d-fine

If you want to join discussions about Self-Sovereign Identity, this paper is a good place to start

analytical. quantitative. tech.

Jan 2023

Content

If you want to join discussions about Self-Sovereign Identity, this paper is a good place to start, January 2023

Abstract

Regulatory, economic, but also sociological drivers have recently led to an increased amount of discussions around the Self-Sovereign Identity (SSI) framework. However, these often highlight certain aspects or problems of the framework, rather than looking at the framework holistically and at what it can solve.

With this short paper, we wish to inform you about (a) what the framework solves, (b) what its elements are, (c) how it relates to current regulatory discussions as well as (d) to other technological elements, like public key infrastructures and blockchain.

After reading this paper, you should be able to understand criticism towards the framework but also to productively discuss how it can be used to solve certain problems, which use-cases may be a good fit for it, and how current issues can be addressed.

01. Problem Statement

Most business processes today require an identification or authentication step. To understand this step better, let us consider an *identity* of a subject to consist of an identifier and a set of claims (See Figure 1).

Identification ("It's really me.") then refers to a proof that a party is associated with or has control over a certain identifier and that this identifier is connected to certain claims. It can either be done by

- self-checks ("Please enter the code we've just sent you to the phone number you provided") or
- by trusting third parties ("Please show me your ID issued by your government").

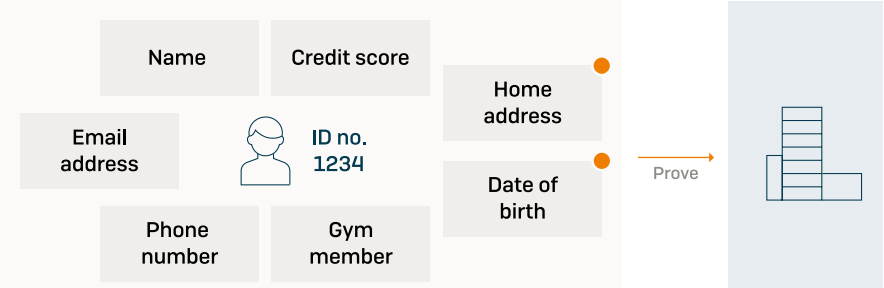


Figure 1: Identification Process

Authentication makes use of previous identification processes, such that the same proof does not need to be performed with the same counterparty again and again. ("I'm really the same entity as I was last time.")

The problem with both these processes lies in the fact, that the internet was designed to connect computers, not people.

For the identication and authentication of humans, machines, and organizations, today we hence mostly use 'workarounds' like

- passwords (siloed approach)
- existing accounts on other platforms, e.g., social media ("Log in with X"; federated approach)
- multi-factor authentication (MFA)
- credit cards (even if we don't intend to buy anything)

Conclusion

Today's approaches, both for identification and authentication lack security, user control, and either convenience or privacy. With "Verifiable Credentials" (VCs), Self-Sovereign Identity introduces a new way of identification and authentication as well as subsequent communication that addresses these problems.

02. Key Benefits of SSI

- Cheaper on-boarding and KYC[1] processes: registration for a new service ultimately becomes as simple as a login
- Higher convenience and security: cryptographic signatures replace passwords and allow for a secure verification of claims
- Out-of-the-box GDPR compliance: identity subjects (*Holders*) store their own claims and decide what to share with whom
- Out-of-the-box PSD2 compliance: holders require a wallet device (something they own) and a private key (something they know) to sign an authentication request
- Increased efficiency and convenience: holders can re-use previously verified claims in several locations
- SSI-based credentials can be used both online and in the physical space
- No single point of failure: no central / single entity required during authentication process
- Increased privacy: possibility to disclose only parts of a credential (relevant claims) or even relative information (e.g., "age > 21" instead of birthdate)
- Higher flexibility: many ecosystems (use-cases, countries, business networks, etc.) can share the same infrastructure and incorporate their individual trust policy framework

1 Know Your Customer

03. SSI Core Components

3.1 Identifiers

Every entity in an ecosystem is uniquely identified by a **Decentralized Identifier** (DID), which is assigned according to cryptographic principles without a centralized entity in place.

