H. Roßnagel, C. H. Schunck, S. Mödersheim (Hrsg.): Open Identity Summit 2021,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021 143

On the Market for Self-Sovereign Identity: Structure and Stakeholders

Michael Kubach[1] and Rachelle Sellung[1]

Abstract: For SSI solutions to make a significant impact, they need to be designed to cater to the requirements of the market to be adopted. Therefore, this paper proposes a structure of the market for SSI solutions, analyses its stakeholders, and surveys its current state.

Keywords: Self-sovereign identity, SSI, digital identity, decentralized identity, identity management, market, eID, stakeholders, trust, network effects

1 Introduction

The digital identity market remains a market with massive growth potential [Di19]. Given its potential, it makes sense that new technologies come along to take on the challenges. In the last years, Decentralized and Self-Sovereign identity (SSI) solutions have claimed to transform identity management. However, in order to transform the identity solutions market, one needs to understand and address market and stakeholder requirements.

In an emerging context, SSI is a term frequently used for blockchain-based identity management approaches. Yet, it is not always applied consistently. This paper follows the definition according to [Mü18], who summarized that a Self-sovereign identity management system allows users to fully own and manage their identity without having to rely on a third party.

In order to design SSI solutions that make an impact by reaching a significant share through adoption by users who can only then take back control of their identity data, we also need to take on a market perspective. However, users will only adopt, if those solutions are adopted by service providers/relying parties as well – and there might be other parties having a stake this process. Therefore, we will have to analyze the market structure for SSI solutions in general and in particular the stakeholder structure. This analysis serves as the basis for further research and recommendations on SSI that go beyond the often prevailing technological and privacy-oriented focus.

This paper explores the market structure of the SSI market in chapter 2. Building on that, in chapter 3 it adds a stakeholder analysis of the market. In chapter 4, it gives a brief overview of the current market offerings for SSI projects. Finally, in chapter 5 a conclusion of the paper is provided.

[1] Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, Germany, firstname.lastname@iao.fraunhofer.de

2 Market Structure

The literature on SSI considering a whole market and/or service provider perspective is scarce. So far, research seems to focus on technology development and on the supply side of identity management – repeating a pattern that has already been observed in Federated Identity Management (FIdM) [Ro14]. Based on the experience with Federated Identity Management as well as web identity management (WIM), we argue that the whole market has to be taken into account – supply as well as demand side. WIM approaches like Facebook Login that provide a clear value for End Users, Service Providers and Identity Providers have been widely adopted, while alternative approaches, even though they were technically sound and privacy friendly do not play a significant role on the market (CardSpace, Uprove, and Attribute Based Credentials) [UP20, Zi16].

Our market analysis builds on the previous work by [ZR12] and their model for the WIM market. The relationship between users and relying parties (service providers using the WIM) is heavily influenced by indirect network effects. One can observe a two-sided market where the "chicken or egg"-problem is apparent: When no services are supporting the WIM, it is not useful for the user. On the other hand, when no users have adopted the WIM yet, service providers' motivation to implement it is quite minimal as there are no users that it can reach thorough the WIM. For a user to gain meaningful reduced sign-on capabilities across the web, a system has to be widely adopted, and its underlying protocol implemented by a wide range of service providers. An important aspect was already highlighted by [ZR12]. Relying parties seem to be scarce even for existing protocols: CardSpace (preinstalled in Windows Vista), and OpenID (AOL alone contributed 60 million accounts), had a huge user base – but were not widely adopted by relying parties. Today, with the Germany national eID we can observe a similar (non-)development: almost every German citizen above 16 years has it in his pocket, but barely anyone uses it as there are no service providers supporting it[2].

One can observe that the utility for both sides in the WIM market significantly depends on the adoption of the WIM-Technology on the other side. This induces indirect network effects with positive feedback: if more service providers adopt a WIM system, more users will adopt, and the other way around. The presence of indirect network effects also identifies WIM as a two-sided market. Such a market serves two distinct types of customers, who depend on each other in some important way. Their joint participation makes the system more valuable to each. This means that there are indirect network externalities between the two different customer groups [Evan03]. One would expect that for SSI or other types of blockchain-based identity management systems this aspect of the market structure is similar because, just as in the case of WIM, we usually have a User accessing a Service Provider using the IdM-System where both, the User as well as the Service Provider need to adopt the IdM-System.

