sedlmeir et al., 2022). The World Wide Web Consortium (W3C) started drafting a standard on Decentralized Identifiers (DIDs), a new type of identifier that allows for verifiable, decentralized digital identity credentials that ought to "enable individuals and organizations to generate their own identifiers using systems they trust [and] prove control over them" (Sporny et al., 2019). Moreover, these systems typically consist of a user-controlled wallet that stores digital credentials.

The implementation of eID models in e-government is contingent on a process that is steadily at the intersection of policy considerations and technical design iterations (Addo & Senyo, 2021; Mir et al., 2020). As such, it is subject to debates shaped by technical and political interpretations of the artifact in question (Wihlborg, 2013). In particular, this holds for SSI: at present, it is caught in a web of ambiguous terminology and controversial socio-political roots, plus variation about which technical components are required (Kuperberg, 2020). Political dynamics, budget realities, path dependencies and a lack of political awareness are factors that are amplifying these ambiguities and affecting the implementation of novel technologies in the public sector (Pollitt, 2008; West, 2007; Wihlborg, 2013).

2.3. Ambiguities of self-sovereign identity

This study considers SSI as an information system that is socio-technical. Amid few implementations, it is ambiguous in both technical and social-political terms; and hence provides ample opportunity for exploratory research (Sedlmeir et al., 2021).

2.3.1. Technical ambiguity

SSI is a heterogeneous artifact in its operationalization and implementation. There are, however, certain technical features that are frequently observed with SSI. Among those are DIDs, which allow users to interact with service providers via end-to-end encrypted communication without an intermediary registrar or account provider (Reed et al., 2021). Another associated technical building block of SSI are Verifiable Credentials (VCs): machine-verifiable and cryptographically secured types of digital certificates, which are characterized by an issuer's digital signature (Chadwick et al., 2019). These types of credentials can be stored, for instance, on a user's device in a so-called 'digital wallet' and used for a broad array of identity documents (Sporny et al., 2019).

Most digital wallets that are part of an SSI model store digital assets and/or identity information (Kuperberg, 2020). The wallet's holdings can be registered on a distributed ledger – which can include hashes of personally identifiable information – hence SSI is often described as "blockchain-based identity" (Kubach et al., 2020: 37). Finally, there is a third type of wallet which neither stores digital assets nor does it use VCs. This highlights that wallets can be both custodial or non-custodial, and that they can store identity credentials and/or digital assets (Barbereau et al., 2022). Suffice to say, there is not yet an orthodox, technical definition for SSI models.

Consequently, SSI is regarded with some "confusion" by technical experts (Ferdous et al., 2019: 103060). SSI standards are still under development, which can pose a challenge to the implementation and interoperability of mature models. Yet, given that this paper does not provide a technical evaluation of design options or attributes of SSI, the subsequent arguments engage with SSI's technological features in terms of technical boundaries – that is, enabling or prescribing constraints that limit the artifact's interpretive flexibility (Doherty et al., 2006).

2.3.2. Socio-political ambiguity

The conception of a 'self-sovereign' identity or a 'sovereign individual' in the digital sphere did not emerge from philosophy, legal theory, or political science texts. Instead, it came from blog posts, magazines, and Internet forums of software developers. They defined SSI as a set of "ethical principles" and an idealistic vision in which individuals become "rulers of their own identity" (Allen, 2016). Traditionally, sovereignty is conceived as an exceptional power, not something possessed by all (Kahn, 2011): the dominion of God, the Crown or the State are examples of such sovereignty. Self-sovereignty, by contrast, denotes something humble: an individual's ability to control the exchange of digital assets and the disclosure of personal information on the Internet. Various SSI projects share this aim (Allen, 2016; Tobin & Reed, 2017).

In the academic literature, Cheesman (2020: 2) identified identity 'ownership' and individual empowerment as common rhetorical themes: SSI putatively "removes the need for powerful, centralized institutional structures by giving individuals control and ownership of their identity information." Specifically, she argued that because the diverse ways in which individuals use digital identity technologies cannot be determined in advance, SSI could potentially empower disenfranchised individuals, yet it could also extend administrative powers and strengthen forms of control (Walters, 2006). The SSI terminology entails an idiosyncratic conception of sovereignty; and self-sovereignty is in turn linked to other informal notions: data sovereignty, digital identity ownership, and personal data ownership (Ishmaev, 2020; Zwitter et al., 2020).

Proponents of SSI tend to appreciate technical features, while not appreciating "moral semantics"; hence, the prevalence of simple narratives that posit SSI as 'good' and big brother as 'bad' (Ishmaev, 2020). Halpin (2020: 18) suggests that the "cultish" libertarian proponents of SSI overlook ethical problems. He coined the term "cryptography theater" to mock the use of cryptography to allay users' concerns. Zwitter et al. (2020) acknowledged that technologies associated with SSI have potential; yet they also identified "a clear need" for critical policy decisions that affect the design and implementation of SSI systems.

3. Theory

Technological artifacts are "inherently political" (Winner, 1980: 123): while they can be designed to open or constrain certain options, they also build order for particular social groups over periods of time. Just as the adoption of today's bicycles (Pinch & Bijker, 1984), the steamship (Geels, 2002), and electric grids (Hughes, 1987) was inherently shaped by relevant social groups, so is the case for e-government (Pollitt, 2008; West, 2007) and digital identity management systems (Van Dijck & Jacobs, 2020). Hence, MacKenzie and Wajcman (1985: 3) argue that a deterministic and "simple cause-and-effect theory of historical change" is an 'over-simplification' that fails to acknowledge socio-political imperatives. Although the physical properties ensure the presence of clear 'boundary conditions' on usage in the technical domain, the social domain often remains unaccounted for. For Information Technologies (ITs) that are technologically immature and novel, their analysis in constructivist terms, therefore, appears adequate (Orlikowski, 2000).

In this article we consciously turn to the Social Construction of Technology (SCOT) (Pinch & Bijker, 1984) and its grounding in

organizational theory and sociology to study SSI in both these terms. At the core of SCOT, is the concept of *interpretive flexibility* which lends itself to understanding the design process and the shaping of IT (Haas, 1999; Orlikowski, 1992).

3.1. The social construction of technology

Under the Social Shaping of Technology (SST), innovation is viewed as a "garden of forking paths" (Williams & Edge, 1996: 866) determined by both a technical realm – composed of constraints or affordances, and a social realm – impacted by stakeholders and negotiations between them. As part of SST, the SCOT approach brought insights from within the Sociology of Scientific Knowledge (SSK) to understand technological development (Pinch & Bijker, 1984). SSK's approach of studying scientific developments in constructivist terms of points of "contingencies" and ambiguities subject to "interpretative flexibility" is useful for the study of technologies and their development (Williams & Edge, 1996). The SCOT approach is divided into two stages, *(1) interpretive flexibility* and *(2) closure*.

3.1.1. Stage 1: interpretive flexibility

In the first stage, stakeholder groups compete with flexible social and technical interpretations to embed particular design features into the technology. Here, the concept of interpretive flexibility– the ability of a given technical artifact to symbolize "different things to different actors" (Law & Callon, 1992: 25) – is of particular importance.

Doherty et al. (2006) developed a conceptualization of interpretive flexibility that gives equal value to the social and technical domain. Their contributed model describes how stakeholders construct (i.e., interpret flexibly) different understandings of the same artifact in the social domain, limited by technical, functional boundaries. To delineate these boundaries, Doherty et al. (2006) introduce two sets of constraints: *enforcing constraints* (which are 'mandatory' technical features, and thus deemed essential for the system's functionality), and *proscribing constraints* (representing functions that do not exist or cannot be used). Doherty et al. (2006)'s model does not account for the second stage of SCOT (closure), and solely focuses on the potential information system and interpretations of an artifact.

In IS research, studies of technology do not strictly account for the interpretive flexibility of technical constraints (Henningsson & Henriksen, 2011). The ones that do, however, take a relatively narrow perspective that does not account for the impact of institutions and influence of organizations on the social domain. Originally, this was iterated in Russell (1986) rebuttal to Pinch and Bijker (1984). Primarily, he argued that SCOT overlooks power differences as social groups may have unequal access to resources, and essentially, closure can be imposed by powerful players. He noted that SCOT fails to formally address influences of the social domain itself, and "must look for an adequate model of the basic social structures which provide the contexts of technological development". In this study on SSI, in consideration of SCOT and the critique by Russell (1986), we therefore turn to Orlikowski (1992) who acknowledges the role of institutions in the formation of technology.

Although Doherty et al. (2006) grounded their model of interpretive flexibility in Orlikowski's work, their contribution focused exclusively on the social and technical domain. In turn, the institutional domain and its properties may indeed be a crucial factor to consider given the ambiguity of SSI (Cheesman, 2020; Zwitter et al., 2020).

3.1.2. Stage 2: closure

Over time, as technologies develop and stakeholders align, the interpretive flexibility collapses through *closure mechanisms*. These mechanisms are the emergence of forms of consensus, that can occur, either rhetorically or by redefining the problem at hand (Pinch & Bijker, 1984). In turn, these play a role in the stabilization of what artifacts are and the role they play. Closure need not to be definitive, as social groups may form and introduce interpretive flexibility in the future.

The second stage of SCOT is outside of the scope of our paper. This is primarily due to the immaturity of operational SSI models and a lack of considerable levels of mainstream adoption: thus far no consensus has emerged as to what exact technical features are required for SSI models, nor is it clear how they are understood in socio-political terms (Sedlmeir et al., 2021; Smethurst, 2023).

3.2. Structural studies of technology

In the advent of Structuration Theory, scholars sought to establish reciprocal links between organizational structures and social agents without giving primacy to either. Prior to these, technology was viewed as an "objective, external force" that impacts organizations in a linear, deterministic manner (Orlikowski, 1992: 398). In response, a theory of structuration which incorporates both, human actors and structural features of organizations, was proposed by Giddens (1979). This view is characterized by duality: while actors give structures agency, structures in turn act as constraints ("structures of domination or control") or enablers ("structures of legitimation") for social actors. Though Giddens (1979) does not explicitly mention 'technology', the work of Orlikowski (1992) builds on his conception to introduce the *duality of technology*.

Her model primarily reflects the dual state of technology: as being shaped by human agents, and in turn, influencing the actions and behavior of users. This view is in line with the constructivist perspective of SCOT. Orlikowski (1992) model further accounts for the organizational perspective in terms of *institutional properties*. In line with Giddens (1979), the model posits that the properties of structures and organizations have an influence on humans' interaction with technology and on humans' construction thereof.

In academic literature *institutionalization* is understood as a framework in which organizations are social contracts subject to norms, rules and expectations that constrain the decisions and behavior of groups and individuals (Frederickson et al., 2018). Outside of SCOT, institutional theory and neoinstitutional theory has been elaborated on extensively. The former focuses on the elements of formal rules, structures, legal systems and governmental processes. The latter seeks to develop an economic theory of institutions (Scott, 1995). DiMaggio and Powell (1983) described mechanisms of institutionalization and identified different types of institutional isomorphism. However, most research dedicated to institutional theory only rarely captures the role of technology as an intermediary between institutions and their pillars in society.

4. Method

4.1. Data collection

We followed a qualitative inductive approach to match our data-driven analysis. The inductive, qualitative analysis method consisted of a qualitative interview study (Myers & Newman, 2007) with a supporting document analysis.

