École Polytechnique Fédérale de Lausanne

A Use Case Oriented Survey of Self-Sovereign Identity

by Frédéric Gerber

Master Thesis

Approved by the Examining Committee:

Prof. Edouard Bugnion
EPFL Supervisor

Michael Bisig
Christoph Graf
SWITCH Supervisors

EPFL IC DCSL
INN 237 (Bâtiment INN)
Station 14
CH-1015 Lausanne

SWITCH
Werdstrasse 2
P.O. Box
CH-8021 Zürich

August 23, 2022

"We didn't know we were making memories, we were just having fun"
— Alan Alexander Milne

Dedicated to my granddad 'Nonno'. I look back very fondly on our time together and I will miss your witty outlook on the world. My goal is to enjoy life as much as you did when traveling around Africa and America.

> *Lieber Frédéric,*
>
> *Du hast mich mit deiner schönen Postkarte nicht nur überrascht sondern auch eine sehr grosse Freude bereitet! Vielen herzlichen Dank.*
>
> *Wenn ich mich nicht täusche bist Du oder wirst Du in Zürich studieren. Ich weiss Du arbeitest viel und wünsche Dir viel Erfolg damit. Was ist eigentlich dein nächstes Ziel?*
>
> *Es freut mich natürlich immer sehr, wenn ich Dich sehen kann und ein paar Stunden mit Dir zu verbringen.*
>
> *Alles alles Gute und liebe Grüsse,*
>
> *Dein Nonno*

Acknowledgements

I want to thank Michael Bisig for giving me the opportunity to work on my Master Thesis at SWITCH and Prof. Edouard Bugnion for the insights he brought to my work during our discussions. Additionally, thanks a lot to the entire TRID team at SWITCH for making me feel so welcome over my time here, both online and in person. In particular, a warm thank you to Christoph Graf, Robert Ott, Lukas Käppeli and Christian Rohrer for giving me feedback on my report and getting into inspiring discussions with me – both on SSI and other topics.

Finally, I am deeply grateful to my family and friends for being there for me in joyful times as well as in difficult ones. In particular, I cannot thank Debora and Roger enough for generously welcoming me in their apartment near Zürich; my closest family Dominik, Myriam, Nicolas and Robin for always supporting me; my grandparents for excellent meals and discussions about anything; and my good friends Andrew, Alexandre, Elsa, Fanny, Marie, Matthieu and Sébastien for letting me come over whenever I needed a place to stay in Lausanne or elsewhere. This work would not have been as much fun without you folks!

Lausanne, August 23, 2022 Frédéric Gerber

Abstract

With self-sovereign identity (SSI), we stand at a crossroads that is leading society to a new kind of digital identity. Under this new paradigm, users no longer have to remember a username and a password; instead they gain full power on the information that is issued to them by trusted entities. From their perspective, using SSI therefore consists in carrying a digital wallet, typically in the form of a smartphone application, where so-called verifiable credentials can be stored in a secure environment behind biometrical identification. However, this high user responsibility raises the first challenge of SSI: wallets are vulnerable and people are prone to losing access to them for various reasons. Therefore, data should be properly backed up, so that credentials can be recovered without altering user experience.

In practical terms, having such a new model for digital identity enables many potential use cases, either by digitalizing existing processes from the physical world or by creating new possibilities thanks to the power of combining data. Consequently, it becomes hard to decide which use cases should be prioritized, let alone which of them are well-aligned with the principles of SSI. Therefore, this work establishes a set of requirements, according to which potential use cases of SSI can be assessed qualitatively. Additionally, a threat model for SSI systems is presented, identifying possible attacks on such use cases in order to help developers take design decisions about their implementations.

Finally, this work focuses on an educational use case and explores a proof of concept implementation based on hyperledger Indy, which is a decentralized network specifically built for identity purposes; and ACA-Py, which is a framework that provides an interface to communicate with Indy underneath. In this context, there are also a couple of issues related to the versioning of functionalities, the beta status of wallet applications and credential schema formats. This highlights the fact that SSI is not yet ready for a public rollout, but it also motivates research and development to put a strong emphasis on it in the coming few years.

Résumé

Avec l'identité auto-souveraine (SSI), nous nous trouvons à un carrefour qui conduit la société vers un nouveau type d'identité numérique. Dans le cadre de ce nouveau paradigme, les utilisateurs ne doivent plus se souvenir d'un nom d'utilisateur et d'un mot de passe ; au contraire, ils acquièrent un pouvoir total sur les informations qui leur sont émises par des entités de confiance. De leur point de vue, l'utilisation de SSI consiste donc en la possession d'un portefeuille numérique, généralement sous la forme d'une application pour *smartphone*, où des *credentials* vérifiables peuvent être stockés dans un environnement sécurisé derrière une identification biométrique. Cependant, cette haute responsabilité des utilisateurs soulève avec elle le premier défi de SSI : les portefeuilles sont vulnérables et les gens sont susceptibles d'en perdre l'accès pour diverses raisons. Par conséquent, les données doivent être correctement sauvegardées, de sorte que les *credentials* puissent être récupérées sans altérer l'expérience de l'utilisateur.

En des termes plus pratiques, l'existence d'un tel nouveau modèle d'identité numérique permet de nombreux cas d'utilisation potentiels, soit en numérisant des processus existants du monde physique, soit en créant de nouvelles possibilités grâce à la puissance de la combinaison de données. Par conséquent, il devient difficile de décider lesquels de ces cas d'utilisation devraient être priorisés, ainsi que lesquels sont bien alignés avec les principes de SSI. C'est pourquoi ce travail établit un ensemble de conditions, selon lesquelles les cas d'utilisation potentiels de SSI peuvent être évalués qualitativement. En outre, un modèle de menace pour les systèmes SSI est présenté, identifiant les attaques possibles sur de tels cas d'utilisation afin d'aider les développeurs à prendre des décisions de conception concernant leurs implémentations.

Ce travail se concentre sur un cas d'utilisation dans le domaine de l'éducation et explore une mise en œuvre de preuve de concept basée sur *hyperledger* Indy, qui est un réseau décentralisé spécifiquement construit à des fins d'identité ; et ACA-Py, qui est un cadre qui fournit une interface pour communiquer avec Indy en dessous. Dans ce contexte, il y a également quelques problèmes liés aux versions des fonctionnalités, au statut bêta des applications de portefeuille et aux formats des schémas de *credentials*. Cela met en évidence le fait qu'SSI n'est pas encore prêt pour un déploiement public, mais cela motive également la recherche et le développement à mettre l'accent dessus dans les années à venir.

Zusammenfassung

Mit der Selbst-Souveränen Identität (SSI) stehen wir an einer Weggabelung, welche die Gesellschaft zu einer neuen Art digitaler Identität führt. Dieses Verfahren erspart den Nutzern, sich an einen Benutzernamen und ein Passwort zu erinnern; stattdessen erhalten sie die volle Kontrolle über die Informationen, die ihnen von vertrauenswürdigen Stellen zugeteilt werden. Aus ihrer Sicht besteht die Nutzung von SSI aus dem Besitz einer digitalen Brieftasche, in der Regel in Form einer *Smartphone*-Anwendung, in der sogenannte verifizierbare *Credentials* in einer sicheren Umgebung hinter einer biometrischen Identifizierung gespeichert werden können. Diese hohe Verantwortung der Nutzer bringt jedoch die erste Herausforderung von SSI mit sich: Brieftaschen sind gefährdet und Menschen können aus verschiedenen Gründen den Zugang dazu verlieren. Daher sollten die Daten ordnungsgemäss gesichert werden, so dass die *Credentials* wiederhergestellt werden können, ohne die Benutzererfahrung zu beeinträchtigen.

In der Praxis ermöglicht ein solches neues Modell für digitale Identität viele vorstellbare Anwendungsfälle, entweder durch die Digitalisierung bestehender Prozesse aus der physischen Welt oder durch die Schaffung neuer Möglichkeiten dank der Macht der Datenkombination. Infolgedessen ist es schwer zu entscheiden, welche Anwendungsfälle priorisiert werden sollten, geschweige denn, welche von ihnen gut mit SSI-Prinzipien übereinstimmen. Daher wird in dieser Arbeit eine Reihe von Anforderungen aufgestellt, anhand derer potenzielle Anwendungsfälle von SSI qualitativ bewertet werden können. Darüber hinaus wird ein Bedrohungsmodell für SSI-Systeme vorgestellt, das mögliche Angriffe auf solche Anwendungsfälle erkennt, um Entwicklern bei der Planung und Umsetzung von Entscheidungen zu helfen.

Diese Arbeit konzentriert sich auf einen Anwendungsfall aus dem Bildungsbereich und untersucht eine Konzeptnachweis-Implementierung auf der Basis von *Hyperledger* Indy, einem dezentralen Netzwerk, das speziell für Identitätszwecke entwickelt wurde, und ACA-Py, einem Framework, das eine Schnittstelle zur Kommunikation mit Indy bietet. In diesem Zusammenhang gibt es auch eine Reihe von Problemen bezüglich Versionierung von Funktionalitäten, dem Beta-Status von Wallet-Anwendungen und den Schemaformaten für *Credentials*. Dies unterstreicht die Tatsache, dass SSI noch nicht für eine öffentliche Einführung bereit ist, motiviert aber die Forschung und Entwicklung, in den kommenden Jahren einen starken Schwerpunkt darauf zu legen.

Contents

1 Introduction

"the Internet's addressing system is based on identifying physical endpoints (machines) on a network. People are not endpoints on a network. Therefore, the Internet has no way to uniquely identify people."
— Andrew Tobin & Drummond Reed [120]

Towards the end of the past century, the internet was introduced in our society. While it was not so clear back then what people would use this novelty for, some engineers believed in it and worked hard to deploy a scalable network that can connect many devices together. In its early years, the internet was still slow and complicated to use, but nowadays it has become so ubiquitous that it is now hard to imagine a world without it. This is certainly due to the recent wide spread of smartphones, which almost made us forget that they even exist. Actually, we interact with the humans behind them rather than with a piece of metal.

1.1 Internet Layering and its Limitations

Theoretically, the internet has been built as a stack, involving the five layers presented top-down in Figure 1.1: application layer, transport layer, network layer, link layer and physical layer [70].

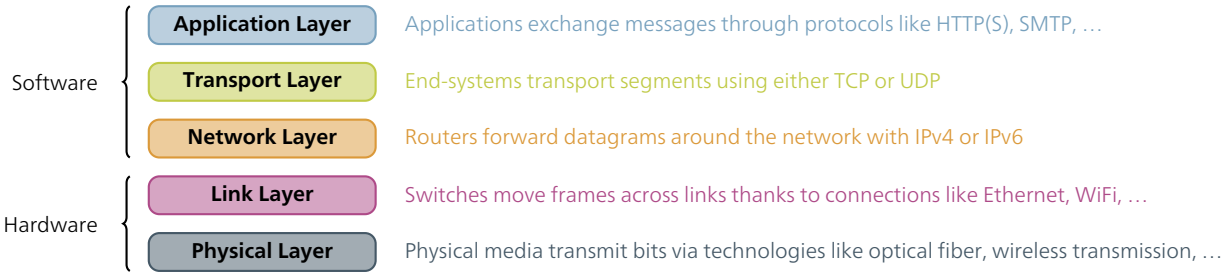


Figure 1.1: Internet Layers

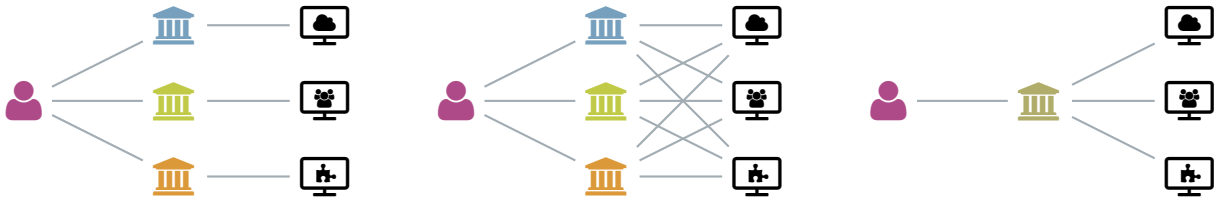
While this system design encapsulates hardware and software co-design with great precision, it lacks an understanding of the human aspect that lies in the users of the internet. More precisely, although IP addresses can be considered indirect *personally identifiable information* (PII)[1], the internet has evolved without a dedicated identity layer [120]. As a result, users can browse the internet without a fixed identity, which is practical for privacy concerns, but quite inconvenient when they want to access a *service provider* (SP) or *relying party* (RP) that proposes personalized content[2]. For example, an email web client should not display the same messages for two different users, so it has to find a way to implement access control itself.

[1] Using IP addresses as direct PII can be seen as a layering violation, since each layer should only ever communicate with the one below or above itself. In this case, a network interface (at the network layer) might not correspond to a unique end-user (above the application layer), despite observable correlation between the two.

[2] Hereafter, the terms SP and RP are used interchangeably because they have the same role. The only difference between them is their authentication protocol, namely SAML for an SP and OIDC for an RP (*cf.* subsection 2.1.1).

1.2 Digital Identity on the Internet

As a consequence to the missing identity layer in the internet, each SP or RP had to build a way to represent digital identities itself. In the early days of web serving, every service did this manually in the application layer with a **centralized identity** (*e.g.* EPFL Gaspar [5], an internal IdP for the EPFL community). Later, over the years, multiple services synchronized their efforts in order to simplify identity checks by allowing **federated identities** from third parties to log into their own (*e.g.* SWITCHaai [25], where any university IdP can be chosen for a given service). More recently, even that approach has been topped with the emergence of **user-centric identities** that do not depend on the SP or RP altogether, but that are directly bound to the end user (*e.g.* SWITCH edu-ID [24], which is unique per student and allows for multiple university affiliations).



(a) **Centralized Identity**: Every service provider (🖵) runs its own identity provider (🏛)

(b) **Federated Identity**: Service providers (🖵) can be accessed via multiple identity providers (🏛)

(c) **User-Centric Identity**: A single identity provider (🏛) enables access to multiple service providers (🖵)

Figure 1.2: Different Models of Digital Identity (1/2)

As this brief overview shows on Figure 1.2, three kinds of digital identities [93, 121] have been developed over time; and still coexist today, since it is hard to get rid of one technology once it has been used on the large scale. Most importantly, what makes the difference between these three models is the role of the *identity provider* (IdP), which is a service responsible for running identity checks for access control:

- In centralized identities, the IdP may consist of lookups to a central database hosted by the company providing the SP or RP;
- In federated identities, multiple IdPs coexist and are run by different companies (*e.g.* Google, GitHub, LinkedIn, Microsoft, SWITCH, …), several of which being allowed to access an SP or RP;
- In user-centric identities, there is again only one single IdP, but it is compatible with many SPs or RPs.

Additionally, each of these models is in a way "centric" to some component of the identity check [54], but of course they each focus on a different one:

- Centralized identities put the SP at the center, since each SP implements its own IdP and users thus have many different identities;
- Federated identities put the IdP at the center, since any IdP may log in to many SPs, but individual users may still resort to different IdPs;
- User-centric identities put the user at the center, since each user only has one single identity to log into any SP.

In practice though, these kinds of digital identities coexist and one user may have all of them in parallel, depending on which model the SPs they support.

1.3 Self-Sovereign Identity as a New Approach

Recently, a new model for digital identity has emerged and it is called *self-sovereign identity* (SSI) [105, 121]. Its goal is to follow a user-centric model, but with direct user *sovereignty* instead of delegation to a dedicated company: this means that the user gets full responsibility for their own data and is able to provide it selectively to the SP or RP. As a result, SSI no longer requires an IdP, since the user can directly show their credentials to the service provider, as is illustrated on Figure 1.3.

(d) **Self-Sovereign Identity**: Every service provider (🖵) requires credentials (🗉) directly from the user

Figure 1.3: Different Models of Digital Identity (2/2)

While older models of digital identity may operate with passwords and possibly multiple factors for authentication, SSI relies on so-called *verifiable credentials* (VCs) which are stored on a wallet application [75, 84, 105] controlled by the user. Such wallet apps have become a reality already, which facilitates adoption for SSI, and they can be unlocked directly with biometrical factors to avoid unnecessary friction.

Since everyone has their own wallet and the need for an IdP no longer exists, SSI becomes a decentralized mechanism for strong authentication. Indeed, self-sovereign identities are special kinds of decentralized identities and they typically rely on a decentralized network to function, for instance a distributed ledger [105]. Consequently, data schemas are accessible publicly, since they are written to said ledger, but only the information that the user has agreed to disclose actually reaches the SP, as it always remains local and does not go through the ledger – not even in the form of a hash. This means that users can freely select attributes and will only ever be asked for the minimal information necessary by the SP in question.

Of course, digital wallets are not a perfect solution to all our problems [7]: indeed, they are just as vulnerable as physical wallets when it comes to loss, damage or theft. In fact, they are arguably even more vulnerable due to the omnipresence of smartphones in our lives today. Moreover, implementing wallet recovery remains an open problem because there exists no standardized process to get back a lost identity card, even in the analog world. Since interoperability is a key principle of SSI [84], there should be a uniform way to recover lost credentials that transcends boundaries [75]. On one hand, one can prevent having to rely on recovery in the first place, namely by using free and open-source wallet apps, installing biometrical factors for unlocking them, locking one's wallet whenever it is unused and regularly backing up the entire wallet data [7].

On the other hand, the problem of honeypots persists (*cf.* subsection 6.1.3): SSI wallets literally contain all the digital data about a person's identity and will thus be a likely target for attacks similar to phishing emails. As a result, it will become increasingly difficult to distinguish between whom one can trust and whom not. One way to address this issue of trust anchors is to directly map actors known from the physical world into the SSI ecosystem [2, 7]. Therefore, entities like universities or authorities keep their role in their interaction with people, and we can rely on our sense for human trust that we already have.

