Analyzing Interoperability and Portability Concepts for Self-Sovereign Identity

Andreas Grüner, Alexander Mühle, Christoph Meinel
Hasso Plattner Institute (HPI)
University of Potsdam, 14482, Potsdam, Germany
Email: {andreas.gruener, alexander.muehle, christoph.meinel}@hpi.uni-potsdam.de

***Abstract*—The Self-Sovereign Identity (SSI) paradigm postulates global unique identities that are controlled by the user. To achieve a widespread applicability, the emphasized interoperability principle supports the proclaimed ambition. Furthermore, identity portability enables the transfer of the identity to another SSI solution. These axioms gain additional momentum due to the development of numerous implementations. In this paper, we examine interoperability and portability concepts for SSI. Initially, we define these principles regarding the blockchain-based SSI model. Subsequently, we outline assessment criteria considering functional scope, governance/ trust, scalability and further characteristics. For interoperability, we evaluate the concepts of protocol and standard, broker, hub and pairing. Besides that, we assess the transformer and auxiliary solutions for portability. We can conclude that all interoperability schemes provide the maximum functional level theoretically. In contrast, portability patterns are fragmented in this regard. Nonetheless, protocol and standards can only be applied in the design phase, whereas broker, hub, pairing, transformer and auxiliary solutions enable interoperability, respectively portability post-deployment of the SSI system.**

***Index Terms*—Blockchain, distributed ledger technology, digital identity, self-sovereign identity, trust, identity management, interoperability, portability**

I. Introduction

Identity management is a core function for an application's security. Thereby, Identity Management Systems (IdMS) recognize users and restrict access to authorized entities. Over time, a shift of the Identity Provider's (IdP) position has lead to the formation of distinct paradigms [1]. Service-specific IdPs exist in the isolated setting. Advancing to the centralized model, the IdP gained a primary position by serving several applications. Furthermore, identity federations establish a Circle of Trust [2] between several IdPs and Service Providers (SP). Within this development, the IdP emerged as an independent Trusted Third Party (TTP) [3], and interoperability became a major concern. At the same time, the user's position degraded continually weaker. In these models, the IdP has absolute power over the user's identity and can completely deny service.

Allen [4] proposed the Self-Sovereign Identity (SSI) paradigm to bring the user back in control of its digital self to rebalance this situation. A definition does not serve as the foundation of the SSI concept. On the contrary, Allen coined the model by providing essential principles. These principles comprise portability and interoperability. Nonetheless, the latter has concerned the Identity Management (IdM) domain ever since. In 2008, Mahler and Reed [5] considered compatible communication as a significant challenge for identity federations. Additionally, in 2009, Cameron [6] emphasized the need for *"inter-working"* IdMS in his laws of identity. Besides that, portability links closely to interoperability. Where interoperability ends between systems, data transfer to another IdP begins. However, moving an identity among IdPs is widely unknown in contrast to interoperating IdPs. Besides that, GDPR [7] grants a citizen's right to data portability and underpins this principle.

Various groups developed a myriad of SSI IdMS based on blockchain technology [8]. At the same time, each solution aspires to provide a global identity that can be used everywhere. Nonetheless, the user and the SP would need to decide on a specific SSI IdMS. Suppose that a user registers at many platforms, then disadvantages comparable to the isolated model emerge. Regarding the SP, an integration to a large number of IdPs bears enormous effort. Hence, we consider interoperability as a fundamental characteristic to achieve a single global identity. Furthermore, portability enables the user to move to a different SSI IdMS if required.

In this paper, we explore concepts for interoperability and portability for blockchain-based SSI IdMS. Starting this analysis, we formalize these two principles. As a next step, we discuss the assessment criteria encompassing functional levels, governance/ trust, scalability and further considerations. The main sections present various concepts, including their evaluation. For interoperability, we devise the concepts of protocol and standard, identity broker, hub and pairing. In addition to the first scheme, we delineate the transformer and auxiliary paradigms for portability. In particular, we contribute the following:

1) Definition of interoperability/ portability for SSI IdMS
2) Description and comparative evaluation of the schemes

To the best of our knowledge, this paper is the first to evaluate SSI interoperability and portability concepts.

The remainder of the paper is organized as follows. In Section II, we describe the background on SSI, interoperability and portability. We review related work in Section III. In Section IV, we outline motivating scenarios. Furthermore, we describe and examine various interoperability and portability concepts for SSI according to criteria in Section V, respectively in Section VI. Finally, we conclude in Section VII.

978-1-7281-2522-0/19/$31.00 ©2021 IEEE

II. Background

In this section, we briefly present background on blockchain-based SSI (II-A) and general interoperability (II-B) and portability (II-C) notions.

A. Blockchain-based Self-Sovereign Identity

A blockchain consists of a consecutively growing chain of blocks [9]. Each block includes transactions and a cryptographic hash of the predecessor as an unforgeable link. A peer-to-peer network agrees on the next block by applying a consensus algorithm. First, Bitcoin's [10] transaction encompasses token transfers. Subsequently, Ethereum [11] established the blockchain as a decentralized execution platform comprising smart contracts. Thus, the blockchain cannot just dissolve a financial institution but any TTP.

The traditional actors in IdM comprise the IdP, SP and the user [12]. The IdP is a TTP that offers IdM functions. These capabilities comprise, for instance, credential management, authentication and attribute management. An Attribute Provider (AP) solely delivers properties. Upon authentication at the SP, the user gets redirected to the IdP. Following this step, the user proves ownership of an identity with a secret. In case of success, the IdP redirects the user to the SP and conveys its attributes. The properties have been verified during the enrolment process at the IdP.

Definition 1 (**SSI IdMS**). *A SSI IdMS $\mathcal{A}$ is a 3-tuple $\langle \Lambda, \Omega, \Xi \rangle_{\mathcal{A}}$.*

- *Λ represents the User Agent (UserA).*
- *Ω reflects the Organizational Agent (OrgA).*
- *Ξ is the Blockchain Network (BN).*

To realize the SSI paradigm, one implements a decentralized IdP on a blockchain. We call such a decentralized IdP the BN Ξ. The BN Ξ provides authentication and credential management through a self-authenticating scheme [13], e.g. private/ public-key cryptography. The BN Ξ implements an identifier or a claim registry [13]. The identifier registry ensures the uniqueness of the designator. Additionally, the claim registry offers a timestamped proof of existence and revocation of verifiable claims. A verifiable claim is an attribute with issuer proof. We refer to such an attribute solely as a claim.

Fig. 1 outlines actors, SSI IdMS components and their interaction paths. The issuer (the AP) delivers or revokes a claim for an identity. Correspondingly, the identity owner (the user) receives the claim. Upon authentication, the user presents its claims to a verifier (the SP). The verifier checks the integrity and validity of the claim. Entities interact with the BN Ξ by an agent. We distinguish the UserA Λ and the OrgA Ω. The OrgA Ω combines functions for issuer and verifier. In contrast, the functions of the UserA Λ differs significantly.

