Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology

Nitin Naik[1] and Paul Jenkins[2]

[1]Defence School of Communications and Information Systems, Ministry of Defence, United Kingdom
[2]School of Computing, University of Portsmouth, United Kingdom
Email: nitin.naik100@mod.gov.uk and paul.jenkins@port.ac.uk

***Abstract*—Digital identity is one of the biggest challenges in cyberspace. This field has been evolving for many decades with a number of Identity Management (IDM) models being proposed and employed; however, few were able to solve the issue of sovereignty of an identity and storage-control of its associated personal and confidential data. Self-Sovereign Identity (SSI) was introduced to solve this crucial issue offering a user full sovereignty of their identity and storage-control of their associated personal and confidential data. Alongside ownership of an identity, it maintains all private information in a Digital Wallet which is owned and controlled by the user. However, SSI is an emerging IDM, therefore it requires careful evaluation of various aspects of SSI for it to become an operative IDM. This paper proposes several specifications to evaluate any SSI solution. Subsequently, it analyses two emerging SSI solutions uPort and Sovrin. Finally, an evaluation of uPort and Sovrin SSI is performed utilising the proposed specifications, highlighting their strengths and limitations.**

***Index Terms*—Self-Sovereign Identity; SSI; Specifications; Digital Wallet; Identity Management; IDM; uPort; Sovrin.**

I. Introduction

Digital identity is a core element of any digital platform for its successful operation. However, it has been one of the most difficult areas for cyber experts to master and provide a complete solution, which is capable of proving the identity of any entity in cyberspace, similar to that of the physical world. Over the years, several IDM models have been proposed and employed. However, until recently no model was able to resolve the issue of sovereignty of an identity and storage-control of its associated personal and confidential data. This issue of sovereignty has affected several other related issues with respect to identity such as security, privacy and safeguarding [1]. With the introduction of blockchain, a new identity management model called SSI was introduced which aims to solve all the above issues and offers a user full sovereignty of their identity and storage-control of their associated personal and confidential data. Alongside ownership of an identity, it maintains all private information in a *Digital Wallet* owned and controlled by the user. The *Digital Wallet* is analogous to a physical wallet saving all digital credentials as physical entities, however, these credentials in the *Digital Wallet* are digitally signed verifiable credentials and much faster to issue and verify than their physical counterpart [2]. Furthermore, it is a peer-to-peer model and does not involve any third-party between the user and organisation.

SSI is an emerging model referred to as IDM 3.0, therefore it requires careful evaluation of its various aspects for it to become an operative IDM. Previously, several specifications for evaluating its predecessor federated IDM 2.0 model were proposed [3], [4]. This paper extends the evaluation of the federated IDM 2.0 model by proposing several specifications to evaluate the new SSI IDM 3.0 model. Subsequently, it analyses two emerging SSI solutions uPort and Sovrin [5], [6]. The uPort SSI solution is built on the public permissionless blockchain Ethereum and the Sovrin SSI solution is built on the public permissioned blockchain Hyperledger Indy. Finally, it evaluates both uPort and Sovrin SSI on the basis of the proposed specifications to highlight their strengths and limitations.

The rest of the paper is structured as follows: Section II elucidates the development of the three IDM Models: Centralised IDM, Federated IDM and Self-Sovereign IDM. Section III proposes the necessary specifications for SSI evaluation. Section IV discusses the two emerging SSI solutions uPort and Sovrin. Section V performs the comparative evaluation of uPort and Sovrin based on the proposed specifications. Section VI presents the summary of the paper and related future work.

II. Development of Identity Management Models

This section presents the development of three IDM models: Centralised IDM, Federated IDM and Self-Sovereign IDM as shown in Fig. 1.

