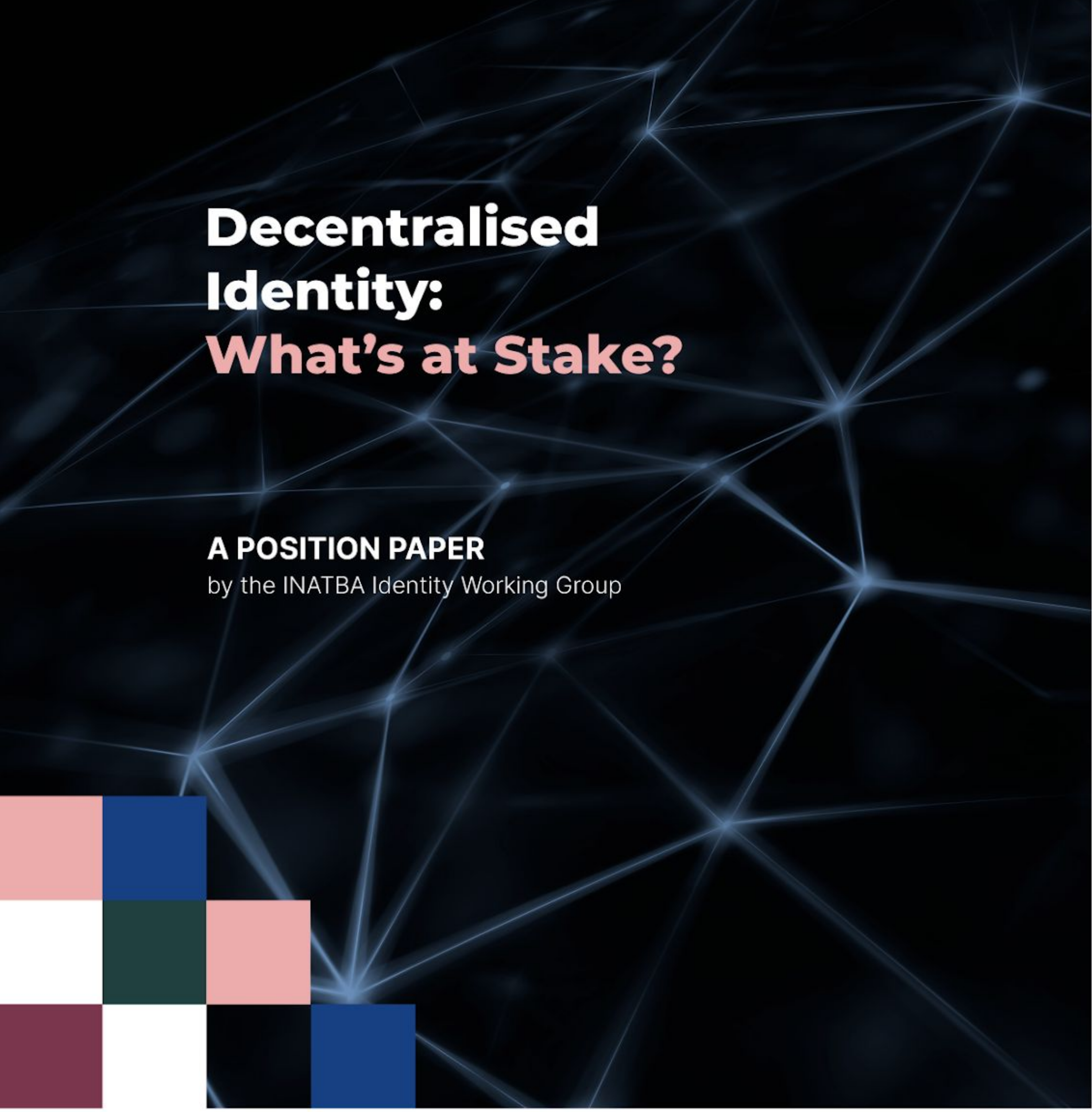


Decentralised Identity: What's at Stake?

A POSITION PAPER

by the INATBA Identity Working Group

International Association for
Trusted Blockchain Applications

NOVEMBER 2020

Authors

Kai Wagner (Jolocom)

Xavier Vila Pueyo (Validated ID)

Nathan Vandy (Blockchain Helix)

Daniel Bachenheimer (Accenture)

Dominik Beron (Danube Tech)

Contributors and Reviewers

Michelle Leech (Tendermint)

Catarina Veloso (Trust Fractal)

Oliver Naegele (Blockchain Helix)

Wim Stalmans (Infrachain)

Edilson Osorio Junior (OriginalMy)

Hervé Bonazzi (Archipels)

Joachim Lohkamp (Bundesverband Blockchain)

Gerrit Steinfort (IBM)

Emiliyan Enev (ReCheck)

Gustavo Prieto (University of Turin) — INATBA AAB

Roberto García (Universitat de Lleida) — INATBA AAB

Table of contents

Abstract

This position paper introduces a scenario-based approach to depict possible futures of digital identity in order to contribute to the important debate on how to best govern the new, highly disruptive approach to digital identity: self-sovereign identity.

Unlike other papers that address self-sovereign identity from a technological perspective, this paper emphasises the need to look beyond questions of technical feasibility. It is necessary to address the questions of political and economic power that are emerging alongside the steady adoption of this new identity model.

We do this by introducing the evolutionary steps that have led to the development of self-sovereign Identity, outlining previous promises and analysing the realities that have since emerged. In examining the potential of self-sovereign identity and its anticipated positive effects, we highlight critical questions that will determine whether this form of identity can reach its projected potential. To contextualise this debate, we provide an overview of the four core work areas that currently characterise the discussion on self-sovereign Identity.

Finally, we invite the community to engage in this discussion, which we perceive as an important aspect of our shared responsibility.

Introduction

This position paper is published by the Identity Working Group of INATBA, intended to contribute to the development of self-sovereign identity and recognition of its regulatory, business and technical realities.

INATBA is exceptionally well-positioned to address the explicit and sometimes implicit challenges surrounding the development and adoption of decentralised identity in its role as a global platform for dialogue between regulators, academics and business stakeholders.

Self-sovereign identity (SSI) is considered the next evolutionary step in the development of digital identities. At a time where the digitisation of our private, public and economic lives is becoming increasingly relevant, digital identity is not solely a question of technological innovation but also requires consideration of political and economic power. Self-sovereign identity puts the individual structurally in control of their own verifiable identity attributes, issued by one or more trusted entities, from which they may selectively disclose information required to access a service. Under informed consent, the information shared can be cryptographically verified to determine its authenticity and integrity without the need to revert back to the issuer or any centralised authority. With an emerging generation of technology produced to disrupt the existing digital identity market, regulators need to find new answers to questions of political and economic power raised by adopting self-sovereign identity.

Our position paper is written by experts and practitioners from the decentralised identity community. It has been reviewed by a diverse set of INATBA member organisations that work on decentralised identity, as well as by members of INATBA's academic advisory body.