3.2 Communication Channels

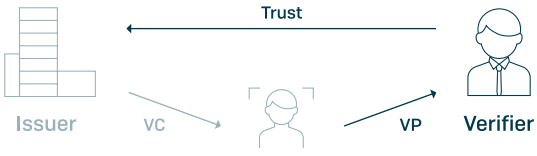
The DID resolves to an associated **DID Document** which contains information like agent service endpoints for communication or associated public keys for encryption.

3.3 Attestation Process

Identity attributes (claims) are issued in **Verifiable Credentials** (VCs) which are stored in the subject's wallet. They cannot be accessed by third parties without the Holder's consent.

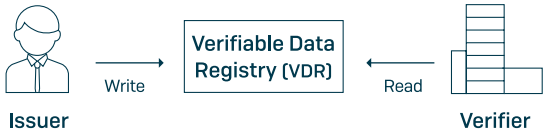
3.4 Authentication Process

Verifiers request a **Verifiable Presentation** (VP) derived from existing VCs. They can choose to trust an Issuer. Verifier and Issuer can also be the same entity.



3.5 Verifiable Data Registry

A **highly available data structure** stores public signatures such that any network participant can obtain them at any time to verify presented credentials without having to contact the Issuer or to trust the Holder. Many networks utilize Distributed Ledger Technology (DLT) or a blockchain instance for this shared ledger. This ledger **does not store the content of a VC or a hash of it**; only issuer signatures.



04. Governance in SSI

The SSI framework does not answer all relevant questions w.r.t. IDs, e.g., whether a credential is valid in a specific context, whether an Issuer has the right to issue a specific credential, or whether a Verifier is allowed to ask for certain claims. In addition to the **technical trust** that SSI can provide via its cryptographic verification mechanisms, the aspect of human trust hence needs to be covered by additional concepts and infrastraucture, and the needs may differ for different ecosystems. Human trust cannot be built by technology alone as it is derived from governmental, sociological, economic, and political structures. **Establishing human trust in SSI is the role of a governance model.**

To refrain from the creation of a sophisticated governance model for all four layers has proven catastrophic in the past.

The most popular organizations to provide concepts for that purpose are the *Trust over IP Foundation* (ToIP) and the *Digital Identity Foundation* (DIF). Their key message is that any SSI application consists of four layers which all need a sound technical solution but also a specific governance model by an **entitled governance authority** for that ecosystem (see Figure 3).