As part of our in-depth interview study, we carried out 41 interviews with knowledgeable experts on credential and identity management. These were conducted as part of a project with Luxembourg's Ministry for Digitalization, spanning over a period of five months (October 2020 to March 2021). Interviewees were selected on the basis of their expertise and the type of organization that they work for (Appendix A). In this context, experts were understood as agents with implicit and relevant factual knowledge about processes and strategic decisions (Mergel et al., 2019). However, we also viewed experts as "representatives of a larger domain, such as the organization, to their privileged access to decision-making processes and people" (ibid.: 4). Therefore, we sought to have an interdisciplinary selection and a fair representation of experts in both the private and the public sector that were involved in digital identity management on various levels

Table 1
Technological features of different SSI solutions.

Provider	SSI Solution	Technological Features						
		Crypto-assets	VCs	Aries-compatible	Issuance fee tokens	Mandatory on-chain identifiers	DLT-based PKI	DIDs
esatus AG*	SOWL		x	x			x	x
Evernym Inc.*	Evernym		x	x			x	x
German Chancellery*	ID Wallet		x				x	
Alastria Consortium	ID Alastria		x			x	x	x
Microsoft	ION		x			x	x	x
Ontology	Ontology	x	x		x	x	x	x
SelfKey Fdn.	SelfKey	x	x		x	x	x	x
Procivis AG	eID+							
Procivis AG	VETRI	x					x	

(implementation, strategy, management, oversight, etc.). The overall average professional experience of the selected interviewees was 22 years. Their average professional experience in their current position, on the basis of which they were chosen to participate in this study, is seven years. The participants come from Europe, North America, the United Kingdom and Australia.

To account for the novelty of SSI and the scarce amount of information available on SSI's implementation, best-practices, and interpretations, we conducted the interviews in a semi-structured manner. Semi-structured interviews have the potential to produce rich data that can offer in-depth, thorough, and genuine acumen about the respondents' social realities and inner worlds (Leech, 2002; Schultze & Avital, 2011). They are useful for studying topics about which there is little existing literature and for gaining a deep understanding thereof (Brinkmann & Kvale, 2015). Since SSI is a relatively niche and under-researched topic, the semi-structured and exploratory approach allowed us to use thematic guides, rather than specific questions, and thereby account for the interviewees' thoughts, perceptions and interpretations of SSI. We conducted the semi-structured interviews using an interview guide (Appendix B) to streamline coverage of the thematic areas (Rubin & Rubin, 2012). During each conversation, we adapted our questions according to the interviewee's role, knowledge and field of expertise (Myers & Newman, 2007). The interviews lasted between 45 and 60 min, were held through video conferencing, and were subsequently transcribed. We had to exclude nine interviews due to a thematic divergence in the discussion. In sum, we considered 32 interviews for the analysis.

The semi-structured interviews were complemented by the analysis of documentation. As a qualitative data source, documents are advantageous given that they are unobtrusive and non-reactive – that is, they are unaffected by the research process and remain "stable" (Bowen, 2009). The focus of the document analysis was on the various descriptions of technical implementations of SSI. We found these in whitepapers and functional documentations of digital identity solution providers which we selected based on preparatory research and upon recommendation of our interviewees. Eventually, we included nine whitepapers and the functional documentation of eight different solution providers (Appendix C).

4.2. Data analysis

Through the lens of Doherty et al. (2006), we analyzed both the social understandings and technical operationalizations of SSI. With the objective to identify patterns and answer our research question within the frame of our theoretical framework, we followed the conventional stages of open, axial, and selective coding (Corbin & Strauss, 2015). We coded our data using the qualitative analysis software MAXQDA (Mayring, 2014). Our codebook is disclosed in Appendix D.

Phase 1: Open coding. We analyzed whitepapers and interviews individually by assigning conceptual labels without having specific domains or categories in mind (Corbin & Strauss, 2015). We mainly paid attention to what interviewees perceived as relevant, which we assessed based on how long they talked about an issue or how much emphasis they put on it. Specifically, we considered information on the successes, challenges, and failures of SSI, such as the motivation to engage in SSI, legal hurdles, technical challenges, but also user benefits. We coded segments that informed about relevant actors in the system, specific technical features, as well as modes of governance of running or upcoming projects. At this stage, we realized that SSI is a name given to several projects and subject to various interpretations.

Phase 2: Axial coding. We clustered codes across sources, elevating them to higher-level themes (Corbin & Strauss, 2015). Specifically, we began congregating codes along a) *technological features*, which predominantly appeared during discussions about the practical implementation of SSI; b) *boundary objects* (Star & Griesemer, 1989)[2] in the social domain, which helped us to group information we received about the societal context endogenous to an SSI system; and c) *institutional properties* (Orlikowski, 1992)[3] in the institutional domain, which highlight associations between the institutional context and stakeholders' interpretations of SSI. For each of these, we regularly reviewed emerging concepts and ensured consistency in the coding system (Klein & Myers, 1999).

Phase 3: Selective coding. At last, we aimed at identifying and creating overarching categories to group the matching themes based on our theoretical lens (Corbin & Strauss, 2015). For the technical domain, we identified enforcing and proscribing constraints (Doherty et al., 2006) of SSI. For the social domain, we created three clusters of boundary objects (Star & Griesemer, 1989) that are related to one another. For the institutional domain, we clustered codified statements along six sets of institutional properties (Orlikowski, 1992). Throughout this final phase, we again ensured consistency through iterations among the team of researchers (Klein & Myers, 1999). After completing the final, selective phase of coding, we ended up with a total of 1376 codes in the technical domain, 1752 codes in the social domain and 745 codes for the institutional domain.

5. Findings

5.1. Technical domain

As anticipated within the technical literature on SSI, its

[2] Boundary objects are abstract or tangible objects, "both plastic enough to adapt to local needs […], yet robust enough to maintain a common identity across sites" (Star & Griesemer, 1989: 393). In other words, for social groups, these are areas of negotiation and contestation, and key in maintaining coherence across groups.

[3] Orlikowski (1992) distinguishes between two categories of institutional properties: (1) organizational dimensions, that may be conceptualized as the internal/endogenous context a certain stakeholder group is exposed to by an institution (e.g., organizational culture, control mechanisms, and standard operating procedures), and (2) environmental pressures, that reflect the external/exogenous context stakeholders face (e.g., regulation, market forces, or socio-economic conditions).

Table 2
Boundary objects in the social domain.

Cluster	Researchers	Not-for-profit	For-profit	Government officials
Good Governance		Trust in institutions User empowerment	Trust in institutions User empowerment	Duty of care over users Institutional prerogative over identity matters Legal compliance Policy realism
Service & Management	User convenience	User convenience User data management Operational efficiency	User convenience User data management Operational efficiency	User-centricity Privacy
Society & Innovation	Data control Digital literacy and skills Decentralization	Data ownership Data control Decentralization Social inclusion	Data ownership Data control Decentralization Social inclusion	Data control Digital literacy and skills Trust and credibility Decentralization

operationalizations diverge significantly (Mühle et al., 2018; Sedlmeir et al., 2021). Our interview data revealed that models labeled 'SSI' may be composed of numerous technical features. Our results witnessed a great variety of operationalizations ranging from and between the use of crypto-assets, Verifiable Credentials (VCs), on-chain identifiers, Decentralized Identifiers (DIDs), and DLT-based Public Key Infrastructure (PKI), to none of these. Table 1 presents an overview of the different implementations of SSI as seen in our whitepapers and interviews. (Solutions discussed in interviews are marked with an asterisk (*)).

While there is not yet an industry-standard definition on technical features of SSI, we observed a common denominator in the form of VCs, DIDs, and DLT-based PKIs (these were previously described in Section 2.3.) From our analysis, we identified enforcing and proscribing constraints of SSI.

5.1.1. Enforcing constraints

To ensure personal identity data management, all stakeholder groups agreed that a software application to hold credentials that runs on a users' hardware or a server in the cloud is an essential enabler for SSI (I3; I4; I7; I10; I11; I13; I17; I24; I30; Alastria Association Network Consortium, 2020; VETRI, 2020). In other words, a mandatory technical building block for SSI is some form of digital wallet. A digital wallet stores a user's private keys and can be used to encrypt messages or prove ownership of a VC. It typically contains a user's digital credential, such as VCs, DIDs or any other form of machine-verifiable document (Sedlmeir et al., 2021).

While a digital wallet is a mandatory common denominator, some 'outlier' SSI solutions exhibit unique enforcing constraints. For instance, the SelfKey Foundation (2017) introduced crypto assets (native token, KEY) for its SSI ecosystem through a public token sale. The purpose of KEY is essential because certain actions on the SelfKey network require an exchange of the token and others will involve placing KEYs in a "locked contract" (e.g., to access the network). SelfKey's native token, KEY, is in this case an enforcing constraint because it is mandatory for the network's overall functionality.

5.1.2. Proscribing constraints

Our interviewees revealed that there is a recurring aversion towards centralized data storage and siloed databases (I3; I17; I18; I22; I31; Alastria Association Network Consortium, 2020; Esatus, 2019; Ontology, 2017; Procivis, 2017; SelfKey Foundation, 2017; Sovrin, 2018; VETRI, 2020).

Thus, SSI seeks to store identity data in a decentralized fashion. Generally, decentralized storage is associated with the use of DLT (Ølnes & Jansen, 2017). While from the whitepapers we could not confirm a uniform implementation of SSI on DLT-based PKIs, there is a strong consensus towards 'concepts of decentralization' and reducing the need of interaction between the identity or credential issuer, the user, and the service provider. For instance, some SSI implementations rely on a PKI with certificate authorities. Such certificate-based models do not use DLT-based PKIs, but they still store the certificates in a decentralized manner on the users' end devices. Other solutions neither rely on a DLT nor on certificate authorities, but by offering digital mobile wallets to users, these schemes are ultimately decentralized. A proscribing constraint would thus be a system that neither uses DLT-based PKIs nor certificate authorities, and which does thus not allow for the storage of data outside the realms of one specific institution. This architecture design would inherently be at odds with the objective of SSI.

5.2. Social domain

Following Corbin and Strauss (2015), we clustered the various interpretations of SSI in terms of boundary objects (Table 2). These were structured in terms of three clusters: (1) *Good governance* as being concerned with questions of mandates and responsibilities of public institutions in a legitimate, participatory, accountable and transparent system; (2) *Service & management* constitutes a boundary object in which the relationship between a service provider and recipient is an essential element of flexibility, particularly between commercial and public management settings; and, (3) *Society & innovation* which encompasses goals to 'improve' the quality of life of all members in society via technology in a more general sense.

5.2.1. Good governance

Government officials emphasized the responsibility of governments to have a duty of care over users and to protect long term needs, such as "privacy" (I9; I18, I23) "social cohesion" and even "life goals" (I18) against impulsive needs, such as efficiency and convenience. It was widely supported that the transfer of control to the user, places a great responsibility on the user as citizen, and with that a potential liability on the state. One of the "largest concerns" was that interpretive flexibility "there is a case of fraud or identity theft", governments will face a challenge in taking responsibility "for citizens who are misled or are doing something unintentionally" (ibid.). Interviewees from not-for-profit and for-profit organizations (I11; I13; I14; I22), on the other hand, emphasized the empowerment of users as an essential principle in public management, arguing that "governments generally should do things in the spirit of General Data Protection Regulation (GDPR), where the spirit of the law is to give people more ability to control [their] data" (I14).