This position paper consists of three sections, preceded by a call to action that highlights the most important points to consider when conceptualising the ideal scenario for self-sovereign identity to be implemented. The first section provides an overview of the evolution from centralised identity to decentralised and self-sovereign identity. The second section indicates the benefits of SSI, its current status, and possible future scenarios. Finally, the third section presents areas that require further attention and development for the ultimately successful implementation of self-sovereign identity.

We hope that this paper will expand the debate on self-sovereign identity beyond its technological feasibility and help the identity field move toward addressing the challenging task of balancing the benefits of this technology with its risks. This task needs to be collectively addressed by regulators, scientists, civil society representatives and businesses. We are ready to engage in this work and look forward to leveraging our full capacity to make this process possible.

Call to Action

Aiming to ensure a safe and accountable introduction of self-sovereign identity into people's everyday lives, in Section 3, we describe various topics spanning four work areas that need to be addressed. These can be found at the end of each of the Work area sub-chapters under the label "Path Forward". Below, we highlight the most important points that need to be addressed to achieve the ideal scenario for implementation of self-sovereign identity (later described in Section 2.3).

- Self-sovereign identity must be regulated in a technologically-agnostic way that ensures a fair distribution of power and liability for all included parties.
- Open standards and specifications are needed to create an innovative and competitive market that does not hinder innovation with vendor lock-in and patent restrictions.
- An agreement must be reached on which SSI building blocks are to be standardised and thus made interoperable. Organisations involved in this process need to ensure transparency and provide access to these discussions and decision-making processes.
- Many of SSI's positive outcomes can only be achieved if the reuse of credentials across sectors is realised (Credential Roaming). Reusable Credentials are technically possible, but Credential Roaming has not reached widespread adoption due to a lack of regulatory clarity.
- Data protection and privacy standards must not be eroded. SSI enables the digitisation and utilisation of additional personal data. A predictable regulatory regime on what identity and personal data can be shared with third parties and how individuals can be protected from its misuse must be created (e.g., GDPR).
- Privacy and data protection regulations are instrumental in ensuring that the currently uneven power relation between identity holders and parties that request data (verifiers) can be structured to protect "personal data" and "sensitive personal data" (e.g., biometric characteristics and health information).
- Regulators should encourage and promote the certification of products, services and processes in line with existing (cyber)security certification schemes and support the creation/consolidation of these standards if not yet in existence.
- Relevant agencies should update their recommendations and guidelines, taking into account all new protocols and algorithms being proposed as de facto standards in self-sovereign identity ecosystems.
- SSI implementers should follow best practices when using cryptography, privileging thoroughly tested algorithms and protocol implementations, conducting risk assessments, and implementing risk management processes that use an Information Security Management System wherever possible.

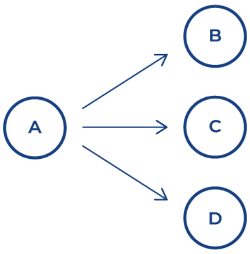
1. From Centralised to Self-Sovereign Digital Identity

Identity can be defined in many different ways, especially when viewed from a "digital identity" perspective. For the purpose of this document, we use identity to refer to "digital identity" defined as the collection of attributes and information about an entity that is used to represent and distinguish the entity in an interaction with the outside world. More specifically, identity refers to what actors look for in the representation of an entity to recognise such an entity as being unique or matching existing criteria.

The history of digital identity can be traced back to the 1960s or even earlier; however, this position paper focuses on more recent history, starting with the advent of the internet in the 1990s.

1.1. Centralised Identity

With the introduction of online interactions and transactions, it became clear that users needed some form of digital identity. Usually, this consisted of a personalised account created for individual users. A user account included associated credentials (typically a username and password) and other information relevant to the interactions and transactions they were authorised to take.

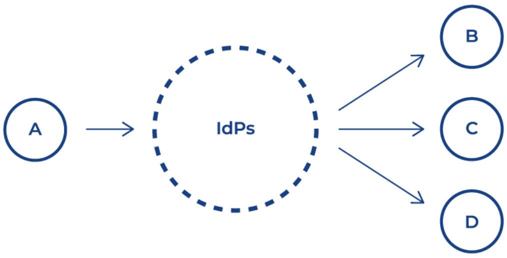


This identity model is organised by those who want to exclusively connect subjects to organisations (employees, customers, etc.). This makes it naturally centralised, with few or no incentives to share data or collaborate between database organisers and owners.

1.2. Federated & User-Centric Identity

There are numerous downsides to centralised identity management, including security vulnerabilities (e.g., most people reuse passwords) and usability challenges (inconvenience of creating and handling a great number of accounts each with its own username and password). Further examples are later detailed in Section 1.3: Limitations & Challenges of Centralised & Federated Identity.

Given the negative aspects associated with centralised identity management, a new approach emerged within the past ten years: federated and user-centric identity. The core idea behind these approaches was to allow individuals to use the same credentials to access services on different sites (separate entities). Following the first initiatives in this field (e.g., Microsoft Passport, Liberty Alliance), the main form of innovation was to introduce so-called "Identity Providers" (IdPs) — trusted authorities that handle user's identity data and accounts. As a result, users do not have to manually create separate accounts with unique usernames and passwords. Instead, users can click a single button and let an IdP manage their information.



In theory, this reduces data duplication, as well as produces fewer security vulnerabilities and higher convenience. Examples include:

- OpenID
- OpenID Connect
- OAuth
- FIDO.

1.3. Limitations of Centralised & Federated Identity

Centralised identity

Centralised identity poses a number of limitations. When users create accounts on separate websites, users store a small part of their digital identity in the databases of these websites and service providers. Consequently, digital identities become fragmented and locked into numerous different databases (data silos) controlled by multiple external third parties. Centralised models that are less fragmented, such as social media platforms or health- and financial services repositories, are target-rich and considered "honey pots" for fraudsters. To summarise, individual entities do not have control over their own data in centralised identity forms; neither the identifiers used to create and access user accounts (e.g., email addresses, phone numbers) nor the actual identity data are stored within these data silos.

Federated identity

The emergence of this new approach to digital identity was supported by the rise of popular platforms that hold large quantities of identity data, such as Facebook, Twitter or Google. However, a number of privacy and security scandals revealed lax data protection practices and diminished user trust in IdPs. Without such trust, Federated Identity loses its foundation.

