The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility

Linda Weigl
University of Luxembourg
linda.weigl@uni.lu
ORCID: 0000-0003-3794-8754

Tom Barbereau
University of Luxembourg
tom.barbereau@uni.lu
ORCID: 0000-0002-8554-0991

Alexander Rieger
University of Luxembourg
alexander.rieger@uni.lu
ORCID: 0000-0001-7996-4678

Gilbert Fridgen
University of Luxembourg
gilbert.fridgen@uni.lu
ORCID: 0000-0001-7037-4807

Abstract

User-centric identity management systems are gaining momentum as concerns about Big Tech and Big Government rise. Many of these systems are framed as offering Self-Sovereign Identity (SSI). Yet, competing appropriation and the social embedding of SSI have resulted in diverging interpretations. These vague and value-laden interpretations can damage the public discourse and risk misrepresenting values and affordances that technology offers to users. To unpack the various social and technical understandings of SSI, we adopt an 'interpretive flexibility' lens. Based on a qualitative inductive interview study, we find that SSI's interpretation is strongly mediated by surrounding institutional properties. Our study helps to better navigate these different perceptions and highlights the need for a multidimensional framework that can improve the understanding of complex socio-technical systems for digital government practitioners, researchers, and policy-makers.

1. Introduction

Electronic identification is essential for the digital interaction between parties who do not know or trust each other [1]. Current digital identity systems give rise to numerous privacy and security concerns regarding the aggregation of personal data. For electronic services provided by governments, citizen's identity data are mostly stored in centralized silos. This architecture is vulnerable to cybercrimes, such as identity theft and personal data misuse [2].

In response to these risks, there is a nascent demand for a decentralized digital identity paradigm that upholds users' privacy rights and does not rely on centralized databases. This demand led to decentralized identity schemes and *distributed ledger technology* (DLT) becoming a noticeable trend [3, 4]. Members of digital identity communities on the Internet began promoting this emancipatory paradigm under the heading of *Self-Sovereign Identity* (SSI) [5, 6]. It promises users the power to 'own' their identities [7].

Although SSI projects do not all use the same technologies, there are three particular components commonly associated with SSI's principles: *decentralized identifiers* (DIDs), an alternative to static identifiers like social security and credit card numbers [8]; *verifiable credentials* (VCs), a new type of digital certificate stored in user-controlled wallet apps that can be used for a broad array of identity documents [9]; and a decentralized *public key infrastructure* (PKI), based on a DLT, such as blockchain PKI [4].

Because of SSI's common association with value-laden technologies like blockchain [10], it is often caught up with DLT-related hype, idiosyncratic visions of a fully decentralized world, and the vaguely defined notion of self-sovereignty [3, 11]. In fact, the competing appropriation and the social embedding of SSI results in a range of different interpretations among stakeholders, such as public sector institutions or private companies. Not only are terms like *self-sovereignty* or *data sovereignty* difficult to grasp, but they are also being diagnosed as '*data dysphoria'* in order to connotate a "type of unease manifest in cyberspace" based on the perceived retreat or failure of social mechanisms and institutions [12]. This suggests that even from an institutional perspective, understandings on

URI: https://hdl.handle.net/10125/79649
978-0-9981331-5-7

decentralized paradigms, like SSI, seem to differ. It appears that particularly libertarian societies gravitate towards decentralized technologies that 'liberate' citizens from centralization and control [13]. However, the decentralization of digital identity management systems also starts to attract the interest of societies that place a higher trust in institutions. The European Union (EU), for instance, published a new legal proposal on a "trusted and secure European e-ID" which foresees the introduction of a European Digital Identity Wallet [14].

In short, the ambiguity of SSI's technical implementations [15], and its manifold social interpretations make SSI capable to be shaped by the flexible interests of social actors that are interacting with this set of technologies. Yet, the undefined and, sometimes misleadingly, value-laden discourse about SSI can damage public understandings, as its contestations go beyond mere confusion. We thus formulated the following research question: *How is SSI shaped by social actors, technical constraints and the underlying institutional context?*

To answer our research question and navigate through the various understandings of SSI on a social, technical and institutional level, we conduct a qualitative inductive analysis grounded in expert interviews and technical documentation. It is important to note that the use of SSI is not restricted to the digital identification of individuals by public authorities. 'Digital identity' is an umbrella term that can express identity attributes of citizens, organizations, and even objects in the field of IoT. Accordingly, SSI is applicable to the identification of both human and non-human agents. This paper, however, focusses on the use of SSI by governmental agencies in the context of identifying individuals.

From a theoretical point of view, we draw on *interpretive flexibility* (IF) – a core concept of the Social Construction of Technology (SCOT) approach [16, 17]. Our primary objective is to map social and technical domains of SSI along Doherty et al.'s [18] model of interpretive flexibility. Given the contextual importance for SSI's interpretive flexibility, we seek to extend Doherty et al.'s model [18] to account for so-called *institutional properties* introduced by Orlikowski [19]. The study offers contributions to both theory and practice. From a theory perspective, this paper extends the IF model to include institutional properties. Implications for practice are provided by the findings which offer a foundation to understand and discuss SSI.

