A Model For Assessing The Adherence of E-Identity Solutions To Self-Sovereign Identity

Cristian Lepore, Romain Laborde, Jessica Eynard, Mohamed Ali Kandi, Giorgia Macilotti, Afonso Ferreira, Michelle Sibilla

A Model for Assessing the Adherence of E-Identity Solutions to Self-Sovereign Identity

Cristian Lepore[1], Romain Laborde[1] Jessica Eynard[2], Mohamed Ali Kandi[1], Giorgia Macilotti[3,1], Afonso Ferreira[3,1], and Michelle Sibilla[1]

[1] IRIT, 118 Route de Narbonne, 31400 Toulouse, France,
cristian.lepore@irit.fr
[2] Université Toulouse Capitole, 2 rue du Doyen-Gabriel-Marty, 31042 Toulouse, France
[3] CNRS, 16 Av. Edouard Belin, 31400 Toulouse, France

Abstract. Self-Sovereign Identity (SSI) represents a new concept to manage digital identities, aiming to empower individuals by giving them control over their data. However, the concept is still elusive, and many design patterns coexist without an agreed-upon standard which allows anyone to build identity systems while declaring adherence to SSI. We contribute by formalizing a definition of Self-Sovereign Identity and a corresponding evaluation model of digital identity solutions. We then demonstrate our model value with an in-depth analysis of VIDchain, a business product that promotes Self-Sovereign Identity services in compliance with European regulations. Ultimately, our analysis discusses the quest for a perfect SSI solution and supplies end users with a tool to choose the SSI e-identity solution that best fits their needs.

Keywords: Assessment, Digital Identity, eIDAS Bridge, Self-Sovereign Identity Principles, Validated ID, VIDchain.

1 Introduction

Digital identity is an essential factor in economic growth for businesses and governments. In 2022, the global e-identity verification market was worth $27.9 billion, with an expected growth of over 16% to 2030 [1]. However, every time an App or website asks us to create an e-identity, we have no idea what happens to our data. Today, nearly 72% of users wish to have more control over their e-identities.[4] This is where Self-Sovereign Identity comes in.

Self-Sovereign Identity (SSI) is a relatively new approach to manage e-identities that aims to give end users control of their identity information. A definition of SSI is still elusive [2], but reference architectures have been proposed. The reference architecture consists of an issuer providing verifiable credentials (VCs), which include specific claims about the subject/holder. The subject may differ

[4] Digital Identity for all Europeans; a personal digital wallet for EU citizens and residents. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

from the holder. The subject/holder composes a verifiable presentation (VP) by combining VCs and delivers it to a verifier. Ultimately, the subject can reveal information to verify their identity to the requester without disclosing it to others. Thus, the subject is sovereign in the use of their credentials.

A legal trust framework is crucial for e-identities to be recognized under the country's jurisdiction. In Europe, the eIDAS regulation supplies a legal framework for the governance of e-identities [3]. Despite the recent amendment that aims to give more control to end users, the regulation is not a governance framework for SSI. Thus, the problem of issuing legal identities in an "SSI environment" is relegated to ad-hoc projects, for example, the eIDAS Bridge. Through the eIDAS bridge, Validated ID – a pioneering company in providing Self-Sovereign Identity solutions – bridges the gap between SSI and legal identity utilizing the development of VIDchain [4].

Today, the emergence of Self-Sovereign Identity solutions outlines the importance of assessing the adherence of those solutions to SSI. Previous studies stress the significance of defining specific criteria for evaluation; otherwise, the contribution of their content analysis is limited [5,6]. Therefore, a rigorous definition of Self-Sovereign Identity would facilitate the design and validation of solutions, addressing their completeness and correctness [7]. Thus, we pose the following research questions:

RQ1: What are the principles of Self-Sovereign Identity? We outline the concept of Self-Sovereign Identity through a rigorous definition of principles that considers the interdisciplinary of the subject. We systematize the literature by analyzing articles on ACM, ArXiv, Google Scholar, and IEEE Xplore. We outline concepts, relationships, and rules governing identity ecosystems' entities and provide a formal specification of principles of SSI.
RQ2: Can we assess any SSI system based on those principles? We delineate a model based on our implementable tweak of SSI principles to assess any worldwide digital identity system. We then demonstrate our model value with an in-depth analysis of VIDchain, a product designed to issue eIDAS-compliant Self-Sovereign Identities. We fill the gap between SSI theory and practical design. Our findings allow us to propose a more pragmatic definition of SSI based on the overall performance of the e-identity system. In the long run, we aim to enable future startups and governments to rank solutions, spot weaknesses, and intervene accordingly.

The remainder of this paper continues as follows. The following Section describes our method to structure the research field of SSI. Section 3 provides our contribution as 1) a holistic definition of SSI and 2) a model to assess e-identity solutions. Section 4 demonstrates our model value through a comprehensive analysis of VIDchain. We discuss our findings in Section 5 and limitations in Section 6 before concluding with avenues for future research.

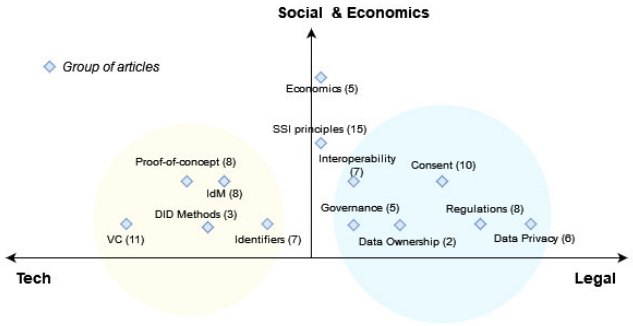

Fig. 1. A systematization of knowledge in a two-axes chart.

2 Methodology

The objective is to structure the research field of Self-Sovereign Identity to spot literature gaps and build new constructs [8]. A systematic review study provides a coarse-grained overview of the research field through several steps as follows [9].

1. Defining research questions. We produced research questions *RQ1* and *RQ2* as outlined in the introduction. From keywording the research questions, we provided the following search strings. We shuffled keywords for better output and corrected strings to avoid wildcards (e.g., SSI and Self-Sovereign Identity and assessing) [10].

- RQ1: "SSI principles"
- RQ2: "Assess" AND "SSI system" AND "SSI principles"

2. Searching. We used search strings to hit articles with relevant keywords in titles and abstracts from ACM, ArXiv, and IEEE Xplore and meta-search engines of academic sources like Google Scholar. That yielded 250 results.
3. Paper Screening. We screened abstracts and conclusions to filter out non-pertinent results through inclusion/exclusion criteria based on the subject matter of interest (SSI), publication year, originality of the work, and proofs-of-concept. We also excluded duplicate results, collecting 95 articles subject to full review.
4. Classification scheme. We read in full the 95 articles and pencilled out information about their objectives, outcomes, state of knowledge, computational method, worked part, and limitations. We rendered thirteen groups based on this information, from Consent management, identifiers, DID Methods, Data ownership/control, Data privacy, Economics, Governance, Identity Models (IdM), Interoperability challenges, Proof-of-concept, Regulations, SSI principles, Verifiable Credentials. We then assigned articles to the most relevant group.
5. Data extraction. We plotted those groups in the two-axis chart of Figure 1, with the horizontal axis (x-axis) sketching technical and legal matters (left to

Table 1. The summary of principles and taxonomies of SSI by different authors.