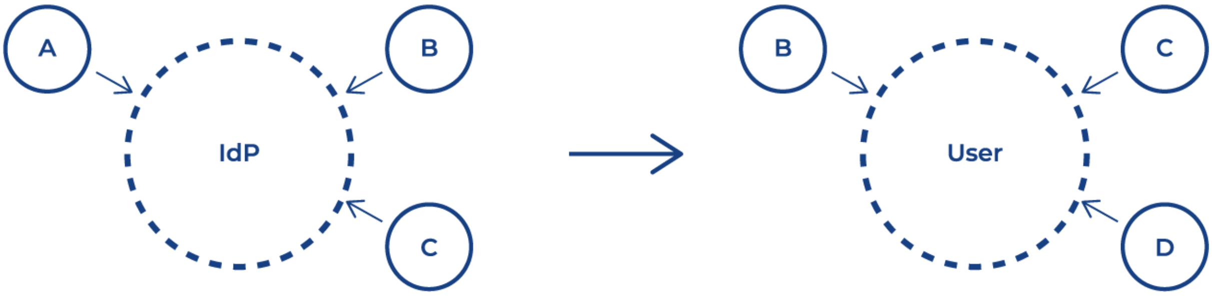
Therefore, the design of current digital identity solutions pose many challenges:

- **Data Acquisition:** Acquiring data is labor-intensive, inconvenient and expensive for both service providers and their users.
- **Data Quality:** Current data acquisition methods often result in suboptimal quality data sets due to either unintentional errors or fraudulent declarations.
- **Data Maintenance:** Most data changes over time (e.g., address, permits, etc.) demand regular updates, making maintenance tedious and expensive.
- **Data Processing:** Service providers often rely on time-consuming, error prone, and manual methods for data processing and verification.
- **Security & Fraud:** Current (paper-based) credentials are often not sufficiently resistant against counterfeiting or fraud. Data verification (integrity, validity, origin) is difficult, expensive and slow (e.g., due to intermediaries).

- **Data Control & Privacy:** The centralised or federated design of current data infrastructures is responsible for the lack of control users have over their data.
- **Data Silos:** Service providers often lack access to data that could facilitate their work and create value for users as data is stored and managed by a central authority that is not the user.
- **Limitations of Current Solutions:** Current systems have a limited scope and cannot support digital identities that represent users in all facets of their lives. The eIDAS framework, for example, covers only a minimum data set for identification and authentication.

1.4. The Evolution of Self-Sovereign Identity

A new approach toward digital identity is gaining momentum: Self-Sovereign Identity[1] (SSI). SSI promises increased individual control over data. Instead of manually creating and handling accounts (Centralised Identity) or trusting IdPs (Federated Identity), SSI centers the individual at each of their digital interactions. This approach is explored more concretely in the following sections.



2. SSI Vision

Self-sovereign identity is more than a combination of existing technological innovations. It is a new way of thinking about digital identity, rooted in the principle that individuals should be in control of their digital identity and its associated data.

However, SSI is not only driven by privacy and data protection advocates. Organisations across multiple sectors and industries are discovering its unique capabilities. SSI bears the potential to solve some of the biggest digitisation challenges we face today — and SSI advocates are ever-increasing.

2.1. Values & Benefits of SSI

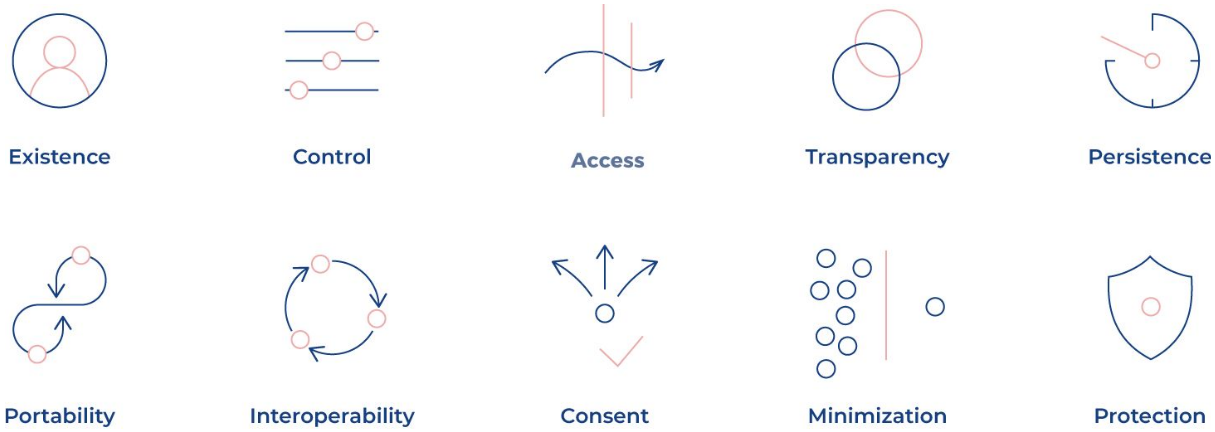
The most paramount value of SSI is returning ownership of digital identity back to the individual, allowing them to control the core functions of their identity

[1] We use self-sovereign identity (SSI) as a term to describe this new approach to digital identity, as it is the most common and also widely agreed upon term to date. Other terms that might refer to the same concepts are: *decentralised identity, self-managed identity, portable identity,* and many more. With this terminology still being debated, we highlight the need to focus on its definition and capabilities mentioned in the ideal scenario (Section 2.3) to distinguish different concepts.

(cryptographic keys). This change in ownership represents a paradigm shift in the way society experiences digitised life — the potential of storing attested identity data in a standardised format with the user should not be undervalued.

SSI creates a portable identity that individuals can use for almost all online processes, from simple authentication requests with one credential (e.g., service log in), to some of the most complex tasks like the sharing of curated identity data for more complex requests (e.g., filling out forms digitally).

Built on open standards and specifications, the emerging ecosystem of SSI modules (wallets, agents, hubs, SSI-services, SDKs, etc.) holds the potential to be interoperable.[2] This creates a coopetitive market environment where identity subjects can freely interact with service providers whose SSI modules may be from different technology vendors, even transitioning from one vendor solution to another without losing control over their data (portability).



Design by Iryna Nezhynska from Jolocom GmbH based on a concept by Christopher Allen

Benefits for Individuals

1. **Control:** Individuals have control over the existence of their digital identity and its associated identity data (e.g., cryptographic keys, storage, consent management and request for deletion and rectification of data).
2. **Privacy & Individual Rights:** SSI offers new ways to enhance privacy and improve enforcement of individual rights, such as granular consent management and data minimisation techniques that enable individuals to provide only the data they want to share (e.g., Pairwise Identifiers, Selective Disclosure & Zero-Knowledge Proofs).
3. **Convenience:** Interactions and transactions are more convenient due to standardised digital credentials that can be used for all interactions and maintained in one place.
4. **Security:** SSI increases data security and helps to prevent identity theft and other forms of fraud by implementing widespread encryption. Decentralised storage and management of identity attributes also significantly increase the relative cost of hacking.

[2] See scenarios in Section 2.3.

5. **Prevention of Lock-in:** By empowering individuals to control and store their identity data on their terms, lock-in effects, such as those associated with current Federated Identity solutions, can be prevented. This empowerment also has important implications for identity and data portability. The ability to move between services creates innovative competition, and individual digital identities become more resilient.
6. **Independence & Resilience:** Management of digital identity in a decentralised manner, with each user in control over their data, allows individuals to become more independent from service providers as providers no longer offer an identity but only added services.
7. **Cost Savings & Personalisation:** The ability to disclose trusted, verifiable identity attributes can significantly reduce the cost of onboarding in terms of time and expense. Service providers can also tailor services based on the verifiable information provided.