[2] Additional reasons might be that (1) it can only serve as alternative means of authentication, as most service providers do not focus solely on German citizens, and (2) it initially required special card readers.

The relationships towards the identity provider are mainly dominated by trust issues in the WIM market – principal-agent trust between users and identity provider and interorganizational trust between relying party and identity provider. Several authors have argued that insecurity and trust issues can make identity management systems fail, as users might be unwilling to delegate the handling of their personal identity information to someone (the identity provider) if they do not trust him. This has led to a strong focus on research and development on security as well as privacy for IdM-Systems [ZR12]. However, this trust is his subjective perception and not a completely objective decision based on the technical features of the identity management system. Research has also shown the limited influence of technological solutions on user's trust perceptions with disposition to trust and institutional trust being important factors [MCK02, ZR12].

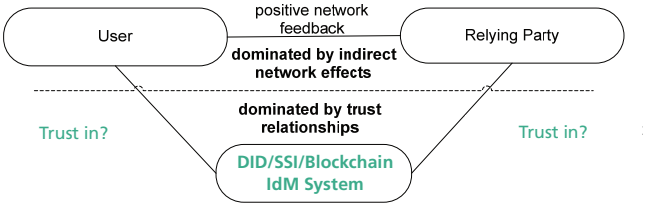

Figure 1: Structure of the SSI market as extension of [ZR12]

In fact, for the average end user it is very difficult to assess whether a certain security solution is technically well-designed, secure, privacy friendly and should thus be trustworthy. As [ZR12] have shown, asymmetric information about the security and/or privacy of an IdM-System is a problem that might lead to market failure. The relationship between identity provider and end use resembles one of a principal (end user) and its agent (identity provider). This makes it challenging for identity providers (agents) as market participants with high standards in terms of quality (i.e., security and privacy) as users cannot value these against identity providers offering solutions with lower quality standards but apparent value to the user (this could be ease of use, lower/no price, large base of Service Providers etc.). This challenge remains in the market for SSI or other blockchain-based IdM-Systems. However, depending on the particular implementation of the IdM-System, there might not be a specific organization acting as identity provider. Calling the trust relationship principal-agent trust might therefore seem impropriate, even though the challenges appear quite similar (it may even be more difficult for the user to assess the quality and trustworthiness of the SSI or other blockchain-based IdM-System as there is not a single provider and the whole system is even more complex). Trust in technology could be an important aspect. There are, however, SSI-Solutions like Sovrin's (https://sovrin.org/) that are governed by a foundation. Sovrin and its branded wallet could appear to the average end user as something like a service provider. In this case, something pretty close to the WIM-model might even be appropriate.

The relationship between relying party and identity provider for WIM is described by [ZR12] as dominated by interorganizational trust. Apparently, the authors expect that relying parties are more capable to assess the trustworthiness of an identity provider

objectively. The information asymmetry does not seem to play such an important role. This might be the case for relying parties with sufficient IT-competence but seems less likely for firms like start-ups or small shops. However, the relying party as organization has to trust the identity provider as organization to act in its best interest. This is of course dependent on the power relationship between both organizations as well as the institutional framework, the possibility to observe violations and to sanction them etc. For SSI Systems, there is no identity provider as a single organization. Therefore, we cannot speak of interorganizational trust here – except for the Sovrin case (or similar ones) as mentioned above. Trust in technology is similarly important as above, as the complexity of SSI system certainly exceeds the IT-competence of many relying parties.

Concluding, regarding the market structure there doesn't appear to be fundamental differences between classic web identity management (WIM) and the newly proposed SSI approaches. One can still observe a multi-sided market that is subject to indirect network effects and influenced by trust relationships. The chicken and egg problem of getting enough service providers for end users while at the same time requiring a large user base to be attractive to service providers persists. For the average end user and smaller businesses as service providers with limited IT-security expertise the trust relationship in the SSI market might be even more complex as it is unclear who the counterparty actually is and what to do in case of problems.

In summary, there are three main challenges that the market faces regarding SSI solutions. First, the challenge of trust management. As described by [Ku20], there is an absence of a natural trust anchor for DLT based digital identities. For example, the problem that SSI-based solutions face is addressing "How can one trust that the credential issuing entity is who they claim to be?". The answer to this could be to add a gate keeper or a centralized governance layer, however, in turn this could be argued to defeat a key reason to use SSI solutions in the first place. Potentially, a decentralized trust architecture such as proposed at [Wa17] could be a way forward here. Second, the aforementioned challenge of network effects that every identity management system aiming at broader adoption faces with the resulting chicken and egg problem. Third, the challenges of establishing viable business models for all relevant stakeholders as also referenced by [Ku13].