1.4 Outlook Towards Potential Use Cases of SSI

While it is not certain that SSI will change our society as groundbreakingly as the internet did, it seems to be establishing itself as a paradigm for digital identity that will endure for some time. For instance, Switzerland has recently decided to develop a new *electronic identity* (eID) based on SSI [12, 68]. As a result, as we will see in chapter 4, concrete use cases arise from current analog processes coupled with identity checks using SSI, for instance [7]: a minimum age check for using age-restricted content without disclosing one's name or birthday, access to an event upon verifying vaccination/recovery/test status regarding some disease, or getting an interview/job after proof that one has earned the required degree. Concretely, all these use cases store credentials directly on the user's device, in a dedicated application called a digital *wallet*. Moreover, data contained in these credentials can be disclosed selectively in a privacy-friendly way. This report will go into SSI design choices once the necessary background is set.

Figure 1.4: Example SSI Use Cases (adapted from [7])

Of course, there exist many more potential use cases as those presented on Figure 1.4, but SSI is not a mature technology yet and we are standing at an early stage of its development. As a result, it is hard to navigate among possible applications. However, when introducing a new identity paradigm, it is of prime importance to select carefully which use cases will be implemented first, at the risk of hindering adoption if the scope is not clearly framed. This motivates the following question:

Which distinctive requirements characterize relevant use cases of self-sovereign identity (SSI)?

To answer this question (*cf.* Figure 1.5), we first provide the necessary background about SSI and *distributed ledger technology* (DLT), and describe some use cases as a motivation. Second, we elicit the requirements and threat model for SSI use cases, and assess the presented use cases based on the resulting framework. Third, we make design choices for a proof-of-concept of a relevant use case and set the foundational blocks for implementing it. This report will be completed with a discussion and a survey of related work.

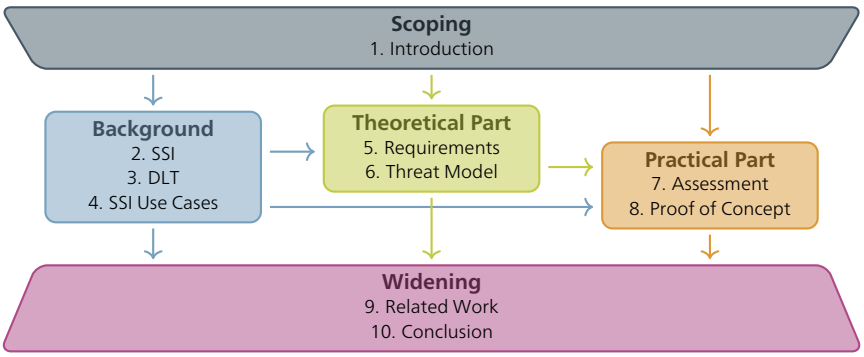


Figure 1.5: Map of this Document

2 Self-Sovereign Identity (SSI)

"Self-Sovereign Identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity."
— Christopher Allen [121]

First of all, although some high-level elements have been shown in the introduction, it is essential to introduce *self-sovereign identity* (SSI) in a proper way. For that purpose, this chapter will go through the SSI principles, its building blocks, architecture, as well as some arguments that provide inputs for a discussion about its adoption.

2.1 Introduction to SSI

2.1.1 Authentication with and without Identity Provider

In the classical models for digital identity described in section 1.2, an *identity provider* (IdP) is responsible for identity information [105]. In this paradigm, when a user connects to an online service, they need to authenticate to an IdP, which in turn provides the necessary attributes to the service itself. This usually happens through a protocol like the *security assertion markup language* (SAML) or *OpenID Connect* (OIDC) [35]. Despite the divergent terminology used in these protocols, the big picture looks as in Figure 2.1 for both.

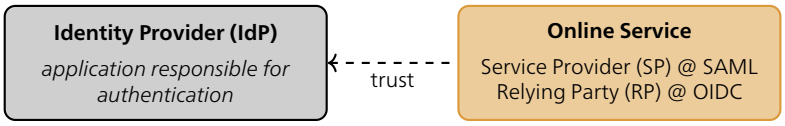


Figure 2.1: Authentication without SSI

As shown on this illustration, trust is established between the service and the IdP, because the IdP is holding information about the user. An IdP is usually organization-centric, as in the federation around SWITCHaai, but it may be user-centric as well, as in the approach taken by SWITCH edu-ID [24]. In the SSI approach [75, 105], the IdP will be completely removed from the picture, and the online service (or *verifier*) will have to trust the *issuer* of the user's (or *holder*'s) credentials instead[3], as shown on Figure 2.2.

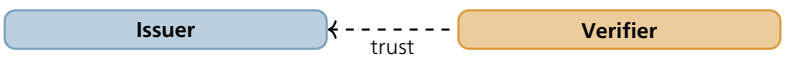


Figure 2.2: Authentication with SSI

[3] In fact, SSI comes with a specific terminology that encompasses the different roles that users can take on; see subsection 2.3.1.

2.1.2 SSI Principles

As we have seen, the use of SSI eliminates the need for an IdP, which pushes more control and responsibility towards the user. Consequently, the user can manage their own digital identity, which is a very elegant way to look at it, since it naturally extends their physical identity. Actually, such self-sovereignty should have been established since the beginning of identity management, but technology simply was not ready to implement it in a practical way. But it turns out that sovereignty is not the only rule of SSI: in fact, there is a number of principles that it is now time to introduce.

Indeed, 10 principles were formulated originally [105, 121], but they have been reorganized over time and there seems to be a new set of 12 principles at this point [75, 76]. However, the latter combines different ideas into single principles and remove some postulates from the former that are actually really important to SSI. Therefore, building on the 10 and 12 principles previously settled, I identified 20 principles for SSI, organized into the 5 pillars displayed on Table 2.1.

Identity	**Agency**	**Accessibility**	**Security**	**Inclusion**
Existence	Control	Access	Privacy	Participation
Representation	Delegation	Transparency	Minimality	Usability
Authenticity	Consent	Portability	Decentralization	Equity
Verifiability	Persistence	Interoperability	Protection	Consistency

Table 2.1: Principles of SSI

With this table uniting all relevant points from [76, 121], all principles underlying SSI are clearly stated and even categorized into a concise set of 5 pillars: identity, controllability, accessibility, security and inclusion. Hereafter, each principle of these categories is further explained [76, 121]:

1. **Identity**
   - **Existence**: Every SSI digital identity must belong to a user (any physical or moral person[4]) existing independently from the digital world.
   - **Representation**: A single user can have any number of SSI digital identities that represent them.
   - **Authenticity**: The data associated with an SSI digital identity can be proven to indeed authentically belong to the corresponding user.
   - **Verifiability**: Any claim that is associated to the SSI digital identity of a user can be verified by means of a (distributed) proof.
2. **Agency**
   - **Control**: SSI users own their data and are granted full responsibility to control it.
   - **Delegation**: In particular, they may delegate the management of their SSI data (in its entirety or parts of it) to a trusted agency of their choice, if they wish to do so (including children and "people lacking legal capacity").
   - **Consent**: Any data presentation may only happen with the SSI user's deliberate consent (not necessarily interactive, but well-understood as in human trust).
   - **Persistence**: An SSI digital identity needs to persist over time, so the corresponding user should keep control of their data on the long term.

[4] SSI users can thus be "any entity – human, legal, natural, physical or digital" [76].

3. **Accessibility**
    - **Access**: SSI users should be able to access all their own data at any time (or at least in an overwhelming majority of the time).
    - **Transparency**: The system underlying SSI interactions should be transparent, through free and open-source algorithms, accessible rules and policies, as well as open standards (for instance published in a public blockchain).
    - **Portability**: Claims about an SSI digital identity should be portable, which includes them being easily transferrable across devices or between users and an agency, but also them being recoverable without too many hurdles in case access is lost.
    - **Interoperability**: Usability of an SSI digital identity should interoperate successfully and securely across the boundaries of countries, technologies and implementations.
4. **Security**
    - **Privacy**: The storage system underlying SSI should ensure that the data and claims of a digital identity be kept private at all times. In particular, holders should be able to remain anonymous to verifiers if they want to.
    - **Minimality**: SSI should strive for the fact that claims about a digital identity contain the least amount of data possible, and when such claims are shared, only the minimal amount of data necessary be disclosed.
    - **Decentralization**: SSI should run on a decentralized infrastructure, so that by design no centralized entity can take control of user data for surveillance, censorship or freezing. This also calls for a distributed root-of-trust with cross-country and chained trust anchors, similarly to *certificate authorities* (CAs) with SSL.
    - **Protection**: The user's rights should be protected in priority, even if and when other stakeholders would join the SSI system.
5. **Inclusion**
    - **Participation**: Every user is free to participate in an SSI system or not, so that everyone can have a solution for every use case, even when SSI is not involved. (attention: some countries have made digital credentials mandatory for accessing e-Governmental services online)
    - **Usability**: The software solution that enables SSI interactions should be user-friendly and as simple as possible, so as to be usable intuitively and without difficulty by most users.
    - **Equity**: SSI should be fair and thus operate regardless of gender, sexuality, ethnicity, nationality and religion.
    - **Consistency**: The user experience should remain consistent over space (e.g. same check-in procedure in different hotels) and time (same procedure now and in ten years), so that every user can be guaranteed to know how to interact with the interface exposed to them by the SSI system.

With these 20 statements, the main idea behind SSI emerges quite naturally: users have the entire sovereignty for their own identity. In the terms of Figure 2.2, this means that we do not only have an issuer and a verifier, but also a *holder* of information in between, to which the entire responsibility is given, as will be described in subsection 2.3.1. Of course, this current description is still very theoretical, but it provides a good intuition as to what SSI is at a high level. Technically, we also care about requirements for SSI use cases, which include for instance the support for revocation, and we need to dig a bit deeper to understand how SSI works under the hood, and this is precisely the purpose of the next section.

2.2 SSI Building Blocks

SSI leverages four building blocks [105]: decentralized networks, decentralized identifiers, verifiable credentials and digital wallets.

2.2.1 Decentralized Networks

A *decentralized network* is an interconnection between multiple devices, or so-called *nodes*, that does not rely on any central component [105]. Typically, the need for decentralized networks is driven by mistrust towards other parties, which contrasts with the centralized client-server model, whereby a relatively small set of nodes "serve" requests from the rest of the nodes that fully trust them.

There exist various kinds of decentralized networks, and they are usually *distributed* over many geographical locations in the form of a *peer-to-peer* (P2P) network, where all nodes can both send and answer requests. Here are a few examples of decentralized networks [105]:

- **Distributed database**: data is stored at various places with either replication or partitioning;
- **Distributed hash table**: data can be stored on several nodes, depending on its hash value;
- **Distributed file system**: data is stored on a virtual file system using separate storage devices;
- **Distributed ledger**: data can be stored by means of transactions that are recorded on multiple nodes.

With the current evolution of SSI, most implementations will likely be built upon distributed ledgers, which is why chapter 3 provides an overview of this kind of decentralized networks, specifically blockchains.

2.2.2 Decentralized Identifiers (DIDs)

A *decentralized identifier* (DID) is a string that uniquely identifies a user of some decentralized network [105]. Indeed, one user can manage a number of different DIDs, but a single DID is always linked to a unique user. As a result, when interacting with a decentralized network, users can identify themselves *via* one of their DIDs, which in turn is linked to a standardized *DID document* in JSON format with information about the user's public key, through a process called *DID resolution*[5].

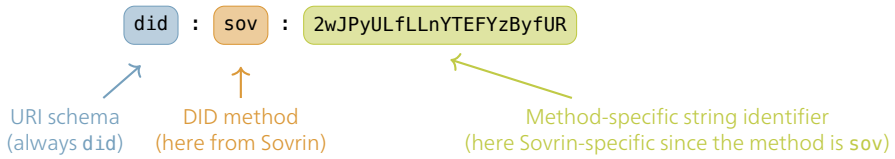


Figure 2.3: Example DID

Technically speaking, DIDs follow the structure illustrated on Figure 2.3 with an example taken from [17]. More precisely, a DID is one specific kind of *universal resource identifier* (URI) and consists of three parts: the `did` prefix, a DID method according to the unofficial registry [85] and a method-specific string.

[5] This resolution process is similar to DNS resolution that maps domain names to IP addresses.

2.2.3 Verifiable Credentials (VCs)

A *credential* is a set of statements that are bundled together in a standardized format. As such, it can contain more than one claim about someone's digital identity and these different pieces of information can be disclosed selectively, at the user's discretion. Actually, one may be familiar with credentials in the form of a username in the context of centralized identity, whereby the corresponding password can somewhat "prove" ownership of the credential. Of course, this is not very secure to verify that the user holds the credential.

As a result, we speak of a *verifiable credential* (VC) when the credential is cryptographically signed by its issuer [105]. In fact, there exist standards for VCs which specify the JSON format behind them[6], including support for *zero-knowledge proofs* (ZKPs), that enable a holder to prove ownership of a VC without even disclosing the data it contains. A simple example VC is provided on Listing 2.1.

```
"verifiableCredential": {
    "id": "0892f680-6aeb-11eb-9bcf-f10d8993fde7",
    "issuer": {
         "id": "did:example:76e12ec712ebc6f1c221ebfeb1f",
         "name": "EPFL"
    },
    "issuanceDate": "2021-05-11T23:09:06.803Z",
    "credentialSubject": {
        "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
        "degree": {
            "type": "MasterDegree",
            "name": "Master of Science"
        }
    },
    "proof": {
        "type": "Ed25519Signature2018",
        "created": "2021-05-17T15:25:26Z",
        "jws": "eyJhbGciOiJFZERTQYjY0Il19..nlcAA",
        "verificationMethod": "https://pathToIssuerPublicKey"
    }
}
```

Listing 2.1: Example VC for a Master Degree with Sample DIDs in JSON Format (inspired by [96])

2.2.4 Digital Wallets

A *digital wallet* is the electronic counterpart of a physical wallet. As shown on Figure 1.4 already, its purpose is to enable management of a number of VCs directly on a user application, that may or may not be integrated to the *operating system* (OS) of the device on which it runs. In any case, it leverages a secure storage environment that is only accessible through authentication. Strictly speaking, the literature sometimes defines a *digital agent* as a front-end interface for a digital wallet [75, 105], but the two terms are very close and in this report, we always speak of a digital "wallet", even when the agent application is meant.

In particular, two important functionalities provided by wallet applications are encrypted backups, for user-friendly recovery; and direct communication with other wallets, not necessarily through the internet [4].

[6] VCs can be in one of two formats, possibly encoded as *JSON web tokens* (JWTs): **AnonCreds** [3], which are flat since they only allow strings as values; or **JSON-LD** [40], which contain *linked data* (LD) and thus enable hierarchical values in the form of arrays.

2.3 SSI Design

The design of SSI can be described from two different perspectives: logical and architectural.

2.3.1 Logical Design: Trust Models

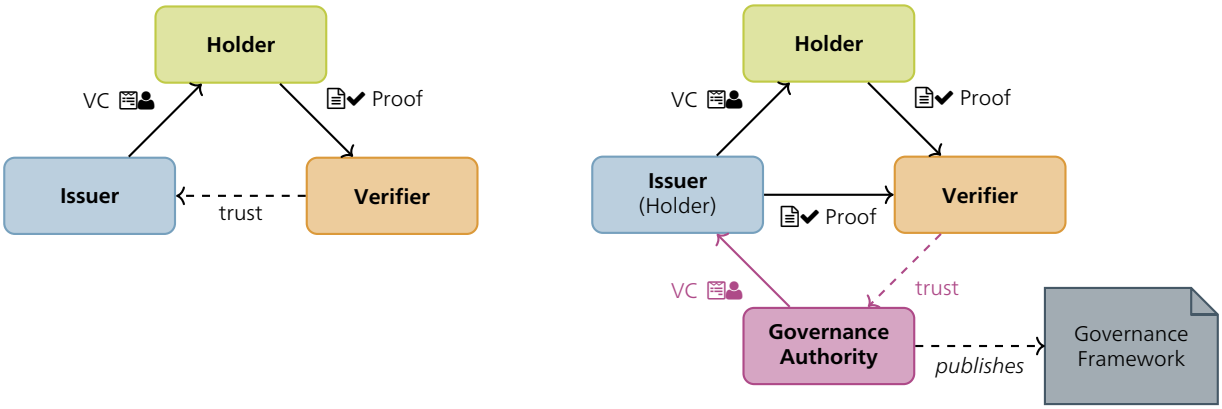
As alluded to in Figure 2.2, SSI users can play the role of an issuer, holder or verifier [75]:

1. **Issuer**: a user in this role "issues" (creates) VCs (usually governments, companies or universities);
2. **Holder**: a user in this role "holds" (manages) VCs (using digital wallets) and "proves" (shows) them to verifiers (for instance with ZKPs);
3. **Verifier**: a user in this role "verifies" (checks) VCs (using PKI digital signatures).

Together, these roles form the so-called *trust triangle* shown on Figure 2.4a. This triangle can be extended into a *trust diamond* to incorporate a fourth role, namely the one of a governance authority responsible of publishing a framework around the ecosystem [105], as added on Figure 2.4b:

4. **Governance Authority**: a user in this role can legitimate issuers, which thus also get a holder role.

The addition of a governance authority is controversial, because it is a central component in a decentralized system, as a result of which it is no longer possible for anyone to issue VCs. However, this role is probably necessary to enable standardization and thus compatibility between different SSI ecosystems[7].



(a) **Trust Triangle**: Issuer trusts holder, holder trusts verifier and verifier trusts issuer

(b) **Trust Diamond**: Verifier trusts governance authority instead of issuer directly (the rest follows the arrows)

Figure 2.4: Trust Relationships in SSI (adapted from [105])

Altogether, the more realistic trust model is the trust diamond, since it encompasses the governance that enables realistic applications. Indeed, much more than technical trust in the infrastructure, we need human trust in the users of the system, and this only works if some entity controls the way SSI is used. However, each verifier is free to decide whether they want to trust any issuer, or only those certified by some governance authority[8].