Moreover, officials (I16; I23) referred to the "long held view" of the government's institutional prerogative over identity matters resulting in a "conflict of perception [...] that is not easy to reconcile so far" (I16). On the other hand, stakeholders from not-for-profit and for-profit organizations viewed SSI as a possibility to re-establish and increase trust in central institutions (I4; I11; I28; I29). It was argued that SSI is a "key enabler to enforce [...] democratic principles" (I11).

5.2.2. Service & management

Researchers (I12; I19), as well as experts from not-for-profit (I1; I15) and for-profit organizations (I4; I7) strongly highlighted increased efficiency and personal data management as crucial benefits of SSI. Several

stakeholders (I4; I7; I19; I22) further expressed a positive feeling towards increased user convenience, in particular through the use of self-managed digital wallets on users' mobile devices. The underlying premise is that "the main driver for the end user is never information control – it is convenience", which in turn requires increased technical security in order to protect users "from themselves" (I7). At the same time, it was argued, that one "cannot ever jeopardize the user experience to a point where security goes before convenience" because it could negatively affect adoption (I7). On the other hand, improved efficiencies were seen as non-generalizable given that this ought to be evaluated on a case-by-case basis. For instance, some interviewees (I28; I29) saw the use of SSI for Know Your Customer (KYC) checks in banking as having greater potential than, for instance, in the case of digital diplomas. In this context, interviewees discussed the topic of interoperability, as well as cross-organizational and cross-border standardization repeatedly (I1; I3; I12; I19; I30). Interviewees from the public sector (I17; I20) acknowledged that SSI could have the potential to enhance user-centricity. According to most officials, the issue of citizens' privacy was a very difficult and sensitive topics, which needed to be addressed. SSI, it was argued, could be one way to do so (I5; I9; I17; I18; I20; I23).

5.2.3. Society & innovation

We observed contestations among stakeholders particularly over the boundary objects 'data ownership', 'digital exclusion' and 'decentralization'. While data ownership was promised or promoted by almost all SSI whitepapers and for-profit interviewees, one public official judged the pledge for ownership to be a "misconception about personal data [...] propagated by SSI proponents" as "the idea of owning digital data makes no sense" (I9) – this claim was supported by multiple researchers (I12; I19). Furthermore, one interviewee emphasized that there is "no such thing as the 'owner of personal data'" and legislation, such as the GDPR "does not even use this concept" (I9). Various participants confirmed that legally the idea of ownership of data is not covered under the current regulatory regime. The idea of 're-appropriating' data to users was heavily disputed, with some suggesting to "never mention ownership, never mention self-sovereign" (I12). Rather than ownership, numerous stakeholders (I9; I12; I19; I25; I30) agreed that SSI would enable some degree of "user control", thereby ensuring an individual's ability to control the exchange, disclosure and restriction of identity data.

The cluster of society and innovation also encompasses the accessibility of SSI for the general public to prevent digital exclusion. In this context, researchers and government officials (I3; I5; I12; I18; I19; I20; I23) shared the view that SSI would require high digital literacy among users because it presupposes the capability of managing and controlling one's own identity data. Both groups questioned whether individuals could be entrusted with the ability of self-management and critical reasoning to assess when to share which data and with whom (I18; I19). Similarly, researchers (I12; I19) argued that SSI requires internet access, the possession of an electronic device, and in some cases a smartphone with biometric authentication methods, potentially leading to further exclusion. Contrarily, stakeholders from governmental and research organizations (I12; I17) pronounced the social inclusiveness of SSI.

With regards to decentralization, one governmental actor (I18) perceived SSI as a "principle-based" construct that lacks trust and credibility. Our data revealed discrepancies between the whitepapers of solution providers and respondents from the for-profit stakeholder group. While most whitepapers advocated for an SSI system using DLT as infrastructure, the interviewees from the for-profit stakeholder group (I4; I7; I11; I25) cautioned against "entering the blockchain discussions too much" (I11) as "blockchain [was] overused in the use case of identity" (I7). One interviewee further associated SSI with "radical" notions of 'decentralization' and 'self-control' (I7). These diverging views were based on the duality of SSI that incorporates libertarian idealism of decentralization on the one side, while calling for government-issued credentials and thus relying on a centralized authority on the other (I16). Therefore, some interviewees (I2; I18; I22) advocated for a complete detachment between SSI and the term of 'decentralization.'

5.3. Institutional domain

The analysis of our data revealed that human agents and their interpretation of socio-technical artifacts are subject to a variety of institutional properties. Following Orlikowski (1992), we categorized these in terms of endogenous ODs and exogenous EPs.

5.3.1. Organizational dimensions

Our interview data yielded two main properties in this dimension: *operating procedures* and *culture & ideology*. The findings are discussed accordingly.

Operating procedures. Our data revealed that for-profit companies based their argumentation for SSI particularly on the drawbacks of current paper-driven and centralized identity systems which would benefit from a decentralized digital identity scheme (I13; I27). Government officials shared this view and referred to legacy technologies in the public sector as the "big problem in our times [...] that come from medieval times" and were "never changed" because "people are accustomed to them" (I5). Other interviewees accentuated this path dependence arguing that "some projects fail because as a government we use a software solution, but we completely turn it inside out because we want it to exactly work like we were used to it working before" (I20) and that "this process is really not organized, and nobody wants to change it" (I2).

Existing operating procedures were identified as a major problem because paper-based systems and a lack of cross-border interoperability not only caused inconvenience for both verifiers and users (I2; I4; I17), but also carried security risks with them (I20; I27).

Culture & ideology. Our interviews with experts from Europe and the Anglosphere highlighted the presence of cultural differences. Numerous interviewees (I3; I10; I16; I18; I21; I28; I29; I32) mentioned the distinction between systems in Europe, Asia and in the Anglosphere. One interviewee (I18) highlighted a key cultural difference consisting of "distrust towards anything 'central'" in states like the United States, as opposed to Europe, where central registries act "as an authoritative source of truth." Another interviewee argued that "in the American context [...] they say, okay, 'here's your responsibility and if you're exploited by other people, that's your own fault'" (I3). Similarly, one researcher (I21) contrasted data governance models between China, Europe, and the United States, arguing that "China believes data belongs to the state or to the respective corporate structure, [while] Silicon Valley capitalists believe that data belongs to [individual data subjects...] and the European Union hasn't decided yet, who the data belongs to". The interviewee further maintained that the answer to this question, the so called 'hegemonic form' of 'contemporary digital capitalism', was "based on [a jurisdiction's] social market ideology" (I21). This cultural aspect to data governance was mirrored in statements by interviewees from the for-profit sector (I11; I28; I29) contemplating that "in our western world, we appreciate freedom, privacy, freedom of choice and being able to voice our opinions" (I11). Consequentially, it was argued, SSI is more aligned with a "libertarian worldview of citizens" (I18), which might explain why "there are more people involved in those discussions in the [United States] than in Europe" (I16).

These cultural differences and values revealed some insights into the underlying ideology of SSI. I16 claimed that "people who are proposing SSI schemes are motivated by ideology". This view was shared by I25. It was further argued that advocates of SSI in the Internet Identity Workshops "have strong ideologies [which lean on] the principles of SSI by Christopher Allen [with the goal to] create a better world where people own their data and can use it for whatever purpose they want" (I25).

5.3.2. Environmental pressures

Our interview data highlighted *regulatory dynamics*, the *political environment*, *knowledge of technology* and *economic conditions* as prevailing institutional properties regarding the interpretation of SSI. We discuss the findings for each of these accordingly.

Regulatory dynamics. With the research rooted in a national project, the interviews primarily focused on the relevant European Union (EU) regulations, specifically GDPR and Electronic Identification, Authentication, and Trust Services (eIDAS), as applicable. As these also affect non-European stakeholders, specifically in the context of transatlantic data transfers, interviewees from both European and non-European countries (I4; I7; I14) acknowledged the repercussions of jurisdictions beyond the EU.

Interviewees from the private sector argued that despite regulatory challenges with the GDPR, data protection regulation also offers opportunities for companies that "employ innovative, privacy-respecting ways." All interview participants (I1–32) highlighted that SSI's features of privacy-by-design would help administrations to comply with the GDPR's principle of data minimization. While generally, interviewees acknowledged SSI's potential to facilitate GDPR compliance, one interviewee (I5) claimed that such compliance would not help to establish trust, but only be based on "box-ticking" to meet regulatory requirements.

Aside from the GDPR, Europe's eIDAS regulation plays a prominent role in our data. Experts from for-profit companies referred to the eIDAS revision during 2020 and 2021, arguing that the open consultation was an opportunity to propose "tweaks in the regulation that will help [...] to establish SSI" in Europe (I11). Public officials (I3; I5; I9; I16; I18) agreed that a revised eIDAS regulation could potentially confer legal validity to a new decentralized identity paradigm. Likewise, one interviewee (I9) denoted how eIDAS-compliant identity credentials set a certain "level of assurance" for validity. Further, the regulation may serve as a "interoperability framework for a sovereign digital identity scheme" (I16) allowing citizens to, for instance, use "cross-border online services" (I9) seamlessly and securely across Europe.

Political environment. Characteristically, our data revealed the role of political will in changing the present digital identity model towards one that is self-sovereign. One interviewee (I1) denoted how "in Spain, for instance, there is no political engagement to substitute the current systems". The same interviewee mentioned that in some Spanish autonomous communities with strong regional identities, however, there is indeed a "strong political will to start exploring new systems [...], because it is [...] different from national identification means." One interviewee (I9) took note of the same trends within other European regions. Given the considerable political will in Estonia, two public officials (I2, I20) referred to the advancements made in the eID space.

Finally, our analysis suggested that the political environment and will is often linked to regulatory dynamics. We noticed a recurring reference among interviewees from both the private and the public sector to the European Commission's support and "proactive approach" (I7) for decentralized digital identity schemes, manifested in the revision of the eIDAS framework (I1; I3; I11; I16).

Knowledge of technology. Interviewees referred to a gap between the pace of technology development and implementations in the public sector (I11; I24). For SSI, government officials may have a "hard time to evaluate which use case makes a lot of sense, because the whole topic is so complex, and [decentralized identity systems are] just so different from the way we're used to thinking" (I25). Likewise, one interviewee (I24) highlighted the difficulty "for governments and policy-makers to change as fast as the technology world changes."

Our interview data revealed that the knowledge of technology can also pertain to the user side. One for-profit stakeholders (I11) and one government official (I2) argued that SSI would reduce complexity in identification and authentication processes for users. On the other hand, the lack of digital literacy on the user side was iterated repeatedly in the context of SSI and VCs more generally (I3; I4; I11; I15; I20; I23). One researcher (I19) maintained that users may be "overwhelmed by this responsibility" given to them, and design should caution against the aversion of users on the grounds that "people probably won't be able to cope with complexity".

Economic conditions. Interviewees highlighted the difficulty in devising business models for SSI, arguing that it is not realistic to "impose an economic model on identity" based on an inherently user-centric system leveraging technical decentralization (I7). Further justifications of this argument cited, among others, a "liability shift" (I27), "standardization" (I3; I32), and the problematic of monetizing the development and distribution of digital wallets (I15).

