IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2023.0322000

Self-Sovereign Identity for Organizations: Requirements for Enterprise Software

RICARDO BOCHNIA[1], DANIEL RICHTER[1] and JÜRGEN ANKE[1]
[1]Digital Service Systems Group, HTW Dresden University of Applied Sciences, Friedrich-List-Platz 1, 01069 Dresden, Germany

Corresponding author: Ricardo Bochnia (e-mail: ricardo.bochnia@htw-dresden.de).

The project on which this publication is based was funded by the German Federal Ministry for Economic Affairs and Climate Action (Grant number 01MN21001A).

ABSTRACT In recent years, the decentralized identity management approach known as Self-Sovereign Identity (SSI) has gained popularity. It aims to give individuals and organizations more control over their identities and credentials. Unfortunately, the adoption of SSI is impeded because the SSI community frequently overlooks the requirements of organizations. The organization's roles as an issuer, verifier, and especially as a holder of Verifiable Credentials (VCs) remain largely unexplored. This is partly because SSI emerged as a user-centric approach focusing on privacy benefits for individuals who act as credential holders. To address this issue, we conducted a multi-method study to identify an initial set of general requirements for organizational SSI software. We used a triangulation approach consisting of a literature review, expert interviews, and product analysis. As a result, we present a comprehensive set of requirements grouped into three main categories: credential management, organizational identity and relationships, and additional requirements. We also examined potential constraints to SSI development and wider adoption in organizational settings. Furthermore, we present gaps between the found organizational-centric requirements and current SSI solutions. Thus, these requirements can serve as a starting point for developing better-tailored SSI software, which represents organizational needs and use cases more closely than current solutions.

INDEX TERMS Enterprise SSI, Enterprise Wallet, Identity Management System, Organizational Wallet, Organizational SSI, Self-Sovereign Identity, SSI, Verifiable Credentials.

I. INTRODUCTION

Organizations process various credentials as part of their daily operations. For example, employee badges are issued to members of an organization, serving as proof of membership to both internal and external relying parties. Organizations can verify credentials issued by other organizations and held by individuals, such as educational diplomas. Lastly, organizations can serve as holders of credentials like carbon emission allowances or commercial registry excerpts, which they can present to other organizations for establishing business relations.

Often these credentials are still physical documents and their processing can be a time-consuming, costly, and laborious task that may require specialized personnel. For example, initiating business between two companies – where each other's identities must be verified – can take weeks or even months [1]. In the past, however, there was often a lack of digital alternatives to physical credentials, which presented a challenge for businesses.

With the rise of Self-Sovereign Identity (SSI) and Verifiable Credentials (VCs), this may change. SSI is a new decentralized digital identity management paradigm that aims to give individuals and organizations more control over their identity and credentials [2]. VCs enable organizations to digitize credentials in a standardized and verifiable manner. It is crucial to highlight that VCs are not limited solely to identity credentials. They can be any attribute attestation from a trusted third party about an entity.

This change is also supported by legislation such as the ongoing revision of the Electronic Identification, Authentication, and Trust Services (eIDAS) regulation. The eIDAS revision introduces European Digital Identity (EUDI) wallets that both individuals and organizations can use to manage their VCs. This entails offering legal person ID VCs which can be used to electronically identify legal entities in the European Union.

Although the SSI domain is relatively new, it has gained increasing research popularity in recent years [3], [4]. However, most studies on SSI have focused on the use of wallets by individuals as credential holders. Organizations' roles as

issuers and verifiers have been recognized but remain largely unexplored. Details of the issuance and verification process have rarely been discussed. Also, the fact that organizations can act as credential holders is frequently overlooked.

However, SSI offers several benefits for organizations, such as cost savings and increased efficiency through the automation of business processes [5], [6]. The UK's National Health Service (NHS) utilized VCs to deploy a digital staff passport during the COVID-19 pandemic, thereby drastically reducing verification time by enabling health professionals to move swiftly between hospitals of the NHS without time-consuming re-verification [7], [8].

Nevertheless, several challenges remain, including infrastructure development, high investment needs, fundamental changes to existing systems and processes, and a lack of understanding of SSI [5]. Furthermore, solutions such as wallets for organizations are still at a very early stage of development and often lack basic functionality [9], making the use of SSI and VCs in organizations even more challenging.

Thus, there is an urgent need for further research in this area to better understand the requirements of organizations regarding SSI and VCs. The main objective of this study is to address this gap and provide an initial overview of the requirements of organizations for SSI software by answering the following research questions:

- RQ1: What potential requirements do organizations have for SSI software?
- RQ2: What gaps exist between the identified requirements and current SSI solutions?

The identified requirements aim to establish a initial theoretical base and to structure the research area on organizational SSI software. Furthermore, they can aid SSI software vendors in developing SSI products that better meet organizations' needs. Despite their importance, industry- and organization-specific requirements were beyond the scope of our research. We also excluded most requirements relating to specific technologies, such as credential formats or cryptographic algorithms, as there are various ways to implement SSI and VCs and it is not clear yet which options will prevail. Thus, we focused on requirements for SSI and VCs, independently of a specific technology stack.

The remainder of this article is structured as follows: The background section provides necessary knowledge about the basics of SSI and presents related work on SSI for organizations. The methodology section explains the approach of a combination of literature review, expert interviews, and product analysis to gain a comprehensive understanding of organizational SSI software requirements. The identified requirements for organizational SSI software are presented in the following three sections: Credential Management, Organizational Identity and Relationships, and Additional Requirements. Subsequently, we elaborate on potential constraints that may impact the fulfillment of identified requirements. Afterward, the gaps between the identified requirements and state-of-the-art solutions are shown. In the discussion section, the implications for practitioners and researchers are explored. Furthermore, some limitations of the study are discussed in this section. Finally, the conclusion summarizes the main findings and presents an outlook for future research.

II. BACKGROUND

SSI is an emerging decentralized digital identity management paradigm that aims to give individuals and organizations more control over their identity and credentials [2]. In the SSI model, digital wallets store and manage VCs. Additionally, systems are required to handle the issuance and verification of these credentials, which are usually carried out by organizations. These systems are often known as agents. The following section explains SSI's foundations and technological components: Verifiable Credentials and Presentations, the Roles in SSI, Wallets, Agents, Decentralized Identifiers (DID), and Verifiable Data Registries (VDR). Related work is discussed at the end of this section.

A. VERIFIABLE CREDENTIALS AND PRESENTATIONS

As the introduction mentions, VCs can be considered digital equivalents of physical credentials. Still, they go beyond just replicating physical documents and thus enable entirely new forms of interactions that are unattainable with traditional paper- or plastic-based credentials [10]. The W3C broadly defines VCs as a set of claims made by an issuer about one or more subjects. They are signed by the issuer with a cryptographic signature proving their authenticity and integrity [11].

When a holder presents a VC to a verifier, it is usually presented as a Verifiable Presentation (VP). A VP is a context-specific collection of claims of one or more VCs signed by the holder and presented to a verifier. One advantage of VPs is that they allow for selective disclosure. Selective disclosure is the possibility of showing only a part of a credential when presented. In this manner, sensitive data can be kept secret if not required by the verifier [2].

B. ROLES IN SSI

In SSI, various roles interact with VCs. These are the issuer, verifier, and holder, which are part of a trust triangle, as shown in Fig. 1, representing the various trust relationships between the roles. For example, the verifier has to trust that the issuer issues the VC correctly and is authorized to do so. Central to establishing trust are governance frameworks. A governance framework is a set of business, legal, and technical rules [12] that govern the handling and structure of VCs [10], such as which credentials an entity can issue. Governance frameworks introduce a multi-layered approach to establishing trust, from the technical to the application layer [12].

In contrast to other depictions of the trust triangle, which position the governance framework below the issuer and verifier, we argue that the governance framework should be situated in the middle. This is because the holder's trust in the issuer and verifier depends on the governance framework. Hence, the governance framework is fundamental not only as a set of rules for issuers and verifiers, but also as a risk

assessment tool for the holder [13]. Placing it in the center of the triangle highlights its vital function in establishing and sustaining trust based on a set of collectively recognized regulations.

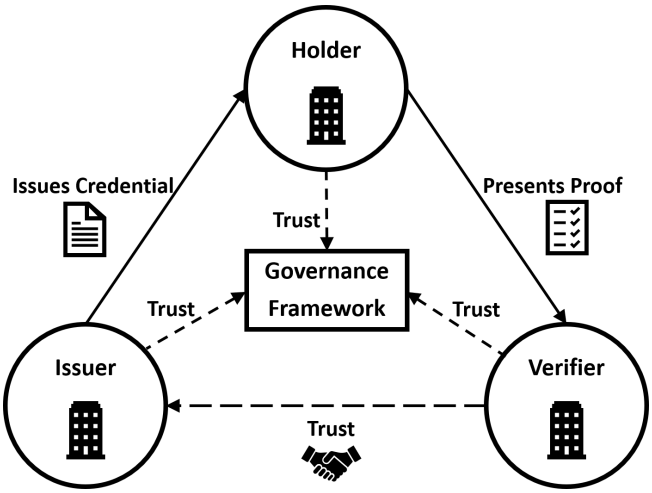

FIGURE 1. **Revised SSI Trust Triangle: In addition to being issuers and verifiers, organizations can also act as holders. To establish trust, governance frameworks are essential. Contrary to conventional depictions, the governance framework occupies the center, emphasizing its role in establishing trust between the holder, issuer, and verifier.**

Each VC has an **issuer** who issues it. The issuer is responsible for ensuring the issued VCs contain accurate and updated data. Examples of issuers include government agencies (identification documents), educational institutions (diplomas), and companies (employee IDs, job references) [11].

The issued VCs are sent to the **holder**, who stores them in their wallet. Although holders often refer to individuals, organizations or objects (such as an IoT device) can also be holders. In addition, the holder is often the **subject** of the credential about whom the credential provides information. However, the holder and subject can also be distinct from each other. For example, when parents manage their children's credentials [11].

Upon request, the holder sends its VCs or VPs as proof to a **verifier**, which verifies their validity. This includes verifying the cryptographic proof(s), validating that the issuer is authorized to issue the credential, and more. For example, a verifier may be an employer who wishes to verify a job applicant's identity. The verifier is responsible for ensuring that the verified VCs are valid and that the information they contain is sufficient for the intended purpose [11].

C. WALLETS, AGENTS, AND VERIFIABLE DATA REGISTRIES

There are several definitions of wallets and agents in the field of SSI. Sometimes, both terms are used synonymously. It is also problematic that the term agent already has numerous other meanings. We decided to use the definitions provided by Preukschat *et al.*, which defines a wallet as software (and optionally hardware) that allows the holder of the wallet "to generate, store, manage, and protect cryptographic keys and other sensitive private data, such as credentials." [2]. Thus digital wallets are essentially the digital equivalent of a physical wallet in the real world and VCs correspond to the cards, bills, or tickets they hold. The agent is used to interact with the wallet. Moreover, the agent communicates and exchanges credentials with other agents. Agents can be divided into two categories based on their operating location: edge and cloud. Edge agents run on the owner's local device, whereas cloud agents run in a cloud [2].

VDRs allow the storage of various data necessary to use VCs. These include data such as DIDs, which are discussed in more detail in the following section, and the revocation status of a VC. There may be not only one VDR but several that are often specialized in storing specific data [11].

D. DECENTRALIZED IDENTIFIERS

According to the W3C a DID is a globally unique digital identifier for an entity managed in a decentralized environment without dependence on a centralized entity [14]. VCs are often combined with DIDs, but this is not mandatory [2]. A DID consists of three parts: the DID URI scheme identifier, the DID method identifier, and the DID method-specific identifier, as shown in Fig. 2. The method is a mechanism by which a particular type of DID and its associated document is created, deleted, updated, or deactivated. There are over 160 distinct methods, with their numbers increasing steadily [15].

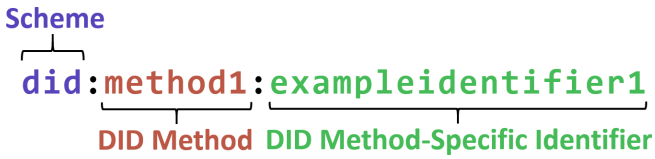

FIGURE 2. **Parts of a DID**

The DID subject can be authenticated through the DID document because it contains the necessary data, such as public cryptographic keys. It can also store data from other entities, such as the public key of a DID delegate, who can represent the subject. This may be identical to a DID controller that can modify the DID document associated with the DID [14].

E. RELATED WORK

As noted in the introduction, SSI research with its user-centric approach, often focuses on the individual. Therefore, the body of academic literature is not very extensive on SSI in organizations. Glöckler *et al.* conducted a review of requirements for Enterprise Identity and Access Management (EIAM) systems and how SSI can offer benefits [16]. Based on the found requirements, they developed an IAM SSI prototype, which was subsequently reviewed by twelve experts with a background in the IAM or SSI industry. The experts acknowledged the advantages of extending IAM systems with SSI. However, as noted by the authors, EIAM systems are just one application of SSI, while our work provides a broader perspective.

Another important study on digital wallets was conducted by O'Donnell, who identified the functions of digital wallets in his Wallet Report, along with various industry partners [17]. In a 2021 update of the report, he criticizes that agents have not yet achieved a serious level of functionality [9]. Although these reports mention several important general requirements regarding wallets, they only briefly touch on organizational wallets. According to O'Donnell, the differences between personal and enterprise wallets are delegation, scale, specialization of agents, such as compliance agents, and additional security considerations, such as a trust framework or penetration testing.

Ansaroudi *et al.* listed some functional and non-functional requirements for digital wallets [18]. However, their requirements are quite general and their main focus is on the technical analysis of wallets. Furthermore, research has been conducted on the usability of SSI [19]–[22]. Although it is mainly based on wallets for individuals, some of the findings can be applied to organizations.