[7] This kind of governance authority is similar to the *root of trust* that exists in PKI, whereby CAs can create an entire chain of trust.
[8] This is again analogous to the way internet applications work with/without SSL, for instance with HTTP *vs* HTTPS.

2.3.2 Architectural Design: Layered Stack

SSI is designed around a stack of four layers, which are depicted on Figure 2.5: governance layer, credential layer, communication layer and identifier layer [75, 105].

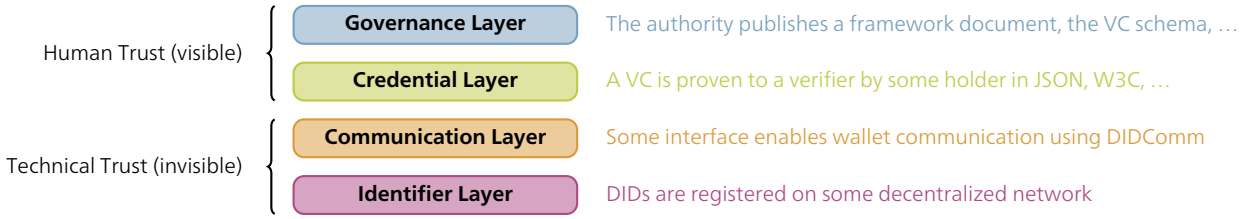


Figure 2.5: SSI Layers

Analogously to hardware/software co-design, SSI mixes human and technical trust, which goes hand in hand with the visibility of each layer. Indeed, the two higher-level layers are visible to the user, since they involve the human trust relationships illustrated in Figure 2.4; and the two lower-level layers are hidden from the user, as they rely on the technical infrastructure underlying SSI. In particular, if we look at this stack bottom-up, the first two layers involve technical details that end-users should absolutely not worry about:

- At the **identifier layer**, most of the interaction happens with the decentralized network, whereby some DID method enables the creation of DIDs. This may use transactions and *smart contracts* on a blockchain (*cf.* chapter 3) or simple loads/stores on a database.
- At the **communication layer**, the DIDComm protocol [4] enables "transport-agnostic" communication[9], which means that two wallets can exchange VCs over different kinds of channels.

On the other hand, users need to get involved directly with the upper two layers:

- At the **credential layer**, the trust relationships shown in Figure 2.4 become relevant. Users decide whom they trust and whom not, whereby they establish the information flow of the data that is created/stored/exchanged in the system. During such an SSI interaction, they can either trust the issuer directly, or require a second proof from said issuer that was itself issued by an authority.
- At the **governance layer**, such a trusted authority is taking decisions about who can issue VCs. This may well be a distributed committee, so as to avoid having arbitrary centralized control. In practice, distributed ledgers are able to generate new trust anchors by using majority voting[10].

It is important to note that the information is not encapsulated in the same way as in the internet layers [70]. As we stated, the two uppermost layers are both visible to the end-user, which encompasses human *trust* into a governance authority and knowledge of one's own *identity* credentials. This trust and identity framework forms the interface that is exposed to users and services. Under the hood, there is a technical platform comprising the two bottommost layers, but these should be completely transparent to both users and services, so that ideally they do not notice the burden of exchanging information anymore.

[9] DIDComm messaging is said to work over "HTTPS 1.x and 2.0, WebSockets, BlueTooth, chat, push notifications, libp2p, AMQP, SMTP, NFC, sneakernet, snail mail" [4].

[10] However, governance authorities are still in an early development stage, since at this point, "not many SSI-specific governance frameworks have been created yet, if even" [105].

2.4 Discussion

The design of SSI is backed by a number of standards already, but its adoption depends largely on the use cases that will be developed to run on top of it. This is why there is an ongoing debate [104, 105] about the pros and cons of SSI, which are listed in the non-comprehensive Table 2.2. These pros/cons are categorized into 6 topics and we are discussing each of them hereafter.

Topic	Pros	Cons
Infrastructure	IdP elimination	Challenging recovery
Trust	GDPR compliance	Infrastructure dependency
Identity	Difficult profiling	Need for many DIDs
Compatibility	Global infrastructure	Interoperability issues
Applications	Wide scope	Adoption hesitancy
Design	Clean ecosystem	Risk of over-engineering

Table 2.2: Pros and Cons of SSI

2.4.1 Infrastructure

As we have seen, the role of an IdP is no longer needed, which diminishes the cost of operation at the concerned companies. However, the fact that users can no longer rely on some external maintenance service means that data recovery becomes more challenging. In particular, private key recovery is non-trivial, analogously to how it works on blockchains, but there exists work in this area. More specifically, two proposed ways to tackle data retrieval are recovery codes and social recovery:

- **Recovery codes**, similar to those in SWITCH edu-ID [48], could retrieve lost VCs if they are properly backed up on an appropriate service[11];
- **Social recovery** could rely on multi-signature transactions[12], analogously to blockchain systems when a certain amount of parties needs to approve a transaction or smart contract (*cf.* subsection 3.1.2).

2.4.2 Trust

On one hand, the SSI principles listed on Table 2.1 comply with the ideas of the *general data protection regulation* (GDPR) [123], specifically when it comes to transparency, data collection and minimal disclosure.

On the other hand, the "right to be forgotten" may be difficult to implement in practice [75] when data is stored on *e.g.* a blockchain, which is *immutable* by design[13]. This introduces a dependency on the underlying infrastructure, which should in theory neither leak to the user, nor influence their technical trust. However, SSI use cases are not planning on storing PII on its underlying data structure, so this concern only holds for VC schemas, which are not critical.

[11] Blockchain identities often operate with a list of 12 recovery words, that one has to store securely when generating the private/public keys, either in a virtual password manager or a safe physical storage.

[12] In such a scenario, one would need to define a set of trusted delegated agents upon opening a digital wallet, which starts to sound like some sort of social media network.

[13] As will be explained in chapter 3, immutability of a data structure means that its operations are append-only, and thus existing data cannot be definitively deleted without erasing the entire data structure.

2.4.3 Identity

Thanks to the privacy-preserving design of SSI, profiling becomes hard or even impossible for interested parties. Additionally, this sends a clear message against privacy breaches, as [104] expresses very well:

> *the right to informational privacy […] constitutes a moral objection to data mining and subsequent profiling that effectuates construals of an individual's identity without his or her input in this process*

Nevertheless, the mechanisms that make correlations about a user difficult require many DIDs to be created by every single user of an SSI ecosystem. This is somewhat mitigated by the fact that there is no unique DID method, which scales much better than a limited set of names[14].

2.4.4 Compatibility

It should be noted that one major concern with SSI is that of compatibility: indeed, while the infrastructure can be built on top of our global internet, common schemas have yet to be defined at the international scale, which requires more work than just sanitizing entries. As a result, interoperability should be a primary area of research and collaboration in international organizations.

2.4.5 Applications

Due to the omnipresence of identity checks on the internet and in the real world, SSI has a very wide range of possible applications. Therefore, many use cases arise, as will be presented in chapter 4, but this also means that people will be hesitant to adopt SSI. In fact, even with technologies that are not meant as replacements for existing ones, adoption goes through a time of transition, where both co-exist, after which one becomes predominant. In particular, issuing institutions may be reluctant to changing their workflows in order to create VCs instead of their physical counterpart.

2.4.6 Design

One last advantage of SSI (or at least the one that will close this discussion) is its clean design. Indeed, due to its natural principles, an SSI ecosystem will provide many benefits as compared to a current solution based on centralized IdPs or even the *public key infrastructure* (PKI). As a counterpart, having everything on the same ecosystem may create over-engineering, in the sense that SSI would not be needed for some of its use cases, but would still be used and make things more complicated [104]:

> *translating existing credentials systems into privacy preserving digital formats […] may lead to the normalization of new standards for cryptographically verified data in the scenarios where individuals previously were not expected to […] provide such data at all*

[14] For instance, IPv4 does not scale very well, since its format has been predefined with a limited length. When it comes to IPv6, the community seems optimistic about the newly added scalability, but the format is again limited, which still does not scale as well as DIDs, for which methods have essentially full control over the unique string they generate.

3 Distributed Ledger Technology (DLT)

"Once you have understood what Blockchain is, you can no longer sleep at night"
— Stephan Karpischek [110]

An SSI ecosystem relies on some decentralized network to store its schemas, DIDs and possibly data; although we choose to never store PII publicly (*cf.* subsection 8.1.3). Despite multiple possibilities, distributed ledgers are commonly used to implement SSI use cases. Thus, this chapter describes *distributed ledger technology* (DLT) top-down in the most accessible way possible, with a special emphasis on blockchains.

3.1 Distributed Ledgers

Generally speaking, a *distributed ledger* [30] is:

- a **ledger**, which is some data structure that keeps track of a series of **transactions** in a form that is append-only, *i.e.* **immutable**;
- that is **distributed** over several nodes, meaning that the state machine representing the data structure is **replicated** at several peers that communicate with, but do not necessarily trust, each other.

In other words, a distributed ledger is a redundant log of transactions, which ensures auditable ownership (one can browse the history), as well as federated validation (participating nodes trigger consensus).

3.1.1 Transactions

More precisely, a *transaction* in a distributed ledger transfers ownership of an asset from some set of input parties, which sign the transaction with their private keys, to a set of output parties, identified by their public keys [124]. Usually, transactions incur some fees towards the system, which is depicted as such on Figure 3.1.

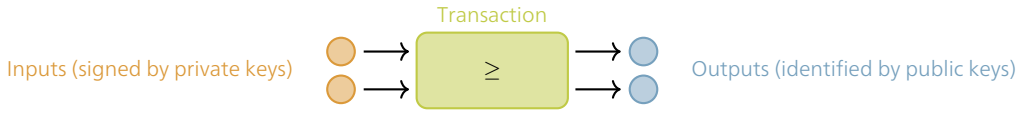


Figure 3.1: Transaction on a Distributed Ledger

3.1.2 Smart Contracts

Smart contracts are advanced transactions [72] which enable agreement over some piece of code that is executed on the ledger, additionally to the transfer of ownership of an asset. More precisely, the input parties agree to execute some transaction according to one of the following two signature formats:

- **Single-Signature**: a single party signs the transaction (either it is the only input party or one signature is sufficient for the considered smart contract);
- **Multi-Signature**: multiple parties need to sign the transaction (typically k out of n need to agree, where $0 < k \leq n$).

Various programming languages, such as Solidity or Vyper, can implement smart contracts, which can be considered low-memory classes with methods as in object-oriented programming. Typically, read operations can be executed for free, whereas write operations have some cost in the form of a transaction fee.

3.1.3 Kinds of Distributed Ledgers

These concepts of transactions and smart contracts provide a good overview of what a ledger can do, and of how its distributed nature enables scalability over a large set of nodes across the internet that continuously tries to reach consensus. Usually, three kinds of distributed ledgers are documented: *blockchains*, *directed acyclic graphs* (DAGs) and other technologies, as shown on Figure 3.2[15].

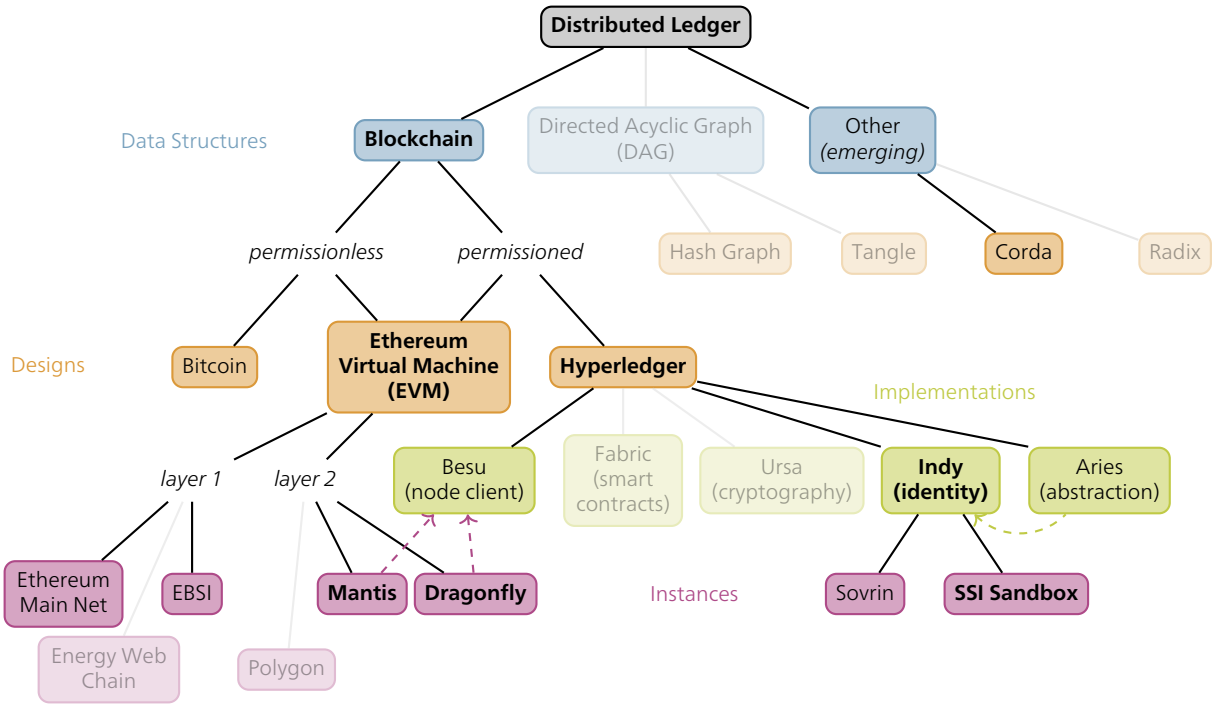


Figure 3.2: Non-Exhaustive Overview of Relevant Distributed Ledgers

[15]This figure emerged over various conversations with Robert Ott. It will serve as a basis for this entire chapter and all of its aspects will be explained hereafter.

3.2 Blockchains

While distributed ledgers may leverage various technologies in order to organize transactions in different ways, we will focus here on blockchains, since these are currently most commonly used. Blockchains organize transactions into **blocks**, so that the entire history of the ledger is a **chain** of blocks (hence the name).

A single *block* contains a list of transactions that attached to it, as well as a pointer to the previous block. Overall, different rules are used across different blockchains [119], but generally there can only exist a single longest chain of blocks since the initial block of the chain, called the *genesis block*. If multiple blocks are created concurrently, then a so-called *fork* happens, but eventually all nodes agree on the longest chain, as is illustrated on Figure 3.3.

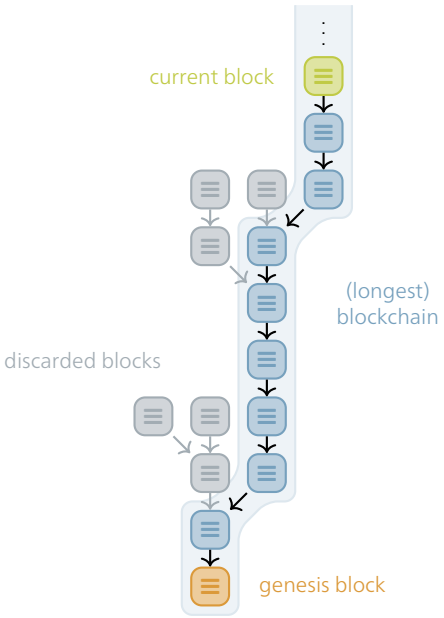


Figure 3.3: Sample Blockchain

3.2.1 Kinds of Blockchains

As shown on Figure 3.2, there are two kinds of blockchain models [101]:

- **Permissionless blockchains**: everyone can validate transactions and create new blocks according to the cryptographic proof in force for consensus;
- **Permissioned blockchains**: only a single architect or consortium of administrators/organizations is responsible for validation and block creation.

Orthogonally to this terminology, one can also distinguish [101]:

- **Public blockchains**: everyone can create transactions (possibly with fees) and see the history;
- **Private blockchains**: only a restricted set of users can issue transactions or see the history.

3.2.2 Cryptographic Proofs for Consensus

Building on top of Merkle trees [44], the original Bitcoin paper [126] brought to life the concept of a blockchain as a tree of blocks for distributed digital ownership without a centralized control instance. In particular, this paper introduced a new way of solving consensus that prevents *double-spending*. In other words, one should not be able to spend the same money twice. Therefore, whenever a transaction is submitted to the system, it needs to be validated and entered into a block.

Let's take the example of two transactions trying to spend the same money: the first of the two is validated into a block, but the second one is considered invalid by that block or any its children, so it may only be validated by a block in a different fork that has not already validated the previous transaction. As a result, only one chain can be considered entirely valid, which prevents double-spending.

As illustrated on Figure 3.3, every block points to its parent block, but forks may happen at any point. Thus, it becomes complicated to select the longest chain if the rate at which new blocks are generated is not constrained. Therefore, every block possesses some cryptographic challenge, and only nodes that can prove that they are allowed to create a child block can actually do so. This proof can take different forms[16] [55]:

- ***Proof-of-work* (*PoW*)**: every block has a cryptographic challenge, which takes computational resources to solve, so only the nodes that put in the "work" (and energy[17]!) can create blocks;
- ***Proof-of-stake* (*PoS*)**: only the nodes that have a certain amount of assets can generate blocks, which is thus proportional to the current financial situation in the blockchain;
- ***Proof-of-authority* (*PoA*)**: there exists a consortium of validator nodes, which are the only ones to be able to validate transactions and generate blocks (as a sweet spot for low energy and moderate trust).

3.2.3 Blockchain Designs

There exist multiple designs of blockchains, of which the most famous is certainly *Bitcoin* [126]. Nevertheless, other designs exist, such as the approach taken by the *Ethereum Virtual Machine* (EVM), under which the Ethereum main net operates, or *hyperledgers*, which enable domain-specific blockchains. For a more detailed overview, Table 3.1 shows the three most common approaches introduced in Figure 3.2 [118].