Centralised Identity Management (IDM 1.0)
Federated Identity Management (IDM 2.0)
Self-Sovereign Identity Management (IDM 3.0)

Fig. 1. Development of Identity Management (IDM) Models

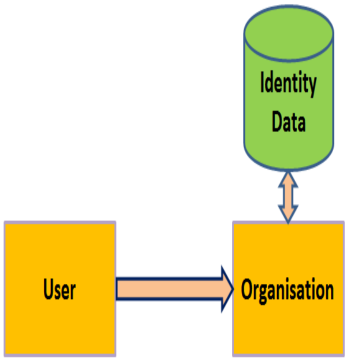

Fig. 2. Centralised Identity Management Model (IDM 1.0)

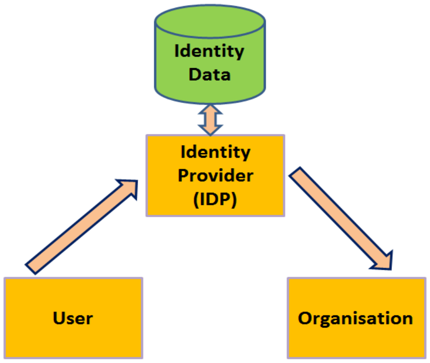

Fig. 3. Federated Identity Management Model (IDM 2.0)

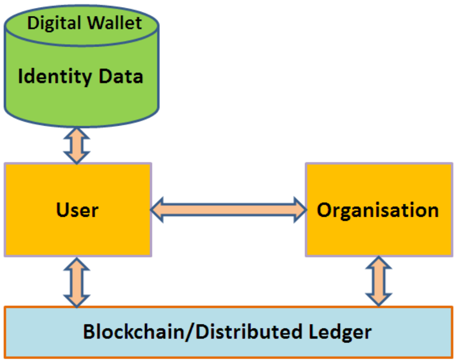

Fig. 4. Self-Sovereign Identity Management Model (IDM 3.0)

A. Centralised Identity Management Model (IDM 1.0)

The centralised IDM model is the oldest IDM model, in which an organization issues credentials to their users permitting them to use their services. The trust relationship between organisation and user is based on a shared *secret*, in most cases, this is typically a login password associated with a username [7]. The users identity related personal and confidential data is always stored and controlled by the organisation. Additionally, the user repeats this process and requires separate credentials for each organisation or system, they wish to obtain service from.

B. Federated Identity Management Model (IDM 2.0)

This federated IDM model solves two major issues: 1) it removes the organisational burden of managing identity and credentials securely by introducing a third-party called the IDentity Provider (IDP), which is an additional task alongside the main business operations and 2) it removes the burden from users to manage several identity related credentials for several systems by offering a Single-Sign On (SSO) facility [8], [9]. However, this IDM model has one similar issue in that the abundance of identity related personal and confidential data of a user is held by the IDP and therefore the user has no control over this information.

C. Self-Sovereign Identity Management Model (IDM 3.0)

This self-sovereign IDM model is an improvement on the federated IDM model, where it removes the third-party IDP and offers a direct connectivity between a user and organisation. Furthermore, it resolves the main issue of ownership of identity related personal and confidential data of a user by offering its full control through the use of a *Digital Wallet*. The *Digital Wallet* saves all the identity related personal and confidential data which is owned and controlled by the user on the device controlled by the user. SSI assumes three key roles i.e. *Issuer, Holder and Verifier*, in its ecosystem as shown in Fig. 5. An issuer creates and issues credentials to a holder. A holder receives credentials from an issuer, holds it and when required, it shares these credentials with a verifier. A verifier receives and verifies credentials presented by a holder.