Bochnia *et al.* presented a taxonomy of organizational credentials consisting of ten dimensions within the three perspectives representation, content, and processing [23]. They used their taxonomy to compare physical credentials with VCs, arguing that VCs already offer many of the capabilities of physical credentials but still lack some, such as modifiability or transferability. Delegation, although an important feature for organizations, was also seen as an unresolved issue as it is not standardized and vendor-specific. However, they question whether VCs need to replicate physical credentials one-to-one, or whether it is possible to redesign business processes with revised credentials.

Moreover, the EU Digital Identity Wallet Consortium, which started in April 2023, is working on a European solution for organizational wallets for eIDAS 2.0. The project started recently and is based on the European Architecture and Reference Framework (ARF). However, the ARF and European Digital Identity Wallet Initiative are still in an early stage of development and are subject to fundamental changes. The goal of the revision is to add SSI to eIDAS while continuing to rely on existing eIDAS infrastructures, such as trust providers [24].

The Global Legal Entity Identifier Foundation (GLEIF) is working on a global system of organizational identities based on the Legal Entity Identifier (LEI) and the Verifiable LEI (vLEI). Organizations in several countries are required to own an LEI to participate in financial transactions. Thus, the LEI is already established in the financial sector. The vLEI is based on VCs and can be used by organizations as an organizational ID derived from their LEI. There are also vLEIs issued to employees that can be used to represent the organization [25].

III. METHODOLOGY

We triangulated using three different research methods, which are explained in the following sections. This approach allowed us to gain an extensive overview of the requirements of organizations regarding SSI.

A. LITERATURE REVIEW

As previously noted, the literature on SSI in organizations is sparse. However, because there is some overlap between the requirements for SSI software for individuals and organizations, the literature focusing on SSI for individuals was included. Systematic mapping studies [3], [4] have served as important references for identifying relevant research.

The literature from related areas, such as public key infrastructures (PKIs) and X.509 certificates, was also reviewed to identify overlooked requirements that have not yet been considered in the SSI domain. Additionally, we utilized the internal documents provided by our partners from the ID-Ideal[1] project. The project focuses on using and managing digital identities in business and government use cases. The provided process documents analyze existing business processes and demonstrate their potential implementation using SSI.

B. INTERVIEWS

We conducted semi-structured interviews with ten experts in the SSI space from industry and research. The experts were from German-speaking countries and their experience with SSI ranged from a few months to several years, with a median experience of 3 years. The majority also had prior experience in the broader field of digital identities. Each expert was approached individually because of their experience in working on projects of the showcase program *Secure Digital Identities*, which is funded by the German Federal Ministry for Economic Affairs and Climate Action. The expert profiles are presented in Table 1.

We opted for semi-structured interviews because SSI software in organizations is relatively new and not thoroughly explored. The semi-structured approach allowed us to provide guidance while still allowing interviewees to elaborate on their thoughts. This allowed us to ask follow-up questions and explore topics of interest more deeply.

TABLE 1. Profile of Experts

No.	Organization	SSI Experience	Job Position
1	SSI Provider 1	4 Years	Sales
2	SSI Provider 2	4 Years	Lead Product Manager
3	Research Institute 1	4 Months	Research Associate
4	Research Institute 1	5 Years	Department Head
5	Research Institute 2	3 Years	Research Associate
6	University	3 Years	Research Associate
7	Research Institute 3	3 Months	Research Associate
8	Project Company	1 Year	Lead Consultant
9	IT Service Provider	1 Year	Project Lead
10	Blockchain Company	4 Years	CEO

In advance, we determined that the optimal length for the expert interviews would be approximately 20–30 min. Before the interviews, the experts received an interview guide to prepare to answer the questions accordingly. This guide included key questions and topics we wanted to explore, mainly

[1]https://id-ideal.de/en/

organizational SSI and wallets and their potential features and use cases. The guide given to the experts beforehand was intentionally open-ended to prevent the interview from being too rigid and to allow divergent and different ideas to be presented. These questions as well as some additional questions asked during the interviews can be found in the Appendix.

The interviews were conducted using videoconferencing software to generate the transcripts automatically. In addition, all interviews were recorded with the interviewee's consent to revise the transcript afterward. A method of analysis was considered before conducting the interviews. Due to the semi-structured interview approach, we could not fully predict the direction of the interviews. Therefore, we decided to use the method of categorizing the corresponding statements after the interviews. Thus, the transcriptions were thoroughly reviewed and important statements that fit the research question were highlighted. In the second pass, the statements were categorized and prioritized based on their relevance to understanding the research question. The results of this categorization were summarized in a spreadsheet for ease of reference.

At a later stage, the transcriptions were revisited and analyzed again using a broader knowledge base. Certain statements previously considered less important were reconsidered and recognized as significant.

C. PRODUCT ANALYSIS

The existing organizational SSI software products are generally in the early stages of development. Various systems have been analyzed to determine the current state of the art. SSI systems that only focus on VC use cases for individuals were excluded from the start as our main focus was on the usage of VCs by organizations, which led to the exclusion of many current SSI solutions. We focused on analyzing ready-to-use SSI products rather than software development kits (SDKs). This enabled us to gain an understanding of the products' functionality and their ability to fulfill organizational requirements. Analyzing SDKs would have meant developing our own solution based on the SDKs, which could have skewed the analysis.

Access to a test version and extensive documentation were necessary conditions for a closer examination. Furthermore, only vendors and products with a certain degree of maturity were considered. Unfortunately, we were unable to analyze a single system that uses vLEIs, as these systems are still in early development and no vLEI vendor was willing to give us access to a test version just yet. Finally, six systems satisfied our requirements and were selected for the final product analysis, as presented in Table 2. Nevertheless, the SSI space is evolving rapidly, with new products and vendors constantly emerging, while others may lose relevance or even exit the market, such as Jolocom.

The first step involved examining each system individually, exploring its features, and grouping them into categories. We then compared different systems according to the identified categories. Features offered by multiple vendors were considered important. However, selected features provided by a single system were sometimes also deemed important if they appeared to be useful to organizations and it was likely that other vendors might offer these features in the future. Finally, requirements were derived from these features.

TABLE 2. The analyzed products and their vendors

Vendor	Product	Link
Bosch	Business Partner Agent (BPA)	https://orgwallet.de
Esatus	Esatus SOWL, Esatus Wallet	https://esatus.com
Jolocom	Jolocom SmartAgent, Jolocom SmartWallet	Out of Business
Neosfer	Lissi Agent, Lissi Wallet	https://lissi.id
Spherity	CARO	https://spherity.com
Trinsic	Trinsic Studio, Trinsic Platform, Trinsic Wallet	https://trinsic.id

D. TRIANGULATION

Using a multi-method approach to gain a holistic view seemed reasonable since the topic of SSI for organizations is rather new. Therefore, a triangulation was carried out across several methods. Each identified requirement found by one method was cross-referenced with the other methods. When multiple methods confirmed a requirement, it added to its credibility. Throughout this process, some of the requirements were refined. They were split into finer-grained requirements or merged into a single requirement based on new knowledge from a particular source. Overall, this approach enabled us to derive a comprehensive set of requirements for organizational SSI software. The requirements were formulated using phrase templates as a guideline based upon the work of Rupp *et al.* [26] as shown in Fig 3.

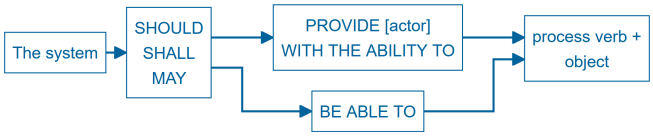

FIGURE 3. The phrase template used for the requirements allows to select one of the following "should," "shall," or "may" based on priority. Adapted from [26].

IV. REQUIREMENTS

This section presents the requirements in three groups: Credential Management, Organizational Identity and Relationships, and Additional Requirements. Each group contains several requirements categories. Within each category, a unique prefix precedes all requirement IDs. The larger categories have been further subdivided, with each subcategory receiving its own prefix. For example, CS01 is the first requirement of the *Credential Schema Management* category, IV-TR01 is the first requirement of the subcategory *Trusted Issuer/Verifier* belonging to the *Issuance, Verification, Presentation* category.

For each group, we provide a table that shows the mapping between identified requirement (sub)categories and the meth-

ods. If identified in the literature, we will cite a maximum of two sources for brevity. Preference was given to those sources that addressed the requirement early or in particular detail. If it was identified by one of the other methods, we add an X to the column to indicate that it was identified by that particular method.

A. CREDENTIAL MANAGEMENT

Credential management is a key aspect of SSI. It encompasses operations that are possible with a credential from issuance to revocation. Organizations require SSI software solutions with feature-rich credential management to fully utilize VCs and their capabilities. Although some of the presented credential management requirements may seem basic, our product analysis revealed significant gaps between the identified requirements and current systems in several areas of credential management, which we will explore in section VI. For example, certain systems offer limited options for validity restrictions and verification. This highlights the need for feature-rich solutions. Table 3 shows the mapping between the requirement categories and methods.

FIGURE 4. Credential operations

According to the credential lifecycle of the Verifiable Credentials Data Model v1.1 [11], the following operations are possible: an issuer can *issue* a VC to a holder, *revoke* the credential, or *respond to a status request from the verifier*. The holder can *store* an issued credential, *present* the credential to the verifier, *transfer* it to someone else who becomes the new holder, and *delete* the credential. The verifier can *verify* a credential presented by the holder or *verify* the credential status either by contacting the issuer directly or by requesting a registry. Additionally, these operations may be associated with specific terms of use or policies. Existing terms of use or policies are significant sources for identifying the requirements of a particular use case.

O'Donnell mentions three other operations: *backup*, *restore*, and *archiving*, both of which are performed by the holder [17]. Richter *et al.* further propose the operation *modification*. This operation describes a change of the credential by a new role, the modifier. Also, it includes the destruction of the credential (which corresponds to the delete operation in the Verifiable Credentials Data Model).

In the end, we identified twelve credential operations as shown in Fig. 4, which extends the Verifiable Credentials Data Model with the operations modify, backup, restore, and archive proposed by O'Donnell and Richter *et al.*. Unlike Richter *et al.*, we consider modify, delete, and revoke as separate operations due to their distinct requirements. Furthermore, we are introducing the validate operation, which focuses on the validity of VCs. Although the operation is mentioned in the Verifiable Credentials Data Model, it is considered out of scope by the specification, as it depends largely on the specific business logic of the verifier [11]. Nevertheless, it is possible to identify certain overarching requirements related to validation that are applicable across different contexts. In the next sections, we explore the following aspects of credential management:

1) Credential Schema Management
2) Credential Requests and Offers
3) Issuance, Presentation, and Verification
4) Revocation and Validation
5) Storage
6) Backup and Recovery
7) Transfer
8) Modification
9) Deletion
10) Archiving

1) Credential Schema Management

Credential Schema Management involves governing and managing schemas that establish the framework for credentials. The possible schema operations are similar to credential operations. However, some required schema operations like archiving, for example, are discussed in the corresponding sections of credential management.

The schema may be created by the issuer or provided by third-party entities like associations. Besides serving as templates during issuance, verifiers also use them to verify credentials properly. Thus, these schemas must be publicly accessible, such as stored in a VDR. Because the specifications for the contents of a schema may evolve, it should be able to update, revoke, and version schemas. Additionally, the issuer authorized to grant credentials for specific schemas should be verifiable. For instance, a schema intended for university degrees must only be used by universities to issue credentials.

Create Schema (CS01) The system shall provide the organization with the ability to create a schema.

Version Schema (CS02) The system should provide the organization with the ability to version schemas.

Retrieve 3rd Party Schema (CS03) The system should provide the organization with the ability to retrieve schemas from a third party during issuance or verification.

Revoke Schema (CS04) The system should provide the organization with the ability to revoke a schema that is no longer used for issuance. However, it is advisable that the schema can still be used for verification unless all credentials issued with this schema are no longer valid.

Validate Schema of Credential (CS05) The system shall provide the organization with the ability to validate a schema used by a certain VC. For example, if the issuer is authorized to use this schema.

2) Credential Requests and Offers

Organizations must be able to initiate specific credential requests or offers depending on their role in a specific credential interaction to interact with one another. This is not limited to issuing and verifying credentials but also includes the broader aspects of the credential lifecycle, such as modifications, renewals, and revocations.

Verifiers may send credential requests to holders. Holders can provide the necessary credentials or decline, preferably providing a reason. The holder's wallet should assist in responding to the request by displaying the requested claims and recommending matching credentials. There may also be cases where the holder offers a credential presentation to a verifier without a previous request. This is especially true when the verifier may not be fully aware of the specific credentials the holder holds and when multiple types of credentials may meet the verifier's criteria. However, verifications initiated by the holder may not be able to be processed automatically (for example, if the specific credential type is unknown to the verifier).

Furthermore, the holder must also be able to request a specific credential from the issuer. An issuer may deny an issuance request but should provide a reason. In some cases, such as ticket purchases, workflows may automatically initiate credential issuance and offer a credential to the holder without a direct request. However, the holder should still be able to decline a request unless they have previously authorized their wallet to auto-accept requests from trusted issuers (see also IV-TR01 and AM01).

Holder-Initiated Requests (CR01) The system shall provide the organization as a holder with the ability to initiate requests for issuance, modifications, renewals, or revocations.

Issuer-Initiated Offer (CR02) The system should provide the organization as an issuer with the ability to initiate offers for credential issuance, modifications, renewals, or revocations.

Verifier-Initiated Requests (CR03) The system shall provide the organization as a verifier with the ability to request credentials from the holder.

Holder-Initiated Offer (CR04) The system should provide the organization as a holder with the ability to offer a credential presentation to a verifier.

Holder Response to Offers and Requests (CR05) The system shall provide the holder with the ability to accept or reject offers and requests while providing an optional reason if rejected.