Definition 2 (**Self-Sovereign Identity (Object)**). *A self-sovereign identity $a \in \mathcal{A}$ is a $(n+1)$-tuple $\langle i, c_1, \ldots, c_n \rangle$ that is rooted on $\Xi_{\mathcal{A}}$ of SSI IdMS $\mathcal{A}$.*

- *i is the identifier.*
- *$c_1, \ldots, c_n$ depict verifiable claims of the identity.*

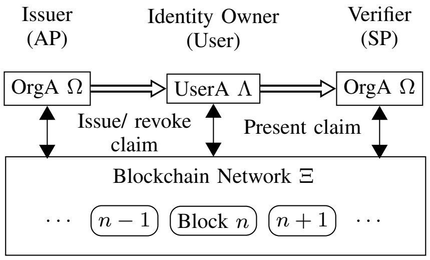

Fig. 1: SSI IdMS components and interaction

In our analysis, we take the presented SSI IdMS model, including the claim registry, as the basis. We refer with SSI, omitting the phrase blockchain, to the paradigm. Furthermore, we differentiate SSI IdMS by capital calligraphic letters and use small letters for identities. Moreover, we define a regular user to SP interaction within one SSI IdMS as the following.

Definition 3 (**Regular SSI IdMS Interaction**). *A user with $a_{User} \in \mathcal{A}$ and a SP with $a_{SP} \in \mathcal{A}$ can regularly interact with the UserA $\Lambda_{\mathcal{A}}$ and OrgA $\Omega_{\mathcal{A}}$.*

B. Interoperability

NIST [14] defines interoperability between two parties as the proficiency to communicate. Originating from the notation, researchers define models comprising different layers of interoperability [15]. These dimensions range from technical, semantic or syntactical aspects to organizational exchange. Besides that, Koussouris et al. [16] name IdM as one of the primary domain for interoperability research with the objective of cross-trust boundary authentication and authorization. Thus, one interprets IdMS interoperability as interchangeability of IdPs at SPs. In particular, Leitold and Zwattendorfer [17] elaborate on the use of electronic identification documents across nations. Besides that, Backouse and Halperin [18] apply the technical, formal and informal cluster model to IdM. The formal layer refers to laws and regulations. The informal domain references culture and habits. In this paper, we focus on technical interoperability concepts for SSI IdMS.

C. Portability

The term portability relates mainly to code execution [19] and data in the cloud domain [20]. Engineers write software that can be executed on various platforms. Thus, the software is portable. Additionally, portability addresses lock-in challenges in cloud computing. Regarding IdM, in our understanding, research neglects the term portability to a certain extent. Authors define data formats to exchange private keys [21] or certificates [22]. Despite that, there is a lack of research concerning the portability of identifiers or attributes among different IdPs. This is no surprise as an IdP runs attribute verification procedures and may not provide properties that have been verified by another IdP. Nonetheless, SSI decouples the identifier on the BN Ξ from issued attributes [3]. Therefore, in this paper, we concentrate on portability schemes that arise with SSI IdMS.

III. Related Work

Related research work addresses interoperability challenges in IdM or between blockchains. In the IdM domain, Backhouse [18] formalizes the layers for interoperability and mentions protocols and standards as a technical approach. Additionally, the development of specific protocols, e.g. SAML2 [23] or OpenID Connect (OIDC) [24] directly achieve interoperable communication. In the realm of blockchain, Koens and Poll [25] evaluate blockchain interoperability concepts that include notary and relay schemes and hash-locking. The authors apply several criteria encompassing scalability, scope, regulation and functional scope. Kannengießer et al. [26] survey cross-blockchain technology implementations according to performance, security, networking, flexibility and administration. The authors consider manual asset exchange, notary and relay schemes, and hybrid solutions. Overall, previous research examines traditional IdM or blockchain interoperability, whereas the latter concentrates mainly on token swaps. In contrast, we focus on the interoperability and portability of SSI IdMS and their IdM capabilities.

IV. Motivating Scenarios

Interoperability and portability belong to the SSI core principles. Apart from a proposition, we describe motivating scenarios to underline advantages for the user and the SP.

A. Select Preferred User Agent

SSI changes IdMS significantly for the user. For instance, the user is acquainted to authenticate with a username and password. In contrast, an SSI solution changes the authentication method to private/ public-key cryptography. Thus, the user must keep the private key secure and recoverable. For this purpose, an SSI IdMS offers a UserA Λ. Additionally, the UserA Λ manages claims and the processes for issuance at an AP and disclosure at a SP. A user chooses to register at SSI IdMS $\mathcal{A}$ with associated UserA $\Lambda_{\mathcal{A}}$ based on its superior usability. For a period of time, the user can perfectly authenticate at SPs that also uses SSI IdMS $\mathcal{A}$. After this, UserA $\Lambda_{\mathcal{A}}$ may not be developed further. The user changes to UserA $\Lambda_{\mathcal{B}}$. With the UserA $\Lambda_{\mathcal{B}}$, the user can still authenticate at the same SPs having the same identity.

B. Integrate only Once

An SP requires an IdMS for service provisioning. The IdP of the IdMS authenticates the user and provide attribute information to the SP. As the users prefer different IdPs, the SP is in an integration dilemma. The SP strives to serve as many users as possible by integrating as few as possible IdPs. We formulate the IdM SP dilemma using an ideal situation.

Definition 4 (IdM SP Dilemma). *An SP seeks to serve all users by integrating to one IdP.*

Concerning SSI IdMS, the SP selects IdMS $\mathcal{A}$. Users choose the different IdMS $\mathcal{B}$ and $\mathcal{C}$. Despite the different preferences, all users can authenticate with their UserAs $\Lambda_{\mathcal{B}}$ and $\Lambda_{\mathcal{C}}$ at the SP without challenges although, the SP integrates with SSI IdMS $\mathcal{A}$ using OrgA $\Omega_{\mathcal{A}}$.

C. Facilitate SSI Growth

Each SSI IdMS comprises a BN Ξ. A peer-to-peer community runs the BN Ξ either in the permissioned or unpermissioned mode. These two coarse-grained categories already represent distinct governance models. However, both approaches can be further detailed based on the applied consensus algorithm. In particular, the acceptance of node composition and the voting scheme in the permissioned case can vary. Based on this, it is unlikely that a single BN Ξ serves a global identity for all users across nations. Community-specific BNs Ξ seem to grow to support their governance peculiarities. The Verifiable Organization Network (VON) [27] in Canada and IDunion [28] in Germany reflect this development. Interconnecting these BNs Ξ facilitates the global applicability of the identity but also fosters the local growth of the SSI IdMS. A user enrolled at SSI IdMS $\mathcal{A}$ can seamlessly authenticate at the SP that is integrated into SSI IdMS $\mathcal{B}$.