Benefits for Organisations

While individual users are often the central focus of SSI projects, organisations (legal entities) benefit on an equal scale from moving to SSI-based interactions. Our working group has collected significant motivations for the shift toward SSI from the private and public sector. The list is based on global SSI projects in which our members have been actively involved:

1. **Increase Data Quality, Availability & Interoperability:** SSI aims to dismantle data silos by making data directly available to its associated users. Thus, service providers can directly interact with users to obtain relevant data.
2. **Improve Service & Product Delivery:** By facilitating data acquisition (across organisations) and improving data availability, quality and processing, SSI enables improvements of services, products and delivery to users.
3. **Transform Interactions:** SSI facilitates access to products and services and improves the efficiency of experiences.
4. **Digitise & Automate Processes:** Many processes are not sufficiently digitised and the lack of interoperability between systems makes the progressive automation of processes unfeasible. SSI can change that by making identity attributes available in a digital format that can be reused in different contexts.
5. **Security & Fraud Prevention:** SSI has strong security properties due to its usage of cryptography (e.g., signatures & hashes), which makes fraud and counterfeiting more difficult.
6. **Save Costs:** SSI can significantly improve the efficiency and effectiveness of processes, consequently reducing operational costs (e.g., data processing, verification). Users can streamline onboarding and authorisation processes as an attribute store will no longer be required due to the individual being able to provide verifiable identity attributes needed for authorisation such as diplomas, qualifications, clearance levels, etc.

7. **Privacy & Compliance by Design:** As users are put in control of data, SSI is an elegant system designed in the spirit of current data protection regulations. That being said, not every SSI approach, particularly not every Blockchain application, is in compliance with certain rights established by GDPR and similar data protection regulation.
8. **Awareness & Perception:** Since users increasingly value privacy, giving them control over data can positively affect the perception of both governments and businesses using SSI.
9. **Decrease System Complexity:** SSI enables a universal infrastructure for digital identity which can potentially be used for any kind of identity data. This eliminates the need for individual systems that are limited to different contexts and lack interoperability.
10. **Unlock Innovation:** SSI enables people and organisations to exchange all kinds of data that service providers can use to improve existing applications and products or develop entirely new ones.

Establishing trust in SSI interactions

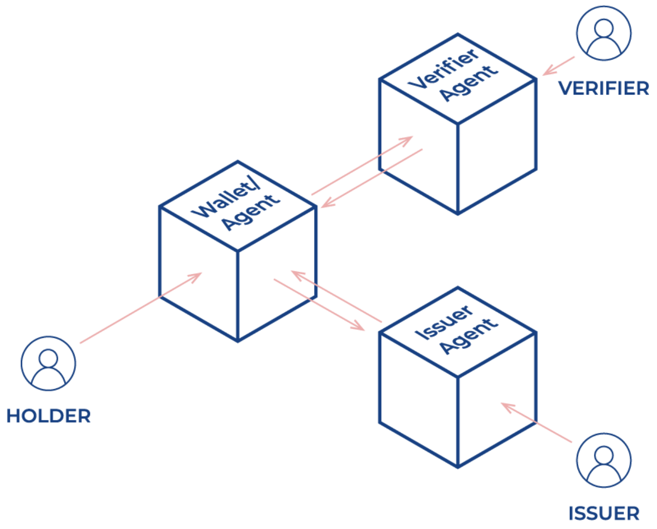
Each interaction authentication and identification using the SSI model relies on three roles (that can be realised by less or more than three actors).

Issuers, including public authorities or businesses that act as Trust Services, can attest identity data (Attributes, Credentials & Claims), issue it directly to associated entities ("Identity Holders") and revoke previously issued identity data if necessary;

Identity Holders control the existence of identity data, most importantly cryptographic keys, and decide what identity data is stored, as well as storage location and means. They can selectively share the identity data required for service with third parties ("Verifiers").

Verifiers can reliably verify identity data, usually without consulting another party,[3] to establish trust and transact. Because Verifiers process identity information, it is also recommended they are part of a trust framework.

[3] With trust of the identity being mostly dependent on the issuer, many use cases will likely require some kind of "Trusted Lists" in order to be able to trust an Issuer. Trust Frameworks that tackle this challenge are currently under development by governments (eg. European Self-sovereign Identity Framework [ESSIF], Pan Canadian Trust Framework, etc.) and private organisations (eg. FINDY, ToIP Foundation).



This Trust model has dominated the history of identification from the time societies moved from word-of-mouth reputation schemes to accepting authoritative documents (Passports, Sealed Letters, etc.). While the authoritative document is under the full control of its holder (who can decide whether to share it or not), it is accepted by counterparties only because its issuer can be trusted. This model creates a well-balanced division of powers, with the issuers having the ability to determine what they are willing to vouch for, and identity holders having the power to independently and autonomously determine whether and how to make use of that tool without having to trust and rely on a middle man or service to act on their behalf.

2.2. SSI Today — What Has Been Achieved

The term self-sovereign identity was popularised in a 2016 blog post made by Christopher Allen.[4] Although the discussion on building digital identity systems that put user-control first dates back well into the early 2000s, the SSI community has widely cited Allen's blog post as kick-starting the development of a shared vision for a self-controlled portable digital identity.

In the years following Allen's blog post, progress has been significant within the global SSI community, with countless startups,[5] corporations, non-profits, business associations and even governments working on conceptualising SSI. Today, there is a diverse community dedicated to working on SSI solutions, ranging from actors building all-encompassing ecosystems to specialist organisations that tackle specific questions such as key-management, zero-knowledge proof based interactions or credential governance.

The merger of substantial development activity, investment and shared principles create an environment where coordination is essential to SSI proliferation. Currently, an interoperability-conundrum is developing. Many organisations work on implementing the SSI vision and search competitively to find the best solution

[4] http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (accessed 22nd November 2020).

[5] As of 21 October 2020, a major Industry Association for SSI founded in 2017 'Decentralised Identity Foundation' has 174 member organisations.

to specific SSI-sub-components. As the latter presents complex compatibility issues, such as every line of code written to solve a problem creating path-dependencies and conflicting interests, counter-incentives might stifle or even obstruct convergence toward overall interoperability.

Consequently, coordination is essential for SSI adoption. Below, we present a scenario-based approach to describe the very different realities that might emerge in the SSI space due to the need for coordination in the sector. Ultimately, the community's ability and interest to cooperate and coordinate will determine which scenario will become a reality.