3) Issuance, Presentation, and Verification

Credential issuance, presentation, and verification are the fundamental operations performed with credentials. As the requirements for these operations are partially interdependent, they are covered in a single section for conciseness. The requirements in this section do not apply to every organization, as some organizations may not perform all three operations since some may only need to verify credentials.

An organization must be able to prove to a third party that it is a trustworthy entity in the role of either an issuer or a verifier. Achieving this depends on the applied governance frameworks, with various mechanisms for verifying trusted issuers and verifiers. Trust in issuers is especially crucial, as they play a central role in the trust of VCs, and fraudulent issuers can inflict significant harm. Moreover, there are a considerably larger number of verifiers than issuers. Given that verifying an organization as a trusted entity typically requires manual labor, it may be reasonable to only verify issuers. Nevertheless, there may be scenarios where specific credentials can only be shared with particular parties, necessitating the vetting of verifiers.

Trusted Issuer (IV-TR01) The system shall provide the organization with the ability to prove its status as a trusted issuer to a third party.

Truster Verifier (IV-TR02) The system shall provide the organization with the ability to prove its status as a trusted verifier to a third party.

The verifier may decide that certain requests can only be answered if the credential has certain schemas and/or is issued by certain issuers. For example, ISO 9001 certifications can only be performed by certain certification bodies. Thus, if an organization wants to verify the ISO 9001 certificate of another organization, it would limit the accepted issuers to the authorized certification bodies.

Schema Restrictions (IV-SR01) The system shall provide the organization as a verifier with the ability to restrict accepted credentials based on their schema.

Issuer Restrictions (IV-SR02) The system shall provide the organization as a verifier with the ability to restrict accepted credentials based on the issuer.

The issuer should be able to restrict who can present the issued credential to the authorized holder(s) and device(s). Additionally, the verifier must be able to verify that only an authorized entity presents the credential. In particular, identifying credentials are good candidates for credential binding [23].

Credential Binding for Issuance (IV-CB01) The system shall provide the organization as an issuer with the

ability to set restrictions on who or which devices can present the issued credentials.

Credential Binding for Verification (IV-CB02) The system shall provide the organization as a verifier with the ability to verify that the entity presenting the credential is indeed authorized.

For particularly valuable credentials, organizations acting as issuers may want to limit the issuance to wallets that meet certain criteria, such as certification by an accreditation body. This is especially important for credentials where misuse could result in severe consequences, such as those issued by government agencies. Therefore, wallets must also be able to demonstrate that they satisfy the required characteristics.

Wallet Restrictions (IV-WC01) The system shall provide the organization as an issuer with the ability to specify criteria that wallets must meet for issuing high-value credentials.

Wallet Compliance (IV-WC02) The system shall be able to demonstrate that it meets the issuer-defined criteria for receiving high-value credentials.

The concept of multiple issuers addresses scenarios where multiple parties issue a single credential such as joint degrees. Although there are many other use cases, see also section IV-B6, the implementation with VCs is still likely to be problematic at present because the specification does not support the feature and is unlikely to be supported in the revised 2.0 version [27]. However, individual issuers may offer separate credentials that can be combined into a composite credential or a single issuer can issue credentials on behalf of a group of organizations.

Multi-Issuer Credentials (IV-MI01) The system may provide multiple organizations with the ability to issue a single credential.

Organizations can utilize terms of use to specify the conditions under which a verifiable credential is issued. For example, whether a credential may be transferred to another party. These terms could serve as a contract and have legal implications. Ideally, the terms of use should be (at least partially) technically and legally enforceable. This reduces the likelihood of misuse, which is important for issuing organizations.

Credential Terms of Use (IV-CT01) The system should provide the organization with the ability to specify terms of use for each credential they issue. Ideally, they should not only be specified but also technically and legally enforceable.

4) Validation and Revocation

Validity involves conditions that must be met for a credential to be considered valid. From a technical perspective, verifying most validity constraints, such as the expiration date, is often identical to verifying any other claim on the credential. From a business perspective, however, they are two different things because validity affects all other credential claims.

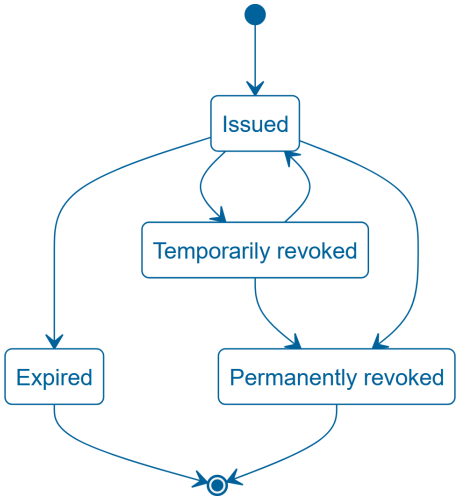

FIGURE 5. Possible states of a credential regarding validity and revocation

An important aspect of validity is revocation, which allows issuers to withdraw previously issued credentials. A special feature is that the revocation state is stored outside the credential. Fig. 5 illustrates the possible states of a credential. Fig. 6 shows the general flow for verifying that a credential is valid and not revoked.

As known from X.509 certificates, it is possible that the revocation status cannot be determined. This also applies to VCs. In this case, the verifier must decide whether to treat the credential as unrevoked (soft fail) or revoked (hard fail), as illustrated in Fig. 6. It may also be possible to treat it as temporarily unrevoked and try to re-verify it later.

Revocation Status Issuer (VR-RE01) The system shall provide the organization as an issuer with the ability to include a mechanism for revocation status.

Revocation Status Verifier (VR-RE02) The system shall provide the organization as a verifier with the ability to verify the revocation status of a credential. Since it is not part of the credential, the verifier needs to use additional means, such as a VDR, to check the revocation status.

Unknown Revocation State (VR-RE03) The system shall provide the organization as a verifier with the ability to decide how to treat a credential whose revocation status can not be determined. It may be treated as either unrevoked (soft fail) or revoked (hard fail) and may also provide an option to re-verify later.

Bochnia *et al.* [23] define the following validity restrictions for credentials:

- Number of uses, e. g., only once
- Time, e. g., expiration date, start date, time frame
- Revocation status
- Unlimited (no restrictions)

An issuer must be able to enforce these restrictions and a verifier must be able to verify these restrictions.

Validity Constraints Issuer (VR-CT01) The system shall provide the organization as an issuer with the ability to

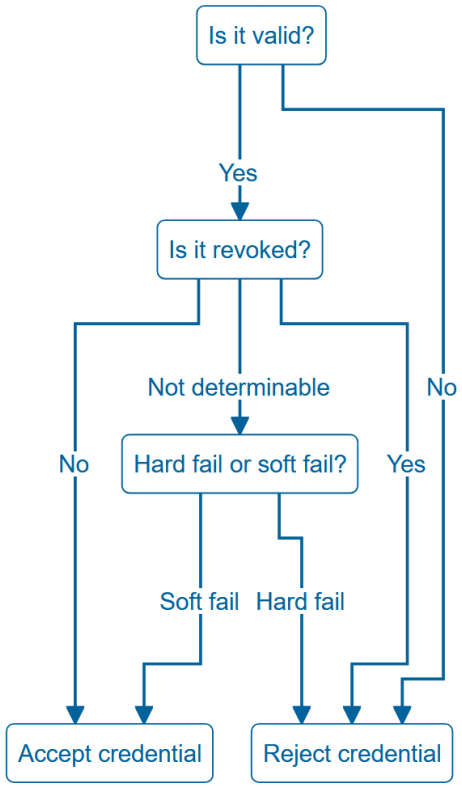

FIGURE 6. **Procedure for checking validity and revocation status**

restrict the validity of a credential. These may include the number of uses, time constraints, such as an expiration date, and a revocation status.

Validity Constraints Verifier (VR-CT02) The system shall provide the organization as a verifier with the ability to verify the validity restrictions of a credential.

In addition to simple validations that check whether a given attribute is equal to, less than, or greater than a given value, many complex validations are required for realistic use cases. These include regular expressions, validating multiple attributes linked with boolean operators, date validation, checking if an attribute value is in a list, and many more.

Complex Validation Issuer (VR-CV01) The system may provide the organization as an issuer with the ability to specify complex validation rules, including regular expressions, boolean operators, date constraints, and list checks.

Complex Validation Verifier (VR-CV02) The system may provide the organization as a verifier with the ability to verify complex validation rules as stated in VR-CV01.

Currently, most SSI systems offer either permanent or no revocation. Temporary revocation has not been widely supported yet. However, it may be necessary. For example, suppose a holder is unsure whether their private key and access to their wallet has been lost. In that case, temporary revocation is preferable to permanent revocation because it is reversible and does not require the issuance of a new credential.

Permanent Revocation (VR-PT01) The system shall provide the organization as an issuer with the ability to revoke a credential permanently.

Temporary Revocation (VR-PT02) The system may provide the organization as a verifier with the ability to revoke a credential temporarily.

When an issuer revokes a credential, the issuer should provide the reason for the revocation and possibly a revocation history, as this may be relevant to the holder and verifier.

Revocation History and Reason (VR-HI01) The system should provide the organization as an issuer with the ability to provide the reason for the revocation and possibly a revocation history, as this may be relevant to the holder and verifier.

5) Storage

Organizations must be able to store the credentials issued to them. In this section, we discuss requirements regarding storage.

> *"The wallet design for private individuals, a mobile app, is not suitable for companies or institutions and, conversely, a cloud wallet that is hosted by someone else, where several people have access, is in my opinion not suitable for a single natural person."* (Expert 1)

When storing their credentials, organizations can choose between on-premise and cloud wallets. While an on-premise wallet aligns better with SSI's core principles, the demand for cloud wallets is growing due to their ease of access [9]. It is worth noting that some wallet providers offer both cloud and on-premises options, allowing organizations to choose based on their specific needs.

On-Premise Storage (ST-LC01) The system should be able to be hosted on-premise for organizations that prioritize data sovereignty and control.

Cloud Storage (ST-LC02) The system should be able to be hosted in the cloud for organizations that prioritize ease of access and do not mind a compromise on certain SSI principles.

Organizations often have complex structures consisting of various units or departments. Thus, organizations may use multiple wallets to store their credentials. This segregation allows for greater control and separated duties but also requires the ability to manage multiple wallets effectively.

Multiple Wallets (ST-MW01) The system should provide the organization with the ability to operate multiple wallets, potentially segregated by organizational units or departments.

For enhanced security, the organization should have the option to store its credentials and keys in a wallet with (hot storage) or without (cold storage) internet access. While hot storage is suitable for everyday use and quicker transactions, cold storage is more secure and thus better suitable for infrequently used items, such as recovery keys.

Hot Storage Option (ST-HC01) The system should be able to allow storage on a wallet with an internet connection, which is suitable for everyday use.

Cold Storage Option (ST-HC02) The system should be able to allow storage on a wallet, which is not internet-accessible and is more secure for storing infrequently used items like recovery keys.

6) Backup and Recovery

The ability to back up and restore a wallet is essential, given the critical nature of the stored data. In the event of a system failure, they can ensure that the data contained in the wallet is not lost. It is recommended that these backups be performed automatically at regular intervals and encrypted [2]. Additionally, strict authorization protocols should be in place to guarantee that only authorized personnel within the organization can perform data recovery.

Scheduled Backups (BR01) The system shall be able to perform automatic backups of wallet data at regular intervals.

Encrypted Backups (BR02) The system shall be able to encrypt backups to maintain data confidentiality.

Recovery (BR03) The system shall provide authorized personnel with the ability to recover data from backups.

7) Transfer

Unlike physical credentials, which can be physically transferred from one entity to another, digital credentials are much more complicated to transfer [23]. This is because it is technically possible for digital credentials to be easily duplicated, which is undesirable in most cases. Thus, it is no coincidence that the Verifiable Credentials Data Model v1.1 mentions the transfer of credentials as a possible operation but does not specify how this should be done [11]. In addition, the transferability of credentials may be restricted by a holder or device binding (as a countermeasure against duplication) or by other issuer specifications, see also IV-CB01, IV-CB02, and IV-CT01. Credentials can be transferred to another holder or a wallet of the same holder.

There are three types of transfers between wallets: between wallets of the same vendor, between interoperable wallets, and between non-interoperable wallets. While transfers between wallets of the same issuer or between interoperable wallets should be possible, transfers between not interoperable wallets are difficult. Issuers may offer solutions that allow credentials to be transferred between not interoperable wallets. Most importantly, transferring between wallets from different vendors should be possible as this reduces the risk of vendor lock-in.

It is also important to consider if the credential is transferred to another wallet of the same holder or to a different holder. Transferring a credential to another wallet of the same holder is usually less problematic as the ownership of the credential does not change. If the holder of a credential changes, the original credential should usually be revoked and deleted from the previous holder's wallet after the transfer. Otherwise, the credential is merely copied, which is undesirable in many cases.

Intra-Vendor Wallet Transfers (TR01) The system should provide the organization with the ability to transfer credentials between wallets provided by the same vendor.

Inter-Vendor Wallet Transfers (TR02) The system should provide the organization with the ability to transfer credentials between interoperable wallets from different vendors to avoid vendor lock-in.

Non-Interoperable Wallet Transfers (TR03) The system may provide the organization with the ability to transfer credentials between non-interoperable wallets, possibly through issuer-led or third-party solutions.

Remove Credential upon Holder Change (TR04) The system shall be able to remove the credential from the wallet upon a successful transfer to a new holder to avoid duplication. For instance, by revoking and deleting the credential.

Issuer Control on Transfer (TR05) The system may provide the organization as an issuer with the ability to control the transfer process, especially if the holder changes. See also IV-CB01, IV-CB02, and IV-CT01.