3 Stakeholder Analysis

Building on the method of a stakeholder analysis, we further analyze the requirements and interests of the different actors in the SSI ecosystems that have to be considered for the market to be sustainable. The most common definition of the term stakeholder goes back to [Fr84]. Hence, an organization's stakeholder is, a group or individual who influences or is influenced by the achievement of organizational goals. Pouloudi and Whitley [PW97] clarify this definition for an information systems context as those actors (persons, groups or organizations) involved in the development process, whose actions influence or are influenced by these factors, both directly and indirectly, in the development and use of a

system. For further analysis, and to address their requirements specifically, stakeholders can be subdivided into groups, which in turn pursue similar demands or can influence the success of the project in different ways. Different categorization approaches have been presented, e.g. by Cotterell and Hughes, [CH95], Sharp et al. [SFG99], and Sillitti and Succi [SS05]. It is clear that those stakeholder categorizations, when viewed individually, each have clear gaps. However, these generic groups of stakeholders proposed in the literature can serve as a starting point to identify stakeholder groups that are relevant for the success of SSI ecosystems. Therefore, we combine those categorizations into one that seems suited for this specific context.

First, we differentiate between two main stakeholder groups: direct participants of the ecosystem and such actors that are only indirectly involved in its daily business. We call the first group "Active Stakeholders" and the second group "Enabling Stakeholders".

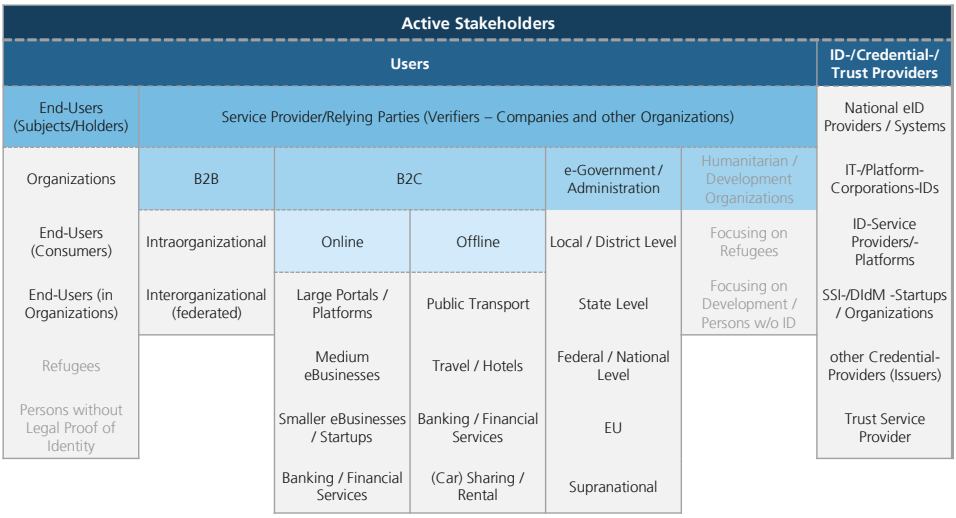

Figure 2: Active Stakeholders in the SSI Ecosystem

Figure 2 depicts the Active Stakeholders as main group in the SSI ecosystem. Active stakeholders can by split into the two types of Users of identity services, whom would be interested in a specific use case that requires an identity service rather than in the identity service itself, and ID-/Credential/Trust Providers. Those two Active Stakeholder groups, the Users and ID-/Credential/Trust Providers, are actively involved in the everyday processes in the ecosystem, e.g., by issuing credentials operating ID-Systems or taking on another role in the ecosystem. In these stakeholder roles, those actors have a high economic interest in the sustainable success of the ecosystem (ID-/Credential Providers) or derive some other kind of direct value from it, e.g., as it supplies them with a secure and easy to use digital identity. With that in consideration, active stakeholders are of high relevance for the value creation in the ecosystem, and thus for the SSI business models.