V. Interoperability

In this section, we start with the definition of SSI IdMS interoperability (V-A) and describe evaluation criteria (V-B). Ensuing, we present various interoperability concepts (V-C to V-G) and examine them based on the defined characteristics. Additionally, we name sample implementations in the SSI or blockchain context if existent and relate to solutions from the traditional IdM models if possible. Furthermore, we outline implementation variants (V-H) and compare the assessment results (V-I and V-J). Table I presents an overview of the assessed schemes, and Table II depicts examples for each concept.

A. Objective

Allen [4] describes interoperability as the universal applicability of an identity. We assume that several SSI IdMS exist and define SSI IdMS interoperability as the following.

Definition 5 (SSI IdMS Interoperability). *SSI IdMS $\mathcal{A}$ and $\mathcal{B}$ are interoperable if an entity with $a \in \mathcal{A}$ and UserA $\Lambda_{\mathcal{A}}$ can interact with another entity $b \in \mathcal{B}$ and OrgA $\Omega_{\mathcal{B}}$.*

Despite naming two distinct entities, the definition refers to the user and the SP. Each actor uses an identity that is rooted on different SSI IdMS. Furthermore, both entities apply separately the UserA Λ and OrgA Ω.

Fig. 2 depicts graphically the interoperability scenario between two entities. A user registers at SSI IdMS $\mathcal{A}$. In contrast, the SP integrates with SSI IdMS $\mathcal{B}$. Considering the interoperability notation (cf. II-B), the user should be able to interact with UserA $\Lambda_{\mathcal{A}}$ at the SP with $\Omega_{\mathcal{B}}$.

The primary interaction path with the BN Ξ is indicated by a solid arrow. It connects the entity with the BN Ξ where the identity is rooted. The dashed arrows reflect potential interoperability channels that are established by the different concepts. Furthermore, the dashed circles refer to the schemes and their adjacent position in the scenario.

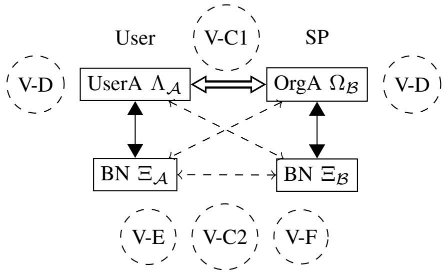

Fig. 2: Schematic interoperability scenario

B. Evaluation Criteria

In this section, we describe the evaluation criteria for assessing the interoperability concepts.

1) Level of Interoperability: The Level of Interoperability (LoI) reflects the functional scope of the concept. Fig. 3 presents the various grades starting with *no interoperability*. In ascending order, the levels provide a wider functional scope. A higher level requires the tier below. At the lowest grade (*no interoperability*), the user and the SP must enroll/ integrate with all SSI IdMS that should be supported. There is no interoperability between the SSI IdMS. The tier *redirection* refers to a sole referral to the required SSI IdMS for login. The next level expresses an interoperable *identity assertion*. The user can prove to be in control of a specific identifier. Building on that, the SP can retrieve interoperable asserted attributes (*attribute assertion*) or issue claims (*claim issuance*). Furthermore, the highest functional grade is *authorization*. At this level, authorization decisions are conveyed in an interoperable manner.

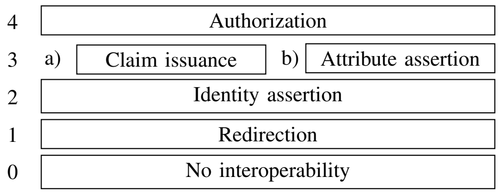

Fig. 3: Level of Interoperability

During evaluation, we determine a theoretic maximum level for the concept and a practically implemented grade for the mentioned examples in the SSI and traditional IdM space.

2) TTP Dependency: The TTP Dependency criterion determines if the concept establishes a new TTP in addition to the user and SP. A TTP centralizes trust and counteracts control, protection and data minimization principles.

3) Scalability: The characteristic scalability refers to the number of entities that must implement the interoperability concept. The effort increases for general interoperability among all SSI IdMS for a higher quantity of entities. We distinguish the scalability as a constant factor, per *user*, *SP*, *BN* Ξ or combinations thereof. The number of users significantly outweighs the volume of SPs. Furthermore, the quantity of SPs is substantially higher compared to the number of SSI IdMS that is reflected by the *BN* Ξ category.

4) Token Cost: The token cost peculiarity describes auxiliary token expenses that are imposed by using the interoperability concept. A concept may not impose additional cost and is, therefore, cost-neutral. In contrast, the scheme can lead to extra required tokens for interoperability.

5) Governance Consistency: A BN Ξ has a specific governance model (cf. IV-C). The model ensures security and trust in the BN Ξ by the participants of the consensus algorithm. If a SP interacts with a user via the SSI IdMS, the SP trusts the governance model of the BN Ξ. Suppose that the scheme provides data from another governance model covertly, this would violate the consistency constrain.

6) Preconditions for Use: The Preconditions for Use (PfU) characteristic delineates the requirements before the user or SP can apply an implemented interoperability concept for a newly emerging SSI IdMS. We differentiate *configuration*, *connector* or *full implementation*. The *Configuration* also encompasses dynamic interactions and the creation of a new identity on the SSI IdMS. In contrast, the *connector* level refers to a lightweight wrapper for an existing solution to integrate a new entity. Finally, the *full implementation* grade reflects a complete new setup of the interoperability scheme.

7) Phase of Consideration: The Phase of Consideration (PoC) differentiates the software development period of integrating the scheme into the SSI IdMS without fundamental adjustments of the system. We distinguish the *design* and the *post-production* phase. Therefore, the first value indicates an integration during the design of the SSI IdMS. In contrast, *post-production* characterizes the applicability after the regular activation.

8) Location: The location differentiates the position where the concept achieves interoperability. We distinguish the side of the *user*, the *SP* and the *BN* Ξ. Additionally, we use the term *independent* to refer to a distinct entity.

C. Protocol and Standard

A protocol [29] specifies agreements for the communication flow and data exchange between several parties. Besides that, a standard [30] delineates data structures that can be processed by different entities. Thus, SSI IdMS owners may collaborate in a community to develop a common set of rules for SSI IdMS interoperability. Subsequently, the agreed directions must be incorporated into the SSI IdMS.

The protocol and standard concept provides the maximum LoI and can theoretically support up to the tier of authorization. The actual level depends on the respective design. Additionally, this scheme does not establish a new TTP because the defined rules are incorporated in the existing SSI IdMS. Therefore, the user and SP apply the adjusted agents. Analyzing the token cost, protocols and standards do not create additional token transfers on a blockchain. In contrast, the scheme modifies the working of the SSI IdMS and adjusts its implementation[1]. Thus, this concept must be already defined

[1] We assume a cost-neutral implementation of the BN Ξ as most likely option. Imposing cost to an entity is an unnecessary drawback. Besides that, we discuss implementation variants in V-H

during the design phase of the SSI IdMS. Otherwise, major rework may occur. Before interacting with a new SSI IdMS, the SP and the user must execute a (dynamic) configuration. For instance, the agent owner defines communication endpoints. Besides the general view, we dissect the classes IdP interaction and IdP routing.