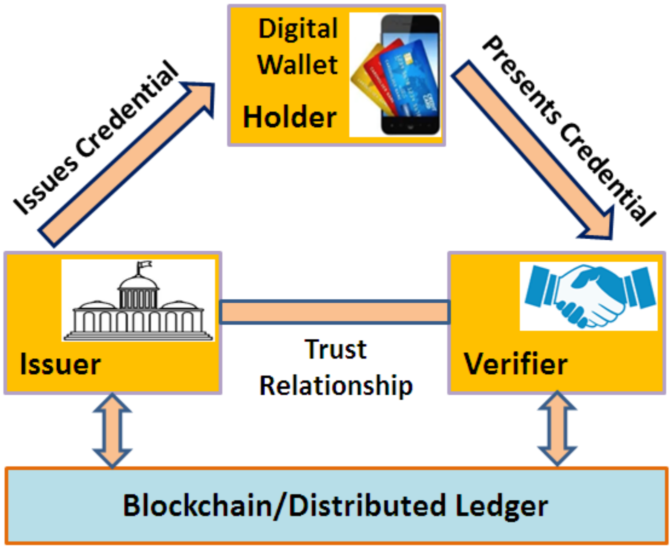

Fig. 5. Self-Sovereign Identity Ecosystem

This SSI implementation is based on the Verifiable Credential (VC) [10] and Decentralized IDentifier (DID) [11] standards which are proposed for creating a cryptographically verifiable digital identity that is fully governed by its owner [12]. A VC is used to represent similar information on the Web to that of a physical credential in the real world. The DID is a permanent, universally unique identifier and cannot be taken away from its owner who owns the associated private key, which is completely different from other ephemeral identifiers such as a mobile number, IP address and domain name [12].

III. Proposed SSI Specifications

Several IDM specifications were presented in the past in different contexts. Whether it was Kim Camerons Laws of Identity [13] or Christopher Allens Guiding Principles of SSI [14], they assisted the evaluation of new and emerging SSI solutions and their success [15]. However, this (SSI) field is evolving rapidly as is SSI requirements and standards. Underlying these changing requirements, this section proposes a revised and extended specifications to evaluate SSI solutions.

A. Sovereignty

Any individual who owns an identity must have the full sovereign control of that identity, and it should not be controlled by any other person, organisation or government. An individual can decide its identity correlation across different contexts without requiring any permission from anybody.

B. Storage-Control

Any identity and its associated personal and confidential data should be owned and controlled by the identity owner, leading to the introduction of the concept of a *Digital Wallet*, keeping all identity related personal and confidential data on the device which is normally owned and controlled by the identity owner.

C. Longevity

Any identity must be eternal as long as its owner wishes, however, it can be revoked or abandoned by an identity owner. Therefore, an identity should be completely different from other ephemeral identifiers such as a mobile number, IP address and domain name.

D. Verifiability

Any identity should be verifiable through its credentials on the Web in a way similar to a physical credential representing the real world identity. This could be digitally signed by the issuer and cryptographically secured; however, its verification may not necessarily require any interaction with its issuer.

E. Recovery

The identity solution should be sufficiently resilient to successfully recover any identity in the event of a lost key, lost wallet or lost mobile/device. It should offer a number of mechanisms to identity owners to recover and reassert their identity in the event of a complete loss of credentials.

F. Cost-Free

An identity should be offered to general users free of cost and it should not incur any hidden cost, licensing fees, or any other financial charges for simply owning an identity. However, this may not apply to costs related to other resources and implementations.

G. Security

The security of an identity and its related communication is paramount for any SSI solution. It includes various security levels for identity such as cryptographically secure connections and communications, digitally signed transactions, and decentralized and encrypted storage.

H. Privacy

As an aim, any identity owner should only be requested to provide or disclose the minimum identity information required for verification or service while maintaining as much anonymity as possible. The SSI solution should not provide any mechanism to correlate biometric data with an underlying identity. Any identity related personal and confidential data should only be shared after seeking the consent from its owner.

I. Safeguard

The freedom and right of every identity owner should be safeguarded. This is accomplished by employing an independent authentication system for an identity. In the case of a conflict between identity owner and the identity network, the rights of an identity owner should be safeguarded.

J. Accessibility

Any identity related solution and services should be user-friendly and accessible by as many people as possible. This is of greater importance for non-technical and vulnerable people.

K. Availability

Any identity related solutions and services should be available to all without any discrimination based on their ethnicity, gender, socio-economic status, or language.