Principles	**Sovrin (2016) [16]**	**Andrieu (2016) [11]**	**Ferdous (2019) [12]**	**Gilani (2020) [13]**	**Sheldrake (2019) [14]**	**BkThDVr (2022) [15]**
Existence	Control	Control	Foundational	Foundational	Foundational	Personal Data
Control	Control	Control	Control	Foundational	Foundational	Control
Access	Portability	Acceptance	Foundational	Foundational	Foundational	Control
Transparency	Portability	Acceptance	Sustainable	Sustainable		Usability
Persistence	Security Control	Control	Security	Security	Foundational	Personal Data
Portability	Portability	Acceptance Zero-Cost	Flexibility	Flexibility		Personal Data
Interoperability	Portability	Acceptance	Flexibility	Flexibility		Usability
Consent	Control	Control	Control	Foundational		Personal Data
Protection	Security	Acceptance	Security	Security		Personal Data
Minimization	Security	Control	Control Flexibility	Foundational Flexibility		Personal Data
Autonomy			Foundational			
Ownership			Foundational			
Single Source			Foundational			
Choosability			Control			
Standard			Sustainable	Sustainable		
Cost			Sustainable	Sustainable		
Availability			Security	Security		
Disclosure			Control	Foundational		
Validity				Security		

right) and a vertical axis (y-axis) grading the social & economic aspects. Diamonds $\diamond$ render groups, while numbers define the instances of articles. For example, the group *SSI principles(15)* indicates nine articles concerning the principles of Self. The position of the diamond in the chart reflects the category of the journal in which the article was published. If most of the articles in the group pertain to technical journals, we aligned the diamond in the technical area of the chart. We used the *Scimago Journal & Country Rank*[5] and *Resurchify*[6] as a reference indicator to compare journals, and conferences, and help us categorize papers (when possible). The more articles published in technical conferences/journals, the more the diamond shifts toward the left hand. An in-depth chart analysis reveals two clusters. We interpret this as a tentative of SSI to combine definitions from players in different fields.

3 A Model to Assess Self-Sovereign Identity Solutions

Our model results from a two-step process as follows.

a. Existing definitions of SSI. From the systematic review study, we synthesized relevant works on SSI principles. Table 1 summarizes the results. The first column reports the principles. The subsequent columns reflect the name of the taxonomy for each work. The analysis of all works shows that the Sovrin Foundation (second column) gathers principles into a three-way taxonomy with Control, Portability, and Security (2016). Andrieu provides a tech-free categorization (2016) [11], and Ferdous extends principles to cover blockchain-based e-identity systems (2019) [12]. Gilani adds Validity as a further security property (2020) [13]. Others considered essential principles of Self (2019) [14,15].

[5] Scimago Journal & Country Rank. https://www.scimagojr.com/
[6] Resurchify. https://www.resurchify.com/

We used past works to produce our definition of SSI, probing for similarities of snippets in the taxonomies. We paired snippets with similar intent and assigned principles to the category with the highest number of instances. We also omitted principles with duplicate meanings, namely Availability and Disclosure, ultimately obtaining a transitory table of twelve principles within their resulting category. To converge to a unique taxonomy, we designed four groups based on the following *what* and *how* questions: What are the fundamental human rights? What properties guarantee those rights? How can security be implemented? How can an e-identity scale up?

b. Producing the model. Our model results from a definition of *Challenges* and *Dimensions*. A challenge questions principles to bind theoretical properties and real-world initiatives. Then, a challenge produces dimensions to encode parameters. The next part details groups, principles and dimensions as reported in Table 2 and Table 3. The definition of the groups results from the previously mentioned *what* and *how* questions.

Individuals' rights. The category encloses principles for human rights.

- Existence: Individuals can assert attributes to services as proof of their identity. This principle includes assigned attributes that typically denote relationships with other entities, such as usernames and passwords [17]. We explore the option to generate new credentials from existing attributes. Additionally, we incorporate multi-factor authentication to finalize entity authentication following ISO 29115 guidelines [18]. We encode legal credentials (e.g., x509 and QWAC) to validate 'qualified' attributes according to CAdES specifications.
- Persistence. Individuals can present the same attributes from multiple issuers. Persistence distinguishes between Qualified and Non-Qualified Trust Service Providers that are comprehensively assessed under eIDAS. We also list private and public bodies that issue credentials without legal weight. Attributes may also be self-issued.
- Protection. It refers to the ability of systems to avoid censorship, ensuring that the list of identity and service providers is fairly managed.