1) IdP Interaction: The IdP interaction category enables the user and SP to communicate directly with the IdP. Specifically, the UserA Λ of an SSI IdMS can interact with the OrgA Ω of another SSI IdMS. Concerning the scalability criterion, the implementation affects the side of the user and SP via their agent and the BN Ξ. Using this scheme, the governance consistency characteristic holds true because the user and the SP are aware of the specific BN Ξ interaction. Furthermore, the location of the interoperability is at the side of the user, the SP and the BN Ξ.

In SSI, the DIDAuth [31] protocol and the DID [32] standard are examples. DIDAuth is an authentication protocol. DID defines a schema for identifiers of an identity. Within the traditional IdM models, OIDC [24]/ OAuth2 [33] and SAML2 [23] belong to the IdP Interaction class. These representatives enable authorization decisions.

2) IdP Routing: Members of the IdP routing class refer to communication among distinct BN Ξ. The user and the SP integrate with different SSI IdMS. Upon interaction, the BN Ξ of the SP forwards the request to the user's BN Ξ and receives a result. The process is seamless to the user and the SP. Concerning scalability, this concept must be supported by the BNs Ξ. Besides that, the governance is inconsistent as data is transparently routed through BNs Ξ. Furthermore, the interoperability location is also at the BN Ξ.

The Interledger Protocol (ILP) [34] is an example in the common blockchain context. ILP enables token exchanges between blockchains. In the traditional IdM domain, EduROAM [35] using the RADIUS [36] protocol allows students to authenticate at foreign universities with credentials that are issued by their home institutions. The universities' IdPs communicate transparently for the students.

D. Identity Broker

The identity broker mediates the communication towards different SSI IdMS. The broker abstracts from the peculiarities of a single solution to a general Application Programming Interface (API) or protocol. For instance, applications of the SP do not need to adapt to a specific OrgA Ω. Additionally, the broker implements drivers to connect to a dedicated SSI IdMS.

The LoI of the identity broker concept offers the maximum level of authorization towards the selected SSI IdMS. Thus, upon interaction, the communication partner decides for a SSI IdMS and the broker redirects to the chosen implementation. Subsequently, one can start processes up to authorization if the SSI IdMS supports the corresponding tier. The user or SP can apply the broker scheme. Therefore, the concept does not establish an additional TTP. Considering cost, this scheme does not impose additional token expenses as the broker runs as an application apart from the BN Ξ. Furthermore, the scheme adheres to the governance consistency property as the broker integrates with the SSI IdMS directly. To integrate a new SSI IdMS, the identity broker requires an additional connector. Furthermore, the hosting entity must register an identity on the respective BN Ξ. Despite that, the concept enables an integration of a new SSI IdMS after its general activation. In this category, we differentiate the user-side and SP-side identity broker depending on the location. Therefore, the broker scales with either the quantity of the users or SPs.

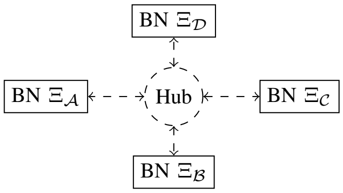

Fig. 4: Hub scheme

In the SSI paradigm, the Universal Resolver (UR) [37] and Grüner et al.'s [38] integration architecture are examples for the SP-side identity broker. The UR resolves a DID into a DID document that comprises communication endpoints. The SSI IdMS-specific interaction process starts subsequently, independent of the UR. Grüner et al.'s solution supports in an integrated manner up to LoI attribute assertion and claim issuance after selecting the required SSI IdMS.

Trusted Attribute Aggregation Service (TAAS) [39] represents a user-side identity broker in the traditional IdM domain. The TAAS can forward a combination of attributes from different APs to an SP. Regarding the general blockchain context, MetaMask[2] implements a user wallet to manage different tokens.

E. Hub

The implementation of a hub relies on the hub and spoke pattern. The pivotal hub manages as a central entity the communication between different BNs Ξ. Comparable to computer networks, the hub mediates the communication between a large number of BNs Ξ. For each supported SSI IdMS a specific connector is used. Fig. 4 depicts the hub concept graphically.

The LoI of the hub concept is the maximum level of authorization. The hub manages all interaction requests among different BNs and distributes them to the correct recipient. The communication has no constraints. The scalability of the concept is a constant factor. A limited amount of hubs, even a single one, can connect unlimited BNs Ξ. Additionally, the hub provides a location independent from existing actors. The scheme does not impose additional token cost on the BNs Ξ because the hub is a separate solution. Concerning governance consistency, as BNs Ξ are connected, the criterion does not hold in this setting. The hub routes data among different BNs Ξ. Thus, user and SP may transparently receive data

[2] https://metamask.io

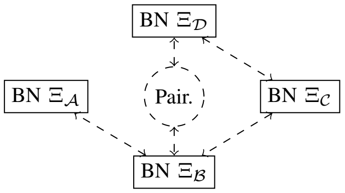

Fig. 5: Pairing scheme

from another BN Ξ. The hub requires an additional connector for a novel SSI IdMS. Therefore, PfU characteristic reflects alike. Furthermore, the hub connects existing SSI IdMS post-production phase without modifying them.

In this category, we distinguish the centralized hub and the decentralized hub. The centralized hub is an application run by an entity. Therefore, it imposes a TTP. In contrast, another blockchain realizes a decentralized hub. Thus, this type may not represent a TTP depending on the governance structure of the blockchain.

In the blockchain context, Polkadot [11] represents a decentralized hub. Polkadot is a blockchain that manages transaction communication between other distributed ledgers. Bitfinex[3] is a token exchange and portrays a centralized hub.

F. Pairing

The pairing scheme connects two BNs Ξ for communication. A pairing is functionally comparable to the hub. In contrast, a pairing serves only exactly two BNs Ξ and provides a decentral pattern for interoperability. Fig. 5 presents a graphical overview of different pairing types among multiple BNs Ξ.

Within this concept, the maximum supported LoI is authorization. A pairing of two BNs Ξ can exchange information for this purpose. Furthermore, the pairing scales with the number of BNs Ξ. In case all existing BNs Ξ require communication, one must establish $\frac{|\Xi|\dot{(}|\Xi|-1)}{2}$ pairings. As data is transparently conveyed between BNs Ξ, governance consistency does not hold. Regarding PfU, before communication between two SSI IdMS can commence, one fully implements a new pairing between the corresponding BNs Ξ. Furthermore, an ecosystem requires several pairings to enable interaction with all BNs Ξ. We dissect this pattern in a centralized, a decentralized and a direct variation.