8) Modification

The modification of VCs is currently not widely considered in research and industry. From a technical standpoint, modifying is similar to issuing a new credential because the VC's content is cryptographically signed and changing the content requires a new signature. Modification is required for credential templates [28]. An example is the vaccination passport, which only becomes a valid credential when the vaccinators make entries. These individual entries form the modification history. In such cases, the issuer explicitly desires or even requires the modification. In addition, it specifies that only people with certain qualifications are authorized to make a change. Nonetheless, not all VCs may need to be modifiable, but they should be able to replace physical credentials that are. In this case, however, a change in the processes is required. In the vaccination passport example, each passport modification could be a new credential. All individual vaccination credentials could be part of a composite credential.

Modification (MD01) The system may provide the organization with the ability to modify a VC if it is authorized.

Support for Credential Templates (MD02) The system should provide the organization with the ability to handle credential templates that can be modified over time.

9) Deletion

Deletion of VCs is possible, but it is difficult to determine whether a VC has been deleted. It is preferable to revoke a VC when it is no longer necessary. Deleting VCs is mainly performed to avoid clutter in the wallet. It may be necessary to delete a VC if it is being transferred to another wallet in the organization and a duplicate copy should not be kept.

Revocation Over Deletion (DE01) The system should provide the organization with the ability to delete VCs

primarily to avoid wallet clutter. The system should encourage organizations to use revocation over deletion for invalidating credentials.

10) Archiving

Due to legal requirements, organizations often need to retain certain documents for extended periods. Thus, some VCs used by organizations may need to be preserved for long periods. However, the specific requirements for archiving depend on legal requirements and internal policies. For our archiving requirements, we relied on eIDAS and its planned revision.

Preservation services are defined in eIDAS Art. 34 and 40 [29]. Their main goal is to extend the trustworthiness of electronic signatures beyond the technological validity period, e. g., by using the European Telecommunications Standards Institute (ETSI) standards of the Advanced Electronic Signature (AdES) family, which define electronic signatures that are suitable for long-term storage [30]. However, preservation services only focus on electronic signatures, seals, and certificates. Thus, in Art. 45g of the eIDAS revision archiving services are proposed, which are required to ensure "receipt, storage, deletion, and transmission of electronic data or documents to guarantee their integrity, the accuracy of their origin, and legal features throughout the conservation period" [31].

Long-Term Storage (AR01) The system shall provide the organization with the ability to store VCs and associated data in long-term storage to comply with legal requirements and organizational policies. However, this does not mean that every VC has to be archived.

Compatibility with existing Archiving Solutions (AR02) The system shall be able to work with existing archiving solutions. For example, the preservation and archiving services according to eIDAS.

Integrity Preservation (AR03) The system shall be able to ensure the integrity of all archived VCs and associated data throughout the required period.

Origin Accuracy (AR04) The system shall be able to guarantee the accuracy of the origin of all archived VCs and associated data throughout the required period.

Legal Feature Preservation (AR05) The system shall be able to ensure that all legal features of archived VCs and associated data are preserved throughout the required period.

B. ORGANIZATIONAL IDENTITY AND RELATIONSHIPS

While the previous section focused on how credentials need to be managed by organizations, this section is more concerned with the organization itself. This includes the identity of the organization, its relationship to other entities, and the internal management of the organization in terms of users, permissions, and organizational units. Table 5 shows the mapping between the requirement categories and methods.

TABLE 3. Mapping between requirements and methods for credential management

Prefix	Requirement Category	L	I	P
CS	Credential Schema Mangement	[17]	X	X
CR	Credential Requests and Offers	[2], [17]	X	X
IV-TR	Trusted Issuer/Verifier	[17]	X	X
IV-SR	Schema and Issuer Verification Constraints	-	X	X
IV-CB	Credential Binding	[2], [17]	-	X
IV-WC	Wallet Compliance for High-Value Credentials	[2]	-	X
IV-MI	Multiple Issuers	[27]	-	-
IV-CT	Terms of Use	[11] , [10]	-	-
VR-RE	Revocation State	[11], [32]	X	X
VR-CT	Validity Constraints	[23]	X	X
VR-CV	Complex Validations	-	-	X
VR-PT	Permanent and Temporary Revocation	[17], [32]	X	X
VR-HI	Revocation History and Reason	[33]	-	X
ST-LO	Location	[2]	X	X
ST-MW	Multiple Wallets	[2], [17]	X	-
ST-HC	Hot and Cold Storage	[2], [17]	-	-
BR	Backup and Recovery	[2], [17]	X	X
TR	Transfer	[2], [10]	-	-
MD	Modification	[10]	-	-
DE	Deletion	[17]	-	X
AR	Archiving	[34], [30]	-	-

L = Literature, I = Interviews, P = Product Analysis

1) Organizational Identity

Organizational identity is a key aspect of SSI software for organizations. Ideally, each organization has a unique digital identity that distinguishes it from other organizations. To do this, an organization needs to prove its identity to others and verify the identity of other organizations. However, like people who have various ways to prove their identities – such as a national ID card, driver's license, or passport – organizations will also have multiple options for identification as they may own multiple unique identifiers, such as a value-added tax identification number (VATIN), Data Universal Numbering System (DUNS) number or a LEI.

> *"In the company, there is something like a client capability, ... that there are multiple organizations underneath – especially when the company is among the larger ones – which then are somehow sub-identities of the original company."* (Expert 6)

To prove their identity, organizations need organizational ID credentials. Depending on the type of organization, different credentials are possible, such as a trade register excerpt, a bank account confirmation, or a LEI entry. A public organization likely needs a different ID type than a private company. For the LEI, an organizational ID already exists on a VC basis with the vLEI provided by GLEIF [25]. Moreover, the EU is working on the Organizational Digital ID (OID) as an ID for organizations [24].

Moreover, large organizations often consist of smaller or-

ganizations, such as a company and its subsidiaries or a state and its agencies. Thus, it is necessary to create a link between organizational IDs that are related since it is important to prove that an organization is indeed a subsidiary of another organization in certain cases.

Organizational Identity Credentials (OI01) The system shall provide the organization with the ability to own and prove its digital identity which is represented by one or more VCs issued by an authoritative third party.

Public Key Identifier Binding (OI02) The system shall provide the organization with the ability to make its identifier public. See also IV-TR01 and IV-TR02

Hierarchical Relationships (OI03) The system shall provide the organization with the ability to establish hierarchical relationships between the organization's ID and its sub-entities, like sub-organizations, subsidiaries, and departments. Thus, the organization can prove that it is the parent of a given sub-entity and vice versa.

2) Relationship Management

Relationship management is also essential for organizations. According to Windley, the purpose of identity systems is not to manage identities but to support digital relationships based on those identities [35]. These relationships can take different forms, as the organization can take on the role of an issuer, verifier, or holder.

> *"This means that the topic of Organization Wallet differs significantly from the topic of Human Wallet in that I have to represent such multiple relationships. I can initiate a contract or establish a relationship from within the company, for example, but in the end, the action is always triggered by a person, and thus a human identity, which makes the whole matter a bit more complicated."* (Expert 10)

It should be possible to establish, change, and delete a relationship with all interaction partners. Onboarding new interaction partners as an organization acting as an issuer is particularly relevant because of the current low adoption of SSI [36]. They could, for example, provide the future holder with a link to download a compatible wallet or offer a cloud wallet service.

Some of these relationships may involve secure and persistent channels. However, not every communication protocol may allow for establishing persistent channels prior to the credential exchange. Thus, the system may also need to support the exchange of credentials without such a persistent channel. Furthermore, providing a relationship history to record conducted transactions may be useful.

The system must ensure mutual identity verification when exchanging credentials between interaction partners. This includes the ability for each party to verify the other party's identity. For example, by presenting a type of identity VC issued by a trusted issuer for organizational identities (see also IV-TR01 and OI01). This is vital to ensure that VCs are not illegally obtained or presented by unauthorized third parties.

From an enterprise perspective, relationships can be categorized as business-to-consumer (B2C), business-to-business (B2B), and business-to-administration (B2A). Depending on the relationship type, there are different requirements. In B2C, the number of interaction partners is usually much larger than in B2B or B2A. As a result, automated transactions are often more prevalent because of the larger number of records being processed, see also section IV-C5.

Finally, many organizations already use existing systems for relationship management, such as accounting, Enterprise Resource Planning (ERP), and Customer Relationship Management (CRM) systems. As a result, an SSI system should ideally be able to integrate with the existing business infrastructure. This is discussed in more detail in section IV-C2.

Multiple Roles (RM01) The system shall provide the organization with the ability to take on multiple roles – such as issuer, verifier, and holder – within the same SSI ecosystem.

Mutual Identity Verification (RM02) The system shall provide the organization with the ability to verify the other party's identity and vice versa.

Relationship Establishment (RM03) The system should provide the organization with the ability to establish a relationship with interaction partners. This may include the establishment of a secured and persistent channel between the parties and saving relevant information about the other party, such as master data.

Onboard Interaction Partners (RM04) The system should provide the organization with the ability to support the issuance of credentials to entities that do not yet have a wallet.

Relationship Modification (RM05) The system should provide the organization with the ability to modify a relationship with an interaction partner.

Relationship Termination (RM06) The system should provide the organization with the ability to terminate a relationship with an interaction partner.

Relationship Types (RM07) The system may provide the organization with the ability to handle different types of relationships in a different way, e. g., by differentiating between suppliers and customers.

Relationship History (RM08) The system should be able to keep a relationship history that records all transactions conducted with interaction partners.

3) SSI as an IAM

Organizations often have traditional IAM systems that manage user identities and their associated rights based on attributes or roles. Leveraging SSI for IAM and managing permission based on VCs may offer benefits such as faster on- and off-boarding, selective disclosure, and a higher degree of automation for better manageability [16]. For example, Microsoft has integrated verifiable credentials (VCs) in their IAM solution Entra, previously called Azure Active Directory [37]. However, according to Glöckler *et al.* and Glaude and

Kudra, most traditional IAM providers show little interest in using SSI inside IAMs [16], [38].

> *"Is the employee authorized to do certain things? For example, if one has completed a training, it can then be entered into the wallet, and certain processes can process this entry... I do believe that with this, one can also rethink the rights system and authorization system within a company. This is a topic that is gaining more complexity in today's world."* (Expert 8)

SSI as an IAM (SI01) The system may be able to be part of an IAM system and be used to manage access to the organization's resources.

4) User and Permission Management

Whereas the previous section described how an SSI system can help manage permissions to the organization's resources, this section focuses on users and permissions within the SSI software. Among the experts, one of the most frequently cited key differences between wallets for individuals and those for organizations is user management, as multiple users use it. In particular, permission management and delegation (see next section) were identified as unresolved issues. Some experts even argued that wallets for individuals and organizations are mainly technically identical, differing only in user administration and permission management.

> *"I believe the biggest difference is the target audience. For a private individual, the individual should have sovereignty over their data, and not a group of people having control over my data, but really just one person. In companies, multiple people should have access to the company's data, and that, I believe, is the main difference that needs to be considered. Therefore, I think two different approaches are needed now with the wallet topic."* (Expert 1)

Currently, there is no consensus on the required permissions and roles in SSI systems. Some systems only distinguish between administrators and regular users, which is insufficient for larger organizations. Other systems offer finer granularity, such as permission to issue credentials, request proofs, and read-only access for auditing purposes. A list of potential permissions and roles based on our triangulation is given in Table 4.

Multiple Users (UP01) The system should be able to handle multiple users.

Roles and Permissions (UP02) The system should provide administrators of the organization with the ability to assign roles and/or permissions to other users. See also Table 4 for potential permissions and roles.

TABLE 4. Potential roles and associated permissions.

Permission	Description
Administrators	Extensive privileges. Can give permissions to other users.
Delegate	Can act on behalf of the organization. There will likely be different types of delegation and certain types may have greater limitations than others.
Issuer	Can issue credentials, may be restricted to certain schemes.
Presenter	Can present credentials in the name of the organization.
Verifier	Can request proof from a holder.
Schema Editor	Can manage schemas.
Proof Template Editor	Can manage proof templates.
Policy Editor	Can manage policies.
Auditor	Read-only access for auditing purposes.

5) Delegation

Delegating tasks and responsibilities is another important topic for organizations as it allows them to use their resources effectively. To do this, organizations may employ delegation credentials to employees, machines, and software, allowing those entities to act on behalf of the organization.

> *"Who actually creates the corporate wallet in the first place? Who authorizes others? And is the person, who authorizes these other authorized individuals, themselves authorized to authorize others? Yes, that is super complex."* (Expert 10)

GLEIF defines two types of delegation credentials. Official Organizational Role (OOR) and Engagement Context Role (ECR) credentials are issued to natural persons. The former is for official positions, as defined in ISO 5009, like the company's CEO. In contrast, the latter is for non-official positions like a buyer at a company [39]. Čučko *et al.* introduce *Verifiable Mandates* as a type of delegation credential [40]. They stress the need for constraints on such delegation credentials, see also VR-CT01 and VR-CT02.

Delegation Credentials (DL01) The system shall provide the organization with the ability to issue delegation credentials to natural persons, machines, or software agents.

Types of Delegation (DL02) The system should provide the organization with the ability to employ different types of delegation. Official representatives are typically recorded in an external registry, like a trade register, whereas other types of delegates are not.

Sub-Delegation (DL03) The system may provide authorized employees of the organization with the ability to delegate to their subordinates.

6) Organizational Units

Representing different organizational units is a feature commonly found in other enterprise software such as ERP or accounting systems. Some of the reviewed systems already offer a similar tenant feature. SSI software that supports organizational units is important for effectively managing complex organizations with multiple sub-units, such as departments or subsidiaries, within a single software instance. While each sub-unit may possess its distinct data and configurations, some components, such as universal policies or credentials, could be shared across the entire organizational structure.