ID-/Credential/Trust Providers provide digital IDs or components or related services in the ecosystem. In this stakeholder role, the focus is not on them using digital identity or trust services themselves. The types of organizations and interests of these stakeholders may differ significantly. Nevertheless, a viable business model remunerating the effort they put into the ID ecosystem needs be developed for all of these entities. With certain restrictions, this even applies to National eID Providers/Systems operated by governmental institutions. In addition, this group includes: IT-/Platform-Corporation-IDs (for example, Google Login, Apple ID, Facebook Login, etc.), ID-Service Providers/-Platforms (Verimi, Yes, etc.), SSI-/DIdM-Startups/Organizations (Sovrin/Evernym, Jolocom, etc.), other Credential-Providers (Issuers, such as Mobile Connect, or even Universities etc.), and finally Trust Service Providers (Schufa, etc.).

The User stakeholder-group, that contains persons or entities making use of digital identities in some form, is divided further into End-Users that are actually using services in the ecosystem (also known as Holders or Subjects – depending on the perspective and use case) and Service Providers/Relying Parties (also Verifiers) that are usually companies and organizations offering a specific service that requires trust or identity information.

Regarding the End-Users (Subjects), who use their digital identity themselves in the ecosystem, we would like to focus in this paper on the identities of natural persons. These are to be distinguished from the digital identities of organizations, legal entities, and in the context of the Internet of Things (IoT), identities of things/devices, e.g., for sensor data. Identities of natural persons are further differentiated into End-Users (Consumers) and End-Users (in organizations), e.g., identities/accounts for employees, since different requirements and interest are of relevance here. Refugees and persons without legal proof of identity are also currently a much-discussed use case for secure digital identities that have high requirements for privacy and trust, but also for international and interorganizational interoperability.

Service Providers/Relying Parties that use digital IDs can be grouped into four categories according to use case: (1) B2B applications, (2) B2C applications, for (3) e-Government/Administration, and (4) Humanitarian/Development Organizations.

In B2B applications, organizations might use digital IDs internally to identify their employees (this is sometimes referred to as B2E - business to employee), for example as a basis of their access rights management. Since today's distributed value chains increasingly involve direct collaboration in digital processes across organizations, this identification of employees is also necessary there – which in turn creates additional challenges (relating als to Federated Identity Management) [Ku14].

B2C applications can be further differentiated into online or offline applications on the basis of their provision. Here, too, different requirements and framework conditions apply.

Online applications are provided, for example, by Large Portals or Platforms. Their requirements and capabilities (financial capacity, IT expertise, etc.) differ significantly from those of Medium-Sized eBusinesses, which in turn must be distinguished from

Smaller eBusinesses / Startups. Banks / financial service providers have special requirements as well – this illustrates that even more types of stakeholders are emerging here, which would have to be differentiated on the basis of the use cases and their specific requirements, so that this list cannot be exhaustive.

For offline applications, only exemplary use cases are listed as well. These include Public Transport, Travel/Hotels (Tourism), Banking/Financial Services, and (Car)Sharing or Rental. In contrast to online use cases, the particular challenge here is that the digital ID (usually stored on the smartphone) must also be suited for verification in the "offline environment". NFC interfaces or QR codes are often used here – forms of visual verification may also be possible.

e-Government / Administration is a stakeholder group that is often in the particular focus of publicly funded digital identity research projects. Here, there is a particular need to digitize processes; at the same time, these organizations are often subject to particularly high requirements regarding the legal security and Levels of Assurance (LoA) of digital identities. This overview is oriented at the federal structure of the German state and its integration into the EU – of course it could easily be adjusted for other national contexts. As stakeholder groups or levels, we identify: municipalities on the Local / District Level, Länder on the State Level, Bund on the State / Federal Level, and the EU (an important player with the eIDAS regulation, among other things). Supranational institutions and agreements (e.g., on digital passports, visas and apostilles) may also have an influence on the development and success of digital identities, which is why they are also listed here.

Finally, there is the group of Humanitarian/Development Organizations. Here, we can differentiate between organizations with a focus on refugees, such as the UNHCR, and others with a focus on development and persons without legal proof of identity in general (the World Bank being very active here).

While Enabling Stakeholders (as shown in Figure 3) are not actively involved in the daily business of a SSI Ecosystem and in this role are neither users nor providers of identity services or components, they are still relevant for its overall success as they are indirectly involved in various forms as can be seen in the following.