1) Centralized Pairing: The centralized pairing represents a TTP to mediate communication that is independent of the other actors. There are no additional associated token costs due to the centralized implementation as an application. Furthermore, the centralized pairing achieves the interoperability post-production phase of the SSI IdMS due to its independence. Reducing an exchange to only two tokens is an example in the blockchain domain.

2) Decentralized Pairing: The decentralized pairing implements a blockchain for the pairing activity. Thus, it does not represent a TTP. The concept does not impose additional token cost due to its independent nature. Comparable to the centralized pairing, the concept can be established as a post-production deployment of the BN Ξ. The restriction of Polkadot to two blockchains is an example.

3) Direct Pairing: A direct pairing implements communication on the two BNs Ξ directly. Therefore, the scheme does not establish an additional TTP. Besides that, the auxiliary token cost might be imposed depending on the actual implementation. Suppose the scheme is realized by smart contracts on top of the BN Ξ. Invocation of the smart contracts requires tokens. In contrast, a direct integration into the core ledger of the BN Ξ avoids cost. Similarly, the PoC is either design phase or post-production deployment. Borkowski et al. [40] propose claim-first transactions for token exchange between blockchains.

G. Hybrid Schemes

The delineated schemes reflect atomic concepts. A combination of these concepts leads to hybrid patterns. To achieve a fully interconnected SSI IdMS landscape, the arbitrary joining of schemes result in numerous hybrid schemes. Therefore, we present two hybrid meta-concepts exemplarily.

1) Functional Composition for a Dedicated Link: The functional composition splits the practical implementation of a hybrid concept at a certain LoI. Despite theoretical support of the maximum LoI by all concepts, the practical implementation of a specific scheme is restricted to a lower grade. Thus, this hybrid scheme combines two atomic patterns to achieve the maximum LoI among two SSI IdMS.

For instance, SSI IdMS $\mathcal{A}$ and $\mathcal{B}$ apply the same protocol and standard of the IdP interaction class to enable identity and attribute assertion and claim issuance for enrolled entities. This approach is transparent for the users and SPs of both SSI IdMS. Furthermore, the SP-side identity broker scheme enables the authorization of entities. In conclusion, one combines characteristics of both schemes to establish a certain link between IdMS $\mathcal{A}$ and $\mathcal{B}$.

2) Vertical Composition for SSI Interconnection: The vertical composition of distinct interoperability concepts target the interconnection of the SSI IdMS landscape. In this setting, the LoI plays a subordinate role. The general applicability of SSI IdMS has priority. This hybrid model can be used to connect entities of a community and to join different communities.

a) Intra-connect one Community: To establish a connected SSI community with different SSI IdMS, one can use the hub paradigm. The hub paradigm can be extended in a simpler manner (connector) compared to a pairing (full implementation). A decentralized hub based on a permissioned blockchain can be governed by the members of the community.

b) Inter-connect different Communities: Once communities have the ability to interoperate with their SSI IdMS, these societies may require communication, too. The hub concept can be applied to this type of network. Furthermore, the connection via paring seems to be a reasonable approach as the number of communities might be smaller than the number of SSI IdMS.

[3] https://www.bitfinex.com

Concept	LoI	TTP Dep.	Scalability	Token Cost	Governance Consistency	Preconditions for Use	Phase of Consideration	Location
IdP Interaction	Authorization	No	User × SP × BN	No	Yes	Configuration	Design	User, SP, BN
IdP Routing	Authorization	No	BN	No	No	Configuration	Design	BN
User-side Identity Broker	Authorization	No	User	No	Yes	Connector	Post-prod.	User
SP-side Identity Broker	Authorization	No	SP	No	Yes	Connector	Post-prod.	SP
Centralized Hub	Authorization	Yes	Constant	No	No	Connector	Post-prod.	Independent
Decentralized Hub	Authorization	No	Constant	No	No	Connector	Post-prod.	Independent
Centralized Pairing	Authorization	Yes	$\frac{\lvert BN\rvert\dot{(}\lvert BN\rvert-1)}{2}$	No	No	Full impl.	Post-prod.	Independent
Decentralized Pairing	Authorization	No	$\frac{\lvert BN\rvert\dot{(}\lvert BN\rvert-1)}{2}$	No	No	Full impl.	Post-prod.	Independent
Direct Pairing	Authorization	No	$\frac{\lvert BN\rvert\dot{(}\lvert BN\rvert-1)}{2}$	Yes/ no	No	Full impl.	Design/ post-prod.	BN

TABLE I: Characteristics of interoperability concepts

H. Implementation Variants

The presented interoperability concepts can be implemented in variations. These variations influence the assessed characteristics.

1) Directionality: The hub and pairing can be implemented in a unidirectional or bidirectional mode. The unidirectional variant allows only one-way communication from SSI IdMS $\mathcal{A}$ to $\mathcal{B}$. In contrast, bidirectional variants enable communication in both directions. Thus, interaction in the opposite direction, from $\mathcal{B}$ to $\mathcal{A}$ is possible. The directionality variation impacts the scalability of the concept. To connect several SSI IdMS, one requires the double amount of unidirectional pairings comparing to the directional variant.

2) BN Implementation Type: The implementation type differentiates a smart contract or direct blockchain implementation. The BN Ξ of an SSI IdMS can be built of either approach. Adding further smart contracts and extending or changing existing smart contracts influence the token consumption during execution. In contrast, changing the ledger itself may not impose extra cost. However, a change of the blockchain may lead to a fork.

3) Decentralization Type: To avoid the TTP dependency, the decentralized hub and pairing implements a blockchain. A peer-to-peer network governs the blockchain with a consensus algorithm. In case the power within the peer-to-peer network is concentrated on one or a few entities, a TTP dependency is re-established. Despite that, the blockchain may require its own tokens to run the interoperability routines.

I. Concept Comparison

Having assessed the schemes (cf. Table I) protocol and standard, broker, hub and pairing, we conduct a comparative study. All evaluated interoperability concepts theoretically provide the maximum LoI of authorization. Therefore, no functional constraint is imposed by selecting a specific pattern.

The centralized hub and the centralized pairing create a dependency on a new TTP. As a consequence, the communication between the connected SSI IdMS is controlled by a TTP. Therefore, this concept impairs data minimization and control principles. In particular, this setting violates the idea of self-sovereignty but might be acceptable to achieve interoperability between SSI IdMS. In contrast, the other patterns do not create an additional dependency on a TTP.

Concerning scalability, the centralized and decentralized hub are the favorable solution. These concepts scale with a constant factor and require only another connector for a new SSI IdMS. Protocol and standard affect most entities. However, if these rules are incorporated during the design of the SSI IdMS, additional work is not required. In between, the broker schemes scale with user and SP. Furthermore, the pairing scales multiplicatively with the BNs Ξ.