In terms of profitability, the design of wallets was indeed seen as particularly contentious (I3; I11; I15). It was argued that "there is no solid business model for why you would invest in a wallet [because] a surveillance approach that a potentially operating wallet could give [is] the wrong purpose" (I15). Similarly, one researcher concluded that "before you start developing technologies, you have to choose: to enforce government authority, to make more profit for your shareholders [...], or [...] pursue the common good" (I21). From a business perspective, navigating this spectrum was indeed perceived as challenging given SSI's ambition to "empower the citizens or the user itself," and effectively, "to not be reliant on whatever centralized identity provider" (I29).

Our data further indicates that, intrinsically, the prospective profitability of digital identity management models is linked to adoption. Reflecting on the said spectrum, one for-profit interviewee (I14) argued that probably "governments are the first to adopt [SSI] because governments care about their citizens, they care about doing the right thing, and for-profit companies don't. They care about making money, which is good, [although] there's much less of an incentive" to develop SSI models. Both government officials and for-profit interview participants (I3; I13; I29) advocated for public-private partnerships arguing that "countries who will be really moving ahead are the countries where governments are [...] together with private firms stepping [towards] a higher height" (I3) in order to "bring together, not only a one-sided consortium [but also], address legal hurdles and the regulatory cases" (I29).

6. Discussion

6.1. The interpretive flexibility of self-sovereign identity models

While mapping out the flexible interpretations of stakeholders in the social and technical domain, in terms of boundary objects and technical features respectively, we discovered that interpretations of SSI are associated with an underlying institutional domain. Dissecting it in terms of institutional properties is an important aspect in understanding the social construction of IT artifacts, as these go beyond stakeholders' interests and their interpretations (Orlikowski, 1992; Russell, 1986). From our findings and supporting literature, the relationship between the institutional and social domain may be demonstrated by three examples for which further evidence is provided by literature.

First, the *culture & ideology* underlying the perception of SSI seem to influence stakeholders' diverging social interpretations. Interviewees from not-for-profit and for-profit organizations from the Anglosphere often referred to SSI's potential to re-establish trust among citizens in centralized institutions. On the other end of the spectrum, public officials from Europe emphasized the government's duties as a supervisor over citizens. This confirms observations made in literature on the diverging interpretations of the concept of sovereignty (Keohane, 2002; Lips et al., 2009; Stillman, 1997). More generally, the role of cultures in IT were studied in, among others, Aladwani (2013) and Schuppan (2009).

Second, the *political environment* of institutions plays a role in stakeholders' view on SSI. Our data reveals that whenever the idea of SSI is associated with initiatives supported by an authority (such as the

European Commission in our case) the views on SSI become more tangible and concrete. Likewise, the political will for the development of SSI models (in both, public and private contexts) was a key factor for all stakeholders involved. Researchers and government officials highlighted the role top-down policy-making based on national interest and mandates played in the evaluation of SSI. Interviewees pointed to the obligation to adhere to "very clear instructions from [the] data protection commissioner" (I23) or contrasted experiences between, for instance, the Scandinavian model where it is "perfectly acceptable to have a [national] identifier [...] whereas in Australia [this is] the cause of a huge political fight." (I26). Thus, political will expressed by public institutions further functions as a tool for either legitimation or rejection of innovations (Gascó, 2003; Hargadon & Douglas, 2001; Luna-Reyes & Gil-Garcia, 2014).

Third, *economic conditions* impact the perception of stakeholders in the social domain. As opposed to public actors, private profit-oriented organizations attempt to monetize SSI through their projects. For public stakeholders on the other hand, the cost of innovation is a concern weighing against implementing a new technological system (Nograšek & Vintar, 2014; Savoldelli et al., 2014; Weerakkody et al., 2011). As a result, stakeholders viewed the need for SSI differently.

Finally, our data indicates a relationship that is intimately tied to Orlikowski (1992): 410) contribution: how a technology could influence institutional conditions by "reinforcing or transforming structures of signification, domination, and legitimation". At this stage, very few SSI implementations have gained an operational foothold in the public sector. Although this makes it difficult to determine to what extent SSI technology influences institutional properties, to the extent of our knowledge, there is one example that underpins this phenomenon. Germany initiated a legal change in its Federal Registration Act with its first SSI use-case for hotel check-in procedures. The change introduced an "experimentation clause" to test further methods of digital registration (Bundeskanzleramt, 2021). Likewise, an experimentation clause was ratified for KYC identification methods under the German Money Laundering Act. These regulatory changes created a legal basis for wallet-based identity management systems and can therefore be considered to have been initiated by the first operationalizations of SSI. The developments in Germany assimilate efforts to develop digital identity systems in the European context, which are typically and primarily shaped by regulatory dynamics as well (Van Dijck & Jacobs, 2020).

In sum, we can account for these relationships in an extension to the model of Doherty et al. (2006). Specifically, we developed the Extended Model of Interpretive Flexibility in the context of SSI models (Fig. 1). It features the three domains – institutional, social, and technical – as identified from our qualitative inductive research approach.

6.2. Implications for theory

Our study contributes to theory by presenting a constructivist theoretical conceptualization; one that beyond acknowledging the duality of technology, incorporates structuration theory on organizations and institutions. Our contribution is respectively supported by the view that technology – and self-sovereign electronic identification systems specifically – share a fundamental duality and may be interpreted flexibly. Crucially, that interpretation, and eventual operationalization of the artifact, is subject to institutional forces.

Applied to the construct of SSI, the Extended Model of Interpretive Flexibility (EMIF) incorporates previous evidence that the emergence, introduction, and adoption of socio-technical artifacts in the public sector can, in similar organizational contexts and institutional settings, result in very different operationalizations and interpretations (Nograšek & Vintar, 2014; Sahay & Robey, 1996; Weerakkody et al., 2011). Therefore, our contribution may account for another "open issue" in the study of technologies more generally (Russell, 1986): the neglect of institutions as a 'left-over' category in SCOT analyses.

To close this gap, the EMIF seeks to embed the, sometimes predominant, role of institutional context in the social construction of IT.[4] We found the institutional domain to consist of an organizational domain and environmental pressures. For SSI specifically, these two domains, in turn, exhibit institutional properties. Although, naturally these properties vary based on the artifact in question, the premise that organizational and environmental properties impact and are impacted by the artifact's interpretive flexibility could be extended to other technological artifacts. Therefore, in Fig. 2, we present our *proposal* of a general, Extended Model of Interpretive Flexibility.

As a theoretical model emerging from the study of SSI, the proposed EMIF (Fig. 2) is not yet established enough to plausibly serve the theoretical analysis of each and any socio-technical artifact. However, for digital government researchers, the proposed EMIF does constitute a foundation for further research to analyze and dissect emerging, complex socio-technical artifacts. Studies have already conceptualized the relationship between technological, institutional and process designs (Koppenjan & Groenewegen, 2005), emphasized the necessity of coherence between the technical and institutional coordination of infrastructures for their performance (Finger et al., 2005), and theorized on the role of institutions in the innovation process (Nooteboom, 2000). The proposed EMIF adds to these by taking stock of the duality of technology beyond structuration theory for artifacts that are nascent and still subject to interpretive flexibility. In that sense, this paper adds to the academic debate on the affinity between institutions and socio-technical systems before they reach "closure" – as exemplified with the construct of SSI (see Fig. 1). Hence, we consider the proposed EMIF to be a model with generalizable potential for research on electronic identification systems and socio-technical artifacts in the public sector, where the role and relevance of institutions is undeniable.

6.3. Implications for practice

Jones (1994) argued that "[p]olicy issues are not just illuminated by information; they are framed by it. When issues are reframed [...], our basic understanding of an issue shifts. Because information sometimes restructures, a marginalist approach to information can be misleading in politics." In response, this paper proposes a theoretical model to counter the "marginalist approach to information" and allow for "reframing" by mapping stakeholders' interpretation of technology including an account for the institutional properties. Indeed, the proposed EMIF is especially useful for digital government practitioners and researchers who seek to contextualize and open the black box of an emerging IT artifact. By accounting for a broad spectrum of interpretation (Arrows A & B in Fig. 2), it is possible to see how, in our example, SSI is framed, communicated and perceived. For some, SSI is a "key enabler to enforce [...] democratic principles". For others, SSI will remain a "principle-based" construct that lacks trust and credibility. It follows that the perception of an artifact will eventually influence whether and how it will be implemented in practice, carrying both benefits, but also risks with it (Pinch & Bijker, 1984). For policy- and decision-makers, it is therefore essential to strip off an artifact's frames and conduct an informed assessment for policy response and potential uptake (Janssen & Helbig, 2018).

To enrich practitioners' socio-technical understanding of an artifact, contextualizing institutional factors (Arrows C & D in Fig. 2) is key to holistically trace and identify stakeholders' requirements (Janowski, 2015), interpretations and technical design features. These factors allow stakeholders' interpretations to be understood in context and reveal much more information about their potential needs, preferences and

[4] This phenomenon can be observed with the World Wide Web Consortium (W3C). The organization established primary standards for DIDs (Reed et al., 2021) and VCs (Sporny et al., 2019), two common technological features of SSI models.