As organizations have a complex structure, various sub-units may act as issuers. These sub-units do not have to be legally independent entities. If they are not legally independent, they can only issue on behalf of the associated organization. In this case, it may be required that both the organization and the organizational unit are stored as issuers (see IV-MI01) inside the credential, even if the organizational unit is its own legal entity.

Organizational Units (OU01) The system shall be able to support the concept of organizational units.

Sub-Unit Issuance (OU02) The system may provide an organization unit with the ability to issue credentials independently. However, it may be necessary to include the parent organization and unit as an issuer. See also IV-MI01.

Delegated Issuance (OU03) The system should provide the organization units with the ability to issue credentials on behalf of the associated parent organization when necessary, especially when the sub-unit lacks the authority to issue credentials independently.

TABLE 5. Mapping between requirements and methods for Organizational Identity, Relationship and User Management

Prefix	Requirement Category	L	I	P
OI	Organizational ID	[24], [25]	X	X
RM	Relationship Management	-	X	X
SI	SSI as an IAM	[16], [41]	X	X
UP	User and Permission Management	[17]	X	X
DL	Delegation	[2], [40]	X	-
OU	Organizational Units	-	-	X

L = Literature, I = Interviews, P = Product Analysis

C. ADDITIONAL REQUIREMENTS

This section delves into other important requirements for SSI in organizations that did not fit into the previous sections. Table 6 shows the mapping between the requirement categories and methods.

1) Compliance

Ensuring compliance with legal requirements and internal guidelines is crucial for organizations. It minimizes the risk of potential violations, which can lead to consequences such as loss of reputation and fines. Lemieux *et al.* mention that SSI solutions that do not capture the exchange of transaction data can be problematic for audit and accountability purposes because there is no proof that the exchange occurred. They suggest a proof registry to ensure that proof data can be validated in the event of a dispute or audit [42]. While logging proofs are important, logging other activities within the system is also necessary for auditing purposes and detection of potential compliance violations.

The four-eyes principle can help improve compliance in organizational SSI systems. It states that at least two people must independently review and confirm certain actions or decisions to prevent error or abuse. Multi-signature is a possible implementation of the four-eyes principle and refers to a set of procedures in which multiple authorized parties must provide digital signatures to approve a transaction or action within a system [43]. It is already used in cryptocurrencies but can also be applied to SSI, for example, when issuing a credential that needs to be approved by multiple actors [44].

Activity Logging (CA01) The system shall be able to log all activities related to the credential operations and other activities like changes to permissions or relationships while adhering to data privacy regulations.

Multi-Signature (CA02) The system shall provide the organization with the ability to use multi-signature by requiring at least two authorized parties to approve certain transactions or actions.

Custom Compliance Rules (CA03) The system should provide the organization with the ability to configure custom compliance rules such as the four-eyes principle.

Real-Time Alerts (CA04) The system may be able to provide real-time alerts for potential compliance violations.

2) Interfaces for Integration

Interfaces can be divided into two categories: Interfaces between SSI systems and interfaces with other systems, such as ERP systems. Using SSI-specific interfaces such as DIDComm is unsuitable to communicate with established non-SSI systems. Instead, it is advisable to rely on established interfaces as illustrated in Fig. 7. Expert 2 highlighted some systems in B2C companies requiring integration, while Expert 4 mentioned the topic of legacy systems:

> *"Then, of course, one must look at how to integrate, for example, support, ticket, CRM systems, and so on. These connections need to be established."* (Expert 2)

> *"One point that comes to my mind is the topic of legacy systems, meaning that I also have to consider what is the system landscape I am operating in?"* (Expert 4)

In particular, providing a REST interface facilitates communication with other systems due to its widespread use [45]. Many SSI agents already provide a REST interface, underscoring its importance. SSI software can be integrated into existing business processes through this interface, provided the REST interface offers sufficient functionality. As an alternative to REST, SOAP may be required for XML document exchange, particularly for legacy systems.

Regarding SSI-specific interfaces, the DIDComm protocol, designed as a communication interface between different SSI systems, has not yet reached the expected level of adoption [9]. A new version of the DIDComm specification is currently under development [46]. Another interface that has recently gained popularity in the SSI world is OpenID for Verifiable Credentials (OID4VC). The advantage of OID4VC is that it is based on the already established OpenID Connect protocol. Ultimately, it remains to be seen which interfaces will prevail in SSI.

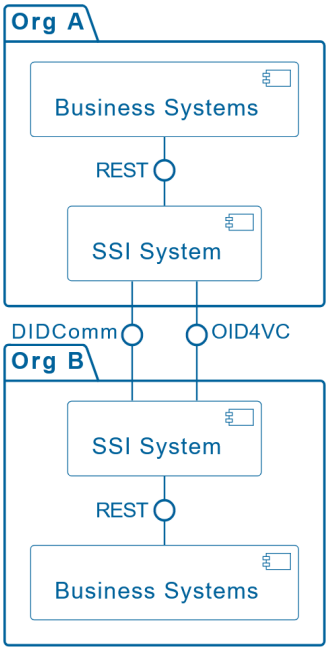

FIGURE 7. Interfaces between SSI systems from different organizations and interfaces between SSI and non-SSI enterprise systems within an organization. Note: This diagram is simplified for clarity. Other interfaces are possible.

Interfaces for Integration (IF01) The system should be able to provide interfaces that allow integration into existing enterprise systems and processes.

REST Interface (IF02) The system should be able to provide a REST API for integration with traditional enterprise systems like ERP or accounting software.

SOAP Interface (IF03) The system may be able to offer a SOAP interface for integration with legacy systems that rely on XML document exchange.

DIDComm Interface (IF04) The system may be able to use the DIDComm protocol for SSI-to-SSI communication.

OID4VC Interface (IF05) The system may be able to use OID4VC as an SSI-to-SSI and even as an SSI-to-Non-SSI interface.

3) Interoperability

An organization's SSI system can only interact with others utilizing an interoperable system. For instance, an organization can only receive credentials from issuers if the wallet is compatible with the format of the credentials issued by the issuer. Expert 5 states why interoperability is needed:

> *"We have not only internal corporate identity management, but an identity management that is so interoperable that it can also be used across company boundaries."* (Expert 5)

Several initiatives have been undertaken to achieve interoperability in the context of SSI. Among these initiatives, the Hyperledger group has developed Aries Interop Profile 1.0 and 2.0, which ensures interoperability among different Aries agents [47]. Furthermore, the W3C Credentials Community Group is working on an interoperability test suite for the Verifiable Credentials v2.0 data model [48].

A recent and extensive examination of the interoperability among SSI systems and a reference model for accomplishing interoperability is presented by Yildiz *et al.* [49]. They also recognize interoperability as essential to the success of SSI but acknowledge that current solutions lack interoperability. O'Donnell believes that interoperability between SSI systems is currently not achievable due to immature standards and the lack of an interoperability compliance suite [50]. He advises focusing on business functionality first and approaching interoperability in small steps [9], [50].

In addition to interoperability between SSI solutions, it is also critical that they are interoperable with other systems in the enterprise, such as ERP or accounting systems, which presents an additional interoperability challenge. An important difference is that these enterprise systems are mature and feature established communication protocols and data formats. Thus, achieved interoperability with an enterprise system will be more stable and require less maintenance than interoperability to another SSI system due to different degrees of maturity and development pace.

SSI-to-SSI Interoperability (IN01) The system may be able to interoperate with other SSI systems. The system shall be able to interoperate with other SSI systems once interoperability compliance suites are available and recognized.

Enterprise System Interoperability (IN02) The system should be able to interoperate with enterprise systems employed by the organizations.

4) Batch Processing

Batch Processing is essential in B2C or administration-to-consumer (A2C) scenarios where organizations must interact with numerous partners efficiently.

Batch Processing (BP01) The system shall be able to execute credential operations on a batch of credentials simultaneously.

5) Automated and Manual Operations

Although it is more efficient to automate operations as much as possible, in some cases, manual operations by humans may be required, for instance, due to legal restrictions or process requirements. However, the system should support automated operations without human intervention, e. g., automated credential offers and requests, as it provides the opportunity for efficiency gains. For example, the automatic presentation and verification of organizational identities can significantly accelerate the onboarding process for new interaction partners. Renewing expiring credentials automatically is another possible option.

Automated Operations (AM01) The system shall be able to execute credential operations automatically.

Manual Operations (AM02) The system shall provide the user with the ability to execute credential operations manually.

6) Offline Capability

Offline capability allows organizations to handle credentials in cases where internet connectivity is not guaranteed or required. In this case, alternative communication protocols like NFC or Bluetooth (LE) are required. In particular, checking the revocation status is challenging because this information is typically stored outside the credentials. Keeping a local copy of data necessary for successful verification, such as schemas or revocation registry entries, may be an option. Another option would be to perform a verification without the revocation status first, followed by a revocation status validation when the internet connectivity is restored.

Offline Capability (OC01) The system may be able to perform operations without an internet connection by using local communication protocols. However, some operations may not work or be restricted without an internet connection.

Local Cache (OC02) The system may be able to cache certain data (e. g., schemas) to allow offline execution of credential operations. This cached data may also be used in online mode for efficiency reasons.

7) Data Organization

Data organization is the system's ability to handle a variety of credentials and related data objects, such as schemas, relationships, transactions, and proofs, in an organized manner. It is required because organizations deal with a large variety of these items and require an organized way to do so. By providing functionalities like searching, categorizing, grouping, and sorting SSI systems, organizations can handle credentials in an organized way.

Search (DA01) The system should provide the organization with the ability to search for data objects.

Categorize (DA02) The system should provide the organization with the ability to categorize data objects.

Grouping (DA03) The system should provide the organization with the ability to categorize data objects. For example, several related credentials may be grouped into a single composite credential.

Sort (DA04) The system should provide the organization with the ability to sort data objects.

8) Notifications

In many cases, affected parties should be notified after a specific operation as they aid parties in remaining informed about the status of their credentials. For example, when a new credential is issued or revoked.

Notifications (NO1) The system should be able to create notifications.

9) Security

There are numerous security requirements for SSI software for organizations, as they have much higher security needs. Given the complexity of this topic and our team's lack of specialized expertise in cybersecurity, we did not go into detailed security analysis. This decision was made to avoid potential incomplete security requirements, which could pose a potential risk to organizations implementing SSI solutions based on these requirements. However, Pöhn *et al.* provided a comprehensive review of potential threats and countermeasures for SSI using the STRIDE threat identification model [51]. STRIDE focuses on spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. Pöhn et al. briefly touch on organizational aspects such as processes, trust, and governance, but they acknowledge that this area is largely unexplored and an area for future research.

TABLE 6. Mapping between requirements and methods for further requirements and potential constraints

Prefix	Requirement Category	L	I	P
CA	Compliance	[17]	X	X
IF	Interfaces for Integration	[2], [52]	-	X
IN	Interoperability	[49], [53]	X	X
BP	Batch Processing	[17], [2]	X	X
AM	Automated and Manual Operations	-	X	-
OC	Offline Capability	[2], [17]	-	-
DA	Data Organization	[21]	-	X
NO	Notifications	[17], [21]	-	X
-	Security	[2], [51]	X	-

L = Literature, I = Interviews, P = Product Analysis

V. POTENTIAL CONSTRAINTS

Due to many potential constraints, we will cover only a few selected ones relevant to many use cases and industries. These include technological, organizational, and legal aspects that should be considered when implementing SSI systems for organizations. The mapping between the constraints and sources can be found in Table 7.

A. EIDAS 2.0

The revision of the eIDAS regulation introduces an EU wallet that organizations can use to store their credentials and prove their identity [54]. This may require SSI systems used in organizations within EU jurisdiction to be compatible with the EUDI Wallet legislation, especially for B2C. The revision is ongoing, and the progress of large-scale pilots will influence the final revision. At this time, it is advisable to monitor the developments in this area closely. In November 2023 a final agreement between the Commission, Parliament, and the Council of the EU was achieved [55]. However, due to privacy concerns [56] additional revisions may occur. In the following, we explore some major points that may have an impact on SSI in organizations. However, uncertainties remain due to the complexity of the legislation and the fact that implementing acts are still forthcoming.

Issuance, use, and revocation of the EUDI wallet is free of charge only for natural persons but can be monetized for legal persons. However, the member states are advised to agree on a common business model and fee structure, that is appropriate for small and medium enterprises. Very large online platforms

will be required to accept the use of the EUDI wallet upon the voluntary request of the user which should facilitate the adoption of SSI solutions.

Every issuer and verifier will be required to register. Thus EUDI-compatible wallets must implement the requirements IV-TR01 and IV-TR02. For verification requests the verifier must provide at least the name, the registration number of the official record as well as its data and the reason for the request.

All issuers of (Qualified) Electronic Attribute Attestations ((Q)EEA), which are credentials certifying specific attributes of an entity, will be considered a (Qualified) Trust Service Providers ((Q)TSP). This means many organizations will likely use a (Q)TSP during issuance instead of becoming a (Q)TSP as they are regulated.

The regulation also aims to ensure technology neutrality. Especially for the new trust service (Qualified) Electronic Ledgers, neither favoring nor discriminating against any technology. This means that blockchain-based SSI solutions can be eIDAS-compliant.

Nevertheless, it is possible that the revised eIDAS will not be adopted widely. This is the case with the current eIDAS, where a public consultation revealed that lack of awareness and relevant services are among the top five limitations [57]. This leads to a lack of incentives for member states and private service providers to participate in the provided cross-border infrastructure [58].