Additional token cost for interoperability can be generally avoided. Nonetheless, the decentralized hub and the decentralized pairing might impose token cost depending on the actual implementation (cf. V-H2). Furthermore, the cost for the direct pairing depends on the type of the BN Ξ.

The IdP interaction protocol class and the user-side and SP-side identity broker provide governance consistency. The remaining concepts allow the transmission of information among SSI IdMS covertly. Nonetheless, communication between the BNs Ξ is comfortable for the user and the SP. These approaches enable community building and interconnection.

Concerning PfU, the protocol and standard concept require configuration solely, whereas the majority of the other concepts demand at least a dedicated connector. Despite that, the pairing requires a full implementation for each new SSI IdMS that needs to be connected to any existing system.

The PoC characterizes the concepts twofold. Protocol and standard must be incorporated during the design phase of a SSI IdMS. In contrast, the remaining concepts can be applied post-production deployment of a SSI IdMS. This enables the bridging of gaps until protocol and standards mature. Furthermore, the location of interoperability schemes is split across all actors. The IdP interaction protocol class affects all entities. The hub and the centralized and the decentralized pairing enable interoperability independently from any party.

Concept	SSI/ Blockchain Sample	LoI	Traditional IdM Sample	LoI
IdP Interaction	DIDAuth [31]/ DID [32]	4	OIDC [24]/ OAuth2 [33] SAML2 [23]	4 4
IdP Routing	ILP [34]	n/a	EduROAM [35]/ RADIUS [36]	4
User-side Id. Broker	MetaMask	n/a	TAAS [39]	3
SP-side Id. Broker	UR [37] Grüner et al. [38]	1 3	-	-
Centralized Hub	Bitfinex	n/a	-	-
Decentralized Hub	Polkadot [41]	n/a	-	-
Centralized Pairing	Red. Bitfinex	n/a	-	-
Decentralized Pairing	Red. Polkadot	n/a	-	-
Direct Pairing	Borkowski et al. [40]	n/a	-	-

TABLE II: Interoperability concept samples

Overall, each concept has its advantages and disadvantages among the assessed peculiarities. We cannot determine an undisputed paradigm that should be selected. Nonetheless, as depicted with the hybrid schemes, one can apply different patterns to build communities and drive interoperability.

J. Example Comparison

Table II provides an overview of the selected examples and their associated concept. Many dedicated initiatives in the traditional IdM and SSI domain cover the protocol and standard class. Furthermore, the SSI realm comprises SP-side identity brokers implementations. In contrast, we could solely name blockchain samples within the further concepts. SSI solutions have not been proposed yet. In traditional IdM, a BN Ξ does not exist. Thus, we did not state any example.

VI. Portability

Analogous to interoperability, we initially delineate a definition of portability (VI-A) and describe evaluation criteria (VI-B). Subsequently, we outline portability concepts and analyze them according to the peculiarities (VI-C to VI-E). Furthermore, we name SSI-related and traditional IdM examples. Table III presents an overview of the examined paradigms and Table IV lists the samples.

A. Definition

The SSI principles [4] summarize portability as information transfer. In particular, data portability avoids lock-in to a specific TTP. The meaning aligns with the general portability notation (cf. II-C). Considering SSI, we delineate portability as the ability to transfer an identity from one SSI IdMS to another.

Definition 6 (**Self-Sovereign Identity (Object) Portability**). *Given SSI IdMS $\mathcal{A}$ and $\mathcal{B}$, a self-sovereign identity $c \in \mathcal{A}$ is portable to $\mathcal{B}$ if a function f exists with $f(c, \mathcal{A}) \Rightarrow c \notin \mathcal{A}$ and $f(c, \mathcal{B}) \Rightarrow c' \in \mathcal{B}$.*

A portability scheme is a concept to establish the rooting for an identity on another SSI IdMS. At the same time, the identifier and attribute should be revoked on the previously used SSI IdMS. A publicly revoked identifier prevents misuse and increases security. Per definition, the identity c is transitioned to an identity c'. Thus, the identifier or claims might change during the transition but stay related.

B. Evaluation Criteria

In the following sections, we present assessment criteria for the portability schemes.

1) Level of Portability (LoP): The Level of Portability (LoP) differentiate the functional scope of the portability concept. We distinguish the grade *identifier* and *attribute*. The tier *identifier* refers to the transfer of the designator. The level *attribute* describes the move of the verifiable claim. In contrast to LoI, the LoP tiers do not establish a hierarchy. A scheme can achieve either or both grades.

2) TTP Dependency, Token Cost, Preconditions for Use, Phase of Consideration, Location: We define these characteristics for the interoperability patterns (cf. V-B) and apply them likewise to the portability schemes.

3) Trust Consistency: The trust consistency criterion describes if the ported claims provide the same trust constitution as before. Thus, trust consistency holds true if the issuer is preserved. Suppose that a ported claim has a new issuer, then trust consistency is violated because the new issuer is trusted differently than the previous one.

4) Timestamp Preservation: The claims registry of an SSI IdMS provide the advantage to obtain an unforgeable timestamp of claim existence and revocation. This timestamp is derived from the block structure of the BN Ξ. The claim may contain an issuing date as well. But the correctness depends on the issuer and is not independently verifiable.

C. Protocol and Standard

Protocol and standard (cf. V-C) encompass agreed rules for data transfer. In particular, this concept can define data formats and export/ import functions for the identifier and attributes. Thus, the scheme covers both LoP, the identifier and attribute. Despite that, there is no additional TTP created because the SSI IdMS owner must implement them in the different components. Aligned to that, the concept affects the location of the user, SP and BN Ξ.

Protocol and standard must be implemented during the design phase of the SSI IdMS. Otherwise, additional implementation effort arises. Considering the PfU characteristic, solely configuration is necessary to port an identity from one SSI IdMS to another. For instance, communication channels require a setup. Suppose claims exist in a generic data exchange format, including an issuer's reference, the issuer and, therefore, trust consistency is maintained.

Furthermore, timestamps in the BNs Ξ claim registry cannot be preserved. Upon transfer to the new SSI IdMS, the point in time of the transfer will be the new timestamp of existence on the BN Ξ.

Concept	LoP	TTP Dependency	Timestamp Preservation	Token Cost	Trust Consistency	Preconditions for Use	Phase of Consideration	Location
Protocol and Standard	Identifier/ attribute	No	No	Yes	Yes	Configuration	Design	User, SP, BN
Transformer	Identifier/ attribute	Yes	No	Yes	No	Connector	Post-prod.	Independent
Change Identifier Mapping	Identifier	No	No	No	No	Configuration	Post-prod.	SP
Re-issuance of Claims	Attribute	No	No	Yes	Yes	Connector	Post-prod.	SP
Claim of New Identifier	Identifier	No	Yes	Yes	Yes	Connector	Post-prod.	User

TABLE III: Characteristics of portability concepts

Additionally, the concept requires token cost for the transfer of the identifier and the attributes because of the rooting on BN Ξ causes transactions.