2.3. SSI in the Future — What's at Stake

I. Ideal Scenario

Full convergence on the core stack with by-default interoperability

Aiming to fully realise the values and Benefits of SSI described in the previous chapter, the SSI community will have to focus its coordination effort on achieving the following capabilities for SSI technology, its associated business models and the relevant regulation:

- As an **Issuer/Verifier**, I can present a standardised interface to request interactions, regardless of what wallet/agent is on the other end.
- As an **Identity Subject/Holder**, I can use any wallet/agent I want. I can seamlessly move my identity across wallets/agents, including encrypted backups, mobile devices, browsers, etc.
- As an **Identity Subject/Holder**, I can determine if a Verifier is trustworthy based on their public key being verifiable without an intermediary.
- As an **Identity Holder**, I can present a Verifiable Credential to a Verifier, regardless of the implementation the verifier or issuer uses, and the wallet/agent I use. (Identity networks/registries need to respect this capability through public readability).
- As a **Verifier**, I can resolve DIDs from any DID method and use the DID Document to verify signatures, regardless of the DID method.
- As a **Verifier**, I can check the integrity of the Verifiable Credential regardless of the implementation method used by the issuer of the credential, format and structure of the data or holder.
- As a **Developer**, I can use any implementation of SSI tools (i.e., libraries, API's, CLI tools) and expect it to perform its function with other deployments.

Multi-layered cooperation and coordination of the SSI stack is required to realise this scenario and achieve by-default interoperability between SSI modules, creating an ecosystem that is fully open to participants who follow the standards and specifications. Currently, the Decentralised Identity Foundation, several W3C working groups, and projects such as the European Self-sovereign Identity Framework (EBSI—ESSIF) and activities in the USA's Silicon Valley Innovation Programme (SVIP) are working in this direction.

II. Functional Scenario

Partial convergence on the core stack with detached ecosystems

Considering the high cost of coordination required to achieve Scenario 1 as well as the presently existing path dependencies created by SSI projects (via their external commitments to customers, as well as dependence on particular monetisation models & communities, blockchain networks, etc.) another outcome is possible: the functional scenario. The latter does not meet the expectations outlined in the 'Values & Benefits of SSI' section and fails to provide the full list of capabilities explicated above.

This type of scenario is best explained using the examples introduced by Anil John,[6] describing two primary outcomes of a functional scenario:

1. "A hub and spoke platform play where one platform or technology is required to mediate interactions between multiple, independent organisations. Often, the platform provider's service arm will work to onboard the organisation into its platform. The demonstration of interoperability requires the organisation to interact with all the other organisations connected to the platform using the platform's APIs or bespoke connectors. This is in no way demonstrates interoperability but is simply a 21st-century version of the enterprise service bus (ESB)."
2. "A subtly different approach is the requirement for each independent organisation to use the same technology stack. The demonstration of interoperability in this scenario tends to be multiple, independent organisations who have chosen the same technology stack, often with open source branding and associated technical governance, using well-documented APIs to showcase how they can all work together. This will work within that particular technical ecosystem, but this is software monoculture and not interoperability."

At this point in time, some sub-communities within the global SSI community are positioning themselves as proponents of this functional scenario. Unfortunately, this insufficient definition of interoperability does not acknowledge the full potential of SSI, but rather aims to create market dominance via infrastructural lock-in and high-cost interoperability.

Instead of an open ecosystem that is interoperable by default, this scenario requires continuous and active implementation between isolated systems, prompting market dynamics to favour larger platform providers. This will increase the risk of re-centralisation and a "winner-take-all" platform mindset, which SSI has aimed to avoid.

III. Dysfunctional Scenario

No convergence on the core stack leading to isolated vendor ecosystems with lock-in.

When it is not possible to achieve the full potential of SSI to create an alternative to the model of centralised and federated identity management, a third scenario

[6] https://www.cyberforge.com/illusion-of-interoperability/ (last checked 16 November 2020).

presents itself. The lack of coordination and convergence on vendor agnostic standards and specifications will result in a return to the status quo for digital identity. While some new technologies developed in the context of SSI will be implemented by the SSI community and made available in use cases (identity wallets, passwordless authentication, zero knowledge proofs), none of them will achieve the potential described in the section "Values & Benefits of SSI". Some SSI actors might be able to remain relevant within niche markets; however, their products will be comparable to centralised and federated identity systems that already exist and do not match SSI capabilities. Even worse, such a failure in coordination and convergence will lead to a situation where the currently dominant platforms in control of identity data will remain unchallenged.

3. Work areas

3.1. Interoperability & Standards

Introduction

In the context of SSI, interoperability means that individuals and organisations can use SSI in a vendor and technology-agnostic way. Technologies and applications should be interchangeable and compete based solely on their merit. To ensure merit-based competition, the industry requires agnostic SSI vendor and technology use — at least within the scope of relevant standards (e.g., Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs)). As described in the previous section, depending on individual preference, users should have the ability to choose which technologies (e.g., Blockchain, DID-Methods, VC/proof formats, protocols for data transfer and encryption) or applications (e.g., wallets) they use.

Interoperability is not only obligatory for the sake of end-users freedom of choice. It is also a necessity for SSI itself. Without interoperability, many of the challenges in digital identity management that are solved by SSI lose their effectiveness. Modular curation of digital identity across vendor systems and use cases and the full control of the identity subject (citizen/customer/organisation) are not possible in existing approaches to digital identity management.

"Interoperability is a characteristic of a product or system, whose interfaces are completely understood, to work with other products or systems, at present or in the future, in either implementation or access, without any restrictions."[7]

There are at least three dimensions to interoperability in SSI. This includes interoperability

- with existing systems ("Backwards-compatible")
- with new systems being developed using new technology
- with future systems (open for extension)

If SSI does not include interoperability, it will likely not achieve universal adoption, and the digital identity space will remain in a state of patchworked solutions and ecosystems.

[7] Source: http://interoperability-definition.info/en/ and Wikipedia.

Therefore, interoperability is vital and must be holistically conceptualised:

1. First, interoperability must be realised within existing systems to prevent "rip-and-replace", i.e., the necessity to replace systems in which organisations have already invested.
2. Second, interoperability must be realised within existing systems and applications to allow for their generalised use as platforms and growth accelerators. Instead of replacing existing applications and systems entirely, SSI may extend them to grow more quickly.
3. Third, interoperability must be realised to prevent technology and vendor-related lock-in, which makes it difficult or even impossible to switch service providers as system-migrations are intrinsically linked to significant investments and possibly the loss of data.
4. Fourth, interoperability must be realised to prevent "artificial" barriers between applications. Similar to the use of an external application to exchange email, it should not matter which SSI-based app one uses to exchange and utilise identity data.

"Interoperability implies open standards ab-initio, i.e., by definition. Interoperability implies exchanges between a range of products, or similar products from several different vendors, or even between past and future revisions of the same product. Interoperability may be developed post-facto, as a special measure between two products, while excluding the rest, by using open standards. When a vendor is forced to adapt its system to a dominant system that is not based on open standards, it is not interoperability but only compatibility."[8]

Where are we now?

Standardisation is a primary driver of interoperability. Currently, different cornerstone technologies of SSI are being standardised.