The enabling stakeholder group is separated further into “Developing Stakeholders” and “Framing Stakeholders”. The first group consists of actors that are developing the technology and standards required for the ecosystem (e.g., SSI/DidM Startups, ID-Technology Companies and Large IT-Corporations). Thus, those stakeholders have an interest in the success of the technology and need to generate some kind of revenue to cover their costs for R&D. Some of those stakeholders could take on the role of an active stakeholder at the same time, when they also operate SSI components, but this does not always have to be the case. Hence, the business model of those stakeholders can differ from the one of active stakeholders.

The second group of Enabling Stakeholders are “Framing Stakeholders”. Those actors set the framework conditions for the SSI Ecosystem without actively using or developing the

actual technology and its components. However, through the development of basic technologies (Research Organizations) or forming the regulatory framework (Regulatory/ Legislative Bodies), overseeing data protection regulations (Data Protection Institutions), influencing public discussions and the legislative process (Civil Society and Multiplicators) and so on, they can be a significant success factor for the ecosystem. Their direct economic interest and investment in the SSI Ecosystem is, however, quite low and, hence, their relevance for the business models in the ecosystem limited.

Figure 3: Enabling Stakeholders in the SSI Ecosystem

In order to achieve market success, SSI solutions need to address the requirements of all relevant stakeholders in a specific use case – and not just focus on a single group i.e., the consumer. The relevant stakeholders' priorities rely on what value creation is gained from a solution. For example, value creation could be having increased usability, security or privacy benefits, greater convenience, or financial benefits depending on the requirements of each respective stakeholder.

4 Brief Overview of the Current Market Offerings for SSI

Due to the novelty of the basic technology, the market for SSI is in a state of dynamic movement. An exhaustive overview of all market offerings currently available or in development is therefore hardly possible. Nevertheless, there have been a few recent papers aiming to summarize and analyze various aspects of SSI solutions or projects and trying to give an overview of the current market situation and maturity.

Dunphy and Petitcolas [DP18] focus their analysis on three solutions (uPort, ShoCard, Sovrin). Regarding usability, they conclude that all of those projects have an "unclear usability and user understanding of […] (the) privacy implications." What they completely disregard in their analysis is a comprehensive stakeholder perspective, in particular of the service providers'. They only evaluate the solutions regarding the "laws of identity" that

solely focus on the user [DP18]. This goes in line with publications of SSI projects that mainly present the benefits in security and privacy for the user while disregarding that service providers have to implement those solutions for users being able to use them.

In an extensive analysis, [Ku19] surveyed 43 approaches to blockchain-based identity management from the enterprise and ecosystem perspective. He applies an impressive set of 12 compliance and liability criteria, 32 end-user experience criteria, and 29 technology, implementation, integration and operations criteria. Quantitative properties such as performance are not included, what he justifies with the low level of maturity of the solutions available. In conclusion, he finds very different levels of maturity and only few solutions that could compete with traditional approaches. Overall, business models are lacking (see also section 2 and 3), so are compliance and enterprise-grade aspects (liability, revocation) and usability.

A recent overview [DT20], analyzed the "most relevant" (without defining this further) SSI solutions regarding the 10 principles of SSI [Al16]. The SSI solutions included in this evaluation were: uPort, Sovrin, ShoCard, IDchainZ, EverID, LifeID, SelfKey, Civic, TheKey, and Bitnation. From this analysis, 8 categories of challenges were derived. Two technical challenges: (1) challenges related to the use of blockchain, and (2) challenges in the context of key management. Six non-technical issues: (1) transfer from legacy systems, (2) lack of regulatory systems adjusted for SSI, (3) lack/immaturity of standards leading to interoperability issues, (4) adoption by users of all sides, (5) accessibility through vulnerable and/or disadvantaged persons, and (6), complex behavior of actors required to adopt the solution. Many of the challenges identified in this analysis go in line with our findings in sections 2 and 3, as well as the analysis of [Ku20].

For this paper we have also reviewed a collection of SSI projects to gain an impression of the current state of the market. Figure 4 presents an overview as of January 2021.