In the SSI domain, examples are the DID [32] and the Verifiable Credential (VC) [42] standard. The VC standard outlines a data format for claims. Besides that, in traditional IdM, X.509 [22] certificates represent this pattern.

D. Transformer

The transformer concept describes an entity that converts identifier and attributes between formats. It transforms these elements from one SSI IdMS to another. As data structures may change, the attributes are newly issued under the identity of the transformer because modification of the data structure invalidates existing signatures. As a central entity, the transformer establishes a new TTP besides the user and SP. Furthermore, the concept does not preserve the claim registry timestamps of the transformed attributes because the claims are newly issued. Thus, the trust consistency constraint does not hold either.

Additional token costs arise due to the newly issued claims. The transformer can support a further SSI IdMS by creation of a specific connector. Despite that, the transformer TTP achieves portability at an independent location and post-production deployment of the SSI IdMS. An example in the blockchain context is HyperService [43]. HyperService proposes a framework to create cross-blockchain applications. A compiler achieves portability of smart contract code.

E. Auxiliary Solutions

Auxiliary solutions encompass portability concepts that support either the transfer of the identifier or the attribute. These schemes partially enable pseudo-portability of an identity. The auxiliary concepts do not create an additional TTP because they are implemented either by the user or the SP. Furthermore, the schemes acquire portability post-production activation of a SSI IdMS.

1) Change Identifier Mapping: The SP stores a mapping between the user's identifier and internal data [44]. Suppose the user creates a new identifier at another SSI IdMS, the change identifier mapping concept targets the replacement of the old with the new designator at the SP. The concept does not create additional token cost because the identifier mapping is solely changed at the SP. The SP may require different configurations for distinct SSI IdMS to obtain the new identifier automatically from the user. Trust consistency and timestamp preservation do not hold because the user changes to a new identifier. Therefore, the attributes must be ported to the new designator as well.

Concept	SSI/ Blockchain Sample	LoP	Traditional IdM Sample	LoP
Protocol and Standard	DID [32] VC [42]	Id. Att.	X.509 [22]	Id./ Att.
Transformer	HyperService [43]	n/a	-	-

TABLE IV: Portability concept samples

2) Re-issuance of Claims: Subsequent to the enrollment at a new SSI IdMS, the user obtains the possessed claims from the original issuers again. The concept leads to changed timestamps of the claims. In contrast, trust consistency holds true because the claims originate from the same issuers. Re-issuance of claims impose additional token costs on the new SSI IdMS. Regarding PfU, the SP (or AP) requires at least a connector to the new SSI IdMS for attribute issuance.

3) Claim of New Identifier: A user registers a new identifier at an SSI IdMS. With the old identity, the user self-issues a claim about the ownership of the new identifier and vice versa. Thus, a verifier can confirm that the user is under control of the old and new identifier and accepts associated claims. This pattern preserves the timestamps of the claims because they stay the same. Similarly, the trust consistency characteristic holds true. The additional token cost might be imposed due to the registration of the new identifier. Despite the location of the user, the SP requires at least a connector to the new SSI IdMS.

F. Concept Comparison

The portability concepts offer different functionality levels of either migrating the identifier or the attributes. The auxiliary solutions target solely one of the artefacts and enable portability in a pseudo sense. Within the concepts, the transformer solely creates an additional TTP. The other schemes are incorporated within existing entities. The portability schemes are located at the side of the user or the SP. Despite that, the transformer acts independently.

Furthermore, the claim of new identifier concept solely preserves the claim's timestamp in the claim registry. The other patterns do not preserve the timestamps because the claims are newly created and registered. Additionally, each pattern except for the change identifier mapping imposes additional token cost for the porting of the identity. Despite that, trust consistency does not hold true for the transformer and the change identifier mapping. The remaining concepts sustain the issuer. Except for the protocol and standard scheme, other concepts can be applied in the post-production phase of a SSI IdMS.

Overall, protocol and standard seem to be favourable because of maintaining consistently the trust. In contrast, the transformer is disadvantageous. The concept neither preserves the issuer nor avoids an additional TTP. The auxiliary solutions do not represent full concepts but can improve portability until full protocol and standard adoption. These schemes are mainly located at the side of the SP.

G. Example Comparison

Concerning the examples, protocols and standards are developed within the SSI and traditional IdM domain. Moreover, HyperService [43] represents a transformer for smart contracts in the realm of blockchain. However, a transformer for SSI does not exist.

VII. Conclusion

The SSI paradigm promotes a global unique identity that is widely applicable and under the control of the user. In this regard, the proclaimed principles of interoperability and portability support the overall SSI objective. To drive understanding, we formalized the definition of these axioms. Based on this, we devised and evaluated various concepts. Protocol and standard, identity broker, hub and pairing enable interoperability between different SSI IdMS. These patterns provide the maximum functional level of authorization.

Moreover, the concepts may create an additional TTP but are unlikely to impose additional token cost. The majority of the schemes can be applied post-production activation of the SSI IdMS. Despite that, sample implementations of the concepts exist only partially in the SSI domain. Thus, future research activities can concentrate on respective implementations. We could not reach a definitive conclusion on a superior interoperability model. Nonetheless, the concepts supports communication during design and post-production phase.

Furthermore, protocol and standard, transformer and auxiliary solutions provide schemes for identity portability. The concepts offer a different functional scope, whereas auxiliary solutions enable solely pseudo-portability. The majority of the schemes cannot preserve the timestamps of a verifiable claim within the claim registry. We consider the protocol and standard as advantageous compared to the other concepts despite incorporation in the design phase of the SSI IdMS.

References

[1] A. Jøsang, J. Fabre, B. Hay, J. Dalziel, and S. Pope, "Trust requirements in identity management," in *Proceedings of the 2005 Australasian Workshop on Grid Computing and e-Research (AusGrid)*, 2005, pp. 99–108.

[2] I. Thomas and C. Meinel, "An attribute assurance framework to define and match trust in identity attributes," in *Proceedings of the 2011 IEEE Int. Conf. on Web Services (ICWS)*, 2011, pp. 580–587.

[3] A. Grüner, A. Mühle, T. Gayvoronskaya, and C. Meinel, "A comparative analysis of trust requirements in decentralized identity management," in *Proceedings of the 33rd Int. Conf. on Advanced Information Networking and Applications (AINA)*, 2019, pp. 200–213.

[4] C. Allen. (2016) The path to self-sovereign identity. (accessed on 2021-06-30). [Online]. Available: http://www.lifewithalacrity.com/previous/2016/04/the-path-to-self-soverereign-identity.html

[5] E. Maler and D. Reed, "The venn of identity: Options and issues in federated identity management," *IEEE Security & Privacy*, pp. 16–23, 2008.

[6] Kim Cameron. (2009) Seven Laws of Identity. (accessed on 2021-06-30). [Online]. Available: https://www.identityblog.com/?p=1065

[7] European Parliament and Council. (2016) EU General Data Protection Regulation (GDPR). (accessed on 2021-06-30). [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[8] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Transactions on Engineering Management*, pp. 1008–1027, 2019.