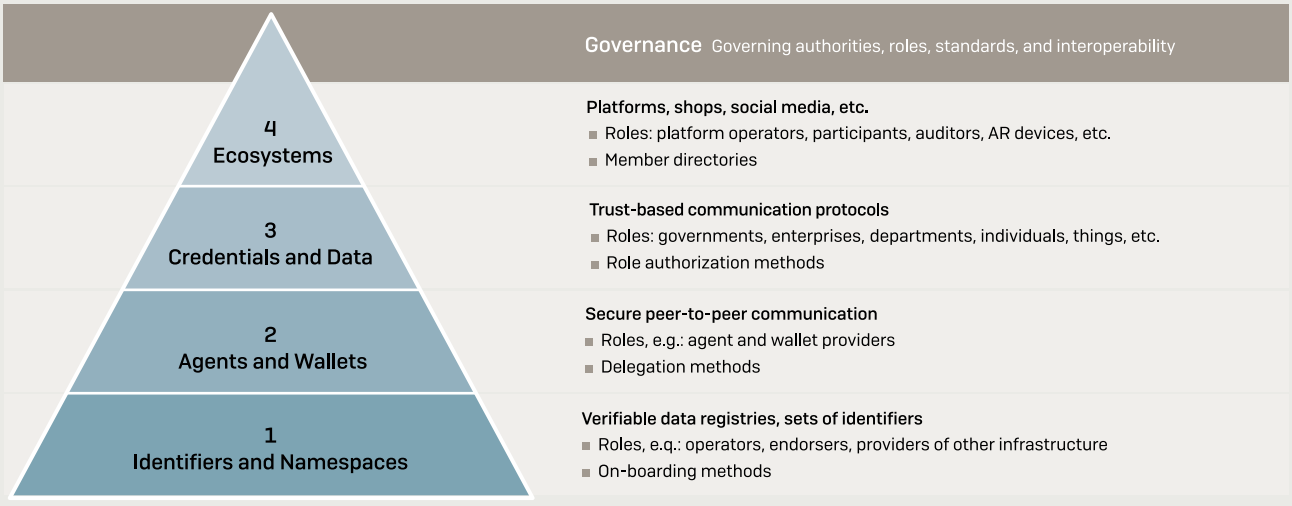


Figure 3: Governance model for all four layers

For all four layers, the technical implementation must follow the requirements for that layer, and the rules dictate how the SSI components are used and complemented with other infrastructure.

Large consortia with specific governance models are, e.g., the **Sovrin Foundation, IDunion**, and the **Evan Network**.

05. SSI and EU Regulation

As the **eIDAS** regulation – among other things – concerns itself with identification, authentication, and electronic signatures, it is often mentioned in the context of SSI. However, the original, over five-year-old document mainly concerns itself with standardization and electronic transactions

Furthermore, it finds that identification should not be left in the hands of unregulated third parties as their services raise security and privacy concerns.

An eIDAS update proposal from June 2021 explicitly mentions self-sovereignty as a market demand.

Both, the original paper and the amendment proposal, remain technologically agnostic. However, none of the content contradicts a utilization of the SSI framework. Consequently, the proposed requirement for all member states to provide an **EU Identity Wallet** for its citizens has become a major driver for collaborations between countries and for SSI-based development of identity apps throughout the EU.

06. SSI vs. Other Approaches

6.1 Public Key Infrastructures (PKIs)

In most online communication today, PKI-based certificates form the basis for authentication and trustful communication (e.g., for websites and browsers). SSI-based Verifiable Credentials (VCs) are in some ways similar to PKI-signed certificates. However, VCs show more flexibility with respect to possible content and to sharing only parts of the contained information (selective disclosure) or only relative information (via zero-knowledge-proofs).

Furthermore, SSI does not require a “root certificate authority”, i.e., a “trust anchor” at the top of a trust hierarchy. Any trust structure (hierarchical, peer-to-peer, multi-layered, etc.) can be captured by the SSI framework, such that different types of ecosystems can share the same infrastrcutre and even existing credentials.

However, PKI-based signatures can still play a role in an SSI-based system, e.g., to secure connections between Issuers and Holders or Holders and Verifiers, or to authenticate Issuers.

6.2 Smart eID and the German ID Card

Electronic identification **(eID)** is a specific ID use-case where **government-issued** credentials are stored and presented electronically. For this use-case, SSI competes with the approach of the Smart eID which describes an electronic identity that is stored in a secure element of a smartphone. Only few smartphones today adhere to the high standards necessary to use the Smart eID, such that the majority of citizens (e.g., all Apple users) would be excluded from such a solution. Additionally, Smart eID requires the availability of an eID server and hence introduces a single source of failure.

The German ID card is another example for a purely governmental approach, in which the Holder presents their **physical card** to a reading device which in turn connects to a certified eID service. The web service requesting the user information then connects to this eID service and retrieves the information. While this approach has been in place for years and also bears certain advantages w.r.t. SSI-based Verifiable Credentials, it isn't used very frequently.

Note that both approaches do not require any form of biometrical confirmation of the holder (i.e., a third person could commit identity fraud if they get a hold of, e.g., the ID card and a connected PIN). However, due to this two-factor approach, the process is considered secure enough.