The paper is structured as follows. To clarify the relevance of IF for digital government, we first elaborate on the development of electronic identification systems as a socio-technical artifact. We subsequently provide different possible socio-political interpretations of SSI and its technical operationalization. We then analyze our data through the theoretical lens of IF and the concept of institutional properties. Finally, we discuss our results, present the extended model on IF, and conclude.

2. Background and Theoretical Lens

2.1. From centralized e-ID to SSI

The management of public service interactions between citizens and public administrations typically relies on citizens' identity information, such as name, date of birth, address or nationality. Since a few decades, governments transitioned from paper-based systems to electronic means of identification [20]. The growing demand for user identification via electronic interfaces is motivated by the objective to mitigate identity theft and to enable government agencies to collaborate more efficiently. For many governments, the introduction of electronic identification systems is also a crucial step towards a more transparent, trustworthy and legitimate information society more generally [21].

Yet, the remote interaction between users and public administrations comes with challenges regarding security, confidentiality, and the authentication of users. At the same time, the increasing digital cooperation of state agencies through a connected web of databases, the so-called vertical and horizontal integration stage of digital government development [22] depends on the exchange of sensitive data. This results in a paradox where electronic identification systems enhance security on the one hand, but may compromise users' privacy on the other. Eventually, data collection, cross-referencing, and the aggregation of metadata could lead to surveillance by the state or third parties [23].

Here, the developments and use of open standards, cryptographic protocols, and decentralized technologies represent significant efforts to address this dilemma. With the advent of DLT, new paradigms of decentralized identity or Self-Sovereign Identity entered the space of identity management [3, 4]. At the same time, electronic identification systems in digital government are steadily at the intersection of policy considerations and technical design. Therefore, they are subject to debates that are shaped by stakeholder's interpretations of the artefact in question. In addition, complex political dynamics, budget realities, path dependencies and the lack of political awareness are recognized factors that can affect the use of novel technologies in the public sector [21, 24, 25]. This gap between politics and technology emphasizes the importance of conceptual meanings around innovation and a commonly shared understanding of technology.

2.2. SSI's technical and social ambiguity

Despite its technical heterogeneity, there are 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 [8]. Another associated technical building block of SSI are VCs. VCs are an advanced machine-verifiable and cryptographically secure type of digital certificates, which are characterized by an issuer's digital signature. 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 [9]. Most digital wallets that are part of an SSI solution store either digital assets, identity information or both of them [15]. The wallet's holdings can be registered on DLT (which can include hashes of personally identifiable information), hence SSI is often described as "blockchain-based identity" [26]. Finally, there is a third type of wallet which neither stores cryptographic assets nor does it use VCs. Suffice to say, there is not yet an orthodox, technical definition for SSI solutions. It is thus viewed as "overwhelmingly confusing" by technical experts [3, 26]. From a technical point of view, SSI standards are still under development, which can pose a challenge to the implementation of mature SSI solutions. Yet, given that this paper is nor a technical evaluation of design options or attributes of SSI, the subsequent arguments engage with SSI's technological "features" [27] on a high-level presentation.

The next observation is socio-political and regards SSI as set of inconclusive socio-ethical principles. The conception of a self-sovereign identity or a sovereign individual did not emerge from philosophy, legal theory, or political science texts; instead, it came from blog posts, magazines, and Internet forums of software developers. Such forums defined SSI as a set of ethical principles and an idealistic vision in which individuals become "rulers of their own identity" [5]. Traditionally, sovereignty is conceived as an exceptional power, not something possessed by all [28]: the dominion of God, the Crown or the State are examples of such sovereign. Self-sovereignty, by contrast, denotes an individual's ability to control the digital exchange of assets and personal information [5, 7].

In the academic literature, Cheesman [11] 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 the control of bureaucracies. The SSI terminology entails an idiosyncratic conception of sovereignty; and self-sovereignty is in turn linked to other informal notions like data sovereignty, digital identity ownership, and personal data ownership [29, 30]. Indeed, proponents of SSI tend to appreciate technical features, yet depreciate "moral semantics"; hence the prevalence of simple narratives that posit SSI as 'good' and Big Tech or governments as 'bad' [30]. Halpin [31] suggests that the "cultish" libertarian proponents of SSI overlook ethical problems. He coined the term "cryptography theatre" to mock the use of cryptography to allay users' concerns. Zwitter et al. [29] 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.

2.3. The Social Construction of Technology

The broad school of the Social Shaping of Technology (SST) is concerned with the design and development of technologies – a process that is, aside from technical considerations, largely patterned by social factors [32]. As such, SST views innovation as a "garden of forking paths" [32] determined by both a technical dimension – composed of 'constraints' or 'affordances', and a social dimension – impacted by stakeholders and negotiations between them."