SSI Projects reviewed in 2021		
Connect.Me	1Kosmos BlockID	Spherity
Uportlandia	Blockpass	Onfido*
Jolocom SmartWallet	Knowmenow	Yoti*
Bloom-Secure Identity	Nuggets	Shocard
Meeco	SelfKey	HelixID
Keepin	Confidare	Blockcerts
Iden3	Civic Secure Identity	Estatus
Onto	mySaveID	OneIdentity
Lissi	Authenteq*	Trinsic
		MAX-Wallet

Figure 4: Overview of SSI Projects at start of 2020 and 2021

In order to be integrated, the projects needed to meet the following requirements: They needed to have a working prototype (available on request) or even be available as a desktop version or from the Android or Apple app store. Projects marked with an asterisk are not solely decentralized / blockchain based wallets but claim to be SSI approaches. At the start of 2020, 23 projects were identified. In an update of the analysis in January 2021,

we could add six projects to the list. It appears that these projects are still in the early and agile stages of development, where even the more advanced projects are still undergoing frequent, noticeable changes or even remove essential features such as key backups.

After reviewing all the forementioned digital wallets, a use case analysis was conducted. We assume that the use cases an SSI solution proposes are those where it assumes to be able to create the most value. In Figure 1, an overview is given of the six key use cases that those solutions present as valuable areas for the application of their product. We also counted, how often a respective use case was proposed in our sample (# Proposed). This could serve as an indicator for the areas on which SSI currently the focuses the most. Of the 29 reviewed projects, the identity verification (19 projects) and exchange of information (20 projects) use cases were proposed the most often.

Use Case	Description	# Proposed
Identity Verification	e.g., public safety enforcement, university, job, doctor's office, pharmacy	19
Document Verification	ID, Green Card, Social Security Card, medical insurance card, driver's license, insurance coverage, employment card, city ID, college transcripts, university diploma, credit score, drug prescription, credit card, public transport ticket, membership (e.g., museum)	16
Application for Services	Applying for citizenship, job, loan/credit, etc.	8
Single Sign-on	Apps, websites, social media, bank account, car renting, games, IoT devices	13
Exchange of Information	Payment, data, person check (renting a room, buy or sell items, date online), exchanging cryptocurrency, multiple forms (auto-fill), token trading	20
Electronic Signatures	Signing of documents with a qualified electronic signature	6

Figure 5: Overview of use cases proposed by SSI solutions

While the Identity Verification, Document Verification, and Exchange of Information Use Cases were proposed by the majority of the reviewed projects, these use cases particularly face the beforementioned trust management challenge. While, as an example, Identity Verification might be a use case that doesn't occur daily for the average user, Exchange of Services and especially Single-Sign-On could be more relevant from this perspective. Generally, our analysis could indicate that the use cases are not driven by the respective business potential and added value for the end user and other stakeholders, but rather by technical feasibility and potential to showcase adherence to the SSI principles. One could cast doubt, whether this is enough for the adoption of the technology by the stakeholders.

5 Conclusion

Overall, SSI solutions that aim to make an impact, need to take on a market perspective to meet the requirements of all relevant stakeholders. The understanding of the market as

well as the stakeholder structure and not only the technical challenges are crucial for the adoption of these solutions. With this understanding, one can design solutions that provide value for all relevant stakeholders, overcoming the "chicken or egg"-problem, to achieve wide adoption. These fundamental steps are needed in order to reach market success for new SSI solutions – and only those with market success can actually be used, and then protect the sovereignty of peoples' identities.

This paper aimed to serve as a basis for further research and development for SSI solutions. We pointed out challenges resulting from the specific market structure – such as the network effects and the complex trust relationship. Moreover, we argued that the SSI ecosystem consist of a number of stakeholders whose specific requirements need to be met – not just those of the end user. We presented a generic map of those stakeholders of the SSI ecosystem – distinguishing active and enabling stakeholders. This can serve as a starting point for a use case-specific stakeholder analysis. The overview of the market that was based on recent literature and our own survey revealed that the current market offerings still have significant challenges to overcome. The analysis of the other authors goes pretty much in line with our analysis here. The market and its offerings are still immature and under heavy development.

Future work could take this market structure and stakeholder analysis as a basis to be expanded by further qualitative and quantitative empirical studies on the needs and requirements of real stakeholders, e.g., service providers, and end users regarding SSI. Regarding this, we see it as important to highlight that non-technical aspects are as important as technical functionalities. User experience, functioning trust management and viable business models are as relevant for the success of SSI as are zero knowledge proofs.

6 References

[Al16] Allen, C.: The Path to Self-Sovereign Identity., https://github.com/ChristopherA/self-sovereign-identity, accessed: 05/02/2020.

[CH95] Cotterell, M.; Hughes, Bob: Software project management: International Thomson Computer Press, 1995.