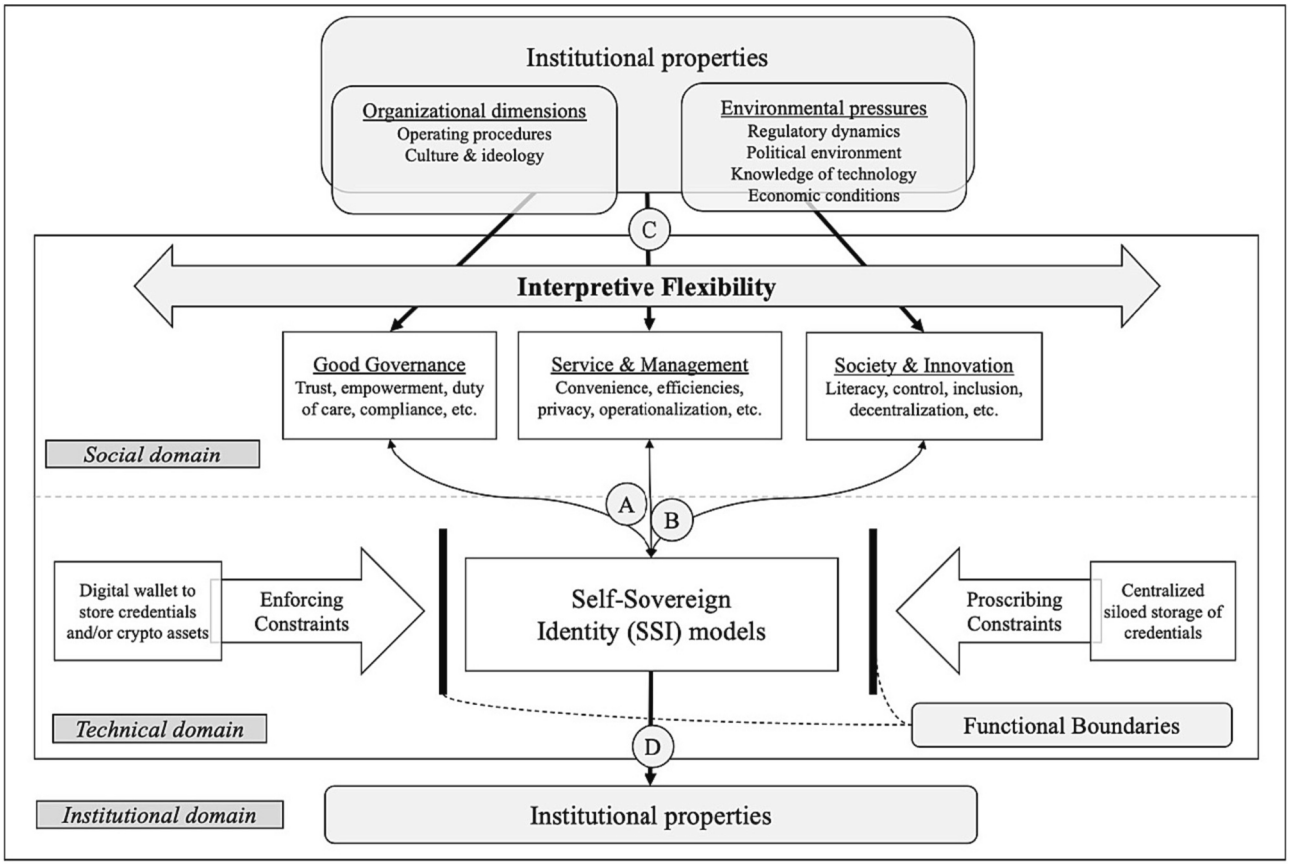

Fig. 1. Extended Model of Interpretive Flexibility adapted from Doherty et al. (2006) and Orlikowski (1992), in the context of SSI.

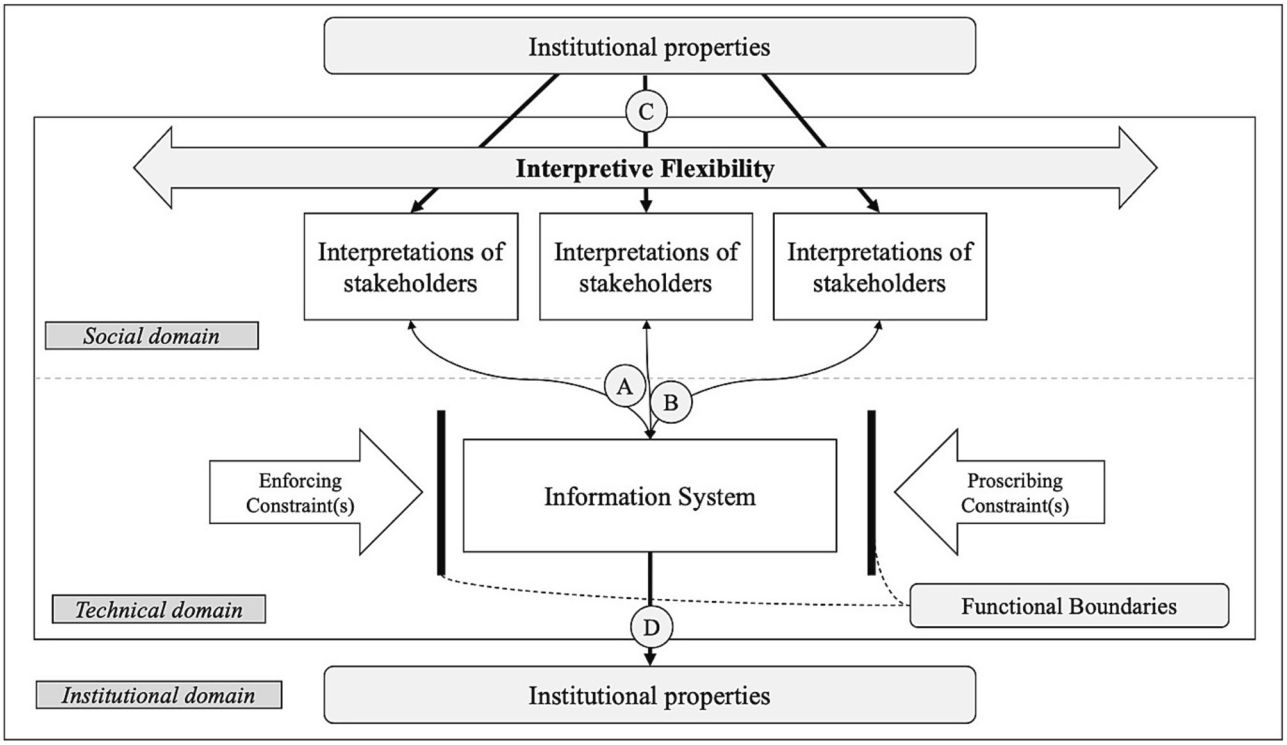

Fig. 2. Proposed Extended Model of Interpretive Flexibility adapted from Doherty et al. (2006) and Orlikowski (1992).

concerns. Beyond conducting interpretive analyses for emerging IT artifacts in general, several policy, managerial and design implications for SSI specifically can be drawn.

Policy. With regard to the service SSI offers to users, results clarified that the idea of SSI corresponds with a convenient and efficient identity management system. From the broader standpoint of a society that undergoes innovation, the implementation and design of SSI systems deserves considerations that weigh data control and decentralization against the reality of a society in which not all members are digitally literate or have access to certain technological devices. Based on this analysis, it is possible to map industry or citizen needs, and incorporate those into potential policies. This is a promising research avenue for public policy scholarship and recommendation for policy-making.

Management. From a managerial or governance perspective, the relationship between citizens and public administrations should be carefully assessed (Janssen & Helbig, 2018). While SSI might be the desired systems to enhance user empowerment and independence, it might not be the necessary digital identity management system in societies that trust and rely on their centralized institutions. Further managerial implications emerge from the difficulty of devising a business model from decentralized digital identity management. This is to a large extent due to the problem of monetizing identity and the non-profitability of wallets for commercial providers. On the one hand, governmental support is needed to create value from SSI for all citizens. On the other hand, technical expertise of private entities is required for effective and efficient implementation. Many experts thus advocate for multi-stakeholder governance models supported by public-private partnerships or consortia. It should be noted that this implication is empirically supported by expert interviews, and not by the assessment of implemented and running SSI projects. Therefore, such institutional partnerships might not be the only recipe to success as further research may investigate experiences from different governance models for the development of SSI that are successful or failed. A sound starting point for these investigations are Sedlmeir et al. (2022), Giannopoulou (2023), and Smethurst (2023).

Design. Although we have to acknowledge the construct of SSI has thus far not reached "closure", some inferences can be made based on our findings, notably regarding the functional boundaries of SSI. The enforcing constraint of SSI is a software application to hold users' credentials, the so-called digital wallet. Therefore, we know that for the design of any SSI project, a digital wallet is essential. The proscribing constraint is centralization, because a decentralized infrastructure is a basic design prerequisite for SSI (see also, Sedlmeir et al., 2022). This should not be confused with the use of DLT as a design requirement. Our analysis finds that the use of DLT does not lie within the functional boundaries of SSI.

Beyond the technical, further design implications can be drawn. All stakeholder groups emphasized the importance of data control and user convenience or user-centricity. With regards to the former, it is crucial that the data subject has the right and ability to access and manage their identity information. Hence, the usability and performance of an SSI system is dependent on the end-user experience – including aspects like simplicity, intuition, or interface aesthetics – which should not be neglected in the design of the system (see also, Sartor et al., 2022).

By giving control over their data to the users, SSI frameworks essentially presuppose an individual's capability of managing and controlling his or her own identity data. Yet, as Hummel, Braun, Augsberg, and Dabrock (2018) rightfully denote, "[individuals] cannot be sovereigns if they proceed under ignorance of central features and abilities of the technology they are using". In other words, it is unclear whether all data subjects can indeed be entrusted with the task of self-management, critical reasoning, and the understanding of data-infrastructures in order to assess in which cases to share data or restrict access. If one assigns users this responsibility, they should have the right to receive the adequate education and training to develop their data literacy (Gray, Gerlitz, & Bounegru, 2018).

6.4. Limitations and future research

Our study comes with certain limitations. First, we recognize that although the qualitative coding of our data has been conducted by three researchers in independent three-stage coding cycles, subconscious biases are difficult to eliminate. Thus, while qualitative coding of documents allows for in-depth exploration of rich and nuanced data, it is always exposed to some degree of subjectivity in coding decisions, making the results less generalizable compared to quantitative research methods. Second, due to the low number of people acquainted with SSI, we only held interviews with experts that, by definition, have a proven track record in eID and hold an interest in SSI. This may have biased the range of interpretive flexibility to some extent. For a full societal view of the interpretive flexibility, surveys could be a valuable method to gain large-scale insights from different stakeholders. Taking into account different stakeholders, we acknowledge that we did not include the perspective of users in the shaping of SSI. They are crucial in the policy-making process of eID systems (Lips, 2010). We foresee this as avenue for future research, in particular when SSI systems are implemented and adopted more systematically. Third, beyond the case of SSI, we did not empirically evaluate and challenge the proposed EMIF. This limitation challenges its generalizability potential, but does not necessarily restrict or deny it. In theory, because institutional regimes undoubtedly play a role in supporting the performance and adoption of technical infrastructures and innovation (Edler & James, 2015; Finger et al., 2005; March & Olsen, 2010; Scharpf, 2018), we expect our proposed model and threefold perspective (social, technical, and institutional) to be appropriate. In practice, however, we foresee that applying, evaluating, and challenging the proposed EMIF presents a notable research opportunity.

7. Conclusion

Decentralized identity management systems are a relevant but still nascent topic for governments. The idea of 'self-sovereign' identity proves particularly paradoxical and ambiguous. The value-laden discourse around socio-technical constructs risk misrepresenting affordances that the technology can offer to users. Further, the limited and incoherent academic literature – stemming from the immature stage of SSI's development, its ambiguous understandings, and the divergent technical operationalizations – suggest an ambivalence to the IT at hand.

To unravel the various understandings of SSI, this study borrowed from the constructivist lens of SCOT and its concept of interpretive flexibility (Pinch & Bijker, 1984). Specifically, to delineate the technical boundaries of SSI, and its spectrum of interpretations among stakeholders, we drew on Doherty et al. (2006) re-conceptualization of IF. Their model provided a starting point to dissect how stakeholders generate different understandings of the same artifact, and how its technical specifications can in turn act as constraints – limiting the ability to be interpreted flexibly. Leaning on Orlikowski (1992), the influence of institutional properties was taken into account, which highlights possible connections between contextual factors, stakeholders' interpretation, and technological boundaries. Consequently, we propose the Extended Model of Interpretive Flexibility (EMIF) – which is a natural extension of the model proposed by Doherty et al. (2006) that takes into consideration the institutional domain.

By applying the EMIF to SSI, we are able to answer the question, asking how stakeholder interests and institutional properties shape the social embedding of self-sovereign electronic identification systems. We find that its socio-political understandings are ambiguous, but can be limited by the enforcing and proscribing constraints in its implementation. From a technical perspective, we identified the digital wallet as the former, and the centralized, siloed storage of identity credentials as the latter. The analysis of the institutional context yielded operating procedures, cultural differences, ideology, regulatory dynamics, political environments, and knowledge of technology as properties that influence

interpretations of SSI in the social domain.