6.3 Soulbound Tokens

While SSI-based Verifiable Credentials make a point of not storing any user-related data on a shared ledger, **soulbound tokens associate certain claims with a public key "on chain"**, such that a user holding the corresponding private key can prove that they control this claim. Technically, soulbound tokens are non-fungible tokens (NFTs) without a working transfer function, such that they are forever connected to a specific public key. With both techniques at hand, anyone building a use-case can decide whether they want to preserve privacy and store personal data only on the user device or whether a certain public availability of claims is preferred or perhaps even required.

07. SSI and Blockchain

Building a use-case based on the SSI framework does not necessarily require the utilization of a blockchain, but the demands on the Verifiable Data Registry (VDR) are often met best by some form of Distributed Ledger Technology (DLT).

Using SSI does not automatically mean that a blockchain is involved. However, in order to cryptographically verify presented claims, Verifiers must be able to obtain Issuer signatures from a trustworthy source, the verifiable data registry (VDR). To account for the decentralized character of the framework, most ecosystems store these signatures on a blockchain. This addresses the problem of a single source of failure. Many ecosystems introduce additional, centralized infrastructure which contains, e.g., registries with trusted Issuers for a given use-case that Verifiers can query.

A recent BSI paper[2] has raised concerns w.r.t. blockchain technology in terms of complexity, missing standardization, and lacking experience and hence potentially low security, especially in the identity space. However, **in the SSI framework, the shared ledger does not contain any data related to the Holders or to single credentials**. And if a blockchain is used, there are still tremendous differences in the type of distributed ledger:

2 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.html

- Public blockchains have the potential to bring the largest degree of decentralization but may also introduce problems like transaction costs for individuals and sometimes ecological issues.

- Private blockchains operated by a small network of providers address these issues and can additionally introduce a specific governance model. However, they can lead to a low degree of decentralization, high operational costs, and hence high fees for users.

- A **public** (read access) **permissioned** (write access) **blockchain** which incentivizes stakeholders in the ID ecosystem to run it according to a **regulatory sound policy framework** can address the issues and comes with all the advantages of a **highly available** and **secure** piece of **infrastructure**.

08. Current Issues of SSI

8.1 Lacking Wallet Security

Wallets which store user signatures and credentials are usually mobile applications which typically do not incorporate any type of hardware security. This results in sensitive cryptographic data being stored in a way hat it can be retrieved by individuals who get physical access to the device. Furthermore, there is usually no biometric proof required by the wallet which would ensure that the data sent actually belongs to the individual holding the phone. However, as the space of digital assets progresses, digital wallets become more sophisticated and identity wallets may be able to benefit from this development.

8.2 A Governmental ID for Everything?

Instead of building SSI-based solutions for their ecosystem, many private entities look to their government to first commit to the technology and introduce **foundational government identities** for citizens. It is hence likely that such identities may then be requested by a number of web services (Imagine copying your ID card for any store in which you want to buy a sweater), instead of relying on pseudonymous **contextual identities**, which would fully suffice for that purpose. Using verifiable, government-issued data in too many places poses a huge privacy risk and can be disadvantegous for certain minorities.

This issue can be addressed by building context- or ecosystem-specific use-cases first and only later combine them with government IDs where necessary.

8.3 Pirates with Verifiable Personal Data

Instead of just showing personal data (as you might with a physical ID card), the Verifier receives a verifiable copy of it. Although the technology prevents them from using the data as their own – if they wanted to, they could now **sell verifiably valid data** instead of just data.

While **this problem is intrinsic to Verifiable Credentials** and does not go away, a possible mitigation could look like this:

1. Clearly separate governmental ("foundational") from "contextual" IDs, such that users do not provide their government IDs in a verifiable way at places where it isn't necessary.