L. Transparency

All systems, protocols and algorithms employed in any identity solution should be free, open-source, and as independent as possible of any particular architecture or proprietorship. Presently, the SSI community has been consulting on several open standards and forums to make this possible such as the Decentralized Identity Foundation (DIF), the World Wide Web Consortium (W3C) and the Organisation for the Advancement of Structured Information Standards (OASIS).

M. Portability

An identity and its associated data should be easily transportable from one platform to another platform. This requires the standardisation of identity, credential and data/file formats.

N. Interoperability

Two different identity solutions should be capable of communicating with each other at scale. This will enable enterprises and government organisations to communicate with each other irrespective of their employed identity solutions.

O. Scalability

Any identity solution should be able to accommodate the increasing demand of a sovereign identity required for a large number of users, organisations and entities. This will determine the effectiveness of an SSI solution with respect to significant proliferation in digital entities in cyberspace.

IV. uPort and Sovrin Self-Sovereign Identity

A. uPort Self-Sovereign Identity

uPort is an open source framework for delivering a decentralized identity for a self-sovereign identity. Based on the public permissionless blockchain Ethereum and utilising its smart contracts [5]. A smart contract is a program written to automatically observe, accomplish and implement an agreement. Employing this framework, users can securely publish their identity including transferring their credentials, sign transactions and control their keys and data. A uPort identity can be created for users, organisations, and other resources. The identity is completely owned and governed by the owner

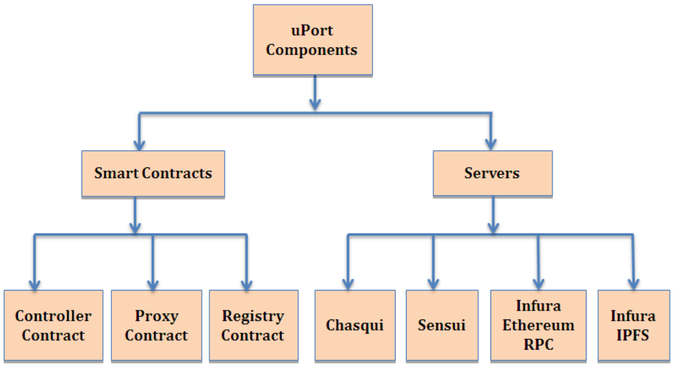

Fig. 6. uPort SSI Components

of that identity and not by the third-party. Additionally, all identity related personal and confidential data is held by the owner in their digital wallet thus, information releases are kept to a minimum [16]. The components of the uPort system are as follows [5]:

1) Smart Contract Components:

Controller Contract: It is the overall control logic with the functionality of controlling the access to the proxy contract. Furthermore, it allows the user to reclaim their identity if the user loses their mobile and private key. It maintains a list of recovery delegates (e.g. selected family members, friends or institutions) who can assist the user to regain their uPort identity.

Proxy Contract: It is the permanent identifier of a user linked with the private key of the user, therefore, it allows the user to replace their private key without affecting their permanent identity.

Registry Contract: It offers a cryptographic link between a uPort identifier and its data attributes or profile data stored off-blockchain (e.g. InterPlanetary File System (IPFS)). IPFS is a peer-to-peer protocol for storing and retrieving data on a distributed file system. The proxy contract can only update the Registry contract.

2) Server Components:

Chasqui: The Message Server manages all aspects of communications with any decentralized app and mobile app.

Sensui: The Gas Fuelling Server avoids the requirement of a new Ethereum user to purchase Ether and paying fees to use the network. It pays the gas fees for the new user allowing them to create a new uPort account instantly.

Infura Ethereum RPC: This Infura API provides a standard RPC interface to allow uPort to communicate with the Ethereum network.

Infura IPFS: The Infura API provides a standard interface to allow uPort to communicate with the IPFS network.