Moreover, several policy, managerial and design implications for SSI can be drawn from our findings. First, we find that SSI is still a controversially constructed artifact with both beneficial and risky implications for society. Second, we question the reconciliation of the decentralized ambitions of self-sovereignty and user empowerment with the fundamental responsibilities of sovereign states vis-à-vis its citizens. Third, we highlight the difficulty of devising a functioning business model from SSI projects in commercial settings. Fourth, while the essential minimum technological feature of any SSI project is the digital wallet, our research sets forth that the use of DLTs in SSI is not a necessary feature and can even be detrimental to the originally envisioned objectives to preserve privacy, security and individual autonomy. As such, the theoretical constructivist frame developed in this paper can serve digital government practitioners and scholars in dissecting information systems and formulating productive agendas for implementation.

Potential future research may further acknowledge the role of standardization and the topic of interoperability, in which institutional properties may play a relevant role. Moreover, SSI's technical immaturity and lack of fully-fledged implementations prevented us from analyzing the perception of SSI among users as a fifth group of stakeholders. Generally, it can be concluded that a user-centric perspective to study SSI is yet another avenue for future researchers and policy-makers to consider.

CRediT authorship contribution statement

Linda Weigl: Conceptualization, Methodology, Investigation, Data curation, Formal analysis, Writing – original draft, Writing – review & editing. **Tom Barbereau:** Conceptualization, Methodology, Data curation, Formal analysis, Writing – original draft, Writing – review & editing. **Gilbert Fridgen:** Supervision, Formal analysis, Writing – review & editing, Funding acquisition.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. PayPal's financial support is administered via the FNR, and by contractual agreement, PayPal has no involvement in the authors' research.

Acknowledgements

The authors thank Johannes Sedlmeir and Reilly Smethurst for their contributions to the technical features table and the references list. They also thank Alexander Rieger for his contributions to the conference paper upon which this article builds. This research was funded by the Luxembourg National Research Fund (FNR) and PayPal PEARL (grant reference 13342933). For the purpose of open access, the authors have applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any author accepted manuscript version arising from this submission.

Appendix A. Interview partners

Table 3
Interviewees.

	Position	Organization	Experience (years)	Affiliation
I1	Legal Expert and Chief Trust Officer	Private eIDAS certified electronic evidence provider focusing on digital trust for legal security.	13	Not-for-profit org.
I2	Director of Computer Management Association	Intercommunal IT solutions provider committed to the transition to smart villages and cities.	15	Government
I3	Blockchain Use Case Convenor	Supranational blockchain infrastructure project for cross-border services.	6	Government
I4	Chief Trust Officer	IT company developing decentralized identity applications.	7	For-profit org.
I5	Director in Cyber Security and Digital Technologies	Ministerial department for e-commerce and information security.	6	Government
I6	Program Manager at Incubator Organization	Publicly funded incubator to develop an infrastructure for the verification of identity data.	2	For-profit org.
I7	CEO at IT Company	Cybersecurity company that provides digital identity technology solutions.	4	For-profit org.
I8	Technical Governance Board	Organization established to administer the governance of SSI on the internet.	7	Not-for-profit org.
I9	Head of Internal Audit	Ministerial branch for IT services for the government, ministries and administrations.	9	Government
I10	Researcher in Digital Identity	National agency for identity data dedicated to the secure and reliable use of identity data.	8	Researcher
I11	CIO at IT Consultancy	IT development and consulting company committed to identity and access management.	9	For-profit org.
I12	Researcher in Information Systems Security	Faculty for research in cyber security, data science, programming, and computational intelligence.	26	Researcher
I13	Head of Innovation Center at IT Service Company	Public-private organization developing a general-purpose, verifiable data network.	5	For-profit org.
I14	CEO of IT Company	IT company developing decentralized identity products, digital wallets and verifiable credentials.	3	For-profit org.
I15	Technical Architect at Independent Foundation	Foundation developing architecture for Internet-scale digital trust.	4	Not-for-profit org.
I16	Digital Solutions Consultant	Business intelligence and data warehousing consultancy.	4	Government
I17	Senior Policy Analyst on Digital Identity	Administrative branch of the committee of ministers responsible for federal financial management.	12	Government
I18	Policy Officer for ICT	National ministry of the interior.	6	Government
I19	Researcher in Data Ethics	Department of industrial engineering and innovation sciences	4	Researcher
I20	Advisor on Consumer Protection	National ministry responsible for consumer protection in the internal market and at national level.	2	Government
I21	Researcher in Sociology and Law	Cross-disciplinary national research center of excellence for automated decision-making and society.	5	Researcher

(*continued on next page*)

Table 3 (*continued*)

	Position	Organization	Experience (years)	Affiliation
I22	Deputy Head of Digital Banking Division	Digitalization unit within national financial institution.	4	For-profit org.
I23	Policy Officer for Government's CIO	National point of contact for the management of IT and digitization in the public administration.	5	Government
I24	CTO at Digital Trust Service Provider	Digital solutions development company and pan-European Qualified Trust Service Provider.	9	For-profit org.
I25	Consultant on Decentralized Identity	IT company developing SSI models for governments and businesses across industries.	1	For-profit org.
I26	Member of Blockchain Steering Committee	Governmental Working Group to support National Blockchain Roadmap Steering Committee.	3	Government
I27	Head of Cloud Applications, Data & AI	Private provider of digital services and communication in both national and international markets.	6	For-profit org.
I28	IT-System Electrician	Publicly funded company providing applications to receive, organize and share trusted data.	3	For-profit org.
I29	Growth and Strategy Manager	IT company offering financial service providers and customers access to digital innovations.	2	For-profit org.
I30	Test & Commissioning Manager	Independent consultant.	2	For-profit org.
I31	Researcher in Information Security	National organization for applied scientific research offering (contract research, consulting services and patent licensing).	20	Researcher
I32	CEO of Air Transport Security Company	Air transport security company offering security programs, training, and compliance assessments.	11	For-profit org.

Appendix B. Interview guide

Personal introduction
Where are you from?
What organization are you affiliated to?
What position do you hold in this organization?
Involvement in electronic identification (eID) projects
How long have you worked with eID management systems?
Please tell us about your experiences working with eID management systems.
How would you describe your current system's security features?
How would you describe your current system's privacy features?
How would you describe your current system's portability or compatibility features?
General understandings and perceptions of Self-Sovereign Identity (SSI)
What is the response to the name Self-Sovereign Identity and the concept of self-sovereignty?
Do you use SSI for login within your own company or organization?
What use cases benefit most from SSI in your opinion?
What are the sectors in which you think that SSI will be adopted first/fastest?
Why is SSI desirable from the perspective of governments? What should a regulator do to support SSI?
What benefits does SSI offer already? Is it production-ready?
What are the major challenges from a technical perspective and from a governance perspective?
Are there any studies on user experience with respect to SSI?
Is there an evaluation framework to help decision makers determine if VCs and DIDs are appropriate for their use-cases?
Would an evaluation framework created independently be of any use to developers and SSI companies?
Do you think that SSI is at risk when end-to-end encryption is attacked by law?
What objections do incumbents raise to SSI?
Mozilla complained that VCs require a high level of digital literacy and user competence. What are your thoughts on this?
Are wallet recovery methods production-ready for average users?

Appendix C. Whitepapers

Table 4
Collected whitepapers of solution providers.

SSI solution	Provider	Description (Information retrieved from the respective websites)
SOWL	esatus AG	SOWL is the Identity and Access Management SSI solution from esatus AG, headquartered in Germany. SOWL uses the Linux Foundations' open source Hyperledger Aries and Indy technology and supports all Indy DLT networks, like Sovrin and IDunion. SOWL can be used together with the esatus Wallet App.
Sovrin	Sovrin Foundation	The Sovrin Foundation, initiated by Evernym Inc. in 2016, is a nonprofit organization established to administer the Governance Framework governing the Sovrin Network – a public service utility enabling SSI on the internet. The Sovrin Foundation is an independent organization that is responsible for ensuring the Sovrin identity system is public and globally accessible. All networks are based on Hyperledger Indy.
ID Wallet	German Government	The German government aims at making as many credentials as possible available quickly, digitally and securely. An SSI ecosystem of digital identities is to be created in close cooperation with business partners. The government's "ID Wallet" was developed by the Digital-Enabling GmbH (a subsidiary of esatus AG).

(*continued on next page*)

Table 4 (*continued*)

SSI solution	Provider	Description (Information retrieved from the respective websites)
ID Alastria	Alastria Consortium	Alastria was founded in 2017 as a non-profit association based in Spain that promotes the digital economy through the development of DLT. ID Alastria is a digital identity model proposed by the Association for use in digital services and inspired by the SSI concept.
ION	Microsoft	ION, launched by Microsoft, is a public, permissionless, DIDs network that implements the blockchain-agnostic Sidetree protocol on top of Bitcoin. Sidetree is an open-source protocol for decentralized identifiers. ION is open source, so anyone can download the code and run an ION node to use the service.
Ontology	Ontology	Ontology is a DLT network launched by Chinese company Onchain in 2017. The Ontology platform specializes in decentralized digital identity and features two coins – the ONT coin and the gas token ONG. Ontology includes the ONTO Wallet and supports a variety of digital assets.
SelfKey	SelfKey Foundation	SelfKey Wallet LLC, a Nevis Limited Liability Company, is a DLT based SSI system. The SelfKey Foundation is a non-profit foundation whose charter and governance enshrines the principles of SSI with a free and open-source identity wallet for the credential holder, a JSON-LD protocol and a native token, KEY. The Portal Services are controlled and operated by the SelfKey Foundation out of the Federation of Saint Christopher/St. Kitts and Nevis.
eID+	Procivis AG	Procivis AG, founded in 2016, is a Swiss corporation that builds applications for SSI and personal data security and develops "e-government as a service" solutions backed by DLT. Procivis' first client is the Swiss canton of Schaffhausen, who is using the digital identity platform "eID+" to deliver e-government services to its citizens as a pilot.
VETRI	Procivis AG	As an extension of eID+, Procivis is working on a SSI and personal data management platform called "VALID" which was later renamed to "VETRI"

Appendix D. Codebook

Table 5
Codebook.