[9] A. Narayanan and J. Clark, "Bitcoin's academic pedigree," *Communications of the ACM*, pp. 36–45, 2017.

[10] S. Nakamoto. (2008) Bitcoin: A peer-to-peer electronic cash system. (accessed on 2021-06-30). [Online]. Available: https://bitcoin.org/bitcoin.pdf

[11] G. Wood. Ethereum: A secure decentralised generalised transaction ledger. (accessed on 2021-06-30). [Online]. Available: https://gavwood.com/paper.pdf

[12] E. Bertino and K. Takahashi, *Identity Management: Concepts, Technologies, and Systems*, 1st ed. Norwood, Massachussets, USA: Artech House, 2010.

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

[14] NIST. (2021) Glossary. Interoperability. (accessed on 2021-06-30). [Online]. Available: https://csrc.nist.gov/glossary/term/Interoperability

[15] R. Rezaei, T. Chiew, S. Lee, and Z. Shams Aliee, "Interoperability evaluation models: A systematic review," *Computers in Industry*, pp. 1–23, 2014.

[16] S. Koussouris, F. Lampathaki, S. Mouzakitis, Y. Charalabidis, and J. Psarras, "Digging into the real-life enterprise interoperability areas definition and overview of the main research areas," in *Proceedings of the 2011 World Multi-Conf. on Systemics, Cybernetics and Informatics (WMSCI)*, 2011, pp. 254–259.

[17] H. Leitold and B. Zwattendorfer, "Stork: Architecture, implementation and pilots," in *Proceedings of the 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe Conf. (ISSE)*, 2011, pp. 131–142.

[18] J. Backhouse and R. Halperin, *Approaching Interoperability for Identity Management Systems*, 2009, pp. 245–268.

[19] D. V. Silakov and A. V. Khoroshilov, "Ensuring portability of software," *Programming and Computer Software*, pp. 41–47, 2011.

[20] D. Petcu, "Portability and interoperability between clouds: Challenges and case study," in *Towards a Service-Based Internet*, 2011, pp. 62–74.

[21] Internet Engineering Task Force. (2015) Rfc 7468. textual encodings of pkix, pkcs, and cms structures. (accessed on 2021-06-30). [Online]. Available: https://tools.ietf.org/html/rfc7468

[22] ——. (2008) Rfc 5280. internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. (accessed on 2021-06-30). [Online]. Available: https://tools.ietf.org/html/rfc5280

[23] OASIS. Saml version 2.0. (accessed on 2021-06-30). [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf

[24] OpenID Foundation. Openid connect core 1.0. (accessed on 2021-06-30). [Online]. Available: https://openid.net/specs/openid-connect-core-1_0.html

[25] T. Koens and E. Poll, “Assessing interoperability solutions for distributed ledgers,” *Pervasive and Mobile Computing*, pp. 1574–1192, 2019.

[26] N. Kannengiesser, M. Pfister, M. Greulich, S. Lins, and A. Sunyaev, “Bridges between islands: Cross-chain technology for distributed ledger technology,” in *Proceedings of the 53rd Hawaii Int. Conf. on System Sciences (HICCS)*, 2020, pp. 5298–5307.

[27] VON Community. Von. verifiable organizations network. (accessed on 2021-06-30). [Online]. Available: https://vonx.io

[28] IDunion Project. Idunion. (accessed on 2021-06-30). [Online]. Available: https://idunion.org/?lang=en

[29] Merriam-Webster Dictionary. Protocol. (accessed on 2021-06-30). [Online]. Available: https://www.merriam-webster.com/dictionary/protocol

[30] ——. Standard. (accessed on 2021-06-30). [Online]. Available: https://www.merriam-webster.com/dictionary/standard

[31] M. Sabadello, K. D. Hartog, C. Lundkvist, C. Franz, A. Elias, A. Hughes, J. Jordan, and D. Zagidulin. Introduction to did auth. (accessed on 2021-06-30). [Online]. Available: https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/final-documents/did-auth.md

[32] Decentralized Identity Foundation. Authentication working group. didcomm. (accessed on 2021-06-30). [Online]. Available: https://identity.foundation/working-groups/authentication.html

[33] Internet Engineering Task Force. (2012) The oauth 2.0 authorization framework. (accessed on 2021-06-30). [Online]. Available: https://tools.ietf.org/html/rfc6749

[34] Interledger protocol v4. (accessed on 2021-06-30). [Online]. Available: https://interledger.org/rfcs/0027-interledger-protocol-4/

[35] EduROAM. Eduroam. (accessed on 2021-06-30). [Online]. Available: https://www.eduroam.org

[36] Internet Engineering Task Force. (2000) Rfc 2865. remote authentication dial in user service (radius). (accessed on 2021-06-30). [Online]. Available: https://tools.ietf.org/html/rfc2865

[37] Universal Resolver. (accessed on 2021-06-30). [Online]. Available: https://github.com/decentralized-identity/universal-resolver

[38] A. Grüner, A. Mühle, and C. Meinel, “An integration architecture to enable service providers for self-sovereign identity,” in *Proceedings of the 18th IEEE Int. Symposium on Network Computing and Applications (NCA)*, 2019, pp. 1–5.

[39] D. W. Chadwick and G. Inman, “The trusted attribute aggregation service (TAAS) - providing an attribute aggregation layer for federated identity management,” in *Proceedings of the 2013 Int. Conf. on Availability, Reliability and Security (ARES)*, 2013, pp. 285–290.

[40] M. Borkowski, C. Ritzer, D. McDonald, and S. Schulte. (2018) Caught in chains: Claim-first transactions for cross-blockchain asset transfers. (accessed on 2021-06-30). [Online]. Available: https://www.borkowski.at/pub/tast-wp2

[41] G. Wood. (2016) Polkadot: Vision for a heterogeneous multichain framework. (accessed on 2021-06-30). [Online]. Available: https://icowhitepapers.co/wp-content/uploads/PolkaDot-Whitepaper.pdf.

[42] M. Sporny, D. Longley, and D. Chadwick. (2019) Verifiable credentials data model 1.0. expressing verifiable information on the web. (accessed on 2021-06-30). [Online]. Available: https://www.w3.org/TR/vc-data-model/

[43] Z. Liu, Y. Xiang, J. Shi, P. Gao, H. Wang, X. Xiao, B. Wen, and Y.-C. Hu, “Hyperservice: Interoperability and programmability across heterogeneous blockchains,” in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2019, pp. 549–566.

[44] U. Kylau, I. Thomas, M. Menzel, and C. Meinel, “Trust requirements in identity federation topologies,” in *Proceedings of the IEEE 27th Int. Conf. on Advanced Information Networking and Applications (AINA)*, 2009, pp. 137–145.