This includes:

- Decentralised Identifiers (DIDs): The World Wide Web Consortium (W3C) is working to standardise DIDs. A W3C Working Draft and a Draft Community Group Report exists.
- Verifiable Credentials (VCs): The World Wide Web Consortium (W3C) is working to standardise VCs. A W3C Recommendation exists.
- Protocols: There are existing protocols that may be used for SSI that already have high adoption levels (e.g., OpenID Connect). However, a number of new protocols are being created, which may emerge as new standards (e.g., DIDComm).
- Distributed Ledger Technologies (DLTs): Even though DLTs are not subject to formal standardisation in the field of identity, their understanding by market participants as well as their improvements and the emergence of new DLTs facilitates and increases their adoption for real-life use cases in the SSI space.

[8] Source: http://interoperability-definition.info/en/ and Wikipedia.

INATBA has a specific Standards Committee to liaison with relevant standardisation committees and bodies. Some relevant standardisation committee and bodies include:

- ISO/TC 307 "Blockchain and distributed ledger technologies"
- CEN/CENELEC JTC 19 "Blockchain and Distributed Ledger Technologies"
- Decentralised Identifiers (DIDs): https://w3c.github.io/did-core/
- DID Resolution: https://w3c-ccg.github.io/did-resolution/
- Verifiable Credentials (VCs): https://www.w3.org/TR/vc-data-model/
- "Issuer" und "Verifier" APIs: https://github.com/w3c-ccg/vc-issuer-http-api and https://github.com/w3c-ccg/vc-verifier-http-api
- Linked Data Vocabulary: https://digitalbazaar.github.io/citizenship-vocab/
- Credential Handler API: https://w3c-ccg.github.io/credential-handler-api/
- DID SIOP: https://identity.foundation/did-siop/
- DID Comm: https://github.com/decentralized-identity/didcomm-messaging
- Trust over IP Foundation: https://trustoverip.org

Barriers and Challenges

From a technology perspective, this means that interoperability is required on a level encompassing all cornerstone technologies:

1. **Decentralised Identifiers (DIDs):** DIDs are a new type of identifier solely created and controlled by individuals (i.e., independently of a central authority). They are usually stored on DLTs and can be resolved to a "DID Document" containing metadata (e.g., public keys, service endpoints, proofs). Different entities can use these to find and authenticate each other as DIDs establish a "Decentralised Public Key Infrastructure" (DPKI).

   Today, there is a growing number of "DID methods" (i.e., different implementations of DID specifications). Similar to DLTs, individual DID methods offer distinct advantages and disadvantages in terms of privacy, security, scalability, cost, performance, storage, etc.

2. **Verifiable Credentials (VCs):** SSI enables individuals and organisations to issue digital claims about themselves or others in a way that such claims can be re-used and reliably verified by others. Simply put, VCs are digital credentials that prove individual attributes (e.g., name, age, financial data, diplomas, work records, citizenship, memberships). They can be issued to an entity by "Issuers", stored and re-shared by this entity referred to as "Holders" and verified by any third party "Verifiers".[9]

[9] Currently, different data formats for VCs are being used (e.g., JSON-LD (with LD proofs or JWT proofs) or JSON (incl. Sovrin's "Anon Creds")) and each format has unique advantages and disadvantages (e.g., Sovrin's Anon Creds have native support for Zero-knowledge proofs; JWT are based on a mature, robust standard).

3. **Protocols:** Protocols are required to securely transfer VCs (and proofs) between different entities. For this purpose, transfers may utilise existing protocols. New protocols which are designed specifically for SSI are also emerging. Examples include DIDComm, Chapi, XDI, OpenID Connect and Solid.
4. **Distributed Ledger Technologies (DLTs):** DLTs play a vital role in SSI (e.g., registries for DIDs, revocation lists, or the notarisation of events). Every DLT offers different advantages and disadvantages that can make it more suitable for certain situations and less suitable for others.[10]
5. **Applications & APIs:** Apart from the lower-level SSI infrastructure (see above), there will likely be a significant number of SSI-based applications. Organisations will also need interfaces between their existing systems, SSI infrastructure components and SSI-based applications of different vendors.

Path Forward

Solving the interoperability challenge means finding a way to enable different solutions and applications to interoperate and leverage different lower-level technologies.

- An agreement must be reached on which SSI building blocks are to be standardised and thus interoperable by default.
  - Organisations involved in this process need to ensure transparency and access to the discussions and, ideally, the decision making processes.
  - Positive examples for such transparency and openness are W3C, DIF and EBSi-ESSIF (with stakeholder meetings co-organised by INATBA).
- Standardisation must be achieved via open standards and active collaboration among stakeholders rather than imposed by market domination, even if the dominant approach was open source.

3.2. Governance

Introduction

Governance, in the context of SSI, is the set of rules that defines how digital trust between any two peers is established and maintained — similar to how the Internet's TCP/IP standards ensure a network connection between any two peers. An overall Governance Framework will define business, legal and technical policies and outline the regulatory environment that satisfies each stakeholder's needs in the identity ecosystem. These policies are instrumental in establishing trust in the ecosystem, which aims to combine cryptographic assurance at the machine level and human trust at the business, legal, and social levels.

Digital identity is not solely a technological construct. The governance decisions and legal accountability are also essential elements in establishing the trust that underpins the identity ecosystems in which SSI can exist.

[10] For example, some DLTs may offer a high degree of immutability and transparency; some may offer sophisticated smart contracts, and others may allow for (non-technical) governance models due to their permissioned nature.

A Trust Framework is a key part of the Governance Framework that defines policies and the criteria and processes for assessing the conformance of different actors to these guidelines. Just as conformance assessments related to security policies and technology provide an understanding of how secure a system is, stakeholders need the Trust Framework to understand the level of trust expected from the identity ecosystem.

Where are we now?

Trust Frameworks were introduced to the digital identity sector very early on, with the eIDAS regulation for Digital Identity and Trust Services in the European Union and the Pan Canadian Trust Framework introduced in 2009 as preliminary examples. Multiple SSI-focused projects for Governance Frameworks have emerged in recent years, with one of the first originating from the Sovrin Foundation who established the Sovrin Governance Framework to define how its network operates. Comparable Frameworks that focus on the Governance of permissioned consortia networks have also been established in Finland (FINDY) and Germany (LISSI).

More recently, the "Trust over IP Foundation" was established in May 2020. It is a Linux Foundation Project with roots in the SSI community brought together by the Hyperledger Foundation. Its aim is to define models and interoperability standards for governance frameworks that enable business, legal, and social trust between entities implementing the Trust over IP architecture stack.[11] The openness and interoperability of this architecture stack will be a key aspect to watch as the organisation matures. Interoperability is the key to widespread adoption and may occur at various technology stack levels, including the ToIP stack shown below. For example, interoperability can be achieved at the wallet level if W3C Verifiable Credentials are exchanged using a data schema, security construct, and interchange protocol that actors define in a mutually agreed upon governance framework.