First-order themes	Second-order categories	Third-order codes	Number of allocated codes
Institutional Domain	Knowledge of technology	Evaluation framework	745
		Lack of clarity	
	Ideology	Brainwash	
		Beliefs	
		Mission	
		Radical	
		Movement	
		Religion	
	Political environment	Inactivity	
		National interest	
		Framing	
		Policies	
	Regulatory dynamics	Political	
		Legal change	
		EU Legislation	
		Compliance	
		Legal validity	
	Culture	Lack of authority	
		(Institutional) trust	
		Lacking trust	
		Continental differences	
		National Differences	
		Freedom	
	Operating procedures	Lack of identity documents	
		Lack of digital evidence	
		National infrastructure	
		Public administrative procedures	
		Paper-based	
		Organizational change	
	Digital identity mechanisms	Data collection	
		Verifiability	
		Decentralized identity	
		Identity card	
		Identity management	
		Authorization	
		Authentication	
		Identification	
Technical Domain	Importance of digital wallet		1376
	Technical problems	Lack of security & data leakage	
		Siloed solutions	
		Legacy IT issues	
		Immaturity	
		Inconvenience & usability problems	
		Cross-border interoperability	
		User complication	
	Technical considerations	Data concentration	
		Data portability	
		Data management risks	
		Level of assurance	

(*continued on next page*)

Table 5 (*continued*)

First-order themes	Second-order categories	Third-order codes	Number of allocated codes
		Interoperability	
		Service providers & verifiers	
		Cryptography	
		Revocation	
		Binding	
		Centralized	
		Decentralized	
		Open source	
		Standards	
		Zero-knowledge-proof	
		Decentralized public key infrastructure	
		Selective disclosure	
		Verifiable credential	
	Technical features	Infrastructure	
		Digital wallet	
		Decentralized identifier	
		Digital signature	
		Public & private keys	
		Biometrics	
		Accessibility	
		User empowerment	
		Impulsive user needs	
	Values	Latent user needs	
		Anchoring values	
		Pushing values	
	Decentralization		
	Risks		
	Hesitant		
	'Policy Realism'		
Social Domain: Good Governance (Duty-oriented)		Unprepared	391
	Public Sector	Decision-makers	
		Certificate authorities	
		Identity provider	
		Financial constraints	
		Database	
	Governments	Audit	
		Protection	
		Supervision	
		Responsibility	
	Exclusion		
	Banks		
	Client		
	SSI for the user		
	Efficiency		
	Digitalization		
	Governmental interest		
	Government as issuer		
		Unnecessary	
	SSI problems	Useless	
		Self-assertive	
Social Domain: Service and Management (Service-oriented)		Complex	316
	Fraud		
	Solutionism		
	Data management		
	Convenience vs. control		
	User-friendliness		
	Experience		
	Inefficiency		
		Cross-sector	
	Digital identity purposes	Cross-industry	
		Cross-border	
		Terminology	
		Unawareness	
	Knowledge, awareness & understanding	Education	
		Digital literacy	
		Lack of understanding	
	Data sharing		
	Data monetization		
Social Domain: Society and Innovation (Socially-oriented)	Technological sovereignty		909
	Data sovereignty	Data control	
		Paradox	
	Conceptual confusion	Misleading connotation: blockchain	
		Misleading terminology: data ownership	
		Principles	
	Techno-optimism	Utopia	
		Hype	

(*continued on next page*)

Table 5 (*continued*)

First-order themes	Second-order categories	Third-order codes	Number of allocated codes
Social Domain: Business and Profit (Profit-oriented)	User	Data portability Data autonomy Lack of trust Lack of control Privacy Empowerment Control Consent Ownership User-centricity Security	136
	Citizens	Individual Technology perception Resistance to digital identity models	
	Big Tech	Microsoft Google Facebook Apple	
	No added value		
	Added value		
	Marketing strategy	Selling SSI Lobbying Persuasion Adoption Interest attraction	
	Business model	Wallet business model problems	
	Financial problems		
	Commercial interest		
	Collaborative governance models	Public-private not-for-profit entity Consortium Cooperative entity	
	Financial benefits		

References

Addo, A., & Senyo, P. K. (2021). Advancing e-governance for development: Digital identification and its link to socioeconomic inclusion. *Government Information Quarterly, 38*, Article 101568.

Aladwani, A. M. (2013). A cross-cultural comparison of Kuwaiti and British citizens' views of e-government interface quality. *Government Information Quarterly, 30*, 74–86.

Alastria Association Network Consortium. (2020). *Whitepaper*. Alastria ID: Privacy Rational.

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

Backhouse, J., & Halperin, R. (2008). Security and privacy perceptions of E-ID: A grounded research. In *16th European conference on information systems (ECIS 2008), Galway, Ireland* (pp. 1382–1393).

Barbereau, T., Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2022). Tokenization and regulatory compliance for art and collectible markets: From regulators' demands for transparency to investors' demands for privacy. In M. Lacity, & H. Treblmeir (Eds.), *Blockchains and the token economy: Studies in theory and practice*. London: Palgrave Macmillan.

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems, 17*, 165–176. https://doi.org/10.1016/j.jsis.2007.12.002

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Brinkmann, S., & Kvale, S. (2015). *InterViews: Learning the craft of qualitative research interviewing* (3rd ed.). SAGE Publications.

Bundeskanzleramt. (2021). *Report. Digitale Identität: Wie ein Ökosystem digitaler Identitäten zu einem selbstbestimmten und zugleich nutzerfreundlichen Umgang mit dem digitalen Ich beitragen kann*.

Bundesregierung. (2021). Germany and Spain and join forces on the development of a cross-border, decentralised digital identity ecosystem. Retrieved from https://www.bundesregierung.de/breg-de/suche/germany-and-spain-and-join-forces-on-the-development-of-a-cross-border-decentralised-digital-identity-ecosystem-194 Accessed April 5, 2022.

Canales, K. (2021). Hackers scraped data from 500 million LinkedIn users — about two-thirds of the platform's userbase — and have posted it for sale online. Retrieved from https://businessinsider.mx/hackers-scraped-data-from-500-million-linkedin-users-about-two-thirds-of-the-platforms-userbase-and-have-posted-it-for-sale-online/.

Cap, C. H., & Maibaum, N. (2002). Digital identity and its implication for electronic government. In B. Schmid, K. Stanoevska-Slabeva, & V. Tschammer (Eds.), *Towards the E-society*. Boston: Kluwer Academic Publishers. https://doi.org/10.1007/0-306-47009-8_59.

Chadwick, D. W., Laborde, R., Oglaza, A., Venant, R., Wazan, S., & Nijjar, M. (2019). Improved identity management with verifiable credentials and fido. *IEEE Communications Standards Magazine, 3*, 14–20.

Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM, 28*, 1030–1044. https://doi.org/10.1145/4372.4373

Cheesman, M. (2020). Self-sovereignty for refugees? The contested horizons of digital identity. *Geopolitics, 27*(1), 134–159. https://doi.org/10.1080/14650045.2020.1823836

Corbin, J., & Strauss, A. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (4th ed.). SAGE Publications.

Dawes, S. S., & Pardo, T. A. (2002). Building collaborative digital government systems: Systemic constraints and effective practices. In A. K. Elmagarmid, W. J. McIver, & A. K. Elmagarmid (Eds.), *Advances in digital government*. Boston, MA: Springer US. https://doi.org/10.1007/0-306-47374-7_16.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160.

Doherty, N. F., Coombs, C. R., & Loan-Clarke, J. (2006). A re-conceptualization of the interpretive flexibility of information technologies: Redressing the balance between the social and the technical. *European Journal of Information Systems, 15*, 569–582. https://doi.org/10.1057/palgrave.ejis.3000653

Edler, J., & James, A. D. (2015). Understanding the emergence of new science and technology policies: Policy entrepreneurship, agenda setting and the development of the European framework programme. *Research Policy, 44*, 1252–1265.

Esatus, A. G. (2019). *Whitepaper*. Identity & Access Management (IAM) – Realisiert mit Self-Sovereign Identity (SSI).

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

Finger, M., Groenewegen, J., & Künneke, R. (2005). The quest for coherence between institutions and technologies in infrastructures. *Journal of Network Industries*, 227–259.

Finnish Government. (2021). Finland and Germany intensify cooperation to promote digital identification. Retrieved from https://valtioneuvosto.fi/en/-/10623/finland-and-germany-intensify-cooperation-to-promote-digital-identification Accessed October 10, 2021.

Frederickson, H. G., Smith, K. B., Larimer, C. W., & Licari, M. J. (2018). *The public administration theory primer* (3rd ed.). New York: Routledge.

Gascó, M. (2003). New technologies and institutional change in public administration. *Social Science Computer Review, 21*, 6–14.

Geels, F. W. (2002). Technological transitions as evolutionary reconfiguration processes: A multi-level perspective and a case-study. *Research Policy, 31*, 1257–1274. https://doi.org/10.1016/S0048-7333(02)00062-8

Giannopoulou, A. (2023). Digital identity infrastructures: A critical approach of self-sovereign identity. *Digital Society, 2*, 18. https://doi.org/10.1007/s44206-023-00049-z

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

Giddens, A. (1979). *Central problems in social theory: Action, structure, and contradiction in social analysis*. London: Palgrave Macmillan.

Gray, J., Gerlitz, C., & Bounegru, L. (2018). Data infrastructure literacy. *Big Data & Society, 5*(2), 2053951718786316.

Haas, C. (1999). On the relationship between old and new technologies. *Computers and Composition, 16*, 209–228. https://doi.org/10.1016/S8755-4615(99)00003-1

Halpin, H. (2020). Vision: A critique of immunity passports and W3C decentralized identifiers. In T. van der Merwe, C. Mitchell, & M. Mehrnezhad (Eds.), *Security standardisation research: 6th international conference*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-64357-7.

Hargadon, A. B., & Douglas, Y. (2001). When innovations meet institutions: Edison and the design of the electric light. *Administrative Science Quarterly, 46*, 476–501.

Henningsson, S., & Henriksen, H. Z. (2011). Inscription of behaviour and flexible interpretation in information infrastructures: The case of European e-customs. *The Journal of Strategic Information Systems, 20*, 355–372. https://doi.org/10.1016/j.jsis.2011.05.003

Herian, R. (2020). Blockchain, GDPR, and fantasies of data sovereignty. *Law, Innovation and Technology, 12*, 156–174. https://doi.org/10.1080/17579961.2020.1727094

Hiller, J., & Belanger, F. (2001). *Privacy strategies for electronic government*. E-Government Series.

Holmes, A. (2021). 533 million Facebook users' phone numbers and personal data have been leaked online. Retrieved from https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4.

Hughes, T. P. (1987). The evolution of large technological systems. In W. E. Bijker, T. P. Hughes, & T. Pinch (Eds.), *The social construction of technological systems: New directions in the sociology and history of technology*. Cambridge, MA: MIT Press.

Hummel, P., Braun, M., Augsberg, S., & Dabrock, P. (2018). Sovereignty and data sharing. *ITU Journal: ICT Discoveries, 2*.

Husz, O. (2018). Bank identity: Banks, ID cards, and the emergence of a financial identification society in Sweden. *Enterprise and Society, 19*, 391–429. https://doi.org/10.1017/eso.2017.43

Ishmaev, G. (2020). Sovereignty, privacy, and ethics in blockchain-based identity management systems. *Ethics and Information Technology, 1–14*. https://doi.org/10.1007/s10676-020-09563-x

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly, 32*, 221–236.

Janssen, M., & Helbig, N. (2018). Innovating and changing the policy-cycle: Policy-makers be prepared! *Government Information Quarterly, 35*, 99–105.

Jin, D. Y. (2015). *Digital platforms, imperialism and political culture* (1st ed.). New York: Routledge. https://doi.org/10.4324/9781315717128

Jones, B. D. (1994). *Reconceiving decision-making in democratic politics: Attention, choice, and public policy*. University of Chicago Press.

Kahn, P. W. (2011). *Political theology: Four new chapters on the concept of sovereignty*. New York: Columbia University Press.