B. Sovrin Self-Sovereign Identity

Sovrin is an open source framework for delivering a decentralized identity for SSI. It is based on the public permissioned blockchain Hyperledger Indy. As it is a permissioned blockchain, therefore, only trusted institutions called stewards can operate nodes while participating in the consensus process. Utilising this framework, users can securely publish their identity including transfer their credentials, sign transactions and control their keys and data. A Sovrin identity can be created for users, organisations, and other resources. Sovrin allows users to create a different identity with its own pair of private and public keys for different contexts to maintain confidentiality. A user determines the type of attributes to be associated with their identity. It uses anonymous credentials based on Zero Knowledge Proofs (ZKPs), a cryptographic method, to keep a user's identities anonymous. The identity is completely owned by the owner of that identity and managed by the user or users appointed guardian service. Furthermore, all identity related personal and confidential data is held by the owner in their digital wallet on the edge or cloud. Components of the Sovrin system are as follows [17]:

1) Sovrin Agents:

A Sovrin Agent is a program required for an identity owner or any other participating entity to interact with each other in the SSI process. Agents work in a peer-to-peer model and share DID and other credentials with each other. They do not require access to blockchain and communicate thorough signed and encrypted messages. Each Agent accesses the wallet and performs cryptographic functions for that entity.

Edge Agent: This agent is hosted on the user's device (edge of the network) such as mobiles, tablets or laptops. This agent may be connected to another app and accesses a wallet containing keys and credentials, performing cryptographic functions for that entity.

Cloud Agent: This agent is hosted on the cloud which is not directly controlled by an identity owner. The edge agent communicates with cloud agent that runs 24x7 and offers a store and forward service to route requests to and from the edge agent.

2) Sovrin Nodes:

A node is a server that runs an instance of the code required to operate a ledger. A node can either be a validator node or an observer node; however, it can only act one at a time.

Observer Node: This node runs the read only instance of the ledger. Anyone can run this node in any numbers; however, its response can be verified by State Proofs.

Validator Node: This node validates all new transactions and writes to the ledger based on the consensus protocol. A steward runs one validator node at a time.

3) Sovrin Ledgers:

It is a distributed ledger for maintaining the records of different types of transactions.

Config Ledger: This is a special ledger for recording transactions related to the configuration of a ledger. It is not public writeable and only Sovrin trustees or their delegates can write to this ledger.

Node Ledger: This ledger is for recording transactions related to identification of authorized nodes. This ledger is public readable but not public writeable and only trustees or stewards can write to this ledger.

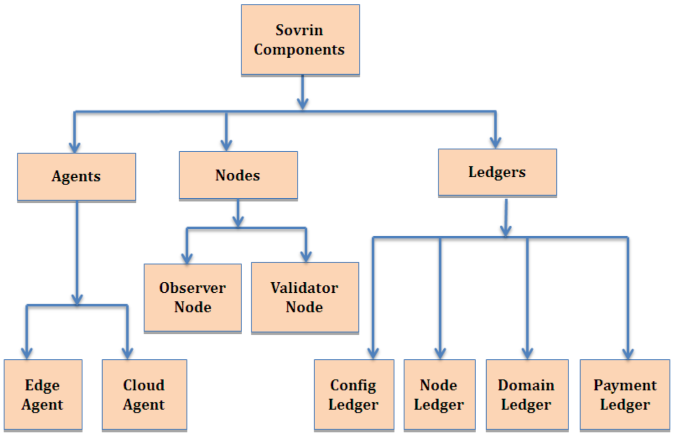

Fig. 7. Sovrin SSI Components

Domain Ledger: This ledger is for recording transactions related to identity management (except payments). This ledger is public readable and public writeable based on the protection method of the Sovrin Governance Framework [18].

Payment Ledger: This ledger is for recording transactions related to payments. It is public readable and public writeable based on the public write access method of the Sovrin Governance Framework [18].