[Di19] MarketsandMarkets: Digital Identity Solutions Market Size, Share and Global Market Forecast to 2024., https://www.marketsandmarkets.com/Market-Reports/digital-identity-solutions-market-247527694.html, accessed: 21/02/2020.

[DP18] Dunphy, P.; Petitcolas, F.: A First Look at Identity Management Schemes on the Blockchain 2018. In: IEEE Computer and Reliability Societies, 2018.

[DT20] Dib, O.; Toumi, K.: Decentralized identity systems: Architecture, challenges, solutions and future directions. In: Annals of Emerging Technologies in Computing Bd. 4, Nr. 5, pp. 19–40, 2020.

[Ev03] Evans, D.: The Antitrust Economics of Two-sided Markets. In: Yale Journal on Regulation Bd. 20, Nr. 2, pp. 235–294, 2003.

[Fr84] Freeman, R.E: Strategic Management: A Stakeholder Approach. Cambridge: Ballinger Publishing Co, 1984.

[Ku13] Kubach, M.; Roßnagel, H.; Sellung, R.: Service providers' requirements for eID solutions: Empirical evidence from the leisure sector. In: Hühnlein, D.; Roßnagel, H. (Hrsg.): Open Identity Summit 2013 - Lecture Notes in Informatics (LNI) - Proceedings. Bonn, pp. 69–81, 2013.

[Ku14] Kubach, M. et.al.: ENX ID – An Architecture for Practical and Secure Cross Company Authentication. In: Hühnlein, D.; Roßnagel, H. (Hrsg.): Open Identity Summit 2014, Lecture Notes in Informatics – Proceedings: Köln, pp. 109–120, 2014

[Ku19] Kuperberg, M.: Blockchain-Based Identity Management: A Survey from the Enterprise and Ecosystem Perspective. In: IEEE Transactions on Engineering Management, 2019.

[Ku20] Kubach, M. et.al.: Self-sovereign and Decentralized identity as the future of identity management? In: Open Identity Summit 2020 - Lecture Notes in Informatics (LNI) - Proceedings. Bonn: Köllen Druck + Verlag GmbH, 2020, pp. 35–47, 2020.

[MCK02] McKnight, D H.; Choudhury, V.; Kacmar, C.: Developing and validating trust measures for e-commerce: An integrative typology. In: Information systems research Bd. 13, Nr. 3, pp. 334–359, 2002.

[Mü18] Mühle, A. et.al.: A survey on essential components of a self-sovereign identity. In: Computer Science Review Bd. 30, pp. 80–86, 2018.

[PW97] Pouloudi, A.; Whitley, E.: Stakeholder identification in inter-organizational systems: gaining insights for drug use management systems. In: European journal of information systems Bd. 6, Nr. 1, pp. 1–14, 1997.

[Ro14] Roßnagel, H. et.al.: Users' willingness to pay for web identity management systems. In: European Journal of Information Systems Bd. 23, Nr. 1, pp. 36–50, 2014.

[SFG99] Sharp, H.; Finkelstein, A.; Galal, G.: Stakeholder identification in the requirements engineering process. In: Proceedings. Tenth International Workshop on Database and Expert Systems Applications. DEXA 99, pp. 387—391, 1999.

[SS05] Sillitti, A.; Succi, G.: Requirements engineering for agile methods. In: Engineering and Managing Software Requirements: Springer, pp. 309–326, 2005.

[UP20] U-Prove., https://www.microsoft.com/en-us/research/project/u-prove/?from=https%3A%2F%2 Fresearch.microsoft.com%2Fen-us%2Fprojects%2Fu-prove., accessed: 2020-09-25.

[Wa17] Wagner, S. et.al.: A mechanism for discovery and verification of trust scheme memberships: The LIGHTest Reference Architecture. In: Open Identity Summit 2017, Lecture Notes in Informatics (LNI), Lecture Notes in Informatics (LNI). Bd. P277. Bonn: Köllen Druck + Verlag GmbH, pp. 81–92, 2017.

[Zi16] Zibuschka, J.; Hinz, O.; Roßnagel, H; Muntermann, J: Zahlungsbereitschaft für Föderiertes Identitätsmanagement, Baden-Baden, 2016.

[ZR12] Zibuschka, J.; Roßnagel, H.: Stakeholder Economics of Identity Management Infrastructures for the Web. In: Proceedings of the 17th Nordic Workshop on Secure IT Systems (NordSec 2012). Karlskrone, Sweden, 2012.