Keohane, R. O. (2002). Ironies of sovereignty: The European Union and the United States. *Journal of Common Market Studies, 40*, 743–765. https://doi.org/10.1111/1468-5965.00396

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 23*, 67–93. https://doi.org/10.2307/249410

Koppenjan, J., & Groenewegen, J. (2005). Institutional design for complex technological systems. *International Journal of Technology, Policy and Management, 5*, 240–257.

Kubach, M., Schunck, C. H., Sellung, R., & Roßnagel, H. (2020). Self-sovereign and decentralized identity as the future of identity management? *Open Identity Summit, 2020*, 1–13.

Kuperberg, M. (2020). Blockchain-based identity management: A survey from the enterprise and ecosystem perspective. *IEEE Transactions on Engineering Management, 67*, 1008–1027. https://doi.org/10.1109/TEM.2019. 2926471

Law, J., & Callon, M. (1992). The life and death of an aircraft: A network analysis of technical change. In W. E. Bijker, & J. Law (Eds.), *Shaping technology-building society: Studies in sociotechnical change*. Cambridge, MA: MIT Press.

Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly, 18*, 122–136. https://doi.org/10.1016/S0740-624X(01)00066-1

Leech, B. L. (2002). Asking questions: Techniques for semistructured interviews. *Political Science & Politics, 35*, 665–668.

Lips, A. M. B., Taylor, J. A., & Organ, J. (2009). Managing citizen identity information in E-government service relationships in the UK: The emergence of a surveillance state or a service state? *Public Management Review, 11*, 833–856. https://doi.org/10.1080/14719030903318988

Lips, M. (2010). Rethinking citizen – Government relationships in the age of digital identity: Insights from research. *Information Polity, 15*(4), 273–289. https://doi.org/10.3233/IP-2010-0216

Luna-Reyes, L. F., & Gil-Garcia, J. R. (2014). Digital government transformation and internet portals: The co-evolution of technology, organizations, and institutions. *Government Information Quarterly, 31*, 545–555.

MacKenzie, D., & Wajcman, J. (1985). *The social shaping of technology*. Open University Press.

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

March, J. G., & Olsen, J. P. (2010). *Rediscovering institutions*. Simon and Schuster.

Mayer-Schönberger, V. (2013). *Big data: A revolution that will transform how we live, work, and think*. Boston: Houghton Mifflin Harcourt.

Mayring, P. (2014). *Qualitative content analysis: Theoretical foundation, basic procedures and software solution. Klagenfurt*.

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly, 36*, Article 101385.

Microsoft. (2018). *Whitepaper. Decentralized Identity: Own and control your identity*.

Mir, U. B., Kar, A. K., Dwivedi, Y. K., Gupta, M., & Sharma, R. (2020). Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India. *Government Information Quarterly, 37*, Article 101442. https://doi.org/10.1016/j.giq.2019.101442

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review, 30*, 80–86. https://doi.org/10.1016/j.cosrev.2018. 10.002

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization, 17*, 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

Newell, B. C. (2014). Technopolicing, surveillance, and citizen oversight: A neorepublican theory of liberty and information control. *Government Information Quarterly, 31*, 421–431. https://doi.org/10.1016/j. giq.2014.04.001

Nograšek, J., & Vintar, M. (2014). E-government and organisational transformation of government: Black box revisited? *Government Information Quarterly, 31*, 108–118.

Nooteboom, B. (2000). Institutions and forms of co-ordination in innovation systems. *Organization Studies, 21*, 915–939.

OECD. (2011). *OECD digital economy papers. Digital identity management: Enabling innovation and trust in the internet economy*. https://doi.org/10.1787/5kg1zqsm3pns-en

Ølnes, S., & Jansen, A. (2017). Blockchain technology as support infrastructure in e-government. In M. Janssen, K. Axelsson, O. Glassey, B. Klievink, R. Krimmer, I. Lindgren, … D. Trutnev (Eds.), *Electronic government*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-64677-0_18.

Ontology. (2017). Whitepaper. In *Ontology: A new high performance public multi-chain project & a distributed trust collaboration platform*.

Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization Science, 3*, 398–427. https://doi.org/10.1287/orsc.3.3.398

Orlikowski, W. J. (2000). Using technology and constituting structures: A practice lens for studying technology in organizations. *Organization Science, 11*, 404–428. https://doi.org/10.1287/orsc.11.4. 404.14600

Otjacques, B., Hitzelberger, P., & Feltz, F. (2007). Interoperability of e-government information systems: Issues of identification and data sharing. *Journal of Management Information Systems, 23*, 29–51. https://doi.org/10.2753/MIS0742-1222230403

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science, 14*, 399–441. https://doi.org/10.1177/030631284014003004

Pollitt, C. (2008). *Time, policy, management: Governing with the past*. Oxford: Oxford University Press.

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

Procivis, A. G. (2017). Whitepaper. In *Procivis eID+ Produktpräsentation Juni 2017*.

Reed, D., Sporny, M., & Sabadello, M. (2021). Decentralized identifiers (DIDs) v1.0 Core architecture, data model and representations. Retrieved from https://www.w3.org/TR/did-core/.

Rubin, H., & Rubin, I. (2012). *Qualitative interviewing: The art of hearing data* (3rd ed.). https://doi.org/10.4135/9781452226651 Thousand Oaks, California.

Russell, S. (1986). The social construction of artefacts: A response to pinch and bijker. *Social Studies of Science, 16*, 331–346.

Sahay, S., & Robey, D. (1996). Organizational context, social interpretation, and the implementation and consequences of geographic information systems. *Accounting, Management and Information Technologies, 6*, 255–282. https://doi.org/10.1016/S0959-8022(96)90016-8

Sartor, S., Sedlmeir, J., Rieger, A., & Roth, T. (2022). Love at first sight? A user experience study of self-sovereign identity wallets. In *30th European conference on information systems, Timişoara, Romania*.

Savoldelli, A., Codagnone, C., & Misuraca, G. (2014). Understanding the e-government paradox: Learning from literature and practice on barriers to adoption. *Government Information Quarterly, 31*, 63–71.

Scharpf, F. W. (2018). *Games real actors play: Actor-centered institutionalism in policy research*. New York: Routledge.

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization, 21*, 1–16.

Schuppan, T. (2009). E-government in developing countries: Experiences from sub-saharan africa. *Government Information Quarterly, 26*, 118–127.

Scott, W. R. (1995). *Institutions and organizations. Foundations for organizational science*. SAGE Publications.

Sedlmeir, J., Huber, J., Barbereau, T. J., Weigl, L., & Roth, T. (2022). Transition pathways towards design principles of self-sovereign identity. In *43rd international conference on information systems (ICIS 2022), Copenhagen, Denmark*.

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

SelfKey Foundation. (2017). *Whitepaper*. SelfKey: The SelfKey Foundation.

Seltsikas, P., & 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*, 93–103. https://doi.org/10.1057/ejis.2009.51

Smethurst, R. (2023). Digital identity wallets and their semantic contradictions. In *31st European conference on information systems (ECIS), Kristiansand, Norway*.

Sovrin. (2018). *Sovrin: A Protocol and Token for SelfSovereign Identity and Decentralized Trust.* Sovrin Foundation.

Sporny, M., Longely, D., & Chadwick, D. (2019). Verifiable credentials data model 1.0. Retrieved from https://w3c.github.io/vc-data-model/WD/2018-07-18/ Accessed May 5, 2021.

Star, S. L., & Griesemer, J. R. (1989). Institutional ecology, translations and boundary objects: Amateurs and professionals in berkeley's museum of vertebrate zoology, 1907-39. *Social Studies of Science, 19*, 387–420.

Stillman, R. J. (1997). American vs. European public administration: Does public administration make the modern state, or does the state make public administration? *Public Administration Review, 57*, 332–338. https://doi.org/10.2307/977316

Thomas, J. C., & Streib, G. (2003). The new face of government: Citizen-initiated contacts in the era of E-government. *Journal of Public Administration Research and Theory, 13*(1), 83–102.

Tobin, A., & Reed, D. (2017). Whitepaper. In *The inevitable rise of self-sovereign identity.* Sovrin Foundation.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance and Society, 12*, 197–208. https://doi.org/10.24908/ss.v12i2.4776

Van Dijck, J., & Jacobs, B. (2020). Electronic identity services as sociotechnical and political-economic constructs. *New Media & Society, 22*, 896–914. https://doi.org/10.1177/1461444819872537

VETRI. (2020). Whitepaper. In *VETRI: Value Your Data*.

Walters, W. (2006). Border/control. *European Journal of Social Theory, 9*, 187–203.

Weerakkody, V., Janssen, M., & Dwivedi, Y. K. (2011). Transformational change and business process reengineering (bpr): Lessons from the british and dutch public sector. *Government Information Quarterly, 28*, 320–328.

Weigl, L., Amard, A., Codagnone, C., & Fridgen, G. (2022). The EU's digital identity policy: Tracing policy punctuations. In *In 15th international conference on theory and practice of electronic governance (ICEGOV 2022), Guimarães, Portugal.* https://doi.org/10.1145/3560107.3560121

Weinberger, M. (2016). It happened again: Yahoo says 1 billion user accounts stolen in what could be biggest hack ever. Retrieved from https://www.businessinsider.com/yahoo-data-breach-billion-accounts-2016-12.

West, D. M. (2007). *Digital government: Technology and public sector performance.* Princeton, NJ: Princeton University Press.

Wihlborg, E. (2013). Secure electronic identification (eID) in the intersection of politics and technology. *International Journal of Electronic Governance, 6*, 143–151. https://doi.org/10.1504/IJEG.2013.058371

Williams, R., & Edge, D. (1996). The social shaping of technology. *Research Policy, 25*, 865–899.

Winner, L. (1980). Do artifacts have politics? *Daedalus, 109*(1), 121–136.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*, 75–89.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* Public affairs, Hachette Book Group.

Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital identity and the blockchain: Universal identity management and the concept of the "self-sovereign" individual. *Frontiers in Blockchain, 3*, 1–28. https://doi.org/10.3389/fbloc.2020.00026

Linda Weigl is a postdoctoral researcher at the University of Amsterdam's Institute for Information Law. Her research interests lie in digital sovereignty, digital regulation, and trustworthiness in the digital society. Linda focuses on platform regulation and digital trust dynamics of decentralized infrastructures. She further analyzes how technology-centric solutions can be reconciled with democratic criteria and public values.

Tom Barbereau is a doctoral researcher at the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg and a visiting researcher at the Institute for Information Law, University of Amsterdam. His-academic research focuses on socio-technical controversies in and of decentralized technologies; not least, in the development of 'self-sovereign' identity regimes, Decentralized Finance, and Decentralized Autonomous Organizations.

Gilbert Fridgen is Professor and PayPal-FNR PEARL Chair in Digital Financial Services at the Interdisciplinary Centre for Security, Reliability, and Trust (SnT), University of Luxembourg. In his research, he analyzes the transformative effects of digital technologies on individual organizations and on the relationship between organizations. He addresses potentially disruptive technologies like Distributed Ledgers, Verifiable Credentials, Artificial Intelligence, or the Internet-of-Things. His research involves information systems engineering, IT strategy and (risk) management, as well as regulatory compliance. In his projects and partnerships, he collaborates with partners in financial services, energy, mobility, manufacturing, consulting, as well as with public bodies and governments.