A more general and technology-agnostic focus is an underlying component of the European Self-Sovereign Identity Framework (ESSIF), an initiative within the European Blockchain Service Infrastructure (EBSI) that is driven by the European Blockchain Partnership (EBP) and the European Commission. This Governance Framework does not define the Network Governance alone but also aims to bring existing regulatory frameworks of the European Union (e.g., eIDAS and GDPR) into the development of SSI. Early progress toward this collaboration is evidenced in the recent study on bridging SSI and eIDAS published by ESSIF that includes an extensive legal report.[12]

[11] https://trustoverip.org/wp-content/uploads/sites/98/2020/05/toip_introduction_050520.pdf as currently defined in Hyperledger Aries RFC 0289 (or its successor as identified in the RFC document itself).

[12] https://joinup.ec.europa.eu/collection/ssi-eidas-bridge.

Barriers and Challenges

Governance requires all stakeholders in the ecosystem to agree on a set of rules and, in some cases, have a role in determining these rules. Governance includes deliberation as to which data schemes are used, who can create verifiable credentials, and who can verify verifiable credentials. The International Civil Aviation Organisation (ICAO) was established primarily to govern the development of globally interoperable identity documents, which requires coordination between representatives from nearly 200 sovereign nations to agree on how systems should select, store, secure and exchange data. Examples such as the eIDAS regulation show how technology-agnostic governance can function in the digital identity space. While such guidelines were not present during its creation, clear pathways have since been defined to connect SSI with the eIDAS regulations governance approach, situating Europe in an ideal position to benefit from SSI innovation immediately. To reap these benefits, regulators and implementing actors will need to collaborate closely in the coming years, focusing on bringing platform-agnostic decentralised identity to the Digital Single Market.

Unfortunately, not all countries and business environments can afford to take advantage of a harmonised Trust Framework. Even within Europe, actors will likely see the development of credential or use-case-specific Governance Frameworks. The above-described projects (ESSIF, Pan-Canadian Trust Framework, TOiP, etc.) are a solid starting point to overcome the hindrances mentioned above. They will only be successful if interoperability and accountability are also achieved.

Path Forward

Decentralised Digital Identity has garnered substantial interest over the past few years. To become a viable alternative to existing schemes, decentralised identity must achieve broad acceptance by public and private entities, as well as be perceived as interoperable, easy to implement and use, reliable, trusted and secure.

For SSI to evolve from an area of shared interest to a widespread measure for adoption, ecosystem partners must establish and adopt Governance and Technology Frameworks that meet their needs, especially ensuring the digital identity trust that the internet lacks (i.e., the TCP/IP stack).

It is inevitable that different ecosystems with unique Governance Frameworks will emerge based on shared missions, industry boundaries and other factors. For global adoption to occur, there must be a means to interact across ecosystems. This is also an evolving topic as governance is working to contend with each layer of the solution stack. Working toward global adoption is an opportunity for the public and private sectors to work together to define and implement the policies required to exchange trusted and verifiable credentials and develop financial models that ensure sustainability. Public and private entities rely on official identity documents for client onboarding and authentication. Government authorities should provide services and related policies that enable the issuance of trusted digital attributes to the highest identity assurance levels. This will allow for authentication that also meets the highest levels of authenticator assurance.

3.3. Security

Introduction

When dealing with digital identity, information security[13] is of utmost importance. A loss of confidentiality, availability and integrity can have dramatic consequences for a variety of stakeholders: losing confidentiality (e.g., in data breaches) undermines trust, not being able to access or provide parts of identity can prevent critical transactions (e.g., bank transactions, e-government) from being performed, and a lack of integrity could result in digital impersonation (e.g., identity theft) or fraud.

Where are we now?

SSI makes use of different technologies to protect against security threats at multiple levels.

The vast majority of DID methods use cryptography in DID Documents. Digital signatures and verifiable timestamps allow DID Documents to be cryptographically verifiable, providing integrity protection. When using DLTs for DID anchoring, such techniques protect against availability threats in verification processes.

At the protocol level (DIDComm, CHAPI, OpenID Connect) cryptography algorithms provide mutual authentication and confidentiality of the information exchanged between the parties.

Verifiable Credentials and Verifiable Presentations use digital signatures to ensure the integrity of the information. Innovations in cryptography, like Zero-Knowledge Proofs, can minimise personal information disclosures, thus improving privacy.

Finally, from a holistic perspective, an SSI-based identity management system can improve security by reducing attacker interest due to fewer personal data pools (honey pots). It also enhances security by replacing legacy password-based systems with public key authentication.

Barriers and Challenges

However, despite the inherent security benefits of using SSI for handling digital identity management, there are still some security challenges to consider:

- There are no widely used, standardised ways to assess the security of software products or SSI products/platforms, apart from limited methods to perform a penetration test or code review.
- There is no "level of security of software products", so it is difficult for non-security experts to assess the risk of software they want to use.
- A certification is a snapshot of the system at a point in time, but as software evolves, new vulnerabilities can be added and discovered.

[13] The ISO/IEC 27000:2018 defines information security as the "preservation of the confidentiality, availability and integrity of information".

- Certifications can be costly and time-consuming and can have a relevant impact on SMEs.
- Many innovations in SSI are nascent. For example, this can lead to issues with certain types of cryptographic keys and algorithms that certain governments cannot adopt as they are not "cleared" by relevant authorities (e.g., NIST). Implementations might also have severe undiscovered vulnerabilities due to the absence of rigorous testing.
- Solving key-management and recovery-related challenges is important because cryptographic keys are the main mechanisms controlling digital identities. Key-management and recovery are essential elements from a security and usability perspective as they enable vital functionalities in every SSI-based system (e.g., authentication, signatures and encryption). At its core, the challenges associated with SSI relate to creating a "Distributed Public Key Management Systems" (DPKMS) that allows for the delegation and guardianship of private keys and secure and easy-to-use key and secret recovery in case of loss or destruction of private keys.

Path Forward

The information held and processed by the entities involved in SSI is susceptible to intentional or unintentional threats. When talking about information security in SSI, it should be determined what information must be considered a critical asset that needs protection against attacks on availability, confidentiality and integrity. This can include, but is not limited to wallets (managing private keys and personal information in the form of Verifiable Credentials), Secure Data Stores[14] (storing personal data) or validation services (implementing DID resolution features).

The appropriate standards for the assessment of criticality can vary according to the use case. Consequently, product or service manufacturers should perform a thorough threat analysis according to their specific needs.

The following recommendations can help vendors, manufacturers, users and the overarching ecosystem improve security, thus improving trust in the system:

- Regulators should encourage and promote the certification of products, services and processes against existing (cyber)security certification schemes[15] and support the creation/consolidation of standards if non-existing.
- Relevant agencies should update their recommendations and guidelines, taking into account all new protocols and algorithms proposed as de facto standards in decentralised identity ecosystems.
- SSI implementers should follow best practices[16] when using cryptography technologies, favouring thoroughly tested algorithms and protocol implementations, and executing risk assessment[17] and implementing risk

[14] As presented in https://identity.foundation/secure-data-store/.