The prevailing rationale of this school is reflected in its seceding approaches, – namely, actor-network theory (ANT), sociotechnical systems theory, and the social construction of technology (SCOT). The SCOT approach seeks to understand technical developments and to highlight the social constructivist component thereof [16]. SCOT contains the concept of *interpretive flexibility* (IF) – the ability of a given technical artefact to symbolize "different things to different actors" [33]. IF allows different social groups to associate different meanings to a technology. For information systems, although the physical properties ensure the presence of clear "boundary conditions" on usage in the technical domain, the social domain remains unaccounted for in positivist approaches [34]. Therefore, information systems ought to be analyzed in constructivist terms, both in their technical and social domains. Arguing that little scholarly attention has been given to how a system's technical specifications may limit its interpretive flexibility, Doherty et al. [18] developed a re-conceptualization of IF in order to analyze the potential to tailor a given information system (Figure 1). Their model describes how stakeholders construct different understandings of the same artefact, and how

its technical characteristics provide *functional boundaries* on the system's ability to be interpreted flexibly. To delineate upper and lower limits with regards to these boundaries, Doherty et al. [18] introduce two confronting constraints. On one end of the spectrum are *enforcing constraints* – which are "mandatory" technical features, and thus deemed essential for the system's functionality. At the opposite end of the spectrum are *proscribing constraints* – representing functions that do not exist or cannot be used.

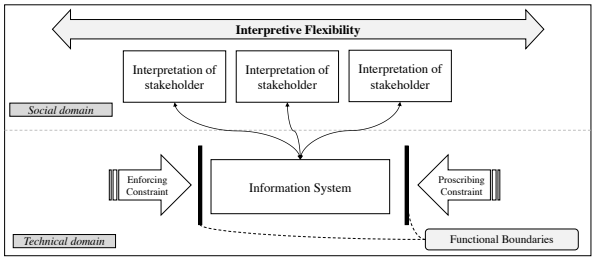

Figure 1. Model of interpretive flexibility

2.4. Structural Studies of Technology

In the advent of Structuration Theory, foundational studies established reciprocal links between structures and social agents without giving primacy to either [17, 19]. This theoretical foundation was employed by organizational researchers studying the relationship between technology and social structures. Orlikowksi [19] conceived technology as fundamentally dual. Her model (Figure 2) reflects this duality: technology is shaped by human agents (A), and in turn, influences the actions and behavior of users (B). Orlikowksi also considered *institutional properties* of organizations (e.g., budgets, business strategies, culture, expertise, regulation, etc.), as having an influence on humans' interaction with technology (C). She suggested that technology has consequences on institutional properties by reinforcing/transforming the status quo (D).

In information systems research, studies of technology do not strictly account for the IF of technical constraints [35]. The ones that do take a narrow organizational perspective without incorporating the impact of institutional properties as suggested by Orlikowski [19]. Although Doherty et al. [18] ground their model of IF in Orlikowski's organizational perspectives, the approach focuses exclusively on the interpretations of stakeholder groups and functional boundaries. For a socio-technical construct like SSI, the institutional properties may be a crucial factor to account for [11, 29]. Studying IF through a more holistic lens – one that includes stakeholders, technical constraints, and institutional properties – serves to answer our research question.

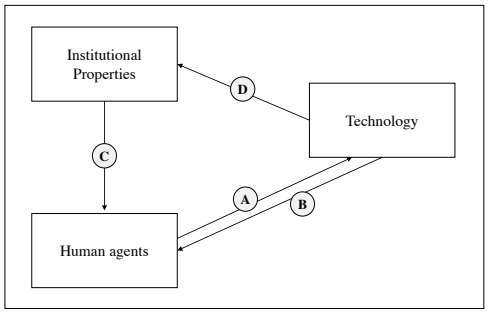

Figure 2. Structuration model of technology

3. Method

We followed a qualitative inductive approach to match our data-driven analysis. The inductive, qualitative analysis method consisted of a qualitative inductive interview study [36] with a supporting document analysis.

As part of our in-depth interview study, we conducted 20 semi-structured interviews with knowledgeable experts on credential and identity management. We conducted interviews to account for the novelty of SSI and the subsequent scarce amount of information available on SSI's implementation, best-practices, and interpretations. The study, executed in the context of a project with Luxembourg's Ministry for Digitalization, spanned over a period of five months. The composition of stakeholders consisted of seven participants that worked in for-profit companies, seven government officials, four interviewees that worked in non-profit organizations, and two researchers. Importantly, there is no conflict of interest with the interviewed researchers or overlap with the author team. Interviews were held individually via videoconference and lasted for about 60 minutes. The participants came from Europe, North America, the United Kingdom and Australia. While the technical boundaries of SSI were discussed with interviewees from all continents, the social and institutional properties mainly focused on the European context.