Design	Consensus	Comments
Bitcoin	PoW	Mostly for financial applications
Ethereum	soon PoS (currently PoW)	Enables smart contracts on both layer 1 and layer 2 blockchains
Hyperledger	often PoA	Can be made compatible with Ethereum

Table 3.1: Three Possible Designs for Blockchains

One important point is the one of *layering*, as alluded to in [22]: while layer 1 blockchains (L1s) can be considered cities, layer 2 blockchains (L2s) can be seen as skyscrapers. In this analogy, one has to walk or take public transportation to get around in L1s, while only a staircase or elevator is needed for L2s. In more technical words, L2s issue a periodic "digest" transaction onto the underlying L1, which makes the two intercompatible while avoiding the overhead of using the L1 directly.

[16] There exist more kinds of cryptographic proofs than the three presented here, but these are the most relevant ones here.
[17] The PoW model is extremely unsustainable due to the huge amounts of energy it consumes, but it does not require P2P trust.

3.3 Hyperledgers

Along with the emergence of the most famous, but slow and congested[18] Bitcoin and Ethereum networks, whose applications lie primarily in the area of cryptocurrencies or distributed applications [118], additional possible uses of blockchains appeared. For instance, the immutable nature that they inherit from distributed ledgers plays along nicely with many use cases that require auditability. Furthermore, the possibility of executing code *via* smart contracts makes them appealing when it comes to automating processes.

3.3.1 Hyperledger Projects

Consequently, the hyperledger foundation, initiated by IBM with the Hyperledger Fabric project [116], has associated itself with the Linux foundation [71] and has since released different implementations for various domains of application. Here, we list the three hyperledger projects that are most relevant to this work:

- **Hyperledger Besu**: Besu [38] provides an "execution client" for Ethereum that supports both PoW and PoA, thus it is frequently used to run nodes, both for the Ethereum main net and smaller instances such as Dragonfly nodes (*cf.* subsection 3.3.2);
- **Hyperledger Indy**: Indy [39] provides an interoperable client for managing digital identities on a blockchain, together with a *command-line interface* (CLI) as well as support for multiple programming languages;
- **Hyperledger Aries**: Aries [37] provides an abstraction layer for managing verifiable credentials (*e.g.* on top of Indy), and it may ultimately become a standard interface for SSI interactions (as a substitute for Indy, using its mechanisms only under the hood).

These hyperledger implementations do not all offer the same functionality. Most importantly, the two latter, which are designed for identity, are not as mature as the first when it comes to EVM specificities.

3.3.2 Hexapods: Dragonfly and Mantis

As an example, SWITCH is participating as a validator node in the Hexapods project, which currently comprises the Dragonfly and Mantis blockchains. Both of them operate under the PoA consensus model among a set of companies as trust anchors; such as IBM, Green, Phoenix Systems, SWITCH and more. They are built as L2 blockchains on top of EVM using hyperledger Besu clients and regularly store hashes of block digests on the Ethereum main net. More precisely:

- **Dragonfly** [31] is the main net and its goal is to serve educational as well as commercial purposes for various use cases of blockchains using DFLY coins;
- **Mantis** [43] is the test net and its goal is to test and optimize blockchain applications for later Dragonfly deployment (a Mantis "faucet" is provided to acquire MANTIS tokens for free).

Both Hexapods blockchains use Besu clients for running L2 blockchain nodes.

[18] This again links back to the analogy of cities, whereby large cities have high traffic volume.

3.4 Decentralized Networks for SSI

By now, it has become clear that different distributed ledgers have different applications. For instance, there is no such thing as "the" universal blockchain. Nevertheless, different ledgers can be made interoperable with each other thanks to abstractions that hyperledgers bring us. Moreover, it is possible to implement so-called *bridging*, whereby two ledgers can become compatible with each other. As we have seen in subsection 2.1.2, interoperability is one core principle of SSI, which advocates in favor of the use of distributed ledgers as the underlying decentralized networks of choice when implementing an SSI ecosystem. In fact, several blockchains with a special focus on digital identity have already appeared.

3.4.1 Sovrin

Sovrin is a "public permissioned" blockchain [120], *i.e.* with "public access with trusted governance" (*cf.* subsection 3.2.1), that is specialized for SSI. It is maintained by the Sovrin Foundation and based on the open-source hyperledger Indy project, which itself is meant for identity applications. In particular, Sovrin enables people to generate multiple DIDs per user, which also links back to privacy "by design" [118]:

> *given the right blockchain economics, DIDs can be cheap, so people can generate as many as they need to protect their privacy*

3.4.2 EBSI

The *European Blockchain Service Infrastructure* (EBSI) [53] is a user-centric blockchain that is meant to operate cross-boundaries in more than 20 countries for *electronic government*al (eGov) purposes. However, it is out of reach for Switzerland due to political reasons, since it is affiliated with the European Union.

EBSI has been in deployment since 2020 and should gain some additional maturity between mid- and end-2022. At the moment, it supports various SSI use cases [29]:

> *EBSI supports the creation of cross-border services that help citizens and businesses manage identity & educational credentials and social security coverage*

3.4.3 Other Instances

In theory, any blockchain could be used for digital identity, but of course those designed specifically for this purpose are much more appropriate. On top of that, there exist some other instances of blockchains with specific additional goals in mind, such as the *Energy Web Chain* (EWC), with sustainability objectives; or Polygon, that is able to interconnect different blockchains with Ethereum. Of course, as a first point of contact with the SSI world, it is also possible to independently run a couple of nodes using hyperledger Indy, for example in the form of an SSI Sandbox environment (*cf.* section 8.1).

With these elements, we should have covered enough background in order to clarify Figure 3.2, which is probably the most important takeaway from this chapter on distributed ledgers.

4 Description of Some SSI Use Cases

"When you hear the term 'VC' or 'Verifiable Credential', think 'authenticatable data container' and you'll be closer to the truth, plus you'll be more effective in explaining VCs to the next person."
— Timothy Ruff [77]

Now that we have covered the necessary background to understand SSI and underlying distributed ledgers, it is time to look at some of its use cases. In fact, Figure 1.4 has shown some motivating examples of verifiable credentials, but it turns out that any kind of data can be encoded as such. Therefore, this chapter looks at existing use cases of SSI, as well as further possibilities, both when it comes to single VCs or combinations thereof. After that, we describe some selected use cases in detail as a preparation for chapter 7, in which we analyze those more in depth, in light of the threat model and requirements elicitation that will follow.

4.1 Existing Use Cases

We start by looking at use cases of SSI that have already been implemented on relatively small populations. In particular, we consider two user-centric approaches to identity applications and employee management.

4.1.1 ID Wallet

ID Wallet [87] is a German project that aims to couple a base state identity with several applications in the private and professional life of citizens. Mainly, the output product of the project is a wallet application to be installed on one's smartphone, which can hold credentials that are supported in various participating places around Germany.

At the moment, two situations have been covered by the ID wallet project: hotel check-in for business travelers and driving license checks in digital form:

- **Hotel check-in credentials** [92]: employees from various companies can facilitate their arrival procedure by proving their affiliation and booking *via* verifiable credentials to the hotel staff;
- **Digital driving license** [91]: citizens can prove their ability to drive digitally to some car sharing services, although they still need their physical driving license when interacting with the police.

This project failed in Germany due to bad scoping: it was meant to be a demonstration, but it used real data, thus theoretically targeting any citizen, which did not scale well. Indeed, the custom distributed ledger underneath was not designed for production use and it quickly saturated [64]. As a result, the ID wallet application can no longer be downloaded at the moment, and the responsible team is working towards fixing security issues that arose due to the small scale of the underlying decentralized network.

4.1.2 Digital Staff Passport (DSP)

In the *United Kingdom* (UK), the *National Health Service* (NHS) has noticed that healthcare employees move quite frequently around different hospitals, especially in the early years of their careers or when different hospitals have different needs. This resulted in repeated identity checks and training participation, which not only frustrated employees, but also made everyone lose precious time that could have gone into patient care for saving lives. The *digital staff passport* (DSP) is the solution to this problem, and it consists of an employee "pass" that is issued based on the SSI principles (*cf.* subsection 2.1.2). It can check for qualifications, so that employees can be employed at other hospitals with an easier onboarding process.

In the frame of this project, two schemas for verifiable credentials[19] have been defined on the Sovrin main net (*cf.* subsection 3.4.1):

- **Employment Credential** (`NHS-X Covid-19 E0`): contains "basic personal details about the staff member", their "current job role" as well as "employment checks" [107];
- **Vaccinator Credential** (`NHS-X-Vaccinator`): additionally provides "vaccination training status by specific vaccine" [33].

Further credentials seem to be planned for the future, but at the moment this well-defined scope is one of the reasons why DSP has been successful until now: it is not overly ambitious. Additionally, it leverages the existing Sovrin blockchain for managing identity, which eases adoption for both staff members and participating hospitals. Lastly, it came at a time of high demand, since the COVID pandemic has required fast moves between institutions to bring qualified doctors where they were most needed.

4.2 Possible Use Cases for Single VCs

When it comes to future SSI use cases, we can look at a much wider range of possibilities, both those involving a single VC and those combining VC of different sectors. For the time being, we will start with single VC use cases, in the areas of immunity, pharmacy and employment.

4.2.1 Immunity Certificates

With the COVID pandemic, our social system had to flexibly adapt to a rapidly changing situation. Therefore, one of the solutions that was set up was the now famous COVID certificate, which enabled traveling cross boundaries thanks to a proof of full vaccination, negative test or recent recovery. As such, these certificates were usable all across European countries, which links back to the SSI principle of interoperability.

However, more generally, the concept of an immunity certificate still makes sense from a global point of view. Indeed, countless countries require specific vaccines when issuing visas, and, even if optimistic thinking provides the best outlook on life, other diseases may appear in the future with similar consequences that the COVID pandemic. As a result, such immunity certificates could be included in future SSI wallets, and there are two possibilities to be taken into account:

[19] Both of these credential schemas (*cf.* hyperlinks on their `NHS-X` names) are visible on IndyScan (`https://indyscan.io/`), which is a transaction explorer that supports Sovrin, since it is built on top of hyperledger Indy.

1. **Immunity linked to prior identity**: Despite the matching interoperability principle, COVID certificates did not use SSI[20]. More precisely, verifying someone's identity still required a physical identity card that could only be linked to the certificate by manual inspection. This shortcoming is probably due to the lack of maturity of SSI at the time where our society needed an urgent response to the occurring events. Future immunity certificates could be plugged onto an electronic identity once it is available in the form of an SSI VC as well.
2. **Immunity without prior identity**: Nevertheless, it is possible to use SSI to show that one is vaccinated/tested/recovered even without an existing electronic identity VC. Indeed, with the presence of undocumented refugees/migrants, it becomes hard to leverage an existing identity for manual checks; this is where SSI can help by providing a legal digital identity to those in need [83].

Both of these flavors for immunity certificates could be integrated into an SSI ecosystem in a form similar to COVID certificates, by linking basic identity information with immunity attributes.

4.2.2 Medical Prescriptions

In the area of health care, there is another use case of SSI that could enable easier interactions between staff and patients, which is the one of prescriptions. Indeed, after a visit to one's doctor, one may receive a paper with a handwritten list of medications to go buy at a pharmacy. However, such a list might be error-prone because it is hard to read, which has caused a number of medical errors in the past [125]. As a result, [79] proposes a scenario where one can get a digitally signed VC at one's doctor instead of a physically signed paper containing the same information.

This use case would enable patient-centric data handling, which does not only make the process of buying medications more privacy-friendly, but it also tackles the readability issue that was raised before. Additionally, it could also ease the interactions with a potential insurance company that would reimburse the cost after the purchase.

4.2.3 Employment Status

When it comes to one's professional life, it could be possible to prove employment or §<unemployment *via* VCs. Indeed, our professional activity is culturally linked with our identity, and its temporary aspect can be covered by revokable or expirable credentials. The applications of such a credential lie in unemployment income authorization, access control for office buildings or even easier opening of bank accounts.

4.2.4 Public Transportation Tickets

Finally, in the area of mobility, public transportation tickets can already be stored in digital wallets, but they are currently not bound to an identity. SSI could enable such a link, and this would further ease the verification process, possibly even drastically reducing the amount of manual checks. For example, IDunion is working on a project for reduced yearly subscription to German public transportation for students.

[20] As explained in [89], digital COVID certificates rely on *public key infrastructure* (PKI), which handles both digital signatures and revocation lists.

4.3 Possible Use Cases for SSI Interactions

The previous use cases are based on single VCs handed to a user, who later transfers them further by disclosing the minimal amount of information necessary for the relevant purpose. Now, let us look at more advanced use cases of SSI which require interactions between multiple VCs at a time.

4.3.1 Transportation as a Service (TaaS)

In the area of mobility, there has been a recent addition to the public transportation service with the development of car sharing. More generally, other vehicle types can be rented in the context of *transportation as a service* (TaaS), be it bikes, motorcycles, electric scooters or even boats. In some of these situations, it is necessary to provide a credit card, a driving license or a proof of attendance for some introductory course on traffic regulations. However, since each of these elements are issued by a different entity, it requires interactions between different sectors as well. Additionally, there exist numerous mobile applications with similar functionality, which creates redundant information flows and possible correlation attacks.

As a result, SSI would be a solution to ease and secure interactions by handing all proof information to the user themselves. In such a scenario, the trusted issuers would be banks, traffic authorities and course organizers, which explains why cooperations becomes much more straightforward when the user takes responsibility for their data and decides where they want to steer it to.

4.3.2 CarDossier

CarDossier [42] is a Swiss project that is planning to leverage a blockchain for all kinds of car-related interactions. It is built on top of Corda [122], which is a distributed ledger focused primarily on financial applications[21]. A pictorial representation shows the idea of CarDossier on Figure 4.1.

Figure 4.1: CarDossier Ecosystem (adapted from [110])

As one can see, the resulting ecosystem is car-centric, but the SSI holder role is still played by a human user. When it comes to transferring ownership, distributed ledgers handle transactions by design, which boils the procedure down to a simple transfer to another public key or DID.

[21] Corda is not a blockchain (*cf.* Figure 3.2), since it propagates transaction information only "on a need-to-know basis" [122].

4.3.3 Student Matriculation and Family Allocations

The last two use cases of this section provide advantages for families[22]. Indeed, the Swiss social system enables family allocations from one's employer if one has a child that is studying in a university or some other higher education institution. However, in order to benefit from those allocations, the employee needs to renew their demand every semester, for their employer to ensure that their child still be a student. In principle, this interaction does not take a lot of time, but it happens repeatedly over the course of a student's studies, which generates a high volume of traffic and a tangible burden on both students and employees.

Here, SSI could help by providing a more user-centric approach to the proving process. For instance, the flow could go as follows: the student gets their matriculation certificate as a VC and shares it with their parent, who in turn discloses the minimal amount of information required to their employer. For instance, it could be sufficient to provide the semester dates and the fact that their child is a student, and not the name of the university. While this last piece of information is not necessarily confidential, it generates more data traffic and it may sit around indefinitely on some possibly insecure server, which contradicts the idea that one should be fully responsible for one's data.

Additionally to these dispositions, if employment credentials would exist as described in subsection 4.2.3, then the employee could also show this VC as a complement to the student's matriculation VC, which would further fortify access control.

4.3.4 Certificate of Residence and GA Travelcard

Staying in the area of family advantages, we now cover the case of GA travelcards. The Swiss railway company, SBB CFF FFS, has a number of available tickets available for purchase for taking the train. Furthermore, there exist subscription-based travelcards which cover the entire network of public transportation, including trains, buses and boats. Such subscriptions provide price benefits if one is traveling frequently enough: with the half-fare travelcard, one only pays half the price for all public transportation tickets; and with the *general abonnement* (GA) travelcard, one can freely take any means of public transport without paying a ticket. Since such GA travelcards are quite expensive, SBB CFF FFS has a special offer described on [51]:

> *Children, single young persons and their parents can obtain the GA Travelcard at cheaper prices […] If at least one parent in the same household has a basic GA Travelcard*

When it comes to verifying that all involved people live "in the same household", all family members have to provide a yearly certificate of residence, which they can obtain at their town's administration office. This is where SSI could help, because if such confirmations of domicile could be issued by the administration as VCs, all family members would only need to show their VC to the railway company instead of signing documents on paper and waiting for them to be delivered by mail.

The advantages of such a user-centric approach are three-fold: first, the process would become more efficient; second, the proof would be more secure than currently, because VCs are digitally signed (as opposed to paper signatures, which can easily be faked); and third, there would be no need for periodic updates since VCs can be revoked once they are no longer valid.

[22] The ideas behind these two subsections were mentioned in discussions with Edouard Bugnion.

4.4 Detailed Description of Selected SSI Use Cases

After having looked at a set of various use cases for SSI on the surface, we now dive a bit deeper into three selected use cases that are of more relevance for the current work. More precisely, let us look at electronic identities, digital diplomas and life-long learning.

4.4.1 Electronic Identity (eID)

First of all, if we consider electronic identities, there exists a European project called *Electronic Identification, Authentication and Signature* (eIDAS) [80], which is building the foundations for a European *electronic identity* (eID). In Switzerland, the eID bill (draft for future law) is also evolving these days, with the goal of being interoperable with other countries as well.

eIDAS in Europe To begin with, eIDAS is envisioning an entire ecosystem of SSI use cases in the context of their *eIDAS Bridge* activity [81], including for instance eID, eSignatures, eTimestamps, eCertificates, eSeals or eDelivery. The main point of such a European eID is to make SSI cross-border, so that it can be compatible from one country to another without additional effort. This goal motivated the eIDAS regulation [32] for secure cross-border transactions. In particular, it has two interoperability objectives similar to the SSI trust stack (*cf.* Figure 2.5):

1. **Technical**: National eIDs should be usable everywhere in the *European Union* (EU);
2. **Human**: Electronic credentials should be legally equivalent to their paper counterparts[23].