Trustworthiness. The group encodes crucial features facilitating digital trust. It considers who can access the list of IdPs and attributes, and what attributes is possible to negotiate with an SP.

- Access. Access questions whether users can access the list of identity providers from a local wallet and get information about their attributes.
- Control. It refers to the possibility of individuals to negotiate attributes to a service provider through a user interface. It foresees the possibility of decoupling Personal Identification Data (PID) from other attributes.
- Transparency. Policies, rules, protocols and algorithms to manage the ecosystem members must be transparent. This refers to the possibility of assessing policies, algorithms, and software used to add/remove ecosystem entities.

Secrecy. The category frames properties for the Secrecy of information.

- Consent. It is the permission individuals give to collect, use, and share their data [19]. We consider the consent banner that appears as a pop-up to request user policy acceptance. Dynamic consent involves a dashboard to manage consent preferences. We included post-consent methods to manage consent preferences constraining the information flow[20].
- Data minimization. Users should only share the essential information with the service provider [21]. We explore options for individuals to selectively disclose information and consider the transfer of one attribute only or the associated information, for example, being over 18 years old.

Sustainability. The group advocates for the large-scale adoption of SSI.

- Cost. A digital identity system must be profitable for individuals, public and private organizations [12].
- Interoperability. Users can attest attributes across private and public services [22,23].
- Portability. Attributes can be transported to other ecosystems (GDPR Art. 20(1)(2)), between public and private services.
- Standard. An e-identity system must use globally recognized standards. We consider the readiness of stakeholders to include future standards reducing entry-level barriers through community groups, the industry sector, and government agencies, etc.

4 Assessment of VIDchain

This section provides a test bench for our model. We evaluate VIDchain, a Validated ID product that exploits the SSI paradigm's potential while issuing 'qualified' e-identities [4]. It complements the SSI-related specifications through software components that include the *VIDcredentials* to manage the creation and revocation of credentials. The *VIDwallet* organizes credentials, identifiers, and cryptographic keys. The *VIDconnect* is a custom implementation of the Self-Issued OpenID and did-auth protocol used to authenticate users towards a relaying party. Finally, the eIDAS Bridge allows issuing eIDAS-compliant certificates as verifiable credentials with legal weight [24]. During the evaluation phase, each dimension obtains a full ● mark to indicate that VIDchain complies with the dimension or an empty ○ mark if not. We assign half mark ◐ whenever the dimension is partially covered. Table 2 summarizes the evaluation of Individuals' rights and Trustworthiness. Table 3 summarizes the evaluation for Secrecy and Sustainability.

- *Existence.* VIDconnect supports authentication through username and password, along with multi-factor authentication. VIDcredentials creates a generic W3C Verifiable Credential in JSON-LD serialization format with LD signature (no legal value). However, the issuer signs the entire message, and the subject/holder cannot extract a single attribute from the JSON format to produce a new credential (empty mark).

Table 2. The list of principles, challenges and dimensions.