To study the various understandings and technical implementations of SSI, we further analyzed nine whitepapers of eight different solution providers and designers: SelfKey Foundation [37], Ontology [38], Procivis AG [39], Esatus [40], German Chancellery [41], Sovrin Foundation [7], Microsoft [42] and the Alastria Association Network Consortium [43].

Through the lens of Doherty et al.'s model [18], we analyzed both the social and technical domains of SSI. With the objective to identify patterns and answer our

research question along the lines of our theoretical framework, we followed the conventional stages of open, axial, and selective coding [44]. We coded our data using the qualitative analysis software MAXQDA [45]. In the first open coding phase, we analyzed whitepapers and interviews individually by assigning initial conceptual labels. In the second stage, the axial coding phase, we clustered codes across sources, elevating them to higher-levels themes. Specifically, we began separating the technical from the social domain, and congregated codes along technological features, social dimensions, and institutional contextual factors. The final process of coding aimed at identifying and creating overarching categories to group the matching themes based on our theoretical lens of the IF model. We used selective coding to identify properties of SSI and deduce social dimensions throughout the existing categories and subcategories [44]. In the technical domain, we sought to identify common technical specifications and constraints of the individual SSI projects. Based on Doherty et al.'s model of IF [18], we matched our cluster of codes with relevant elements of the model, such as 'stakeholders', 'interpretations', or 'functional boundaries'.

To structure our findings for SSI's IF in the social domain, we relied on Bannister and Connolly's taxonomy of public sector values of ICT that can be either *duty oriented*, *service oriented* or *socially oriented* [46]. We classified every stakeholder group's interpretation of SSI along each value orientation. We further observed a certain congruence with Orlikowki's [34] institutional properties, as our data approached an association between the institutional context and stakeholders' interpretations' of SSI.

4. Findings

We first analyzed our data from a technical and social (stakeholder) perspective. The technical IF of SSI is limited by *functional boundaries* consisting of both enforcing constraints and proscribing constraints. For the social domain, we discovered that the *social interpretive flexibility* is particularly pronounced in duty and socially oriented values of SSI. Our data analysis revealed a third, institutional dimension as SSI's social IF is subject to *institutional properties* – consisting of both organizational dimensions and environmental pressures.

4.1. Functional boundaries

As anticipated within the technical literature on SSI [4], its operationalizations in practice diverge significantly. Our interview data revealed that solutions labelled 'SSI' may be composed of numerous technical "features" [27]. 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. 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.

To ensure personal identity data management, a software application to hold credentials that runs on a users' hardware or a server in the cloud is essential. In other words, a mandatory technical building block we identified is a 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. While a digital wallet is as mandatory common denominator for an *enforcing constraint* [18], some 'outlier' SSI solutions exhibit *unique* enforcing constraints. For instance, the SelfKey Foundation 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 KEY in a "locked contract" (e.g., to access the network). SelfKey's native token, KEY, is indeed an enforcing constraint because it is mandatory for the network's overall functionality.

The *proscribing constraints* relate to functionalities that a system does *not* have or can or should *not* do. Our

Table 1. Different implementations of SSI

		Technological features						
Affiliation	**'SSI' solution**	Crypto- assets	VCs	Aries-compatible	Issuance fee-tokens	Mandatory on-chain identifiers	DLT-based PKI	DIDs
esatus AG	SeLF		X	X			X	X
Findy Coop.*	Findy		X	X			X	
Streetcred ID Inc.	Trinsic		X	X			X	X
Evernym Inc.*	Evernym		X	X			X	X
Sovrin Fdn. *	Sovrin		X	X			X	X
Main Incubator GmbH	IDunion		X	X			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+							
Verifiable Cred.Ltd.*			X					

interview data revealed that there is a recurring aversion towards centralized data storages and siloed databases. Thus, SSI seeks to store identity data in a decentralized fashion. Generally, decentralized storage is associated with the use of DLT [10]. While 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 solutions 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.

4.2. The social interpretive flexibility

We clustered the various interpretations of SSI along Bannister and Connolly's [46] taxonomy of public sector values (Table 2). The framework defines three types of values that typically underpin digital government services. *Duty oriented* values encompass the duty-bound aspects and mandates of public officials as servants to the state. *Service oriented* values for digital government incorporate values, such as efficiency, that seek to ensure high standards of services to citizens. Finally, *socially oriented* values cover a wider spectrum of political and social goals to generate added value to citizens and further social integration.

With regard to duty oriented SSI values, experts from not-for-profit and for-profit organizations viewed SSI as a possibility to re-establish and increase trust in central institutions as a "key enabler to enforce […] democratic principles." Public officials, on the other hand, emphasized the government's responsibility to have a "duty of care" over users and to protect long term needs, such as "privacy", "social cohesion" and even "life goals" of citizens against impulsive needs, such as "efficiency" and "convenience."

With regard to service oriented values, all stakeholder groups expressed a positive feeling towards increased user convenience generated by SSI, in particular through the use of self-managed digital wallets on users' mobile devices. Experts from not-for-profit and for-profit organizations strongly highlighted increased efficiency and personal data management as crucial benefits of SSI.