With these two points in mind, eIDAS is preparing the ground for a European eID, which can have multiple applications in the life of a citizen [109]: student mobility, taxation, SIM card ownership, patient record issuance and even *Know Your Customer* (KYC) in the context of finance[24], where parties want to trust each other on a personal level.

eID in Switzerland In Switzerland, the main source of trust is the physical identity card, but there exists a law called ZertES [97] that regulates digital certificates (similarly to eIDAS elsewhere in Europe). In the sense of digitalization, a popular initiative was subject to vote in March 2021, but it was rejected by a surprising majority [8], mostly because of concerns related to the IdP delegation to private companies and the resulting privacy insecurities [8]. As a result, the *Federal Office of Justice* (FOJ) wrote a discussion paper about the eID vision [67], where three approaches are considered for an eID implementation:

1. **Centralized Identity Provider (IdP)**: Under this solution, the government would take on the role of a centralized IdP, following the user-centric model for digital identities (*cf.* Figure 1.2). When it comes to interoperability with other countries, a federation could be set up, to which the Swiss eID could participate, enabling citizens to use cross-boundary services. Having the government as an IdP would speed up adoption of an eID, but it contradicts the idea of a private identity and may not convince citizens that were concerned about a private company auditing their data. Therefore, it could be a better option to rely on well-known technologies such as PKI.

[23] This human law, however, needs to be enforced by cryptography, which brings some technical background underneath.
[24] In Switzerland, this KYC use case can be categorized under *Finanzmarktaufsicht* (FINMA).

2. **Public Key Infrastructure (PKI)**: Using PKI boils down to relying on asymmetric cryptography to ensure that credentials are digitally signed with private keys and encrypted with public keys. Similarly to the approach taken by digital COVID certificates (*cf.* subsection 4.2.1), this solution would rely on some scalable database with accessible public key information. However, it is unpractical to use because it doesn't support data selectivity: the identity certificate could be shown either as a whole or not at all. Therefore, it would be difficult to operate at the desired granularity when showing only one aspect of one's eID to someone. A potential mitigation would consist in issuing application-specific certificates, but SSI contains this minimality principle by design.

3. **Self-Sovereign Identity (SSI)**: A user-centric ecosystem can be designed using the SSI principles presented earlier. Since the EU is moving towards adopting SSI, this would also tackle the interoperability with other countries. As we have seen, VCs can be issued and revoked, which closely relates to the real world situation, and the eID would just be one VC among many others. However, fake VCs may be issued or presented in practice, because people could very well find a way to abuse the system. Despite these challenges, the government has conducted a discussion and then decided to use an SSI implementation for the future eID [68], because it effectively tackles the main concerns that voters initially had when private companies were supposed to be responsible for their data [8, 98].

Orthogonally to these three possibilities for implementing an eID, [67] defined three "levels of ambition":

1. Digital identification with eID only;
2. State-regulated certificates linked to, but not limited to, eID;
3. Digital proofs within a wide range of so-called "sectors".

In accordance with the reactions to this discussion paper, the Swiss government decided [65] to settle for an SSI implementation with the third and thus broadest level of ambition. In other words, it is "building a Swiss digital trust ecosystem" [2]. Among other elements, this report presents the infrastructure of trust that should underlie the common SSI ecosystem across the public sectors illustrated on Figure 4.2.

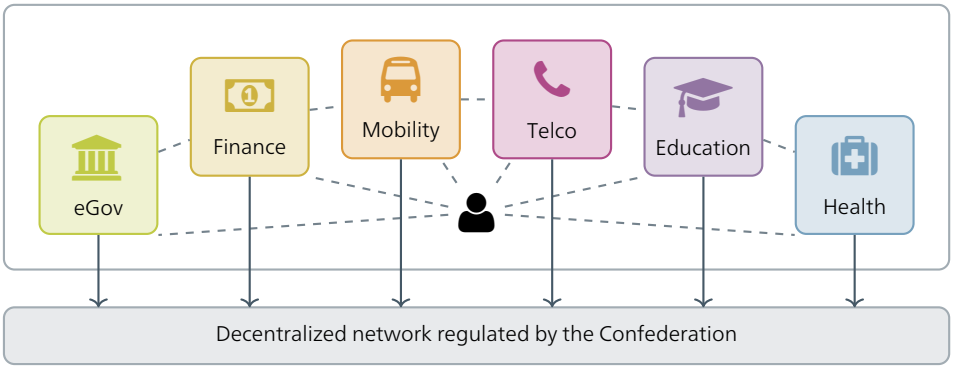


Figure 4.2: Vision for Sectoral SSI Ecosystem in Switzerland (adapted from [65])

Most recently, the Confederation has prepared a law draft [41] about the eID in order to open a public consultation process between June and October 2022 [12]. This shows that the eID project is moving a lot at the moment, especially regarding cooperation with national and international communities. Additionally, several use cases related to electronic identity can be envisioned, such as eVoting, electronic initiatives, certification of documents or data sharing [94]. This eID ecosystem will be further explored in chapter 7.

4.4.2 Digital Diploma Credentials

As illustrated on Figure 4.2, since the eID project is more ambitious than a simple eID VC, different sectoral use cases can integrate the ecosystem. In this section, we thus focus specifically on the education sector. Indeed, within the academic community, digital diplomas have been a long-term project for several years and SSI is bringing new life to the discussion[25]. Given the ambition level of Switzerland's involvement in the eID project and the parallel cooperation between several European countries, this academic use case could be a great opportunity to ease the exchange of information between educational institutions, students and employers. Therefore, this section explores the evolution of the digital diploma use case across its different forms, both without and later with SSI.

Verification of Paper Diploma Documents First of all, several tools exist for diploma verification, which is the process of checking that a diploma has actually been issued by a university to someone that claims to have a degree from there. While such a step initially needed to be performed by phone, universities have soon started providing an online service for easy diploma verification. For example, EPFL provides a website [28], where the name, surname and diploma number can be entered in order to check whether the diploma has indeed been issued by EPFL.

Verification of Digital Diploma Documents In order to further accommodate the digital needs of today's society, some universities have started issuing digital diplomas already, in the form of certified PDF documents or QR codes that can in turn be verified directly. In particular, two products achieve a similar goal at the moment when it comes to educational documents:

- **SWITCHverify** [50]: SWITCHverify, which is a service by SWITCH in collaboration with Certifaction, enables subscribed universities to compute a hash of the diploma and send it to SWITCHverify over an API that puts it on the Ethereum main net *via* a smart contract. From the student's perspective, SWITCHverify corresponds to receiving a "digital twin" of their diploma additionally to their paper degree. Later, when they want to (have someone) verify it, they can upload the PDF to the SWITCHverify website, which computes the hash and internally checks the blockchain for verification. On top of that, it is possible for universities to include a QR code on the diploma, so that the paper document can still be scanned and verified even if one has lost its electronic counterpart.
- **CERTUS** [26]: SICPA has a service called CERTUS which is able to issue and certify any kinds of documents by means of QR codes containing signed data. CERTUS is thus not limited to academic diplomas, but it also requires larger QR codes than *e.g.* SWITCHverify because the data format needs to account for different kinds of items. Therefore, since cameras need to read QR codes reliably, it works best when certifier and verifier can agree on a reasonably sized data standard[26].

There are several benefits to issuing digital twins of diplomas as opposed to digitally signing PDFs. First, when a student changes their name after having obtained a diploma, the certified diploma can be revoked, followed by the creation of a new one. Additionally, even though only new diplomas are certified automatically, it is possible to certify older diplomas on demand, and store them on the long term just like more recent ones.

[25] In fact, according to Niels van Dijk, digital diplomas lie on every table talking about SSI [56].

[26] What is about data standards, it would be interesting to see if these two services are interoperable, *i.e.* whether it is possible to use CERTUS to verify a diploma that has been certified by SWITCHverify, or the other way around.

Electronic Diploma Formats A diploma can be augmented by the issuance of an electronic version of its data. For such a process to be widely adopted, data standardization is an instrumental step. For instance, the Bologna process introduced "diploma supplements", which may look different across universities, but always contain the same additional information about a diploma. Another approach is that of the *American Transfer Articulation Database* (ATAD), which maintains equivalences between courses/credits across universities in the *United States* (US) based on crowd-sourcing and transitivity. When it comes to encapsulating and exchanging diploma information directly, several formats have been developed over time, two of which seem to dominate the landscape today:

- **EMREX ELMO** [23]: EMREX is a long-established project for the exchange of diploma data, predominantly in relation with student mobility[27]. The idea behind EMREX is the lack of a standard for exchanging university data, specifically in the context of exchange students. Therefore, the ELMO standard has been designed, using three kinds of actors: national contact points for host institutions, a student mobility plugin for home institutions and a trusted EMREG registry that lists all approved actors. The EMREX ELMO format is derived from a former "ELMO" format (which was discontinued and is no longer compatible), which is why it is based on XML.
- **EBSI Verifiable Diploma Schema** [52]: In activities around EBSI (*cf.* subsection 3.4.2), schemas for diploma data have also being established for academic applications. Contrarily to EMREX ELMO, the EBSI schema for diplomas puts a strong emphasis on being compatible with the *World Wide Web Consortium* (W3C) VC standards for integrating SSI, which is why it uses the JSON format. For instance, the EBSI schema is aligned with the format for Europass digital credentials [36]. Indeed, the idea of EBSI is to use the *European Self-Sovereign Identity Framework* (ESSIF) [57], which follows the global vision of "new education paradigms" where students would be "stacking credentials".

An example snippet of an EMREX diploma can be found on Listing 4.1 (inspired by the example in [23]), whereas the EBSI schema looks similar to Listing 2.1. Actually, the latter provides a seamless integration with VCs, which motivates the use of SSI when it comes to manipulating diplomas. In fact, there exists a converter from XML to JSON by IDunion that targets precisely diplomas of secondary schools [11].

```
<elmo xmlns="https://github.com/emrex-eu/elmo-schemas/tree/v1">
  <generatedDate>2015-10-31T12:00:00+02:00</generatedDate>
  <learner>
    <citizenship>PL</citizenship>
    <identifier type="nationalIdentifier">83041200000</identifier>
    <givenNames>Wojciech Lukasz</givenNames>
    <familyName>Rygielski</familyName>
    <bday>1983-04-12</bday>
  </learner>
  <report>
    <issuer>
      <country>PL</country>
      <identifier type="schac">uw.edu.pl</identifier>
      <title xml:lang="en">University of Warsaw</title>
      <url>http://www.uw.edu.pl</url>
    </issuer>
  </report>
</elmo>
```

Listing 4.1: Sample EMREX ELMO snippet in XML Format

[27] EMREX ELMO is currently used within Germany, Norway, Italy, Poland and more, but without SSI integration.

Digital Diploma Credentials with SSI As the EBSI format for digital diplomas is alluding to, digital diplomas are gradually moving towards the SSI world. In fact, having students transport their own VCs provides more privacy than they currently have and enables an entire range of new possibilities to study more flexibly [14], thanks to SSI principles (*cf.* subsection 2.1.2) such as those applied to diplomas in Table 4.1.

SSI Principle	Application in the digital diploma use case
Authenticity	Improving security by using strong (biometrical/hardware) authentication instead of relying on public keys, that are not linked to one's identity[28]
Control	Showing employers a verifiable degree directly from one's digital wallet, bypassing any "external" service such as SWITCHverify or CERTUS
Transparency	Using SSI for managing one's diploma in a world where free and open-source software is not yet the standard, to bring back the freedom of their own data to the students themselves, at least when it comes to their diploma
Portability	Recognizing international diplomas at an official place in each country, which can legalize foreign diplomas, but also issue diplomas on behalf of a university that no longer exists or should not be contacted anymore
Interoperability	Simplifying the process of accrediting equivalent courses in the context of student mobility by giving all information to the students themselves[29]
Minimality	Deciding for the granularity[30] of the diploma proof, be it **coarse-grained** (*e.g.* pass/fail information) or **fine-grained** (*e.g.* selected course grades)
Equity	Linking diploma information with one's eID, which can automate changes in one's identity such as name or gender, or even make an anonymous diploma verifiable by using pseudonyms (*i.e.* `pseudo:...`)

Table 4.1: SSI and Digital Diplomas

As elicited by this matching with SSI principles, the diploma use case is not only linked to the academic sector, since a company may offer trainings that entitle employees to perform certain tasks, which could also be implemented by means of a VC. Additionally, VCs can be integrated into existing solutions, for instance SWITCHverify, which could issue structured JSON data additionally to a digital twin of a diploma. As a result, encoding diploma information into a VC makes a lot of sense from the SSI use case point of view. Essentially, there are two antagonistic points of view about this academic use case:

- **Extensive use of SSI**: In this scenario, VCs are issued for very fine-grained situations, such as individual projects or homework assignments. Later, students can combine such learning opportunities and present them to get their course grade, or present their transcript credential to get their degree [14].
- **Conservative use of SSI**: The previous situation can be seen as massive over-engineering, especially in the early years of SSI development. In this viewpoint, even SSI itself does not bring much to diplomas, since there already exist solutions such as SWITCHverify or CERTUS that can verify diplomas. When it comes to student mobility, which is not accounted for by these existing solutions, another service then needs to be used, for instance one based on EMREX ELMO, which is already known in Europe.

This discussion input will be pursued in the requirement analysis of chapter 7.

[28] This is what Mihály Héder means when saying he does not "think there is a way back to PKI when it comes to digital signatures" [1].

[29] Actually, this student-centric view would open the gates towards a new educational system without the need for host institutions, because "Student mobility for both, identity and records, will be a reality (on Student's Mobile wallet)" [106].

[30] The question of macro- *vs* micro-credentials has been raised a lot in task forces working on digital diplomas, but this terminology is ambiguous (*e.g.* a credential can contain many **small** attributes, or it can consist of a **single** attribute, both of which can be considered "micro" in some sense), so I use the words "coarse-grained" and "fine-grained" in this report.

4.4.3 Life-Long Learning

Nowadays, most universities tend to create digital identities for their students. However, their IdPs often follow a centralized or federated identity model, which means that students can only log into educational services while they are enrolled at the university. However, this model is deprecated for three reasons. First, student mobility is developing at a rapid rate, which multiplies the number of identities per student without a good reason for it. Second, many students may still want to access well-known study platforms once they are no longer enrolled at their university, because they envision to continue learning even after their studies. Third, user-centric identities are perfectly able to store so-called "affiliations", which precisely enable situations where students are enrolled in multiple institutions at the same time, or no institution at all while still wanting to use a basic educational identity.

Let's consider for example the SWITCHaai [25] federation, which is the original implementation of digital identity for Swiss universities, where each of them hosts their own IdP or delegates SWITCH to host it for them. Later, when the user-centric approach to identity emerged, SWITCH edu-ID [24] was developed with a stronger focus on the identity of a person. As a result, former students can now keep their educational identity and embark on their journey to *life-long learning*. While the transition from AAI to edu-ID is still ongoing, the need for individual IdPs is fading and more than 700'000 identities are running under edu-ID today in Switzerland [9]. Across Europe, there exist other user-centric edu-ID identities within national ecosystems, because cross-boundary compatibility in education is only ensured *via* federations at the moment.

Logging in with an edu-ID succeeds *via* SAML or OIDC (*cf.* subsection 2.1.1) using the *single sign on* (SSO) paradigm, meaning that a login on one service provider provides a browser session with all available attributes. As such, these attributes are only released on a need-to-know basis per service, and the user needs to give consent for it to happen. However, the data is still stored on a server and there is still an IdP that needs to provide the attributes to the server.

This is where SSI can help setting up a more privacy-friendly and self-sovereign edu-ID, opening a new range of possibilities, not only for educational identities, but identities more broadly. Indeed, when an eID will be ready in Switzerland for instance, a "user mapping" between a SWITCH edu-ID unique identifier and an eID identifier (provided by the Swiss Government) could be performed[31], fitting into the picture of Figure 4.2. Therefore, student's wallets would first contain their edu-ID credentials, but over time this could be gradually integrated with the eID or even its European counterpart, the euID.

In this new self-sovereign educational identity, students could disclose their credentials in the form of OIDC VCs for example, which builds a bridge between the "new" SSI world and the "old" OIDC world, whereby VC attributes can be mapped to OIDC claims. Here as well, two scenarios are considered:

- **Identity attributes**: Most edu-ID attributes are embedded into a VC and issued to students on demand by the current IdP (*e.g.* SWITCH);
- **Affiliations**: Only affiliations are released as VCs, either by the IdP storing the edu-ID attributes (*e.g.* SWITCH) or directly by the affiliated institution.

Both of these ideas will be considered in chapter 7.

[31] Since such an eID would only be provided to Swiss students, no solution exists currently for foreign students/employees, which creates another possible role of SWITCH in the future of edu-ID [105].

5 Requirements Elicitation for SSI Use Cases

"Several factors influence the adoption or acceptance of a new solution in any domain. There are some specific requirements for adopting SSI"
— Mohammed Shuaib, Shadab Alam, Mohammad Shabbir Alam and Mohammad Shahnawaz Nasir [82]

The SSI use cases presented in the previous chapter are numerous and vary significantly in terms of adoptability. Especially in the beginning of the SSI era, it is of key importance to clarify what we are expecting of this new technology, to prevent us from applying it to any use case without having good reasons for doing so. Therefore, this chapter abstracts SSI into a set of requirements that characterize "good" use cases of it.

5.1 Motivating the Need for a Set of Formal Requirements

When starting to implement SSI use cases, scoping matters a lot. In fact, the goal lies in finding a right balance between too narrow and too wide, which would both be harmful for SSI adoption:

- **Narrow scope**: Implementing only "few simple use cases" will limit SSI adoption because it would simply not be well-known enough to spread to global and interoperable ecosystems;
- **Wide scope**: if there are too "many complex use cases", the ecosystem will be over-engineered and thus too complicated to do one thing well, which hinders its actual use again.