Individuals' Rights (a)			
Principle	**Challenge**	**Dimension**	**Eval.**
Existence	- What attributes can attest to an e-identity?	- Assigned attributes/ID tokens (Username and Password)	●
		- Multi-Factor Authentication (e.g., One-Time Password)	●
		- Combine attributes for a new credential	○
		- Legal credentials (e.g., x509/QWAC)	●
		- Other credentials (e.g., JWT-based, AnonCreds, ntQWAC)	●
		- Know Your Customer (KYC)	●
Persistence	- Who can issue attributes?	- Qualified Trust Service Providers (QTSPs)	●
		- Trust service providers (Non-Qualified)	●
		- Other public bodies (e.g., government agencies, Univ.)	◐
		- Other private bodies (e.g., Microsoft, Financ. Inst.)	◐
		- Foundations & intergovernmental organizations (IGOs)	○
		- Non-Governmental Organizations (NGOs) and others	○
		- Self-issued	○
Protection	- Who maintains the list of IdPs and SPs?	- Private sector (e.g., banks, credit bureaus)	○
		- Consortium of organizations (e.g., Kantara)	○
		- Government agencies (e.g., national identity authority)	●
		- Supranational organization (e.g., EU Commission)	○
		- Foundations & intergovernmental organizations (IGOs)	○
		- Open community of contributors/NGOs	○
		- Nobody	●
Trustworthiness (b)			
Principle	**Challenge**	**Dimension**	**Eval.**
Access	- How users obtain information about their attributes? - Can users access the list of IdPs?	- Local agent (wallet)	●
		- Shared ledger of IdPs	◐
		- History of attributes	○
Control	- Do users negotiate the release of attributes to SPs?	- User negotiates attributes but PIDs	○
		- User negotiates PIDs	○
		- Users can choose the service provider	◐
Transparency	- Are policies, rules, protocols and algorithms to manage ecosystem members open and clearly stated?	- Guidelines only	●
		- Transparent rules and procedures	●
		- Open protocols	○
		- Transparent algorithms	○
		- Open code/sftw	○
		- Open APIs	●

– *Persistence.* VIDchain can issue attributes provided by Qualified Trust Service Providers and Trust Service Providers under the eIDAS [3]. However, it accepts credentials from only a few private companies and a restricted number of financial institutions. The KYC onboarding process allows users to get government-issued credentials only from ID cards and passports. Although VIDchain produces credentials from phone numbers and email addresses, self-issued credentials, are not allowed.
– *Protection.* The Self-Issued OpenID Provider does not maintain a list of identity providers. However, under the eIDAS regulation, Member States establish, maintain and publish the trusted list of TSPs and QTSPs (Article 22 (1) of the eIDAS regulation).
– *Access.* There is no central map of trust service providers in the SSI ecosystem. However, the Commission holds it for TSPs and QTSPs in eIDAS[7]. Finally, there is no tool to track the history of attributes and those shared with services.
– *Control.* There is no user interface to negotiate the release of attributes, and the choice of service providers is constrained to those accepting verifiable credentials.
– *Transparency.* The Self-Sovereign Identity (SSI) and the eIDAS define rules and the legal basis for ecosystem entities. Validated ID supplies APIs for all the endpoints. However, it is impossible to investigate the endpoints' source code.

[7] EU/EEA Trusted List Browser. https://www.eid.as/tsp-map/#/

Table 3. The list of principles, challenges and dimensions.

Secrecy (a)			
Principle	**Challenge**	**Dimension**	**Eval.**
Consent	- Does consent result adequately expressed and managed?	- Consent banner	●
		- Dynamic consent	○
		- Post-consent	○
Minimization	- Does the service lawfully collect only the minimum amount of information?	- Selective disclosure of attributes but PIDs	○
		- Selective disclosure of PIDs	○
		- Transfer a new subset of attributes	○
	- Do users employ techniques to limit data sharing?	- Transfer one attribute at a time	○
		- Transfer the associated information only	○
Sustainability (b)			
Principle	**Challenge**	**Dimension**	**Eval.**
Cost	- To what extent does the e-identity is profitable for stakeholders?	- Profitable for public services	◐
		- Profitable for private services	◐
		- Profitable for citizens	◐
Interoperability	- To what extent can IdPs attest attributes to SPs across different jurisdictions?	- Among public services	◐
		- Among private services	◐
		- Among others (NGOs, IGOs, Found., etc.)	○
Portability	- To what extent can users transport the list of attributes on different ecosystems?	- Between public authorities	○
		- Between private authorities	○
		- Between others (NGOs, IGOs, Found., etc.)	○
Standard	- Who can issue standards for e-identity systems?	- Working/Community groups (e.g., W3C)	●
		- Industry sector (e.g., Okta)	●
		- Public agencies (e.g., NIST)	●
		- Other (Univ., NGOs, IGOs, Found., etc.)	●