A great variety of interpretations of SSI emerged among socially oriented values. We observed contestations among stakeholders particularly in aspects regarding data ownership, digital exclusion and decentralization. While *data ownership* was promised or promoted by almost all SSI whitepapers and private sector organizations, researchers and public officials judged the pledge for ownership as a "misconception about personal data […] propagated by SSI proponents." Another interviewee emphasized that there is "no such thing as the owner of personal data and GDPR does not even use this concept." Indeed, legally the idea ownership of data is not covered under the current regulatory regime. While the idea of 'reappropriating' data to users is heavily disputed, all stakeholders agreed that SSI would enable *user control*, thereby ensuring an individual's ability to control the exchange, disclosure and restriction of identity data.

Socially oriented values also encompass the accessibility of ICT for the general public in order to prevent *digital exclusion*. In this context, researchers and government officials shared the view that SSI would require high digital literacy among users because it presupposes the individual's capability of managing and controlling one's own identity data. Both groups questioned whether all individuals could be entrusted with the ability of self-management and critical reasoning to assess when to share which data or restrict access to whom. Similarly, researchers argued that SSI requires internet access, the possession of an electronic device, and in some cases even a smartphone with biometric authentication methods. Contrarily, stakeholders from not-for-profit and for-profit organizations pronounced the social inclusiveness of SSI – addressing individuals that are unable to prove their identity in "paper-based, nationally driven, government identity systems." On the socially oriented

Table 2. Overview of the interpretive flexibility interpretive flexibility in the social domain of SSI

	Researchers	Not-for-profit	For-profit	Government officials
Duty oriented		- Trust in institutions	- Trust in institutions	- Duty of care for citizens
Service oriented	- User convenience	- User convenience - User data management - Efficiency	- User convenience - User data management - Efficiency	- User convenience
Socially oriented	- Data control - Digital Exclusion	- 'Data ownership' - Social inclusion	- 'Data ownership' - Social inclusion	- Data control - Digital Exclusion - Decentralization

value of *decentralization*, some governmental actors perceived SSI as a "principle-based" construct that lacks trust and credibility. This view was based on the duality of SSI that incorporates a libertarian idealism on the one side, while calling for government-issued credentials and thus relying on a centralized authority on the other. In sum, SSI is interpreted flexibly in the social domain. This leads to confusion about SSI as a novel, electronic identity paradigm.

4.3. Underlying institutional properties

The analysis of our data revealed that human agents and their interpretation of socio-technical artefacts are subject to a variety of institutional properties. Following Orlikwoski [19], we categorized these in terms of endogenous *organizational dimensions* (ODs) such as business strategies, ideology, culture or standard operating procedures, as well as exogenous *environmental pressures* (EPs) such as regulations, vendor strategies, or state of knowledge about technology. We present our findings in Table 3 and indicate the strength of the impact of each institutional property on the social groups' interpretations of SSI with the numbers 1 (low impact) to 4 (high impact). It is noteworthy that the analysis of our data showed that researchers as a stakeholder group are not impacted by institutional properties. The reason for this may be due to researchers, working on a scientific basis, tend to assess IT artefacts objectively and independently from cultural or political influence.

For the ODs, we identified two prevalent institutional properties: *operating procedures* and *culture*. In the realm of operating procedures, we found 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." Government officials shared this view and referred to shortcomings of legacy issues in the public sector as the "big problem in our times that we are using approaches that come from medieval times", which were "never changed" because "people are accustomed to them." Our interviews with experts from Europe and the Anglosphere further highlighted the presence of cultural differences. Many interviewees mentioned the distinction between systems in the Anglosphere which are characterized by a tendency of "distrust towards anything 'central'" as opposed to Europe, where central registries act "as an authoritative source of truth." Therefore, people in the United States, for instance, would be more involved in the discussion on self-sovereignty than in Europe. As a consequence, the lack of discussion around SSI could "give the impression that [users] don't need to rely on any […] authoritative source to prove your identity."

For the EPs, a frequently recurring theme in our data was related to *regulatory dynamics*, as well as the *political environment*, which was particularly reflected in the European legal and political landscape. This is because EU regulation, especially in the context of transatlantic data transfers, also affects non-European stakeholders. As such, non-for-profit and for-profit organizations acknowledged the repercussions of the GDPR into jurisdictions beyond the EU. Interviewees from the private sector argued that despite regulatory challenges with the GDPR, there are also opportunities for companies that "employ innovative, privacy-respecting ways." Interview participants highlighted how SSI's selective disclosure mechanisms would help administrations to comply with the GDPR's principle of data minimization. Public officials' view on this was heterogenous. While some acknowledged SSI's potential to facilitate GDPR compliance, others claimed that such compliance would not help to establish trust, but only be based on "box-ticking". In another case, experts from for-profit companies referred to the revision of the European regulation on electronic identification and trust services for electronic transactions (eIDAS), arguing that the open consultation was an opportunity to propose "tweaks in the regulation that will help […] to establish SSI as one of the key factors." Public officials agreed that eIDAS could potentially confer legal validity to a new decentralized identity paradigm. With regard to the political environment, we noticed a recurring reference among interviewees from both the private and the public sector to the European Commission's support and "proactive approach" for decentralized digital identity schemes. It seemed to be motivated by the ambition to improve Europe's digital competitiveness next to major global actors.