Contrarily to the three levels of ambition for the eID (*cf.* subsection 4.4.1), the goal here is **not** to settle for a global vision of an ecosystem, but to find a "golden spot" to begin with SSI use cases that are simple enough for the implementation to remain accessible, yet numerous enough to ease medium-term adoption.

Non-Functional Requirements	Functional Requirements
Privacy-Preserving	Authorization-Granting
Selectively Disclosable	Time-Limited
Cross-Sector	Revocable
Multi-Issuer	User-Centric
Distributed Authority	Human Trust
High Volume	Identity-Specific

Table 5.1: Overview of SSI Use Case Requirements

As a result, Table 5.1 lists a set of non-functional and functional requirements for SSI use cases. Roughly, the more of these criteria are fulfilled, the better the use case is suited for an early SSI implementation.

5.2 Non-Functional Requirements

We begin with **non-functional** requirements of SSI use cases, which focus on security and usability aspects thereof, without constraining what they actually have as objectives. With this point of view, the design of an SSI use case should be:

1. **Privacy-Preserving**: As explained previously, SSI typically relies on a distributed ledger, which requires great care when it comes to publishing data, because transactions remain visible forever once they are executed. As a result, privacy needs to be an absolute priority when is comes to using SSI productively. Indeed, digital processes have side effects that our brains do not have (*i.e.* computers never forget information). When using (centralized) PKI, there is an IdP that gathers all information at a single place, which is not only bad in case it is malicious, but also because it provides a single point of failure as an attack surface to attacking entities (*cf.* chapter 6).

   On the other hand, SSI shines with its decentralized approach, solving both of these problems at once. For instance, connecting two parties that should not know about each other would justify that the user be provided with an SSI verifiable credential instead of a solution based on PKI, because they can perform the proving step themselves, relying on a public distributed ledger where they can be identified by some *ad-hoc* DID. What is publicly available should be carefully thought through, though, for instance by selecting "public" attributes very specifically, by minimizing information in the form of a hash or by not even publishing VCs on the ledger to provide "privacy by design". These aspects will be considered in the design choices of chapter 8.

2. **Selectively Disclosable**: SSI verifiable credentials contain various fields of information called attributes, which correspond to data in real life as well. However, according to the trust we have in other humans and possibly technical solutions we are already using, we do not disclose any information to anyone or to any service. For instance, when logging into a service with edu-ID (*cf.* subsection 4.4.3), one can decide whether or not to give consent for data provisioning. In the same sense, the idea of selective disclosure is to provide such a consent mechanism at a finer granularity.

   As a result, when proving an SSI claim to a verifier, a holder should be able to select which fields/attributes they want to show (and prove cryptographically) and which should remain private, which links to the privacy-preserving aspect as well. The support for zero-knowledge proofs could also be enabled on-demand for critical attributes. Such selective disclosure thus allows for minimality in the VC proof, which is one of the foundational SSI principles listed in subsection 2.1.2. In fact, it is strictly more powerful than minimal disclosure, since it also makes it possible to share more data than what is strictly required, but under the user's conscious responsibility.

3. **Cross-Sector**: A use case for SSI should involve multiple sectors of the public domain (*e.g.* among eGovernment, finance, mobility, telecommunications, education and health, as illustrated for Switzerland on Figure 4.2). In that sense, it will enable cooperation across different sectors that would otherwise have to go through paper for instance. With SSI, a sector can adapt its infrastructure to support VCs from other sectors so that users can reuse them directly. This enables a global SSI ecosystem with multiple coexisting sectors, as envisioned by the Swiss government in their eID project [67], or by the Sovrin foundation which targets a "worldwide ecosystem" [118].

   For instance, an eID should be the VC with most reuse across all sectors, because it provides a base identity (*cf.* similarly to the IDwallet project in Germany presented in subsection 4.1.1). Additionally to such a coarse-grained identity VC, other VCs can be presented in combination to some verifier, as in uses cases from section 4.3. When it comes to the privacy-preserving aspect, DIDs can be generated on-the-fly for connection-specific identification without possible correlation.

4. **Multi-Issuer**: Typically, in SSI, there are three roles: issuer, holder and verifier (with a possible fourth one that is the governance authority). While the holder consists of a single user only, having the entire responsibility of their data, several to many possible issuers need to coexist for SSI to become relevant. Indeed, if there was only one issuer, then an easier solution would consist in using PKI to issue signed documents, since only a single entity would need to be known globally. However, the power of SSI lies in letting anyone issue credentials, because what makes it work is the trust the verifier has in the issuer.

   Consequently, as multiple issuers come into the game, it becomes gradually simpler to use a system like SSI, where anyone can issue verifiable credentials and they can be verified by looking up DID documents on a distributed ledger. Different concrete cases can be found to support this idea, but one of the most striking ones consists of multiple institutions providing the same service, and thus issuing the same kind of credentials. For instance, all universities have to issue diplomas for their students upon graduation, several Swiss cantons organize voting sessions on the same date, and multiple hospitals may participate in a program for employee passports [15].

5. **Distributed Authority**: In the context where a governance authority is at the root of trust, it is important that this authority be shared across different entities. In particular, the authority publishing the data schema corresponding to a use case, as well as the one framing the scope of the use case, should be distributed across multiple trust anchors. This might take the form of different people taking decisions together in a physical room, but in general it should be distributed over different DIDs, or even different countries if applicable, for instance by delegating the schema preparation to a dedicated committee with representatives from various backgrounds.

   With authority distributed in such a way, we ensure the interoperability principle of SSI. Thus, this distributed authority requirement should apply to any use case of SSI, because an SSI ecosystem should be made to work with other SSI ecosystems as well. A good analogy here is the way COVID Certificates were made compatible from one European country to another [83], because they were deployed so rapidly thanks to the cooperation of several countries towards the same product around the same time.

6. **High Volume**: Chances are that SSI use cases rely on a distributed ledger infrastructure, which may well leverage some existing blockchain by means of additional smart contracts, or set up a custom hyperledger specifically for this purpose, possibly with some bridging that enables interoperability between different ecosystems. As a result, uses cases for SSI need to happen frequently enough for it to be worth setting up the underlying hardware and software stack.

   Additionally, there are existing solutions for dealing with *e.g.* authorizations, access control or sealing, which are already in place and work reasonably well. However, as people perform such operations more often, the burden on them increases and can gradually be further mitigated by SSI. For instance, a single unique onboarding process may not be enough to justify SSI, but a couple of interactions per year definitely consist of a "higher volume" use case, which could be effectively improved by SSI, especially if the use case involves multiple people or entities. As a result, this concept of high volume is meant as a rough measure for the frequency of an interaction between parties.

With these first six requirements, we already provide a clear overview of how SSI use cases should regulate the privacy, governance and frequency of their VCs. In particular, we have raised multiple SSI principles such as control, consent, interoperability, privacy and minimality.

5.3 Functional Requirements

When it comes to *functional* requirements, we touch upon the practical applications of use cases and the way electronic devices, typically wallet applications in our case, interact with people. In that sense, the functionality of a use case of SSI should be:

1. **Authorization-Granting**: The idea in SSI is to hold a digital wallet with verifiable credentials that one can show some verifier to convince them that one possesses the required credential without having to prove one's identity as well. Indeed, one's identity is baked into SSI, either *via* some eID credential or through the biometrical unlocking process which requires strong factors. While the identity-specific requirement will be described a bit later, this still motivates the fact that a use case of SSI needs to have an inherent component of authorization which justifies the simplified identity verification process. In other words, a VC proof should grant access to some service, be it physical or digital. This is the case, for instance, when only a subset of people is allowed to enter a building, based on a credential they have received, typically by their employer or their university.

   On the other hand, when showing the credential doesn't give access to some additional service, then SSI does not help more than a simple verification of a public hash on a publicly available decentralized network that is unlinked to a person's identity. Note that SSI may still be simpler to use nonetheless, since it is integrated into one's wallet; especially if an entire SSI ecosystem is already in place. This aspect will also be considered in the analysis of chapter 7.

2. **Time-Limited**: Among the SSI principles, we find the one of persistence. According to this idea, an identity as per the SSI paradigm needs to be long-lived, similarly to what a physical identity card represents or similarly to the concept of life-long learning explained earlier (*cf.* subsection 4.4.3). However, in the physical world, we have expiration dates on almost all official documents that are linked to our identity, be it a passport, an ID card or event a credit card.

   Indeed, the world is ephemeral and our abilities change over time, so for use cases to be relevant, issued verifiable credentials should be limited in time, as is the case with physical credit cards for instance. This holds especially true for the authorization-granting aspect explained just before, since we may not be entitled to access a building forever; only for the time of our intervention there for example. This calls for the scenario where verifiable credentials can expire after some amount of time, which is either set at a specific date (as in fixed-time employment) or a given time after its issuance (as in ID cards). In case VCs need to "live" longer than what is planned by their expiration date, they can be re-issued regularly if the need for them still exists. Otherwise, one may want to resort to revocability hereafter.

3. **Revocable**: With the same idea of issuing verifiable credentials according to an authorization-granting use case, it is important that claims be temporary. In other words, the issuer should be able to nullify them at any point in time. In fact, as alluded to previously, credentials are in principle long-lived, but they should have a built-in mechanism for revocation which makes them effectively equivalent to expired ones if they are revoked at some point. For example, this can be invoked in the case academic fraud is detected after some diploma credential has been issued.

   This requirement is different from the time-limited one because it corresponds to a radically different scenario in real life: revocations should happen infrequently, which may justify the need for a separate revocation register; whereas expirations should be regular, thus very predictable, and they can reuse the same issuance mechanism that is already in place. In other words, it may be enough if only one of these two requirements is satisfied, but this will also be analyzed on a per use case basis later.

4. **User-Centric**: SSI gives the entire responsibility of an identity to the holder of a digital wallet. In other words, the verifiable credentials issued to a user are stored on their device and can only be controlled by them; except possibly in the scenario of delegation when a user is unable to hold their data responsibly or that of recovery where they might need some multi-signature smart contract to retrieve data to which they have lost access. Additionally, in the case where a DID is assigned to some other entity, such as a pet animal or an object like a car (*cf.* subsection 4.3.2), some user needs to hold these VCs in their own wallet through delegation, which again lies these VCs in their area of competence. In all these scenarios, users are therefore "decentrally" responsible for the VCs that have been issued to them.

   Due to this high level of responsibility, any use case of SSI should strive to be user-centric, meaning that the user's intervention should be explicitly necessary to bridge the gap between multiple parties. In other words, while it would be possible to flow the information directly behind the user's back, SSI is justified when the burden on the user is reasonably low and simplifies the process in the high-level. On top of that, only having the user manipulate their own data preserves privacy as well, which is still baked into the system by design. Actually, whether the user is attached to verifiable credentials *via* their global DID or any domain-specific ones is irrelevant in the context of this principle, as long as the user is the one that manages these identifiers themselves.

5. **Human Trust**: Even though there exist fundamental differences between the physical and the digital worlds (as we have seen, computers do not forget, as opposed to humans), an SSI use case is meant to replace (or, at least, to complement, in an initial transition period) a workflow that we know from the physical world using digital devices. Our interaction with authorities, for example, still uses a lot of paper, but we do trust the authorities because we understand how they manipulate our data. The idea of human trust lies precisely here: SSI should replicate the workflows we know and understand as closely as possible, so as to avoid any bad surprises.

   In that sense, a use case for SSI should provide a user experience that is analogous to what would happen in the physical world. Of course, one cannot perform the exact same actions, but at least the general feeling should be consistent with one's idea of the process. Consequently, the same human trust is achieved between different parties, because the same actors are responsible for issuing the governance frameworks and credentials as those who prepare the information flow in the real world. As a counterexample, eVoting has not worked (yet) in Switzerland [114] because the lifecycle of an eVoting process was different from the one of voting on paper; and indeed, corresponding security flaws were identified in the trial phase.

6. **Identity-Specific**: A use case of SSI should be closely related to a user's identity, meaning that at the core of a verifiable credential should lie its holder's identity (or some entity's identity that has been delegated to the holder). This link can go through a set of DIDs that belong to said user, but it may also involve their eID directly. In any case, such a direct mapping enables direct verification of the relevant identity from the verifier's point of view, without any additional means than SSI credentials themselves. In other words, SSI is self-sufficient when it comes to identity issuers, holders and verifiers.

   Of course, the scope can be slightly broader, since a use case should combine someone's identity with at least one other aspect, making use cases other than an eID relevant. But this latter aspect should be tightly coupled to the identity data, which narrows the scope of the use case. This requirement can be slightly controversial, since credentials should do one thing well, but they should also enable use cases that may be harder to implement without SSI, which encourages discussion.

Again, these requirements will be analyzed further in a future chapter, but it is already notable that they brought up some more SSI principles, among which representation, verifiability, delegation, privacy, decentralization, participation and consistency.

5.4 Links and Distinctions Between Use Case Requirements and SSI Principles

As we have noted, requirements for SSI use cases allude to SSI principles, which justifies their importance, but may also blur the differences between them. In this section, we clarify how these requirements differ from SSI principles despite relying on them. In that sense, let us first clarify the terminology:

- **Principles** are general guidelines that apply by design to any SSI ecosystem. For instance, "privacy" is a principle of SSI, since all data relative to some user can be stored directly on their own device instead of transiting through an IdP.
- **Requirements** are specific criteria to which potential use cases (of SSI) should match in order to be relevant. For example, "privacy-preserving" is such a requirement, because if the considered use case does not call for privacy preservation, it would not require SSI, which has an innate "privacy" principle.

Despite their distinct goals, principles and requirements are related, as each use case requirement leverages one or more SSI principle(s). In Table 5.2, each of the previous requirements is mapped to the three principles on which it relies the most.

Requirements	Underlying Principles
Privacy-Preserving	Privacy, Minimality, Decentralization
Selectively Disclosable	Verifiability, Consent, Minimality
Cross-Sector	Portability, Interoperability, Decentralization
Multi-Issuer	Verifiability, Interoperability, Decentralization
Distributed Authority	Transparency, Interoperability, Decentralization
High Volume	Access, Interoperability, Usability
Authorization-Granting	Authenticity, Verifiability, Consistency
Time-Limited	Existence, Persistence, Transparency
Revocable	Persistence, Access, Transparency
User-Centric	Representation, Protection, Equity
Human Trust	Existence, Delegation, Participation
Identity-Specific	Existence, Verifiability, Control

Table 5.2: Use Case Requirements and Matching Underlying SSI Principles

This table covers all SSI principles, which ensures that the use case analysis is complete. On top of that, some principles appear under multiple requirements, which highlights them compared to others, thus realistically reflecting discussions in European task forces working on SSI use cases that focus primarily on:

- **Verifiability**: The cryptographical background on which SSI relies is still subject to discussions, for instance when it comes to ZKP for minimal disclosure, because this is precisely where a new technical solution enables us to replace physical identity cards;
- **Interoperability**: Since many working groups across numerous countries are working on SSI use cases in parallel, the question of how these ecosystems can cooperate and understand each other's standards is central to the design decisions that are being taken;
- **Decentralization**: The idea of SSI is to rely on a decentralized network, but the exact instance that is used depends on each use case, which also links to interoperability questions since use cases should be compatible with each other, at least by being stored on a common wallet application for instance.

6 Threat Model for SSI Systems

"Forensic analysis is difficult because the system is decentralised and cryptographically well protected. If e-ID or other proof is misused, this can make it difficult to prove that 'it wasn't me'."
— Christian Heimann [67]

Now that the requirements for SSI use cases are clear, it is important to tackle a primary challenge for any new technology, which is its attack surface. According to most of the literature, SSI is considered quite safe against attacks precisely **because** the different trust anchors don't have control over the data. For example, some universities have been targets of ransomware attacks and their systems were broken into, which lead to loss of data. On the other hand, a decentralized network contains data that is replicated at every participating node, which keeps the data safe even when one of them lies under attack. In other words, attacking a blockchain for instance would take a very concerted effort, which makes it difficult to fake VCs. Nevertheless, SSI is not perfect and this chapter will model the threats that can attack an SSI ecosystem.

6.1 Limitations of SSI

The decentralized nature of self-sovereign identities gives hackers a hard time accessing or even compromising user's data. For instance, when a blockchain is used as a decentralized network for powering SSI, there always needs to be a majority of validator nodes that accept each write transaction, so any dishonest entry can be discarded directly, especially when a governance authority is responsible for defining the credential frameworks. Yet, there are still some issues with SSI that cannot be solved technically, which starts with the relationships defined in the trust triangle of Figure 2.4 (or its diamond extension).

6.1.1 User Responsibility

In particular, while SSI gives full responsibility of VCs to the user, recall that "the user is the weakest link", as it is often the case in information security. This simple statement covers multiple scenarios with SSI, of which some are listed below in no particular order:

- Someone cannot access their identity anymore due to a software bug in their wallet;
- Political tensions may hinder the service to function as expected;
- Users are human and may thus damage or lose their device, as well as forget their (recovery) keys;
- Thieves can physically steal devices, thus depriving individuals of their VCs.

To account for the most possible number of attacks to the user, the following sections describe the threat model for SSI systems in great detail, going through each possible role that SSI actors can play.

6.1.2 Different Models

One possible issue with threat modeling is the one of different models across ecosystems, which can become a hurdle for interoperability. For instance, before Bitcoin even existed, the Estonian government started experimenting with blockchains [115], which came as a mitigation against attacks that had taken place earlier. Therefore, their threat model included rogue agents trying to access/modify databases, which resulted in protection for data integrity. On the other hand, the threat model for recent COVID certificates issued in Switzerland (*cf.* subsection 4.2.1) didn't include such a clause, yet thousands of illegitimate COVID certificates have been issued [95], so there actually was little control over integrity.