V. Comparative Evaluation of uPort and Sovrin Based on the Proposed specifications

Table I displays the comparative evaluation of uPort and Sovrin SSI solutions based on the proposed SSI specifications. This comparative evaluation shows that both uPort and Sovrin satisfy the major SSI specifications of sovereignty, storage-control, longevity and verifiability which are fundamental requirements for SSI solutions. Furthermore, they support recovery, cost-free, security, privacy, safeguard and accessibility specifications, however, their degree of support varies with each specification for example Sovrin presently offers greater security and privacy features, whilst the uPort design architecture is simple and easy to use. The crucial commercial and operational specifications of availability, transparency, portability and interoperability are yet to fulfilled completely by uPort and Sovrin in order to establish them as a mature SSI solution. As SSI is an emerging IDM model and uPort and Sovrin are emerging SSI solutions, therefore, the successful implementation of these commercial and operational specifications require the development and adaptation of a set of common protocols and standards provided by standard organisations such as the Decentralized Identity Foundation (DIF), the World Wide Web Consortium (W3C) and the Organisation for the Advancement of Structured Information Standards (OASIS). Presently, the scalability specification is one of the important implementation issues for both uPort and Sovrin, currently being resolved by employing various design optimisation techniques to fulfil the growing demands of sovereign identity globally.

VI. Conclusion

This paper proposed necessary specifications for evaluating emerging SSI solutions. Subsequently, it analysed two emerging SSI solutions uPort and Sovrin including their architecture, components and working. Finally, this paper evaluated both uPort and Sovrin SSI solutions to ascertain whether they comply with the proposed SSI specifications, highlighting their strengths and limitations. In future, the security aspects of these two SSI solutions would be analysed. Furthermore, it is worthwhile analysing some other emerging SSI solutions based on the proposed SSI specifications.

References

[1] P. Windley. (2017) Fixing the five problems of internet identity. [Online]. Available: https://www.windley.com/archives/2017/10/fixing_the_five_problems_of_internet_identity.shtml

[2] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *The Sovrin Foundation*, vol. 29, 2016.

[3] N. Naik and P. Jenkins, "A secure mobile cloud identity: Criteria for effective identity and access management standards," in *2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud 2016)*. IEEE, 2016.

[4] ——, "Securing digital identities in the cloud by selecting an apposite federated identity management from SAML, OAuth and OpenID Connect," in *11th International Conference on Research Challenges in Information Science (RCIS)*. IEEE, 2017, pp. 163–174.

[5] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena. (2018) Uport: A platform for self-sovereign identity. [Online]. Available: https://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf

[6] Sovrin.org. (2018) Sovrin: A protocol and token for self-sovereign identity and decentralized trust. [Online]. Available: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

[7] T. Ruff. (2018) The three models of digital identity relationships. [Online]. Available: https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186

[8] N. Naik and P. Jenkins, "An analysis of open standard identity protocols in cloud computing security paradigm," in *14th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2016)*. IEEE, 2016.

[9] N. Naik, P. Jenkins, and D. Newell, "Choice of suitable identity and access management standards for mobile computing and communication," in *2017 24th International Conference on Telecommunications (ICT)*. IEEE, 2017, pp. 1–6.

[10] W3C. (2019) Verifiable Credentials data model 1.0. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[11] ——. (2019) A primer for Decentralized Identifiers. [Online]. Available: https://w3c-ccg.github.io/did-primer/

[12] Sovrin.org. (2018) Sovrin: A protocol and token for self-sovereign identity and decentralized trust. [Online]. Available: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

[13] K. Cameron, "The laws of identity," *Microsoft Corp*, vol. 12, pp. 8–11, 2005.