Table 3. Overview of the institutional properties of SSI's interpretive flexibility

		Researcher	Not-for-profit	For-profit	Government
Organisational dimensions	Operating procedures	0	1	3	4
	Culture	0	3	4	4
Environmental pressures	Regulatory Dynamics	0	3	4	3
	Political Environment	0	1	2	4

5. Discussion

Using empirical data from interviews and project documentation, we investigated the functional boundaries and social dynamics of SSI. While we were able to define and map these, we realized that the IF of SSI is associated with an underlying institutional 'domain'. This domain seems to influence social groups and their understandings of SSI. We accounted for this third domain in a model that respects both Doherty et al.'s [18] two dimensions, as well as Orlikowski's [19] structural approach. Based on these two models, we propose an extended model of IF (Figure 3) that builds on Doherty et al. [18]. Already accounted for in the original model of interpretive flexibility, the arrows A and B reflect the duality of technology. That is, how human agents shape technology, and in turn, how technology influences the actions and behavior of users. Here, we investigated how different value sets of stakeholders affect the flexible understandings of SSI.

Our data suggested that underlying institutional properties play an important role in stakeholder's interpretation formation. These latent dimensions are an important aspect in understanding the social construction of IT artifacts, as they go beyond stakeholders' interests and their interest-based interpretations. This association is denoted by arrow C. Specifically, *IT legacy issues* were important contextual factors for for-profit companies and governments in interpreting SSI. As such, they served as a justification of service oriented values, such as user convenience, data management, and efficiency brought about by SSI. Moreover, *continental differences* regarding the perception of SSI seemed to influence stakeholders' diverging interpretations of SSI's socially and duty oriented values. Based on these geopolitical differences, 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.

We further discovered that *regulatory dynamics*, such as the GDPR and its user-centric focus served as a duty oriented premise to increase the legitimacy of SSI. Similarly, the revision of eIDAS was used as a tool for SSI proponents to voice suggestions to confer legal validity to SSI paradigms. Although the actual revision did not foresee any adjustments to legally cover SSI technologies, it raised the attention of policy-makers and allowed to roughly embed a 'foreign' SSI construct into a European legal context. This observation illustrates how underlying legal developments can initiate debates about user-centric values such as privacy or security, and can then be utilized as tool of legitimization in the social construction of technology.

The *political environment* also played a role in stakeholders' view on SSI. Our data revealed that whenever the idea of SSI was associated with initiatives supported by the European Commission, the views on SSI became more tangible and concrete. This applied to stakeholders in both the private and the public sector.

Finally, Orlikowski's [19] work also highlights a fourth connection: how a technology could influence institutional conditions by "reinforcing or transforming structures of signification, domination, and legitimation" (arrow D). At this stage, very few SSI implementations gained operational foothold in the public sector. This makes it difficult to determine to what extent SSI technology impacts institutional properties. However, to the extent of our knowledge, there is one example that underpins this tendency. As one of the front-runners of SSI, Germany initiated a legal change in its Federal Registration Act with its first SSI use-case on hotel check-in procedures which proposed the introduction of an "experimentation clause" to test further methods of digital registration [47]. A similar draft on an experimentation clause was ratified for Know-Your-Customer identification methods covered by the German Money Laundering

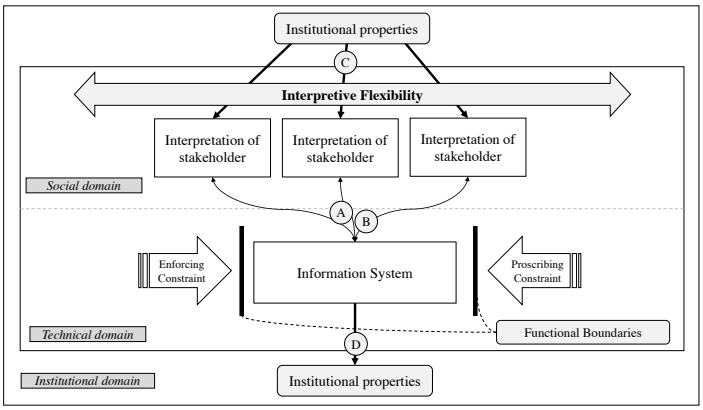

Figure 3. Extended model of interpretive flexibility

Act. These regulatory changes created a legal basis for wallet-based identity management systems and can therefore be considered to have been initiated by SSI.