[15] Check EU cybersecurity certification framework.

[16] Advancing Software Security in the EU - ENISA.

[17] NIST Special Publication 800-30 - Guide for Conducting Risk Assessments.

management processes that use an Information Security Management System when possible.

- Vendors, manufacturers and users should promote the deployment and maintenance of public repositories that have disclosed vulnerabilities, best practices for security in place and designated methods to mitigate common security risks.

3.4. Privacy and Data Protection

Introduction

The centralised or federated design of current identity data infrastructures is responsible for a growing number of privacy and security scandals, leading to diminished trust in centralised and federated identity providers. As users' general awareness and value of privacy increases, governments and businesses are beginning to value the unique capabilities that SSI offers, namely its increased privacy and data protection levels and additional user control.

As part of SSI's inherent design, users are put in control of data, which closely matches the trends of current data protection regulations. In the EU, GDPR regulates users' data-rights. Its far-reaching territoriality has sparked an international shift in the management practices of processing users' personal data. However, not every approach to SSI, particularly not every blockchain design, is in compliance with the law, especially regarding certain rights established by the GDPR and similar data protection regulations, such as the right to be forgotten.

Where are we now?

SSI is rapidly evolving and holds the potential to solve some of the biggest digitisation challenges in the formulation and enforcement of high levels of privacy and data protection. In principle,[18] SSI achieves this by including:

- additional user controls such as granular consent (enhanced consent management). The control of personal data by the user increases transparency of the "how, why, who and when" at different stages of processing, sharing and deletion of data.
- in accordance with GDPR, SSI prevents uncontrolled automatic processing of personal data as the user has full determination of purposes and means of processing of their personal data.
- the ability to have the user's consent and control over data processing. This eliminates excessive data processing by controllers and introduces data minimisation in its design.
- diminished risk of data being shared with unknown parties via opaque and unclear privacy policies and data sharing practices.
- the use of digital signatures in Verifiable Credentials and Presentations. This ensures the integrity of information and enables innovations in

[18] These features are supported by the standards but are still dependent on the design curated by the developers.

cryptography, for example in using Zero-Knowledge Proofs which help improve privacy by minimising personal information disclosures.

- increased data protection and data portability
- data deletion/revocation by design. This is possible either by direct or automated deletion of the users' data. Additionally, SSI offers users transparency on when data is deleted.

Barriers and Challenges

Although SSI offers many benefits related to privacy and data protection benefits, its current technical implementation often faces compatibility issues with data protection regulations. The majority of these issues stem from the typical use of blockchain and its immutability characteristic, which is problematic when considering an individual's right to be forgotten. Even under traditional identity systems, implementing the right to be forgotten can be difficult. Blockchain adds to the difficulty as its append-only security benefit and inability to have data deleted from its database means users also no longer have the possibility to delete their saved data. The challenge is threefold:

- discerning a valid deletion/revocation request (a step supported by SSI's user authentication)
- identifying what constitutes "personal data" (a classification issue that requires clarification of the law)
- actual deletion of data (a trust and transparency issue that requires strong compliance)

Another major challenge is cross-border data sharing, which is made extremely difficult due to different jurisdictions and standards involved with country-specific privacy and data protection.

Path Forward

There are clear steps forward to ensure that this technology and the standards derived from it will improve privacy and data protection. Different SSI approaches, with varying credential-based models and the use of "off-ledger" DIDs alongside certain types of permissioned blockchains, as well as some approaches removing the use of blockchain altogether, are making more seamless GDPR-compliance possible.

As different SSI approaches converge and consolidate, stakeholders should update regulations (e.g. GDPR) and legal frameworks (e.g. eIDAS) to provide more legal certainty on the technical specificities that contribute to the process of data being considered as personalised, pseudonymised or anonymised.

Human error/malicious behaviour, which is difficult or even impossible to erase in a Blockchain setting, also needs to be addressed. The latter has liability consequences for a data controller/processor as they might be unable to delete data or confirm that data shared with third parties has been deleted — questions regarding indemnification and compliance enforcement remain.

Privacy and data protection and the anonymisation of data are essential aspects of the GDPR personal data framework. It must be clarified whether the cryptographic standards used in SSI protocols are sufficient for data to be considered anonymous. If not, official bodies will need to provide guidance on the technical and operational measures required to reduce possible user profiling.

That being said, it is important that data protection and privacy standards remain strong and protected from erosion. SSI enables the digitisation and utilisation of an even larger quantity of personal data and — if unchecked — may have dramatic implications for citizens' privacy and autonomy.

Glossary

Identity	A set of attributes that allows a subject to be sufficiently distinguished/uniquely describes a subject within a given context
Attestation	An attestation is the confirmation of a claim through evidence or verification
Attribute	An identity trait, property, or quality of an entity
Claim	A statement or assertion that one DID subject, such as a person or organisation, makes about itself or another DID subject. The claim will relate to one or more attributes about a DID Subject
Credential	A set of one or more claims about a subject
Digital identity	Defined as the data points that identify something (whether an individual, entity, process or thing) in digital form
DID (decentralised identifier)	A type of identifier intended for verifiable digital identity that is "self-sovereign", i.e., fully under the control of the identity owner and not dependent on a centralised registry, identity provider or certificate authority
DID Document	Contains a set of key descriptions, which are machine-readable descriptions of the Identity Owner's public keys, and a set of service endpoints, which are resource pointers necessary to initiate trusted interactions with the Identity Owner
Entity	A resource of any kind that can be uniquely and independently identified, ranging from individuals to legal persons such as businesses and public institutions as well as IoT devices and machines
Identifier	Something that enables an individual, entity, process or thing to be discovered and identified in a given context. The Decentralised Identifier or DID is the building block of SSI. In the context of this document, we refer to DIDs when speaking about identifiers
Identity Holder	An individual or organisation that controls the private keys associated with a given DID. While all types of entities, including natural persons, processes, organisations, smart agents, and things (e.g., IoT devices, machines, etc.) may have DIDs that identify them, the private keys associated with a DID will still be controlled by an individual or organisation (who will also be legally liable for it)

Individual	A natural person
Natural or physical person	An individual human being, as opposed to a legal person created by operation of law
Personal Data	"Any information relating to an identified or identifiable natural person ('data subject')" as defined in Article 4(1) of the GDPR
Self-Sovereign Identity	A model of digital identity where individuals and entities alike are uniquely in full control over central aspects of their digital identity, including their underlying encryption keys, creation, registration, and use of their decentralised identifiers or DIDs, and control over how their credentials and related personal data is shared and used
Subject	Refers to the subject of a given claim or credential

Contact details:

Website	inatba.org
Identity WG Co-chairs	identity-wg-cochair@inatba.org
Join INATBA	membership@inatba.org