B. GDPR

Many organizations will have to deal with credentials that contain General Data Protection Regulation (GDPR) relevant data. While credentials about the organization itself are not subject to the GDPR, credentials about people such as employees, customers, or citizens are. SSI can be GDPR compliant, but there may be legal uncertainties depending on the specific case and a privacy impact analysis may be required [59]. An example of a possible GDPR issue was given by Expert 5:

> *"For instance, if you produce master data for manufactured devices, this consequently leads to various employees creating separate certificates, and then of course, one must also consider GDPR compliance, because if every user, every employee has their own private-public key pair and ultimately issues certificates, this might be undesirable because it involves the transfer of personal data to third parties."* (Expert 5)

C. IMMATURE STANDARDS

The lack of maturity of standards in the SSI world is a significant barrier to the current implementation of SSI solutions, as organizations may face technical challenges and uncertainty. For instance, the W3C's recommendation of the DID specification in 2022 was heavily criticized by Mozilla and Google [60]. They argued that there is no practical interoperability and that the DID architectural approach would lead to new DID methods rather than promoting interoperability. However, these objections were overruled by the W3C director. There are currently more than 160 DID methods, 30 more since the DID specification has become a recommendation [61]. In addition, the v1.1 Verifiable Credentials Data Model will be replaced by a v2.0 version in the future [62].

D. LACK OF BEST PRACTICES AND UNFAMILIARITY WITH SSI

Another important limitation is the unfamiliarity with SSI in organizations [5] and the lack of best practices for implementing SSI technologies in organizations, making it difficult to implement and use these systems effectively. But best practices for individual wallets are emerging, such as for user experience [19], which may be relevant to organizational wallets as well. In the EU, ongoing large-scale pilots and the upcoming EUDI reference wallet have the potential to establish new best practices.

E. BUSINESS MODEL CHALLENGES

In the expert interviews, expert 10 was critical of the potential of SSI and saw thinking in terms of new business models as a major challenge. Pasalic and Laatikainen *et al.* both mention that SSI requires new business models that must be developed [5], [63]. An analysis of enterprise business models leveraging SSI and how they may offer value to businesses can be found in [64]. Expert 10 elaborated on why he thinks that SSI for companies has more potential than for individuals. Expert 6 and Expert 10 explained that focusing on master data management is worthwhile. While Expert 1 talks about the issue of monetizing an open-source SSI solution:

> *"Google has an economic goal. They say: We want to achieve this. We want to get as many users as possible, offering user functions. We provide these functions to users for free, because then we get their data...*
> *I [as an SSI provider] cannot do anything with the user's data, because I don't have it. This means that one has to think in entirely new business models, and I believe this won't happen on its own...*
> *We have put a lot of thought into how to actually get SSI into the market, and many are still approaching the topic by starting with human identity. I believe, for the aforementioned reasons, that it is extremely difficult to gain widespread acceptance and reach the masses... In companies, there are really practical use cases, and they can operate in a small microcosm without involving the government or anything like that."* (Expert 10)

> *"Master data management, this could be a first use case where one actually sees the first applications. Which, as mentioned, is currently really very expensive, mainly due to the fact that the data sources are probably very diverse."* (Expert 6)

> *"So our idea is not the classic license model, but rather support and maintenance for large installations."* (Expert 1)

As Kubach *et al.* shows in several studies, there is a low willingness to pay despite great dissatisfaction with existing identity systems among end users and service providers [36], [65]. They propose government investment as a solution for building a basic infrastructure. They argue that widespread adoption increases willingness to pay [65]. The bankruptcy of Jolocom, a pioneer company in SSI, exemplifies the challenges of finding a viable business model within the SSI industry.

TABLE 7. Mapping between potential constraints and methods

Constraint	L	I	P
eIDAS 2.0	[66], [67]	-	X
GDPR	[59], [68]	X	X
Immature Standards	[50]	X	X
Lack of Best Practices and Unfamiliarity with SSI	[5]	X	-
Business Model Challenges	[64], [65]	X	-

L = Literature, I = Interviews, P = Product Analysis

VI. COMPARISON WITH CURRENT STATE

Table 8 provides an overview of the fulfillment degree of each requirement category by the analyzed products. It indicates the areas effectively addressed and those that require improvement. As the list of requirement categories is rather extensive, we only present a brief overview. However, in the discussion section, we will delve deeper into our assessment of the current state of the art and how identified gaps could be addressed.

Some of the analyzed products did not support several credential operations, such as deletion, backup, recovery, and revocation. Transfer, modification, and archiving were not supported at all.

Regarding organizational identity and relationships, we have found that relationships and user and permission management are already supported. However, the concept of delegation and organizational units remains a challenge.

Another point of note is the lack of support for more advanced features, such as Wallet Compliance for High-Value Credentials, Complex Validations, Multiple Issuers, and Offline Capability. In addition, interoperability remains an issue.

VII. DISCUSSION

This section provides a summary of our research before delving into its implications. We have organized our implications into two sections to address practitioners and scholars separately. We examine the current state of SSI systems and explore potential systems and components. We additionally describe how our work extends current wallet definitions, which focus mainly on wallets for individuals. Finally, we present the limitations of this study.

Our first research question was *What potential requirements do organizations have for SSI software?* We have compiled the first comprehensive collection of requirements for SSI software for organizations, which can serve as a foundational guide for further development. We also investigated to what extent existing products match the identified requirements in response to our second research question, *What gaps exist between the identified requirements and current SSI solutions?* The presented data in Table 8 reveals numerous gaps, indicating that current systems remain in their early developmental stages.

TABLE 8. Requirement categories where the majority of products a) met the requirements, b) only partially met the requirements, c) did not meet the requirements, d) no product met any requirement.

	Prefix	Requirement Category
Group a	CS	Credential Schema Management
	CR	Credential Request and Offers
	IV-SR	Schema and Issuer Verification Constraint
	ST-LO	Storage Location
	RM	Relationship Management
	UP	User and Permission Management
	IF	Interfaces for Integration
	NO	Notification
	BP	Batch Processing
	AM	Automated and Manual Operations
Group b	IV-TR	Trusted Issuer/Verifier
	IV-CB	Credential Binding
	VR-RE	Revocation State
	VR-CT	Validity Constraints
	VR-PT	Permanent and Temporary Revocation
	ST-MW	Multiple Wallets
	OI	Organizational ID
	DA	Data Organization
Group c	IV-WC	Wallet Compliance for High-Value Credentials
	IV-CT	Terms of Use
	VR-CV	Complex Validation
	VR-HI	Revocation History and Reason
	BR	Backup and Recovery
	DE	Deletion
	SI	SSI as an IAM
	OU	Organizational Units
	CA	Compliance
	IN	Interoperability
Group d	IV-MI	Multiple Issuers
	ST-HC	Hot and Cold Storage
	TR	Transfer
	MD	Modification
	AR	Archiving
	DL	Delegation
	OC	Offline Capability

Security is excluded as no requirements were identified.

A. MANAGERIAL IMPLICATIONS

This section explores the implications of our research for practitioners who develop SSI solutions or plan to adopt an SSI solution. We assess the current state of the art and compare it to previous assessments. We further seek to propose ideas for implementing enterprise SSI systems, considering the identified requirements and gaps in current software solutions.

1) Current SSI Solutions: Gaps and Opportunities

Our findings align with the result of the 2021 update of the Wallet Report [9], which noted that SSI software development has been slow to date and that agents, in particular, continue to offer only basic features with limited specialization or advanced functionality. According to O'Donnell *et al.*, one reason for this is the excessive focus on technical aspects and early interoperability at the expense of business logic implementation [9], [50]. However, new specialized agents are emerging and becoming more mature. The analyzed product CARO by Spherity is a specialized SSI system for pharmacy supply chain compliance in the US. Esatus SOWL is mainly an SSI IAM software. The Business Partner Agent by Bosch focuses on managing the master data of suppliers and B2B customers.

Moreover, our requirements for SSI software for organizations can be seen as an extension of the requirements discovered in the Wallet Report [17], which focused on digital wallet requirements, mostly for individuals. In contrast to the Wallet Report, we offer a more comprehensive analysis by examining the systems for organizations that act as issuers, verifiers, and holders concurrently.

Although we identified multiple gaps, not all of them require immediate attention. For example, issues such as offline capability or modification are not required for every use case. Other requirements, such as those related to revocation, delegation, or organizational units, hold greater importance as they are relevant for various use cases where organizations may use SSI. It is important to consider the specific industry or use case when evaluating the priority of a particular requirement. With the upcoming eIDAS revision, there will likely be an alignment in the sector as certain features will be mandated by the regulation, while others will be optional.

Most systems offer revocation. However, current solutions often lack scalability or have privacy issues [69]. It remains to be seen how these issues can be solved. Other already established approaches, such as the widely used X.509 certificates for TLS/SSL, still struggle with revocation and have evident shortcomings [70], [71]. Often, the status of revocation of these certificates is not validated, even though it should be [71], [72]. This raises the question of whether the revocation challenge will be properly solved for VCs. An alternative to revocation would be credentials with a short validity period that must be constantly renewed, but this has its own drawbacks.

Another unresolved issue for organizational SSI software is verifiable organizational identity. Proving your identity as an organization requires a recognized digital organizational identity. This is especially challenging in cross-border interactions as it needs to be recognized across multiple countries. However, unlike private individuals who own passports, organizations have no equivalent. This makes it difficult for organizations to utilize SSI in the current state. However, this challenge also presents an opportunity for SSI to provide a potential solution for organizational identity.

One potential solution is the emerging vLEI for Legal Entities, a VC-based organizational ID [25]. It also provides a solution for delegation by chaining credentials to create a chain of authority. However, many products for vLEIs are still in development and new product releases are expected in the coming months. If the vLEI ecosystem lives up to its promise, it could prove to be the approach to organizational SSI.

Another potential solution for organizations in the European Union is to use their qualified electronic seal for VC signatures, which provides the advantage of a signature that is already legally valid [40], [73]. This enhances trust in credentials signed with an electronic seal, particularly in use cases that require a high level of assurance. Moreover, this strategy helps bridge the gap until a European Organizational ID becomes accessible.

2) Designing SSI systems

It is possible that meeting the identified requirements will require multiple SSI systems or components integrated into enterprise systems rather than a single SSI system. These systems include dedicated issuance, storage, and verification systems, which can also serve as standalone systems. While the term wallet for systems that store credentials is established, no terms exist for issuing or verification systems – except for the rather generic term agent. For instance, some organizations may solely focus on verifying credentials and do not issue or hold any VCs. A verification system (and possibly a wallet) suffices for such organizations and can be marketed at a lower cost than a complete SSI solution. Therefore, at least three distinct systems or components can be envisioned, as presented below, but they can also be consolidated into one system or integrated into existing enterprise systems.

1) **Issuing systems** are responsible for issuing credentials and do not necessarily need to store or verify credentials. For example, if credentials must be verified before issuance, this can be performed using a separate system.
2) **Wallets** are primarily used to securely store credentials. In the case of wallets for organizations, additional features such as user and permission management are particularly important.
3) **Verification systems** are primarily responsible for verifying the presented credentials.

Fig. 8 visualizes the interaction between these systems using the example of a manufacturing company that wants to receive its ISO 9001 certificate from a certification body after a successful audit. The certification body serves all three roles in this interaction, whereas the manufacturer does not have to act as an issuer and thus does not require an issuing system.

In practice, such separation is already visible in some cases. For example, esatus divides its SOWL SSI solution into four products: SOWL_ISSUE, SOWL_VERIFY, and their union SOWL_ACCESS. There is also a version called SOWL that can be self-hosted. Furthermore, the wallet is also a separate application [74].

There is also the question of how generic SSI systems should be. Should they implement business logic? Verifying

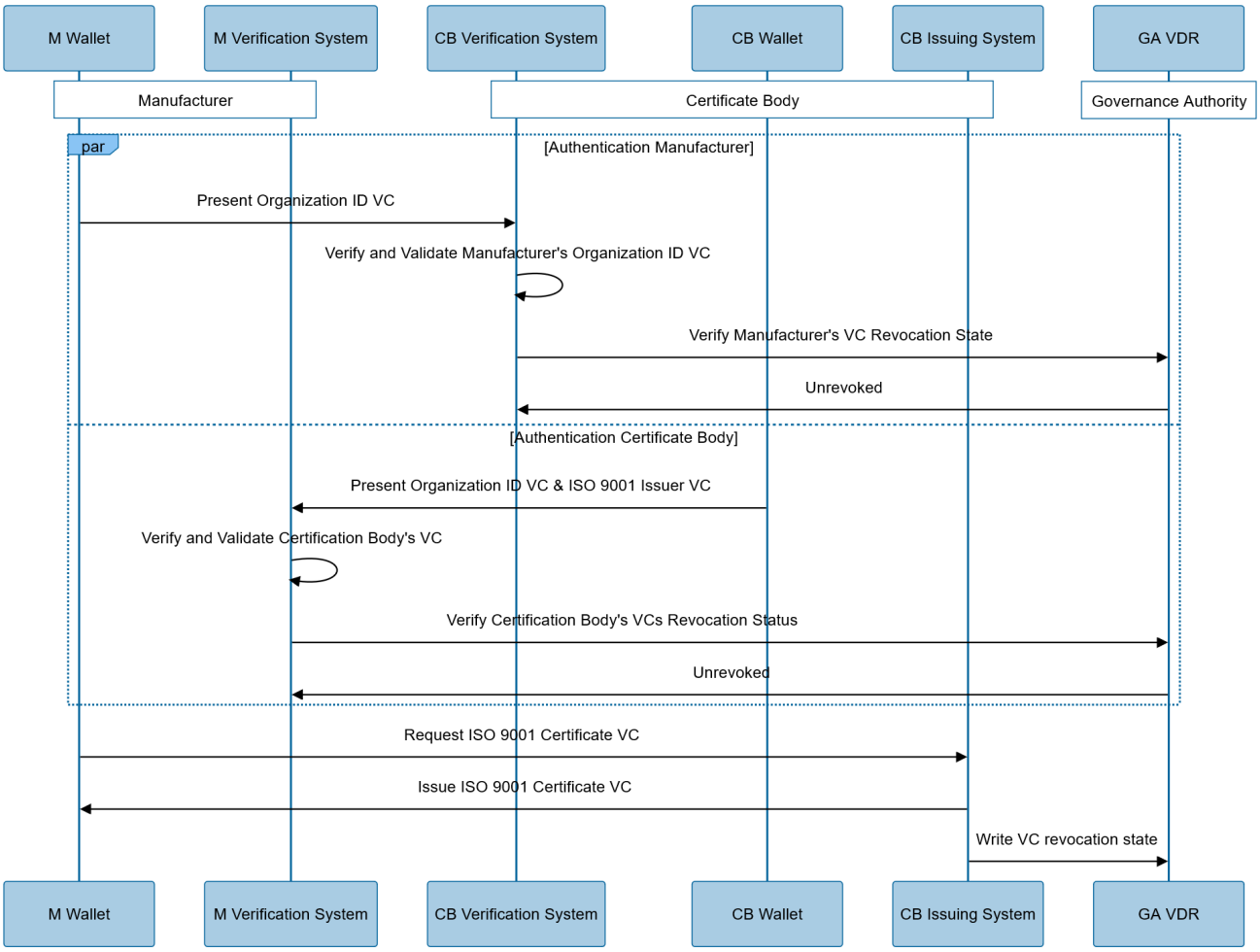

FIGURE 8. **Illustration of the interaction between the individual systems using the example of an ISO 9001 certificate issued after a successful audit. Note that in this use case, the certification body acts as issuer, holder, and verifier. For clarity, some interactions have been omitted.**

the issuer or the revocation status of a credential is a generic task. However, determining that a credential is valid for a certain use case can be quite complex. There may be already other systems in place that contain the business logic for the validation. Thus, it may be plausible that the SSI system only verifies the credential's authenticity and integrity and passes the claims inside the credential to other systems containing the business logic. This would allow SSI systems to focus on their task: managing credentials. However, there may be use cases where SSI systems only have to deal with certain credentials, e. g. supply chain credentials. In those cases, it may be advisable to develop SSI systems that are specialized and contain business logic.