Functionally, the centralized Estonian model can notify users upon someone accessing/modifying their data (*e.g.* the police or rogue agents), while it is not so hard to do it since there are no firewalls. In the Swiss model however, which is decentralized, one cannot be notified upon breaches, but there are firewalls that make accesses/modifications much harder. How we balance these two aspects is highly dependent on threat modeling: indeed, people **will** find a way to abuse the system, so one should be prepared for this, but if different ecosystems are prepared for different attacks, there may be compatibility problems.

6.1.3 Honeypots

As we have seen, SSI brings the entire sovereignty over their data to holders. As a result, each user needs to be aware of this new responsibility. Indeed, next to the danger of losing access to one's phone, cyber-attacks targeting specific users are still possible. In fact, it is just as inconvenient as having one's physical wallet stolen, but digital wallets form so-called data honeypots, because they contain a lot of information about someone specific. Therefore, we should educate people that (digital) wallets are valuable and vulnerable, but it is hard to give up on compromises, let alone to rely on a single device for holding all VCs issued to one person.

Consequently, it makes sense to use some recovery mechanism, which could rely on encrypted backups for instance. In such a scenario, one has to trust the operator of the backup storage; but of course one has to trust the designer of the wallet application anyway in the first place, so it all boils down to the trust anchor in the end. However, it would be terrible for some big company if it ever came out that their wallet or recovery storage was not safe, so people may "naively trust the good side of capitalism" [13].

6.1.4 Underlying DLT Back-End

It is likely that SSI use cases will be implemented using a distributed ledger, for instance a blockchain. This comes with all the benefits of such a technology, which has matured a lot over the past decade, but as we will see, even blockchains can be targets of attacks, specifically when they operate proof-of-authority (PoA) consensus based on a small set of validator nodes.

Thus, one has to consider the decentralized aspect as a first-class citizen of the threat modeling process, which also explains why DLT has been described in such great detail in this report. In the following sections, system components and threats will thus contain both SSI and DLT elements to account for the entire infrastructure layers presented on Figure 2.5.

6.2 System Components and Interactions

From the complete trust diamond describing the SSI trust relationships, we derive the main individual components of the system. In the following description, we assume a system relying on a layer 2 blockchain based on a hyperledger, which is the case in the demonstration implementation that will be described in chapter 8. Nevertheless, it also applies to other decentralized networks with the appropriate changes. In that sense, the system components, depicted for clarity on Figure 6.1, consist of:

- A **layer 1 blockchain** (*e.g.* the Ethereum main net) serves as the primary source of storage, since it is accessible by anyone and stores regular digests of transactions in the form of hashes;
- A possible **layer 2 blockchain** (*e.g.* the Dragonfly main net or some instance of hyperledger Indy, such as the SSI sandbox described in section 8.2) provides local storage for VC schemas and DID documents specific to the ecosystem, which in turn is bridged to the public blockchain;
- The **governance authority** (GA) publishes a framework according to which the VCs should be created (which can also be stored in the blockchain) and issues VCs to authorize issuers;
- Each **issuer's wallet** holds a VC from the GA that authorizes them to issue VCs on their own (similarly to the SSL certificate trust chain);
- Each **issuer's wallet** is responsible for connecting to holders *via* one of their DIDs in order to issue valid VCs (if we want a truly decentralized system, we can ignore the two previous components and have the root of trust here, as in the trust triangle);
- A **holder's digital wallet** generates a secure domain-specific identifier and can store/display/share VCs that have been issued to it;
- A **verifier application** can be used to verify any VC at any time by asking to see the specific known attribute (this application can possibly also be authorized to verify VCs with a similar VC that authorizes issuers to issue them, but this would require the GA and thus its related components, yielding a less decentralized system);
- An **interface** enabling applications to communicate with the underlying system (for instance an API or a set of smart contracts, depending on the nature of the decentralized network), *e.g.* with helpers for storing hashes on the blockchain, checking for them, and possibly for bridging blockchains as well.

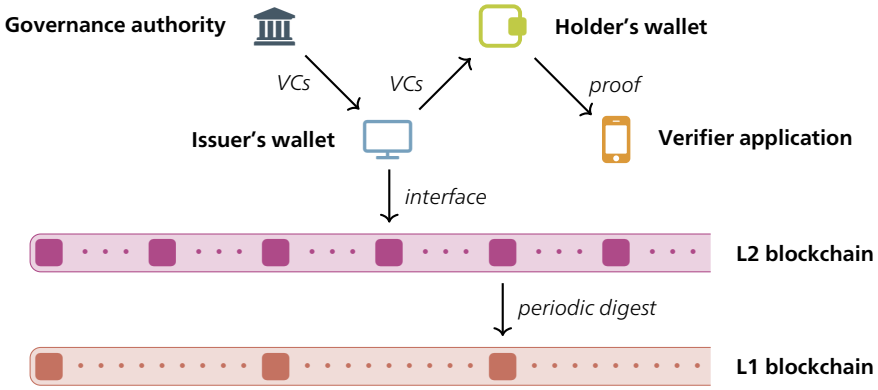


Figure 6.1: Components of SSI System

6.3 Vulnerable Assets and their Exposure

The high-value assets of the system are listed below:

- The **identifier** used for identifying a user is linked to other data in the form of other VCs, which makes DIDs an important asset of each SSI interaction. Domain-specific identifiers may mitigate the importance of these DIDs for potential attackers.
- The **other VCs in the wallet** attached to the same user (or others) are also sensitive, because these should absolutely not be disclosed upon showing one VC related to a specific use case. This data should not get in the wrong hands outside of an SSI interaction, either.
- The **governance authority** is the primary source of trust (if any), so it must absolutely be secure. For instance, people working there need to be proven trustworthy, since a fault would result in fake VCs being issued, and wrong people being allowed to verify them.
- The **data** contained in the VC should be protected, and only be disclosed by the user themselves, and only if they agree to it. In particular, it should not be published on any blockchain due to privacy concerns (at the absolute most, hashes could be accessible to the public). Moreover, the data should not be directly modifiable; it should only be revokable (followed by the issuance of a new VC if needed).

6.4 Relevant Threats and Known Attacks

In this section, we build an attacker model in a similar way as in the DP3T paper [108]. In that sense, we will clarify the following points, as suggested in [73]:

> *For each adversary, the capabilities and the kind of risk they pose for the system should be made explicit.*

The kinds of adversaries depend largely on the use case, but, when ordering them according to SSI roles, we get at least the threats listed in Table 6.1.

Governance Authority	Issuer	Holder	Verifier	Other
Corrupt authority member	DDoS issuer	Unconscious user	Participating eavesdropper	Blockchain explorer
Intrusive authority	Corrupt issuer	Regular user	DoS verifier	Fake recovery initiator
DDoS authority	Spoofing issuer	Whitehat hacker	Arbitrary verifier	Phishing attacker
Non-technical politician	Replay attacker	Tampering holder		App or system developer
Blockchain influencer				Non-participating eavesdropper
				Physical attacker

Table 6.1: Overview of Relevant Threats

Let's look at each of the attacker models from the table in detail:

1. **Governance Authority**
    - **Corrupt authority member**: tries to modify the schemas and regulations arbitrarily (thus, we need elections and consensus, but in Switzerland, this is the case now already);
    - **Intrusive authority**: tries to learn information about the population (thus, by design, we should not leave the possibility of information disclosure in a database; which may advocate for using a blockchain, with built-in ownership);
    - ***Distributed Denial-of-Service* (DDoS) authority**: tries to write schemas on the blockchain continuously (this doesn't really make sense thanks to transaction fees on most ledgers, which essentially guarantees blockchain availability);
    - **Non-technical politician**: tries to understand technical details without the necessary background and thus may set unrealistic goals or even prevent developers from going forward (we need to clearly distribute roles, use *free and open-source software* (FOSS) and most importantly explain the concepts in a clear way without hidden spots);
    - **Blockchain influencer**: tries to gain power by using multiple so-called "Sybil" identities, corrupting a group/majority of miners/validators or partitioning the network to prevent routing (this is mostly a concern for PoW or PoS blockchains, since these are usually permissionless, and thus we should rely on PoA, which also complies with the idea of a governance authority).
2. **Issuer**
    - **DDoS issuer**: tries to create a huge number of VCs in a row (if VCs are not stored on any ledger but only on the holder's device, this does only affect one user, who can close the connection at any time if the wallet supports this functionality);
    - **Corrupt issuer**: tries to issue credentials on purpose, that hold fake or erroneous data (we thus need human trust in the issuer or some kind of control mechanism where *e.g.* a multi-signature framework prevents a single person from creating data, because a federated effort would be much harder to set up);
    - **Spoofing issuer**: tries to pretend they are a valid issuer in order to generate VCs that look real, but are actually fake (to mitigate this, the governance authority can store public keys of authorized issuers for authenticity checks during verification)
    - **Replay attacker**: tries to issue the same credential multiple times, possibly to different holders, even though the control should actually be given to the user when it comes to sharing proofs of their VC (for instance, all blockchain entries and VCs could include timestamps, so that new entries invalidate all previous).
3. **Holder**
    - **Unconscious user**: tries to use the system as intended, but doesn't care that much for privacy (thinking *e.g.* they have "nothing to hide"); this may lead to them not installing proper authentication for their wallet or even leaving it unlocked (to account for such users who are vulnerable to identity theft, we need proper schooling and possibly mandatory biometrical factors for unlocking wallets, as well as timeouts so that the wallet doesn't remain unlocked for too long);

- **Regular user**: tries to use the system as intended, through the graphical user interface, which is probably the case for most users (this is no particular threat, except for software bugs or implementation flaws, where we rely on the FOSS nature of the system and thus peer-reviewing);
- **Whitehat user**: tries to read source code and algorithms with the goal of learning or finding bugs to signal to the developers (we should publicly encourage the search for bugs and make the infrastructure FOSS);
- **Tampering holder**: tries to tamper a VC that they have received, modifying data in it in order to show false information to a verifier (this is negligible, since we are using cryptography in VC proofs and the attacker cannot reasonably break cryptography; other systems would break before SSI if cryptography was compromised).

4. **Verifier**
   - **Participating eavesdropper**: tries to obtain VCs that they are not allowed to get, either passively or actively, with the intent of redistributing or even selling the data (here, we can rely on human trust, as established in society already, technically "approve" valid verifiers, make VCs short-lived when being shown to someone, or even use zero-knowledge proofs all the time so that no information flow can happen at all);
   - **DoS verifier**: tries to verify data on the distributed ledger a huge number of times within a short time span (this should be accounted for by a blockchain and, if the system is well-designed, also bottlenecked by the human factor, because one can only verify a VC when it is being presented, since the data it contains is nowhere else);
   - **Arbitrary verifier**: tries to disregard the verification outcome to "accept" or "refuse" all presented VCs (this could be a breach to human trust, but it touches the core idea of SSI trust, so it is a bit out of scope, since this kind of behavior would not really be in the verifier's interest).
5. **Other**
   - **Blockchain explorer**: tries to infer private information based on data stored on public blockchains (do not store any VC information on a public blockchain, but only VC schemas, some PKI information and potential trust claims);
   - **Fake recovery initiator**: tries to pretend they have lost access to someone else's wallet in order to gain access to that person's VCs (we need country-specific workflows for recovering VCs, *e.g.* go to the police with a physical identity card, show electricity bills, …);
   - **Phishing attacker**: tries to perform social engineering to get data or private keys (we need education and proper awareness about wallet vulnerability);
   - **App or system developer**: tries to add rogue functionality since they are working on the source code (there is no need to worry, since FOSS code is observable and this would get noticed);
   - **Non-participating eavesdropper**: tries to intercept VCs by observing whichever communication channel is being used between a holder and a verifier (this depends on the communication channel, but it could be mitigated with zero-knowledge proofs or some DIDComm protocol involving timestamps and challenges);
   - **Physical attacker**: tries to steal or break the device on which VCs are stored to prevent access to data (there is no evidence that such an attack would be directly targeted at SSI, nor that it would disappear with the use of SSI, so we need a backup/recovery mechanism for VCs, which is possibly country-specific).

7 Requirements Assessment for Described SSI Use Cases

"It becomes increasingly clear that SSI goes far beyond issuing a digital identity card. It unlocks its full potential in the context of an ecosystem of digital credentials."
— Stéphane Mingot [18]

Now that we have considered use cases, requirements and threats, it is time to assess the most important use cases in light of the two latter chapters. Indeed, while all presented use cases make sense and can be implemented with SSI, some of them match with the requirements better than others and should thus be considered in priority. In particular, use cases closely related to identity can be plugged into an SSI ecosystem more easily (especially in the presence of an eID credential), but those with a looser link to identity enable more interesting applications by combining VCs in a sensible way. Since establishing a new technology such as SSI takes a while, it is instrumental to select the most relevant use cases first.

In this chapter, we thus check each requirement from chapter 5 for the described SSI use cases in detail. To do that, we answer the questions in Table 7.1, which results in a newly established table that we call the "SSI matrix". It is depicted in Appendix B and contains orthogonal entries for each requirement and for each presented use case.

Requirement	Question
Privacy-Preserving	Is it of major concern that the use case preserve privacy?
Selectively Disclosable	Does the structure of the use case support selective disclosure?
Cross-Sector	Do the envisioned credentials bridge a gap between sectors for easier collaboration?
Multi-Issuer	Would different entities be issuing credentials?
Distributed Authority	Would the governance authority be distributed over multiple entities?
High Volume	Does the use case happen frequently enough (at the very least more than once)?
Authorization-Granting	Does the use case grant some authorization on the spot?
Time-Limited	Do the envisioned credentials support expiration dates?
Revocable	Are the envisioned credentials revocable?
User-Centric	Does the use case benefit from having the holder at the center (if this is the case at all)?
Human Trust	Would the use case involve trust in the same actors as it would do in the physical world?
Identity-Specific	Is identity authentication/verification at the heart of the use case?

Table 7.1: Questions for SSI Use Case Requirements

First, we allocate one section to each of the selected use cases presented in section 4.4 (eID, diplomas and edu-ID) and then we outline the rest of the use cases in a more synoptic way (existing use cases, those involving single VCs and those enabling SSI interactions, in the order they were described in chapter 4).

7.1 Electronic Identity and its Derivatives

First, we analyze the eID use case, with an emphasis on the currently ongoing Swiss eID bill. Indeed, after the initial discussion has taken place, several companies have taken position in favor of SSI. For instance, SWITCH has written a statement [66] which encourages the government to target the widest ambition level in order to create a whole ecosystem of SSI credentials around the official eID. Accordingly, the government has indeed chosen to pursue this path and has recently published a draft law about eID [41]. It is under this perspective that we analyze the eID use case, directly citing related articles of [41] when relevant hereafter.

Privacy-Preserving To begin with, it is absolutely crucial that the electronic identity card be privacy-preserving. Indeed, it contains information that can uniquely identify a person, and it would cause major damage if someone gained access to it with malicious intentions. In theory, if SSI were implemented as intended, all private information would be issued by the state and then only be available on the citizen's devices. However, for historical and practical reasons, there exist registers at the municipal, cantonal and national levels, which will continue to exist in parallel of the eID.

Additionally, the *federal police* (fedpol) is newly entitled to maintain an information system with data about requested and issued eID credentials (Art. 11), including among other things each holder's social security number, eID number, issuance date and validity time (Art. 2). These attributes can be stored from the moment of the eID request until five years after the expiration of the eID VC, as illustrated on Figure 7.1. Since one's social security number can uniquely identify a person during their lifetime, this information enables linkability, but this is not as problematic as in the US, where this identifier is constantly misused and abused[32]. Therefore, if this data is properly encrypted, privacy is preserved accordingly, since there is no other private information on an eID-specific storage.

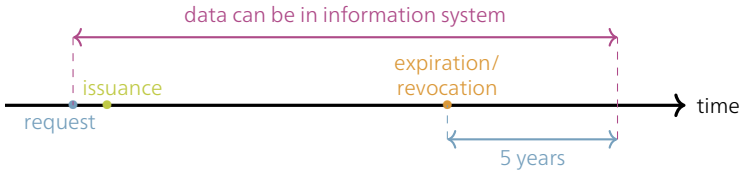


Figure 7.1: Timespan for Supplementary eID Data Storage in Fedpol Information System

Selectively Disclosable As we have seen, for the electronic identity to function, a certain amount of attributes are issued and held by each citizen participating in the project. In the sense of selective disclosure, the draft law aims at minimizing data in the first place (Art. 1), and ensures that people can present only part of their eID if they do not wish to disclose all information (Art. 16, Art. 10). Therefore, selective disclosure is supported and one can prove only the minimal amount of attributes strictly necessary to a verifier.

Cross-Sector By definition of an identity card, an eID is to be used in all kinds of situations where one's identity needs to be verified. This includes all situations where we already show physical identity cards as of now, as well as situations where presenting an eID simplifies the process because one needs not be at a specific place in person. In particular, any verifier accepting the eID should also accept valid (physical) alternatives as envisioned by previous laws (Art. 10). This typically includes all sectors as shown on Figure 4.2.

[32] The *social security number* (SSN) in the US can enable identity theft since opening bank accounts can be done based on this number only [90]. This is not possible in Switzerland, since the social security number alone cannot enable access to any service [34].

Multi-Issuer In the "physical" world, identity cards are issued by the cantons for citizens living in Switzerland, or by the local embassy for those living in foreign countries. This idea is not replicated one-by-one for the digital world, since fedpol is in charge of issuing eIDs (Art. 4). Therefore, one might think that issuance is centralized at a single place.

However, since the eID project targets an ambitious ecosystem with all kinds of verifiable credentials, anyone can issue credentials if they are registered on the official infrastructure (Art. 12), possibly after having paid some fee to the Confederation (Art. 26). This is probably due to the actual transaction fees for writing on the underlying distributed ledger[33], and it also discourages people from issuing "garbage" credentials.

Distributed Authority First of all, inside Switzerland, nobody can take decisions by themselves, since democracy is designed in a way that gives power to a majority of people within a group. Additionally, in order to have interoperability with other countries, Switzerland should get involved with international projects, such as the one designing the euID. In fact, mutual compatibility can be enforced by agreements (Art. 27) and the government ensures that international standards will be respected to facilitate this step.