The extended model of IF serves to account for varying dimensions at-play during the design and development of information systems. By analyzing contextual institutional factors, stakeholders' interpretations are more traceable and assessable. This is especially useful for both digital government practitioners and academic scholars, who seek to evaluate the history of a new IT artefact and its attributed public values. For researchers dealing with digital government, the extended model of IF constitutes a foundation for further research as a new theoretical lens to analyze complex socio-technical IT artefacts. For practitioners, the devised model addresses the current confusion and ambiguity around SSI by systematically unravelling the social, technical, and institutional context that influences the understanding of SSI.

6. Conclusion

Decentralized identity management systems are a relevant but very young topic for governments. Unfortunately, vague and value-laden interpretations around socio-technical constructs can distort the public discourse and risk misrepresenting values and affordances that technology can offer to users. To unpack the various understandings of SSI on a social, technical and institutional level, our study delineated the technical boundaries of SSI, mapped its spectrum of socio-political ambiguities as novel electronic identification paradigm, and provided insights into the institutional properties of stakeholders. From a technical perspective, we identified the digital wallet as an enforcing constraint on the one side, and the centralized, siloed storage of identity credentials as a proscribing constraint for SSI on the other. In the social domain, the most diverging interpretations occurred in duty and socially oriented values of SSI. Using Orlikowski's structuration model [19], we identified legacy procedures, cultural differences, regulatory dynamics and political environments as institutional properties that are associated with SSI's interpretive flexibility. Our results allowed us to extend Doherty et al.'s [18] model on IF – a multidimensional framework that serves to improve the understanding of complex socio-technical systems. The findings of this study can serve as a backbone for future research in this field and provide a foundation for policy discussions around SSI.

However, studying a nascent phenomenon such as SSI comes with certain limitations. Because of its technical immaturity, we were not able to investigate full-fledged implementations and analyze the perception of SSI among users as a fifth group of stakeholders. Further, due to the limited number of people acquainted with SSI, we were only able to interview experts that, by definition, have an interest in SSI. This may have biased the range of IF to some extent. The robustness of the extended model of IF can be tested against in future case studies. Likewise, it can be worthwhile to consider aspects of critical theory, such as the critical capability approach of technology, or other theoretical perspectives of technological transition or social construction. As such, these limitations provide avenues for follow-up research on decentralized identity systems that can build on the technical, social, or institutional insights on SSI presented in this study.

7. Acknowledgements

The authors would like to thank Johannes Sedlmeir and Reilly Smethurst for their contributions to the technical features table and the references list.

Supported by PayPal and the Luxembourg National Research Fund FNR, Luxembourg (P17/IS/13342933/PayPal-FNR/Chair in DFS/ Gilbert Fridgen).

8. References

[1] Laurent, M., J. Denouël, C. Levallois-Barth, and P. Waelbroeck, "Digital Identity", In *Digital Identity Management*. Elsevier, 2015, 1–45.

[2] Bélanger, F., and L. Carter, "Trust and risk in e-government adoption", *The Journal of Strategic Information Systems 17*(2), 2008, pp. 165–176.

[3] Ferdous, M.S., F. Chowdhury, and M.O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology", *IEEE Access 7*, 2019, pp. 103059–103079.

[4] Mühle, A., A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity", *Computer Science Review 30*, 2018, pp. 80–86.

[5] Allen, C., "The Path to Self-Sovereign Identity", *Life With Alacrity*, 2016.

[6] Preukschat, A., and D. Reed, "Self-Sovereign Identity", *Manning Publications*, 2021.

[7] Tobin, A., D. Reed, F.P.J. Windley, and S. Foundation, "The Inevitable Rise of Self-Sovereign Identity", 2017.

[8] Reed, D., M. Sporny, and M. Sabadello, "Decentralized Identifiers (DIDs) v1.0 Core architecture, data model and representations", *W3C Candidate Recommendation Draft*, 2021.

[9] Sporny, M., D. Longely, and D. Chadwick, "Verifiable Credentials Data Model 1.0", *W3C Recommendation*, 2019.

[10] Ølnes, S., J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing", *Government Information Quarterly 34*(3), 2017, pp. 355–364.

[11] Cheesman, M., "Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity", *Geopolitics*, 2020, pp. 1–26.