Some requirements, such as multiple issuers or modification, may be solved using composite credentials, which act as a (virtual) container for related credentials. For example, in the vaccination passport example in the modification section, each vaccination would be a single credential, and the composite credential would be the whole vaccination passport. Thus, the vaccination credential itself does not need to be modifiable as the composite credential can be ''modified''. Another example would be a trade register credential and a bank account credential that could be part of an organizational ID composite credential. Grouping credentials into composite credentials makes the handling of related credentials easier. Instead of displaying each credential individually to the holder, they could be displayed as a single credential. This concept is similar to VPs that allow the combination of multiple VCs into a single proof. While combined VPs are for the verifier, composite credentials are for the holder. Composite credentials could be either created by the issuer or the holder. How composite credentials would be implemented is open to debate.

B. RESEARCH IMPLICATIONS

In the previous section, we mainly focused on the practical implications of the development of SSI software for organizations. In contrast, this section provides implications for the future research of these enterprise SSI systems. Since these SSI systems are largely unexplored in research, we present one of the first investigations in this area. However, recent studies focusing on SSI and organizations, like [16] and [64],

indicate that the interest in this area is increasing.

With our identified requirements, we show that the existing concepts of SSI wallets are insufficient for organizations. Individual and organizational wallets differ fundamentally. Although several requirements are similar, organizations have additional requirements – user and permission management, organizational units, and compliance – that are irrelevant to individuals' wallets. They are not merely an extension of wallets designed for individuals but a conceptually distinct category. We thus provide a comprehensive description of an organizational wallet and related SSI enterprise software, e. g., for issuance or verification. The requirements we identified and their structuration allow for a more detailed discussion of specific use cases and technology choices for SSI in organizations.

Furthermore, as discussed in VII-A2 it seems unlikely that a single system could meet all identified requirements. Rather, multiple systems or components are required depending on the organization's needs. Understanding the necessary systems, their components, and their real-world interactions is an area for future research. Additional research is needed to determine how SSI systems interact and integrate with existing enterprise systems.

C. LIMITATIONS

As we focussed on SSI software for organizations in general, we did not explore industry-specific requirements in depth, primarily due to their vast scope. However, identifying these requirements could extend the presented requirements, leading to a follow-up study. An example is the case study of the NHS digital staff passport [7], [8]. In this case study, SSI enabled health professionals to move swiftly between NHS hospitals. Specific requirements in this case included interfaces to the hospitals' different human resources systems and compliance with regulatory requirements of the British health care system. For instance, a rigorous identification process was implemented before issuing credentials, and mandatory attributes were incorporated into the credential.

Another limitation is that our research focused primarily on Europe. Region-specific regulations significantly influence the use of SSI software. For instance, European SSI solutions are subject to legislation such as the eIDAS and the GDPR. A global perspective would have considerably increased the complexity of identifying requirements, such as recruiting experts worldwide. Further research could explore additional regions and reveal their similarities and differences.

The SSI industry is rapidly evolving and becoming increasingly popular, resulting in the emergence of numerous vendors and products that create a fragmented landscape of SSI offerings. Furthermore, many products are frequently replaced in a short time frame. For instance, Trinsic v1 was introduced in 2020. In 2021, Trinsic Ecosystems, with new technological capabilities and features, was released and by 2022, it began replacing Trinsic v1. Additionally, many SSI vendors concentrate primarily on use cases for private individuals. SSI systems for organizations and concepts such as an organization ID credential are only recent developments. Consequently, selecting which systems to consider is challenging. Ultimately, we conducted an in-depth analysis of six products offered by established SSI vendors. While we believe these products provide a representative sample, examining a wider range of products may yield further insights.

VIII. CONCLUSION

Our objective was to address the following research questions:

1) What potential requirements do organizations have for SSI software?
2) What gaps exist between the identified requirements and current SSI solutions?

Regarding RQ1, we identified numerous requirements and provided the first comprehensive overview of requirements for SSI software tailored for organizational use. It is important to note that this compilation is by no means complete. Instead, it can serve as a starting point for future research. It is also important to consider the specific requirements regarding use cases, industries, and organizations that were not in the scope of our study. Furthermore, technological advancements, evolving standards, and new regulations will lead to new requirements or constraints. The evolving understanding of what defines SSI may also change and influence the requirements. An illustrative example lies in the early days of SSI, where it was often associated with blockchain technology [75]. This perspective has evolved, and several SSI approaches operate without a blockchain as there were criticisms of blockchain's scalability, inherent complexity, and regulatory challenges.

Concerning RQ2, we observed that SSI software for organizations and organizational IDs based on VCs are still in their early stages. The lack of development in some fundamental features is one of the reasons for this situation. For example, efficiently revoking, archiving, or transferring credentials between different wallets remains challenging. Despite numerous efforts, interoperability remains an issue. Additionally, critical functions for organizations, such as delegation and managing organizational units, are either rudimentary or absent.

By answering the proposed research questions, our research offers the following main contributions:

- Providing the first comprehensive overview of requirements for enterprise SSI software for organizations
- Highlighting gaps between identified requirements and current solutions
- Extending the current concept of an SSI wallet and related SSI enterprise software
- Demonstrating that the numerous requirements will likely not be fulfilled by a single system but rather by multiple interacting systems, depending on the organization's needs.

We further propose the following areas for potential future research:

- Examination of components and their interactions in real-world organizational implementations.
- Investigation of industry- and region-specific requirements.
- Further refinement of the individual components and their interactions to address common use cases.

When developing SSI systems, it is important to consider the requirements of organizations, not just end users. Organizations play a pivotal role in shaping SSI infrastructure, and the inherent potential of SSI and VCs for these entities is significant. However, current SSI products do not meet the needs of organizations completely. Thus, further research and development are necessary to address the identified requirements.

APPENDIX A
GUIDELINE EXPERT INTERVIEW

Below are the questions from the interview. Because the interviews were semi-structured, additional questions were asked in each interview, depending on the respondents' answers.

1) In which context did you first come into contact with SSI? / How long have you been working in the context of digital identities?
2) What differences do you see in the use of digital identities by private individuals and organizations?
3) What are your goals in using SSI (organizational wallets)?
4) What specific problems would you like to solve with the use of SSI (organizational wallets)?
5) Do you see further areas of use for SSI in organizations in the future?

APPENDIX B SELECTED ADDITIONAL QUESTIONS

We provide a few selected questions that were asked in the semi-structured interviews, which were not included in the interview guide.

Expert 1

- And is there a difference in the architecture [between organization and human wallet]?
- And how would your company earn money if it [the SSI product] were offered as open source?

Expert 2

- So would you say that within the context of the company, it is definitely important who the customers [B2C or B2B] are?
- And would you say that this [different customer types] also requires different basic wallets, or can you not make a statement here?

Expert 10

- You mentioned an authorization concept. Is that really the case for your solution?
- It is really the case that every person in the company who now has access to the wallet would create a user account?

ACKNOWLEDGMENT

We thank Justus Becker and Susanne Kreitschmann for their assistance in conducting the interviews.

REFERENCES

[1] O. Santolalla, D. Reed, and A. Tobin, "Unlocking Trust: Exploring vLEI & Self Sovereign Identity (SSI) with Drummond Reed & Andy Tobin, Gen," 2023, Accessed: Sep. 21, 2023. [Online]. Available: https://www.ubisecure.com/podcast/exploring-vlei-and-ssi-drummond-reed-andy-tobin

[2] A. Preukschat and D. Reed, *Self sovereign identity: Decentralized Digital Identity and Verifiable Credentials.* Shelter Island, NY, USA: Manning, 2021.

[3] v. Čucko and M. Turkanović, "Decentralized and Self-Sovereign Identity: Systematic Mapping Study," *IEEE Access*, vol. 9, pp. 139 009–139 027, 2021.

[4] F. Schardong and R. Custódio, "Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy," *Sensors (Basel, Switzerland)*, vol. 22, no. 15, 2022.

[5] G. Laatikainen, T. Kolehmainen, and P. Abrahamsson, "Self-Sovereign Identity Ecosystems: Benefits and Challenges," in *12th Scandinavian Conference on Information Systems*, IRIS. Association for Information Systems, 2021. [Online]. Available: https://aisel.aisnet.org/scis2021/10/

[6] D. Richter and J. Anke, "Exploring Potential Impacts of Self-Sovereign Identity on Smart Service Systems," in *24th International Conference on Business Information Systems*, 2021, pp. 105–116.

[7] M. Lacity and E. Carmel, "Implementing Self-Sovereign Identity (SSI) for a digital staff passport at UK NHS," White Paper, University of Arkansas, 2022.

[8] ——, "Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet," *MIS Quarterly Executive*, vol. 21, no. 3, pp. 241–251, 2022, Accessed: Mai. 10, 2023. [Online]. Available: https://aisel.aisnet.org/misqe/vol21/iss3/6

[9] D. O'Donnell and D. Reed, "Digital Wallet Report 2021 UPDATE," 2021. [Online]. Available: https://www.continuumloop.com/the-wallet-report-update/

[10] D. Richter, C. R. Praas, and J. Anke, "Beyond Paper and Plastic," in *ECIS 2023 Research Papers*. Association for Information Systems, 2023.

[11] M. Sporny, D. Longley, and D. W. Chadwick, "Verifiable Credentials Data Model v1.1," W3C, 2022, Accessed: Feb. 15., 2023. [Online]. Available: https://www.w3.org/TR/2022/REC-vc-data-model-20220303/

[12] T. O. I. Foundation, "Introduction to Trust Over IP," White Paper, Trust Over IP Foundation, 2021, Accessed: Jul. 19, 2023. [Online]. Available: https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf

[13] S. Ebert, A.-M. Krauß, and J. Anke, "Towards informed choices: A decision model for adaptive warnings in self-sovereign identity," Mensch und Computer 2023 - Workshopband, 2023.

[14] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, M. Sabadello, and J. Holt, "Decentralized Identifiers (DIDs) v1.0," W3C, 2020, Accessed: Aug. 5, 2023. [Online]. Available: https://www.w3.org/TR/did-core/

[15] O. Steele and M. Sporny, "DID Specification Registries – DID Methods," 2023, Accessed: Aug. 5, 2023. [Online]. Available: https://w3c.github.io/did-spec-registries/#did-methods

[16] J. Glöckler, J. Sedlmeir, M. Frank, and G. Fridgen, "A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity," *Business & Information Systems Engineering*, pp. 1–20, 2023, pII: 830. [Online]. Available: https://link.springer.com/article/10.1007/s12599-023-00830-x

[17] D. O'Donnell, "The Current and Future State of Digital Wallets," 2019. [Online]. Available: https://thewalletwars.s3.amazonaws.com/The-Current-and-Future-State-of-Digital-Wallets-v1.0-FINAL.pdf

[18] Z. E. Ansaroudi, R. Carbone, G. Sciarretta, and S. Ranise, "Control is Nothing Without Trust a First Look into Digital Identity Wallet Trends," in *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, Cham, 2023, pp. 113–132. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-37586-6_7#Sec4

[19] R. Sellung and M. Kubach, "Research on User Experience for Digital IdentityWallets: State-of-the-Art and Recommendations," in *Open Identity Summit 2023*. Bonn: Gesellschaft für Informatik e.V., 2023, pp. 39–50.

[20] S. Sartor, J. Sedlmeir, A. Rieger, and T. Roth, "Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets," in

30th European Conference on Information Systems - New Horizons in Digitally United Societies, ECIS 2022, Timisoara, Romania, June 18-24, 2022, R. Beck, D. Petcu, M. Fotache, S. Matook, R. Helms, M. Wiener, L. Rusu, and T. Tuunanen, Eds., 2022. [Online]. Available: https://aisel.aisnet.org/ecis2022_rp/46

[21] A.-M. Krauß, S. Kostic, and R. A. Sellung, "A more User-Friendly Digital Wallet? User Scenarios of a Future Wallet," in *Open Identity Summit 2023*. Bonn: Gesellschaft für Informatik e.V., 2023, pp. 73–84.