– *Consent.* VIDchain utilizes the consent banner to ask for consent preferences. However, it does not implement different mechanisms to handle consent differently, such as dynamic or post-consent solutions that constrain the information flow.
– *Minimization.* In JSON-LD data is transformed and then hashed and then signed by the issuer with its private key. The holder can only present the entire credential as a verifiable presentation or non. This denies selective disclosure of attributes.
– *Cost.* The limited number of public/private institutions accepting verifiable credentials slows down the spread of this technology. On the other hand, VIDchain "bridges" SSI with eIDAS, thus opening a large ecosystem of approved identity/service providers.
– *Interoperability.* Interoperability among institutions is limited to a handful of accredited bodies and those who shifted to the new SSI paradigm by accepting VCs.
– *Portability.* The VIDwallet does not hold features for the export/import of credentials.
– *Standard.* Validated ID relied on SSI specifications, standards and recommendations. These standards and specifications are provided by many stakeholders, from Working/community groups, governments (eIDAS Bridge), W3C, DIF, Hyperledger Indy, Sovrin, ISA2 program, etc.

5 Discussion of the Results

VIDchain excels in safeguarding individuals' rights by attesting attributes in various serialization formats. The product accepts attributes from public and

private identity providers; some of those services undergo major assessments under the eIDAS framework, and their list is free for everybody to browse. Notably, the absence of a centralized list of identity providers in SSI is also positive even though under the eIDAS, Member States maintain control over this list. Using the wallet guarantees end users reasonable control over their e-identities, and eIDAS contributes to robust interoperability across Europe.

Concerns exist regarding the product's adherence to secrecy standards for end users. While it incorporates recommendations from various stakeholders, these standards may not adequately prioritize user secrecy of information. Verifiable credentials are signed by the issuer before issuance, namely the holder cannot combine those attributes forming a new credential and can either share every claim or non. This prevents selective disclosure of information. To address this, the wallet should implement features for attribute negotiation, allowing users to choose specific attributes to share. VIDchain also falls short in leveraging the Self-Sovereign Identity (SSI) paradigm for consent preferences and lacks a user-friendly dashboard for managing such preferences. Additionally, the absence of features for importing/exporting credentials hinders seamless movement across platforms.

6 Limitations and Conclusions

The study proposes a formalization to assess system adherence to Self-Sovereign Identity (SSI), using the VIDchain product as a test case. The model is intentionally general to avoid overfitting to specific solutions. As a consequent limitation, many implementation-specific parts were left blank for practitioners to fill in and were not tested by our model. For example, we generalized privacy-related issues of wallet authentication. Rapid technological advancement presents challenges in accurately anticipating all possible future scenarios, and the model may not consider new emerging technologies or unexpected changes in the technological landscape. Additionally, regulatory frameworks vary widely among jurisdictions, and regulation changes can significantly impact the scalability and adaptability of electronic identity systems. Therefore, incorporating the different regulatory contexts within which electronic identity systems operate may pose a challenge. At the current stage, the model does not address legal and compliance aspects that play a role in the implementation of electronic identity solutions. Lastly, the model lacks a user-friendly result, opting against a single score to prevent misconceptions. In summary, predicting the future technological landscape is challenging, and the model may not encompass all relevant factors, including emerging technologies, regulatory changes, and human-related aspects. Despite these limitations, the focus is on transitioning from theoretical principles to practical evaluation, marking the initial step toward creating a framework for assessing e-identity systems. Thus, future goals involve enhancing the model's quality by considering additional perspectives, testing in various jurisdictions, and incorporating industry initiatives to refine dimensions.