[12] Herian, R., "Blockchain, GDPR, and fantasies of data sovereignty", *Law, Innovation and Technology 12*(1), 2020, pp. 156–174.
[13] Keohane, R.O., "Ironies of Sovereignty: The European Union and the United States", *JCMS: Journal of Common Market Studies 40*(4), 2002, pp. 743–765.
[14] European Commission, "Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity", 2021.
[15] Kuperberg, M., "Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective", *IEEE Transactions on Engineering Management 67*(4), 2020, pp. 1008–1027.
[16] Pinch, T.J., and W.E. Bijker, "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*(3), 1984, pp. 399–441.
[17] Sahay, S., and D. Robey, "Organizational context, social interpretation, and the implementation and consequences of geographic information systems", *Accounting, Management and Information Technologies 6*(4), 1996, pp. 255–282.
[18] Doherty, N.F., C.R. Coombs, and J. Loan-Clarke, "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*(6), 2006, pp. 569–582.
[19] Orlikowski, W.J., "The Duality of Technology: Rethinking the Concept of Technology in Organizations", *Organization Science 3*(3), 1992, pp. 398–427.
[20] Thomas, J.C., and G. Streib, "The New Face of Government: Citizen-Initiated Contacts in the Era of E-Government", *Journal of Public Administration Research and Theory*, 2003, pp. 83–102.
[21] Wihlborg, E., "Secure electronic identification (eID) in the intersection of politics and technology", *International Journal of Electronic Governance 6*(2), 2013, pp. 143–151.
[22] Layne, K., and J. Lee, "Developing fully functional E-government: A four stage model", *Government Information Quarterly 18*(2), 2001, pp. 122–136.
[23] Hiller, J., and F. Belanger, "Privacy Strategies for Electronic Government", *E-Government Series*, 2001.
[24] Pollitt, C., *Time, Policy, Management: Governing with the Past*, Oxford University Press, Oxford, 2008.
[25] West, D.M., *Digital government: technology and public sector performance*, Princeton University Press, Princeton, N.J. Oxford, 2007.
[26] Kubach, M., C.H. Schunck, R. Sellung, and H. Roßnagel, "Self-sovereign and Decentralized identity as the future of identity management?", *Open Identity Summit 2020*, 2020, pp. 1–13.
[27] Griffith, T.L., "Technology Features as Triggers for Sensemaking", *The Academy of Management Review 24*(3), 1999, pp. 472–488.
[28] Kahn, P.W., *Political Theology: Four New Chapters on the Concept of Sovereignty*, Columbia University Press, New York, 2011.
[29] Zwitter, A.J., O.J. Gstrein, and E. Yap, "Digital Identity and the Blockchain: Universal Identity Management and the Concept of the 'Self-Sovereign' Individual", *Frontiers in Blockchain 3*(26), 2020, pp. 1–28.
[30] Ishmaev, G., "Sovereignty, privacy, and ethics in blockchain-based identity management systems", *Ethics and Information Technology*, 2020, pp. 1–14.
[31] Halpin, H., "Vision: A Critique of Immunity Passports and W3C Decentralized Identifiers", In T. van der Merwe, C. Mitchell and M. Mehrnezhad, eds., *Security Standardisation Research: 6th International Conference*. Springer International Publishing, Cham, 2020, 148–168.
[32] Williams, R., and D. Edge, "The social shaping of technology", 1996, pp. 865–899.
[33] Law, J., and M. Callon, "The life and death of an aircraft: a network analysis of technological change", In *Shaping Technology/Building Society: Studies in Socio-technical Change*. MIT Press, Cambridge, MA, London, 1992, 29–52.
[34] Orlikowski, W.J., "Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations", *Organization Science 11*(4), 2000, pp. 404–428.
[35] Henningsson, S., and H.Z. Henriksen, "Inscription of behaviour and flexible interpretation in Information Infrastructures: The case of European e-Customs", *The Journal of Strategic Information Systems 20*(4), 2011, pp. 355–372.
[36] Myers, M.D., and M. Newman, "The qualitative interview in IS research: Examining the craft", *Information and Organization 17*(1), 2007, pp. 2–26.
[37] SelfKey Foundation, "SelfKey: The SelfKey Foundation", 2017.
[38] Ontology, "Ontology: A New High Performance Public Multi-Chain Project & A Distributed Trust Collaboration Platform", 2017.
[39] Procivis AG, "Procivis eID+ Produktpräsentation Juni 2017", 2017.
[40] Esatus AG, "Identity & Access Management (IAM) - Realisiert mit Self-Sovereign Identity (SSI)", 2019.
[41] Bundeskanzleramt, "Digitale Identität: Wie ein Ökosystem digitaler Identitäten zu einem selbstbestimmten und zugleich nutzerfreundlichen Umgang mit dem digitalen Ich beitragen kann", 2021.
[42] Microsoft, "Decentralized Identity: Own and control your identity", 2018.
[43] Alastria, "Alastria Id: Privacy Rational", 2020.
[44] Corbin, J., and A. Strauss, *Basics of Qualitative Research : Techniques and Procedures for Developing Grounded Theory. 4th ed*, Sage, Los Angeles, 2015.
[45] Mayring, P., "Qualitative Content Analysis", 2014, pp. 1–145.
[46] Bannister, F., and R. Connolly, "ICT, public values and transformative government: A framework and programme for research", *Government Information Quarterly 31*(1), 2014, pp. 119–128.
[47] Deutscher Bundestag, "Entwurf eines Gesetzes zur Erprobung weiterer elektronischer Verfahren zur Erfüllung der besonderen Meldepflicht in Beherbergungsstätten", 2021.