2. By law, have verifying entities provide the user with the information whether they are allowed to obtain governmentally verified information. For this, existing PKI-based approaches can be used.

3. Where possible, introduce the legal requirement for Verifiers to store only the data itself, not the proof around it.

Note that SSI has other advantages in terms of privacy and flexibility, which – for certain use-cases – may outweigh this problem.

8.4 Missing Standardization

In order to unleash the full potential of Verifiable Credentials, a high degree of **standardization** is required.

- When an entity joins a network, other participants need to know how to resolve their DID.
- A web service needs to know, what an attribute is called and in which schema it can find it.
- Verifiers need to know how to find out whether they can trust an issuer.

As large technology firms, which control a lot of the identification and authentication business today, hardly have an interest in pushing for a decentralized solution, standardization is mainly driven by idealists, consortia, and some governments, who wish to roll out **foundational identities** for their citizens – together a small fraction of the market.

This may change with the development of further use-cases and the on-boarding of large amounts of users, such that the one or the other standard prevails.

8.5 A Chicken-and-Egg Problem

As long as only few Issuers provide Verifiable Credentials to Holders, not many services will be able to use them for identification and authentication, which again results in few users requesting VCs from Issuers.

However, looking at this network effect the other way around: As soon as a consensus has been reached, we may be able to log in to any web service with just a click, no password manager required, or to register for new services using existing credentials.

09. Outlook

As of today, several SSI-based networks and consortia have been formed. Several use-cases have already been built, some on the government side, some by the private sector; most of them in the identity space, but some just to share data securely and with a proof of authenticity.

We see a large number of proof-of-concepts being created with SSI-related technology, some driven by regulation, some by customer demand, and some by the wish to increase efficiency or security.

Use-cases today and in the future range from banking to energy systems, to automotive, or to ESG data sharing. Basically, whenever you'd like to migrate your user profile from A to B, when you want to pick an identity of yours to join a platform, if you need to be certain you're talking to the correct entity, or anytime you want to initiate a payment in a secure way, SSI may prove useful.

The framework and the technology are still young. As long as further steps towards standardization, an increase in data security, and the creation of required infrastructure are being made, SSI is on a solid track to become a standard for how we provide identification and share information across ecosystems in the future.
In the end, any live solution will likely consist of a mix of SSI and other security approaches.

Author

Dr Marc Henniges
Expert for Digital Assets, Payments, and Identity
d-fine GmbH, Frankfurt am Main
marc.henniges@d-fine.de

d-fine

Berlin
d-fine GmbH
Friedrichstraße 68
10117 Berlin
Germany
berlin@d-fine.de

Dusseldorf
d-fine GmbH
Dreischeibenhaus 1
40211 Dusseldorf
Germany
duesseldorf@d-fine.de

Frankfurt
d-fine GmbH
An der Hauptwache 7
60313 Frankfurt
Germany
frankfurt@d-fine.de

Hamburg
d-fine GmbH
Am Sandtorpark 6
20457 Hamburg
Germany
hamburg@d-fine.de

London
d-fine Ltd
14 Aldermanbury Square
London, EC2V 7HR
United Kingdom
london@d-fine.co.uk

Milan
d-fine s.r.l.
Via Giuseppe Mengoni 4
20121 Milano MI
Italy
milano@d-fine.com

Munich
d-fine GmbH
Bavariafilmplatz 8
82031 Grünwald
Germany
muenchen@d-fine.de

Stockholm
d-fine AB
Nybrogatan 17
114 39 Stockholm
Sweden
stockholm@d-fine.se

Utrecht
d-fine BV
Stadsplateau 7
3521 AZ Utrecht
Netherlands
utrecht@d-fine.nl

Vienna
d-fine Austria GmbH
Seilerstätte 13
1010 Vienna
Austria
wien@d-fine.at

Zurich
d-fine AG
Brandschenkestrasse 150
8002 Zurich
Switzerland
zuerich@d-fine.ch