[14] C. Allen. (2016) Self-sovereign identity principles. [Online]. Available: https://github.com/ChristopherA/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md

[15] M. Graglia, C. Mellon, and T. Robustelli. (2018) The nail finds a hammer self-sovereign identity, design principles, and property rights in the developing world. [Online]. Available: https://www.newamerica.org/future-property-rights/reports/nail-finds-hammer/

[16] M. Sena. (2018) Privacy preserving identity system for Ethereum dApps. [Online]. Available: https://medium.com/uport/privacy-preserving-identity-system-for-ethereum-dapps-a3352d1a93e8

[17] Sovrin.org. (2019) Sovrin Glossary V2. [Online]. Available: https://sovrin.org/wp-content/uploads/Sovrin-Glossary-V2.pdf

[18] ——. (2019) Sovrin Governance Framework. [Online]. Available: https://sovrin.org/library/sovrin-governance-framework/

TABLE I
COMPARATIVE EVALUATION OF UPORT AND SOVRIN SELF-SOVEREIGN IDENTITY SOLUTIONS BASED ON THE PROPOSED SPECIFICATIONS

Specifications	**uPort**	**Sovrin**
1. Sovereignty	It is a self-sovereign identity.	It is a self-sovereign identity.
2. Storage-Control	Identity and its associated personal and confidential data is stored in the Digital Wallet at the device owned and controlled by the identity owner.	Identity and its associated personal and confidential data is stored in the Edge Wallet at the device of Edge Agent controlled by the identity owner; It may be stored in the Cloud Wallet at the device of Cloud Agent (protected from unauthorized access).
3. Longevity	It utilises Decentralized Identifiers (DIDs).	It utilises Decentralized Identifiers (DIDs).
4. Verifiability	It utilises Verifiable Credentials (VCs).	It utilises Verifiable Credentials (VCs).
5. Recovery	Social Recovery Method: Recovery Delegates (e.g. selected family members, friends or institutions) nominated by an identity owner, who can assist the user to regain its uPort identity.	Social Recovery Method: Recovery Key Trustees trusted by the identity owner store recovery data on their own agents on the behalf of an identity owner and help them to recover their identity.
6. Cost-Free	Presently identity is free for users, however, all transactions have an inherent cost.	Presently identity is free for users, and no financial cost to identity transactions.
7. Security	It requires a PIN/Password and Biometry for controlling identity through blockchain. Users can securely publish their identity including transfer their credentials, sign transactions and control their keys and data.	It requires a PIN/Password and Biometry for controlling identity through blockchain. Users can securely publish their identity including transfer their credentials, sign transactions and control their keys and data using powerful cryptography.
8. Privacy	It is a Privacy Preserving. Users do not need to disclose personal data in order to create uPort identifiers for low value accounts. It uses various methods to minimize the correlation of a users on-chain smart contract interactions between different dapps.	It is a Privacy by Design and Privacy by Default. It uses anonymous credentials based on Zero-Knowledge Proofs (ZKPs), which allows users to share the information that maintain the anonymity of users.
9. Safeguard	Users right to privacy should be protected.	Users right to privacy should be protected.
10. Accessibility	Simple design architecture and easy to use. At present it has no provision of a Guardian/Agent.	Complex design architecture and some users might require a Guardian to manage the identity on their behalf.
11. Availability	Users should require their smart-phone to manage their identity.	Users should require smart-phone but not necessarily its ownership.
12. Transparency	It is based on open standards and open source projects.	It is based on open standards and open source projects.
13. Portability	It is limited, however, uPort is using several open standards to make it portable, e.g., Verifiable Credential (VC) and Decentralized IDentifier (DID).	It is limited, however, Sovrin is using several open standards to make it portable, e.g., Verifiable Credential (VC) and Decentralized IDentifier (DID).
14. Interoperability	Presently it is evolving, therefore, it requires a further alignment with other SSI solutions.	Presently it is evolving, therefore, it requires a further alignment with other SSI solutions.
15. Scalability	It is limited. The public Ethereum blockchain can process nearly 15 transactions per second. It is resolving this by avoiding creation of multiple smart contracts on the blockchain and letting users to create Ethereum key pair.	It is limited. It is resolving this by using two rings of nodes: a ring of validator nodes to accept write transactions, and a much bigger ring of observer nodes to run read-only copies of the blockchain to process read requests.