[22] M. Korir, S. Parkin, and P. Dunphy, "An Empirical Study of a Decentralized Identity Wallet: Usability, Security, and Perspectives on User Control," in *Eighteenth symposium on usable privacy and security (SOUPS 2022)*, 2022, pp. 195–211.

[23] R. Bochnia, D. Richter, and J. Anke, "Lifting the Veil of Credential Usage in Organizations: A Taxonomy," in *Open Identity Summit 2023*, H. Roßnagel, J. Günther, and C. H. Schunck, Eds. Bonn: Gesellschaft für Informatik e.V., 2023.

[24] EU Digital Identity Wallet Consortium, "EU Digital Identity Wallet Consortium," 2023, Accessed: Jul 26, 2023. [Online]. Available: https://eudiwalletconsortium.org/

[25] GLEIF, "Introducing the verifiable LEI (vLEI)," 2023, Accessed: Aug. 8, 2023. [Online]. Available: https://www.gleif.org/en/vlei/introducing-the-verifiable-lei-vlei

[26] C. Rupp and Sophisten, *Requirements-Engineering & -Management*. Hanser, 2014.

[27] G. Cohen, "Representing Multi Issuer Credentials in the VCDM · Issue #932 · w3c/vc-data-model · GitHub," 2023, Accessed: Mai 28, 2023. [Online]. Available: https://github.com/w3c/vc-data-model/issues/932

[28] B. Smith, O. G. Loddo, and G. Lorini, "On Credentials," *Journal of Social Ontology*, vol. 6, no. 1, pp. 47–67, 2020. [Online]. Available: https://www.degruyter.com/document/doi/10.1515/jso-2019-0034/html

[29] European Union, "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," 2014. [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32014R0910

[30] S. Schwalm, "Sustainability in EU Digital Identity -Long-Term preservation and evidence of (qualified) attestation of Attributes with and without DLT," Trusted Economy Forum, Warsaw, 2023, Accessed: Jun. 30, 2023. [Online]. Available: https://www.researchgate.net/publication/371178826_Sustainability_in_EU_Digital_Identity_-Long-Term_preservation_and_evidence_of_qualified_attestation_of_Attributes_with_and_without_DLT?channel=doi&linkId=64785385d702370600c5dbe1&showFulltext=true

[31] 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," 2014, Accessed: Sep. 25, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

[32] S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell, and D. Cooper, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 5280, May 2008, Accessed: Jun. 5, 2023. [Online]. Available: https://www.rfc-editor.org/info/rfc5280

[33] GLEIF, "verifiable LEI (vLEI) Ecosystem Governance Framework v1.0 Qualified vLEI Issuer Identifier and vLEI Credential Governance Framework," 2023, Accessed: Aug. 8, 2023. [Online]. Available: https://www.gleif.org/en/vlei/introducing-the-vlei-ecosystem-governance-framework

[34] Kusber, Tomasz and Schwalm, Steffen and Dr. Korte, Ulrike and Schamburger, Kalinda, "Records Management and Long-Term Preservation of Evidence in DLT," in *Open Identity Summit 2021*. Bonn: Gesellschaft für Informatik e.V., 2021, pp. 131–142.

[35] P. J. Windley, *Learning Digital Identity*. O'Reilly Media, Inc., 2023. [Online]. Available: https://learning.oreilly.com/library/view/learning-digital-identity/9781098117689/

[36] M. Kubach and R. Sellung, "On the Market for Self-Sovereign Identity: Structure and Stakeholders," in *Open Identity Summit*, A. Roßnagel, C. H. Schunck, and S. Mödersheim, Eds. Gesellschaft für Informatik, 2021, pp. 143–154.

[37] Microsoft, "Microsoft Entra Verified ID," 2023, Accessed: Sep. 10, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-verified-id

[38] M. Glaude and A. Kudra, "SSI for Identity & Access Management (IAM) with André Kudra [SSI Orbit Podcast]," 2021, Accessed: Aug. 11, 2023. [Online]. Available: https://northernblock.io/ssi-for-identity-access-management-iam/

[39] GLEIF, "verifiable LEI (vLEI) Ecosystem Governance Framework v1.0 Legal Entity Official Organizational Role vLEI Credential Framework," 2023, Accessed: Jul. 10, 2023. [Online]. Available: https://www.gleif.org/vlei/introducing-the-vlei-ecosystem-governance-framework/

[40] Š. Čučko, V. Keršič, and M. Turkanović, "Towards a Catalogue of Self-Sovereign Identity Design Patterns," *Applied Sciences*, vol. 13, no. 9, p. 5395, 2023, pII: app13095395. [Online]. Available: https://www.mdpi.com/2076-3417/13/9/5395

[41] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, and S. Guerreiro, "SSIBAC: Self-Sovereign Identity Based Access Control," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020, pp. 1935–1943.

[42] V. Lemieux, A. Voskobojnikov, and M. Kang, "Addressing Audit and Accountability Issues in Self-Sovereign Identity Blockchain Systems Using Archival Science Principles," in *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2021.

[43] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and cryptocurrency technologies*. Princeton University Press, 2016.

[44] Y. Ding and H. Sato, "Self-Sovereign Identity as a Service: Architecture in Practice," in *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2022, pp. 1536–1543.

[45] Postman, "2023 State of the API Report | API Technologies," 2023. [Online]. Available: https://www.postman.com/state-of-api/api-technologies/#api-technologies

[46] DIDComm User Group, "DIDComm V2 Guidebook," 2023, Accessed: Oct. 9, 2023. [Online]. Available: https://didcomm.org/book/v2/

[47] Hyperledger, "Aries Interoperability Test Results · A summary of the Hyperledger Aries Interoperability Profile (AIP) Tes," 2023, Accessed: Aug. 3, 2023. [Online]. Available: https://aries-interop.info/

[48] M. Sporny, "[PROPOSED WORK ITEM] W3C VCDM Confidence Method Extension · Issue #245 · w3c-ccg/community," 2023, Accessed: Aug. 3, 2023. [Online]. Available: https://github.com/w3c-ccg/community/issues/241

[49] H. Yildiz, A. Küpper, D. Thatmann, S. Göndör, and P. Herbke, "Toward Interoperable Self-sovereign Identities," *IEEE Access*, pp. 114 080 – 114 116, 2023.

[50] D. O'Donnell, "Premature Standardization & Interoperability," 2022, Accessed: Feb. 27, 2023. [Online]. Available: https://www.continuumloop.com/premature-standardization-interoperability/

[51] D. Pöhn, M. Grabatin, and W. Hommel, "Modeling the Threats to Self-Sovereign Identities," in *Open Identity Summit 2023*. Bonn: Gesellschaft für Informatik e.V., 2023, pp. 85–96.

[52] K. Yasuda, T. Lodderstedt, D. Chadwick, K. Nakamura, and J. Vercammen, "OpenID for Verifiable Credentials," 2022, Accessed: Dec. 5, 2022. [Online]. Available: https://openid.net/wordpress-content/uploads/2022/06/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials-V2_2022-06-23.pdf

[53] A. Grüner, A. Mühle, and C. Meinel, "Analyzing Interoperability and Portability Concepts for Self-Sovereign Identity," in *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2021, pp. 587–597.

[54] European Commission, "European Digital Identity Wallet Pilot implementation," 2023, Accessed: Jul. 17, 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation

[55] ——, "Final agreement on EU Digital Identity Wallet," 2023, Accessed: Nov. 17, 2023. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651

[56] "Joint statement of scientists and NGOs on the EU's proposed eIDAS reform," 2023, Accessed: Nov. 30, 2023. [Online]. Available: https://eidas-open-letter.org/

[57] European Commission, "EU digital ID scheme for online transactions across Europe," 2020, Accessed: Aug. 11, 2023. [Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-EU-digital-ID-scheme-for-online-transactions-across-Europe/F_en

[58] European Parliamentary Research Service, "Revision of the eIDAS Regulation," 2022, Accessed: Jul. 19, 2023. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/\699491/EPRS_BRI(2022)699491_EN.pdf

[59] G. Kondova and J. Erbguth, "Self-sovereign identity on public blockchains and the GDPR," in *The 35th Annual ACM Symposium on Applied Comput-*

ing, C.-C. Hung, T. Cerny, D. Shin, and A. Bechini, Eds. Association for Computing Machinery, 2020, pp. 342–345.

[60] W3C, "Director's Decision on DID 1.0 Proposed Recommendation Formal Objections," 2022, Accessed: Feb 28, 2023. [Online]. Available: https://www.w3.org/2022/06/DIDRecommendationDecision.html

[61] O. Steele and M. Sporny, "DID Specification Registries," 2023, Accessed: Jul 19, 2023. [Online]. Available: https://www.w3.org/TR/did-spec-registries/#did-methods

[62] M. Sporny, D. Longley, and D. W. Chadwick, "Verifiable Credentials Data Model v2.0," 2023, Accessed: Jul 19, 2023. [Online]. Available: https://w3c.github.io/vc-data-model/

[63] Pasalic, S, "Successfully launching a Blockchain SSI application for career credentials," Master's thesis, Eindhoven University of Technology, Eindhoven, Netherlands, 2020.

[64] T. Kölbel, M.-C. Härdtner, and C. Weinhardt, "Enterprise Business Models Leveraging Self-Sovereign Identity: Towards a User-Empowering Me2X Economy," in *Proceedings of the 56th Annual Hawaii International Conference on System Sciences : January 3-6, 2023*, 2023, p. 4006. [Online]. Available: https://publikationen.bibliothek.kit.edu/1000157627

[65] M. Kubach and H. Roßnagel, "Auf der Suche nach ökonomisch tragfähigen Identitäts-Ökosystemen: Gibt es einen Markt für digitale IDs? [In Search of Economically Viable Identity Ecosystems: Is there a market for digital IDs?]," *HMD Praxis der Wirtschaftsinformatik*, vol. 60, no. 2, pp. 422–436, 2023, pII: 948. [Online]. Available: https://link.springer.com/article/10.1365/s40702-023-00948-2

[66] S. Schwalm, D. Albrecht, and I. Alamillo, "eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI," in *Open Identity Summit 2022*. Bonn: Gesellschaft für Informatik e.V., 2022, pp. 63–74.

[67] S. Schwalm, "The possible impacts of the eIDAS 2.0 digital identity approach in Germany and Europe," in *Open Identity Summit 2023*. Bonn: Gesellschaft für Informatik e.V., 2023, pp. 109–120.

[68] T. Kusber, S. Schwalm, K. Shamburger, and U. Korte, "Criteria for trustworthy digital transactions - Blockchain/DLT between eI-DAS, GDPR, Data and Evidence Preservation," in *Open Identity Summit 2020*. Bonn: Gesellschaft für Informatik e.V., 2020, pp. 49–60.

[69] Andreas Freitag, "A new Privacy Preserving and Scalable Revocation Method for Self Sovereign Identity - The Perfect Revocation Method does not exist yet," *Cryptology ePrint Archive*, 2022. [Online]. Available: https://eprint.iacr.org/2022/1658

[70] N. Korzhitskii and N. Carlsson, "Revocation Statuses on the Internet," *CoRR*, vol. abs/2102.04288, 2021. [Online]. Available: https://arxiv.org/abs/2102.04288

[71] T. Smith, L. Dickinson, and K. Seamons, "Let's Revoke: Scalable Global Certificate Revocation," in *Network and Distributed System Security Symposium 2020*, D. Xu and A.-R. Sadeghi, Eds., Internet Society. Curran Associates Inc, 2020.

[72] D. G. Berbecaru and A. Lioy, "An Evaluation of X.509 Certificate Revocation and Related Privacy Issues in the Web PKI Ecosystem," *IEEE Access*, vol. 11, pp. 79 156–79 175, 2023.

[73] X. Vila, "SSI eIDAS Bridge (SEB) Project Summary," 2023, Accessed: Mai 16, 2023. [Online]. Available: https://gitlab.grnet.gr/essif-lab/infrastructure/validated-id/seb_project_summary

[74] esatus AG, "SOWL Products," 2023, Accessed: Aug. 2, 2023. [Online]. Available: https://esatus.com/index.html%3Fp=8009&lang=en.html

[75] J. Sedlmeir, T. Barbereau, J. Huber, L. Weigl, and T. Roth, "Transition Pathways towards Design Principles of Self-Sovereign Identity," *ICIS 2022 Proceedings*, no. 4, 2022.

RICARDO BOCHNIA holds a Master's degree in Applied Informatics from the Faculty of Informatics and Mathematics at HTW Dresden University of Applied Sciences. As a research associate in the Digital Service Systems Group at the same institution, he is currently involved in the ID-Ideal project, which is funded by the German Federal Ministry for Economic Affairs and Climate Action. His primary research focus encompasses decentralized and self-sovereign identities, with a specialized interest in their application within both public and private organizations

DANIEL RICHTER holds a Master's degree in Applied Informatics from the Faculty of Informatics and Mathematics at HTW Dresden University of Applied Sciences. As a research associate in the Digital Service Systems Group at the same institution, he is currently involved in the ID-Ideal project, which is funded by the German Federal Ministry for Economic Affairs and Climate Action. His current research interests include the design and use of digital credentials in service ecosystems at the interface between technology, trust, and governance.

JÜRGEN ANKE holds a computer science doctorate from TU Dresden and a post-doctoral degree in information systems from Leipzig University. He is currently a professor of software engineering and information systems at HTW Dresden University of Applied Sciences, where he also leads the Digital Service Systems group. His research interests are digital service ecosystems, particularly processes, methods, and models for service innovation and design. A key aspect is the application of digital identities and verifiable credentials as a foundation for trustworthy digital interactions in these ecosystems.