References

1. Yuxia Fu, Jun Shao, Qingjia Huang, Qihang Zhou, Huamin Feng, Xiaoqi Jia, Ruiyi Wang, and Wenzhi Feng. Non-transferable blockchain-based identity authentication. 2023.
2. Christopher Allen. The path to self-sovereign identity. Available online at http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html, April 2016. Accessed on: 2023-07-21.
3. Regulation (eu) no 910/2014 of the european parliament and of the council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec. Available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910. Accessed on: 2023-11-29.
4. Vidchain — vidchain documentation. Available online at https://docs.vidchain.net/docs/intro. Accessed on: 2023-11-21.
5. Kaja Schmidt, Alexander Mühle, Andreas Grüner, and Christoph Meinel. Clear the fog: Towards a taxonomy of self-sovereign identity ecosystem members. In *2021 18th International Conference on Privacy, Security and Trust (PST)*, pages 1–7. IEEE, 2021.
6. Abylay Satybaldy, Mariusz Nowostawski, and Jørgen Ellingsen. Self-sovereign identity systems: Evaluation framework. *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers 14*, pages 447–461, 2020.
7. Frederico Schardong and Ricardo Custódio. Self-sovereign identity: A systematic review, mapping and taxonomy. *Sensors*, 22(15):5641, 2022.
8. Reid Cushman, A Michael Froomkin, Anita Cava, Patricia Abril, and Kenneth W Goodman. Ethical, legal and social issues for personal health records and applications. *Journal of biomedical informatics*, 43(5):S51–S55, 2010.
9. Laurie Badzek, Mark Henaghan, Martha Turner, and Rita Monsen. Ethical, legal, and social issues in the translation of genomics into health care. *Journal of Nursing Scholarship*, 45(1):15–24, 2013.
10. Sifatullah Siddiqi and Aditi Sharan. Keyword and keyphrase extraction techniques: a literature review. *International Journal of Computer Applications*, 109(2), 2015.
11. Joe Andrieu. A Technology-Free Definition of Self-Sovereign Identity. Technical report, 2016.
12. Md Sadek Ferdous, Farida Chowdhury, and Madini O Alassafi. In search of self-sovereign identity leveraging blockchain technology. *IEEE Access*, 7:103059–103079, 2019.
13. Komal Gilani, Emmanuel Bertin, Julien Hatin, and Noel Crespi. A survey on blockchain-based identity management and decentralized privacy for personal data. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 97–101. IEEE, 2020.
14. Philip Sheldrake. Generative identity — beyond self-sovereignty. Available online at https://blog.akasha.org/generative-identity-beyond-self-sovereignty/, 2019.
15. BlockTechDiVer - Potential of blockchain technology for digital consumer participation. Available online at https://blocktechdiver.de/. accessed on 2022-08-30.
16. Andrew Tobin and Drummond Reed. The inevitable rise of self-sovereign identity. *The Sovrin Foundation*, 29(2016):18, 2016.

17. Alex Preukschat and Drummond Reed. *Self-sovereign identity*. Manning Publications, 2021.
18. Iso/iec 29115:2013 - information technology — security techniques — entity authentication assurance framework. Available online at https://www.iso.org/standard/45138.html, 2013. Accessed on: 2023-11-21.
19. Eoin Carolan. The continuing problems with online consent under the eu's emerging data protection principles. *Computer Law & Security Review*, 32(3):462–473, 2016.
20. Helen Nissenbaum. Available online at https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right, 2018. Accessed on: 2023-07-21.
21. Joe Kilian, Silvio Micali, and Rafail Ostrovsky. Minimum resource zero-knowledge proofs. In *CRYPTO*, volume 89, pages 545–546, 1989.
22. Hakan Yildiz, Axel Küpper, Dirk Thatmann, Sebastian Göndör, and Patrick Herbke. A tutorial on the interoperability of self-sovereign identities. *arXiv preprint arXiv:2208.04692*, 2022.
23. Sudeep Choudhari, Suman Kumar Das, and Shubham Parasher. Interoperable blockchain solution for digital identity management. In *2021 6th International Conference for Convergence in Technology (I2CT)*, pages 1–6. IEEE, 2021.
24. Steffen Schwalm and Ignacio Alamillo-Domingo. Self-sovereign-identity & eidas: a contradiction? challenges and chances of eidas 2.0. *Wirtschaftsinformatik*, 58:247–270, 2021.