When it comes to preparing VC schemas other than the base eID, issuers can enter their own "means of electronic proof" (as well as revocation information) on the public register designed for this purpose (Art. 17). As a result, the authority is well-distributed across politicians, fedpol and individual issuers, which corresponds well to the spirit of SSI.

High Volume It is hard to tell at this point how frequently one would use the eID in practice, but at least based on the physical ID card use cases and the cross-sector aspect of this electronic counterpart, it seams only logical that one would use the eID regularly in their interactions with authorities, but also organizations requesting (electronic) identity checks (Art. 9) such as universities, companies, hotels, *etc.*

Additionally, different actors of the Swiss democracy are in charge of helping citizens in case they have trouble managing the lifecycle of their eID (Art. 8), which helps making the eID more user-friendly, thus easing adoption for more frequent use as well.

Authorization-Granting Since both the state but also private companies or even individual people can issue credentials, verifiers can choose who they trust, although they **have** to trust the official eID wherever it needs to be accepted. In any case, proving one's identity with an (electronic) identity card enables authorizations in all sectors of the public domain, be it for age categories, "opening bank accounts" or even signing documents digitally [67].

Time-Limited As shown on Figure 7.1 already, an eID has a limited timespan which is stored in the VC itself as well as on fedpol's information system (Art. 11). How much time separates the expiration date with the issuance date is unclear at the moment, but it is probably similar to the analogous time for physical ID cards or passports (ten years for adults). Anyway, the duration of validity is limited (Art. 6), which corresponds to the SSI requirement.

[33] Although, it seems that the specific decentralized network has not been chosen yet (Art. 28).

Revocable Additionally to being limited in time, the eID is also revocable (Art. 5), to account for several scenarios that are described in the draft law [41]. For instance, people may ask for deletion or abuse the eID system, but revocation also happens upon death of the citizen or when a newer eID has been issued to them. Consequently, this satisfies the SSI requirement about revocation.

User-Centric The way data is stored is decentralized (Art. 1), which suggests that users have sovereignty over their own eID and related VCs. As suggested, VCs cannot be transmitted between people, except when VCs are not issued to a person (Art. 15). This corresponds to an entity-centric perspective (*cf.* subsection 9.1.4) and comprises use cases such as CarDossier (*cf.* subsection 4.3.2) for instance.

Additionally, holders are free to choose the wallet application they use (Art. 14), even though there will exist an official one provided by the state (Art. 19). When it then comes to proving VCs to verifiers, issuers should not be notified of the process (Art. 16). This ensures that VCs be truly user-centric and remain free from interactions with issuers once they have been passed on to the holder.

Human Trust What is about replicating the infrastructure that exists in the analog world, the eID starts with delegating issuance and maintenance of the eID credentials to fedpol (Art. 4), which is a bit different to the process citizens are used to, but at least it involves a trustworthy actor from the state that is already established in the physical world.

Moreover, trust is built into the eID ecosystem by design, since when custom issuers decide to create their own VCs linked to the eID, they have to provide some basic information to the register (Art. 12), which provides trust to their legitimacy. On top of that, the source code is public (Art. 23), which makes the algorithms transparent, as proposed by the original SSI principles.

Identity-Specific Finally, the last requirement is that the eID by identity-specific, which is of course the case since its purpose is to encode one's identity electronically. When it comes to derived use cases such as eVoting for instance, the identity aspect is important as well, since only citizens can vote, but this can be linked *via* the proof system, *i.e.* without disclosing information that is not needed.

Takeaways on eID The eID is probably the most relevant use case for SSI at the moment, because it is general and corresponds exactly to an identity that can be represented through a verifiable credential. Moreover, once the eID is established, cryptographic links can create dependencies from other VCs to the basic identity, which enables an entire ecosystem of use cases that are related to each other. These aspects will also be explored in further analyses of use cases later in this chapter.

When it comes to SSI, the only aspect that is not well-aligned is the one of delegation, whereby one could choose an agent that would take care of their credentials. As of right now, such a scenario does not seem to be planned by the Swiss government, but it may only concern portability rather than delegation. In other words, the holder of one's credentials should not change, but it can be someone else than the subject of the eID. Other than that, the most important element that is yet to be clarified is probably interoperability, since the future eID needs to be recognized in other countries and Swiss verifiers need to accept foreign eIDs as well. This will take some time to set up, but the project is going in the right direction.

7.2 Digital Diploma Ecosystem

In the light of the previous eID use case, digital diplomas already belong to a higher level of ambition than the base identity provided by the state. In other words, it may create a link to a basic identity, be it a Swiss eID, an euID or some other VC from elsewhere on the world; or simply be presented in the same cryptographic proof. In any case, concrete proposals are being made for both student mobility transcripts and end-of-studies diplomas, for instance in the context of EBSI [52]. In the analysis that follows, we consider the approach where several attributes about a diploma (or academic certificate) are being issued within a VC to the student.

Privacy-Preserving Back in the day, lists of university graduates were published in the newspapers, which essentially makes the information public. However, such an announcement is made in a local geographical environment and is thus published for a moderate target audience, as opposed to the internet, where everything can be audited by anyone. Moreover, newspapers are sources for fast information and therefore usually short-lived, which makes information fade rapidly with time, contrarily to computers that never forget information once it is online. Thirdly, there is no additional data about the transcript or other diploma data when a simple list of names is made public in the context of a newspaper, because such information should remain private as long as the diploma holder does not disclose it.

For all these reasons, depending on the information included in the diploma credential, it is best if privacy is of concern. In particular, fine-grained attributes such as those in diploma supplements or in transcripts of records should remain private unless one explicitly chooses to share them.

Selectively Disclosable As mentioned above, fine-grained diploma credentials need to be selectively disclosable, which can be useful when showing a subset of one's grades to a future employer, for instance only for relevant courses. For coarse-grained digital diplomas, selective disclosure is not strictly necessary, much less applicable if only pass/fail information is included. However, one may want to prove that one has some diploma, or show the field in which they completed their studies, which already advocates for at least two VC attributes.

As a result, while the exact schemas for digital diploma VCs is not standardized yet, it seems sensible to support selective disclosure. Alternatively, if the information contained in the VC is already minimal, then the minimality principle is respected by design. Consequently, both of these cases comply with SSI principles.

Cross-Sector Diplomas, or more generally educational certificates, can take versatile forms. For instance, a student may receive a VC for completing their studies, but an employee might also get a VC for attending some training. Further, to bridge the gap between the academic and professional worlds, students usually show their diplomas as part of their application to a potential employer. In that sense, the diploma use case connects at least two sectors of the public domain.

When a diploma VC is being used within the sector where it has been issued, for instance in the case of a professional training course, then internal communication could be leveraged for seamless communication without going through an SSI holder. Nevertheless, such a workflow would require standards as well and, especially in the context of an entire eID ecosystem, it would be best to work in accordance with an existing infrastructure.

Multi-Issuer This last statement holds particularly true when the situation involves multiple distinct issuers. Indeed, trainings are offered by various organizers, which generates a wide range of possible issuers, almost like a series of "micro-sectors". Additionally, in the situation where a university graduate receives their diploma, this document/credential is usually issued by their home university, which is different for each student. All these issuers can be registered as valid and trustworthy on the official infrastructure by the state (*cf.* section 7.1). Therefore, diplomas are arguably both cross-sector and multi-issuer, which shows that the role distribution is well-designed for a potential SSI implementation.

Distributed Authority Regarding credential schemas, several projects are currently receiving momentum, such as the EBSI *verifiable diploma schema* (VDS) [52] in the EU, with various representatives from the blockchain world and the European Commission. In Switzerland, which is *de facto* excluded from EBSI, higher-level possibilities are being considered [14], without a specific emphasis on VC schemas. However, likewise to the eID situation where international collaborations can enable interoperability, participating in the discussion and thus distributing the authority about diploma VCs is the safest bet when it comes to ensuring compatibility between Swiss and European digital diplomas based on SSI.

High Volume The effort of establishing diploma credentials for an SSI ecosystem only pays off if these VCs are actually used frequently in practice. For sure, one does not need to show their diploma every single day in the current "analog" world. In fact, this is because repeatedly showing a paper document (or a scan thereof) is not the most practical situation for controlling access to some service. Whether sharing diplomas would become more common with the use of SSI remains an open question at this point. Accordingly, it may be a bit too early for implementing digital diplomas in practice, since other processes may be more urgent to modernize.

Authorization-Granting Showing a diploma can grant authorizations to different kinds of services, such as an alumni portal, an employment interview or even specific infrastructure in the context of a professional training. Depending on how the verifier infrastructure is participating, the process of showing a VC can directly enable some authorization based on the released attributes.

One could argue, to the contrary, that a diploma itself cannot provide access to a building, for example, because access control is usually time-limited, while a diploma is in theory valid for a lifetime. (Or is it?)

Time-Limited In the real world, a diploma is issued for an undefined period of time. Indeed, in principle, once one has it, one can keep it forever. However, academic dishonestly is still possible, which may lead to the issuer deleting the associated hash from the verification system in place.

Since such a situation is not meant to happen every day, it does not make a lot of sense to limit diploma VC validity in time; otherwise, they would have to be re-issued regularly.

Revocable However, the case where a diploma loses validity can be covered by revocation, since SSI VCs can support this feature *via* some revocation registry for instance. Actually, although time-limited and revocable credentials describe two distinct scenarios, they both converge towards the same goal of preventing "eternal" credentials. In that sense, revocability accounts for shortening diploma lifespan, since at least one of the two options holds.

User-Centric Most existing solutions for digitizing diplomas take a "document-centric" approach, meaning that some PDF file becomes a signed digital twin of the paper diploma, without any link to other data that is already in digital form. Having the user at the center of the diploma use case would enable linking a diploma VC to other VCs of the ecosystem, either with common identifiers or by checking the presence of, say, an eID, to couple the new information with an existing base identity.

As a result, SSI's capabilities can be exploited in much more depth. Indeed, when the user is at the center of sovereignty over their VCs, they can selectively disclose information in the form of combined VC proofs in order to get access to some service.

Human Trust When it comes to trusting the right people, it is not currently planned that issuers/verifiers would become different in the digital world than in the physical one. However, with the approach taken by the Swiss eID project, any university or company can be registered as a trusted issuer. Moreover, foreign or older diplomas could be legitimated by some official place in each country that is already responsible for recognizing and acknowledging diplomas from abroad.

Later, deciding whom to trust thus remains a question for the verifier to think about, although some "official" issuers may stand in an (inter?)national register which could help/force verifiers to trust at least a minimal set of universities/companies/authorities that are officially legitimated[34].

Identity-Specific For checking the diploma itself, there is no need to have an eID, as is clear from existing products such as SWITCHverify or CERTUS, where diplomas can be successfully checked without an ounce of SSI involvement. However, in order to make sure a diploma belongs to the person presenting it, it may be useful to rely on an eID, which can be shown together. In other words, self-sovereign **identity** in a strict sense may be out of scope for now, since its main goal is to provide a digital identity, but it could be interesting to see how it could be coupled with diplomas.

Takeaways on diplomas The diploma use case is not directly linked to identity checking, and may not require as private information as expected, but this highly depends on the format of the diploma. For instance, granular information may not be needed *per se* in the context of an employment interview, while no end-of-study diploma is available yet upon someone completing their student exchange (*e.g.* abroad). However, arguably, diploma supplement document **do** exist and, in the context of an ecosystem of digital trust, they would fit in very well with other verifiable credentials to form digital proofs.

Regarding authorization grants, it is true that one would not show their diploma every day to their employer in the current analog situation, but having SSI readily available on one's fingertips actually enables new possibilities, which also links to the "high volume" aspect: how frequently would one use such a VC in real life? This is probably where the answer is the blurriest at the moment, since the ecosystem is not yet in place. Therefore, the diploma use case is overall a reasonable match with SSI requirements, but it will take perhaps a few years to establish itself until the ecosystem is more present in society.

Hence, the research and education community should strive for getting some standards ready, because adopting SSI will certainly take a few years, but this is the perfect timespan for collaborating towards the common goal of easy diploma/certificate interoperability all across the widest possible compatibility area.

[34] The official procedure for establishing such an officially acknowledged trust anchor would however differ from country to country, however, which reflects the reality of law divergences.

7.3 Life-Long Learning with edu-ID Credentials

In the area of academical learning, user-centric identities that contain information about personal details as well as educational affiliations have established themselves all across Europe and beyond. In fact, several "edu-ID" projects have been implemented and the nearest example is the one of SWITCH edu-ID [24], which is establishing itself as the standard in Switzerland, as illustrated on Figure 7.2.

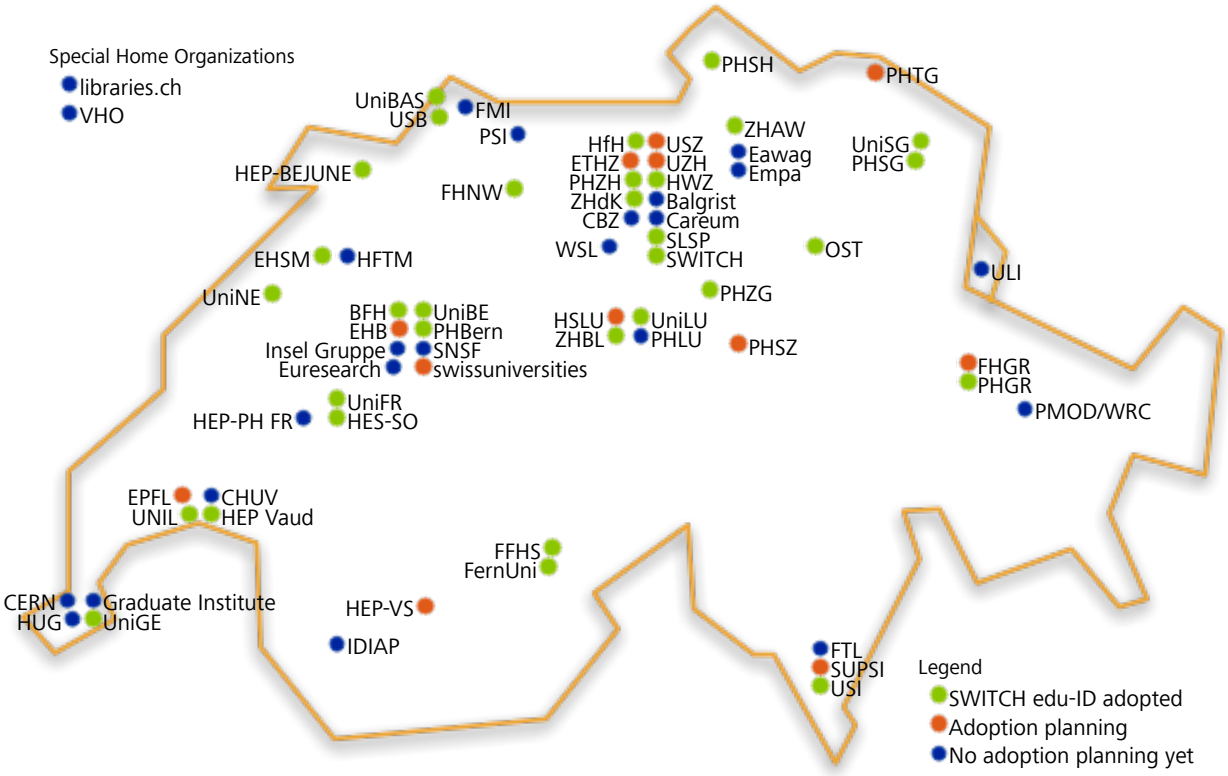


Figure 7.2: SWITCH edu-ID Adoption as of August 2022 (adapted from [49])

Even though this educational identity is unique per student, the responsibility of the related data still lies in the hands of SWITCH, which can be seen as privacy-breaching even though it is framed by strict laws. This is why SSI credentials could be released with edu-ID attributes, in an effort to shift the power to the users of educational services directly. In a first step, they would be issued in parallel of an existing edu-ID, but SSI could go as far as replacing existing identity federations on the very long term.

Privacy-Preserving edu-ID credentials include someone's name, address, phone number, university enrollments and possibly even SSH public key. In fact, such information is and should remain private.

Selectively Disclosable Selective disclosure is already supported in the SWITCH edu-ID model, since each service provider is free to require different attributes. Moreover, attributes are only provided by the IdP if there is a valid reason for the SP to require it, implying minimality. Therefore, moving towards SSI would not incur too many changes to the existing infrastructure, except for the translation from SSI attributes to *e.g.* OIDC claims. In any case, the fine granularity of edu-ID allows for selective disclosure by design.

Cross-Sector The cross-sector aspect of edu-ID is debatable at the moment. Indeed, it all depends on the connected services. In that sense, the more institutions migrate to edu-ID and participate in the project, the more sectors will effectively be covered. For instance, it is possible to create edu-ID affiliations to all Swiss universities and higher education institutions, because they all support SWITCHaai [25]; but libraries are also entering the ecosystem, as shown on Figure 7.2, which widens the scope towards other sectors related to education.

Multi-Issuer In the context of an identity, some information always comes from the people themselves, such as their name, email addresses or phone numbers. However, the issuer of **verifiable** credentials can only ever release information that is indeed verified, *e.g.* by sending a text message to a phone number with a couple of digits to check that the person has access to it. In that sense, even though users themselves can be thought of as "issuing" information, SWITCH is actually the trusted issuer when it comes to verifier trust. Additionally, all participating universities can also issue affiliations, which actually encompasses all institutions for higher education in Switzerland and not only those marked as "migrated" on Figure 7.2[35].

On the international landscape, several edu-ID projects exist and it would make a lot of sense to make them interoperable by supporting VCs issued by other *National Research and Education Networks* (NRENs), such as SWITCH in Switzerland. Such a common project would also go in the sense of collaboration between NRENs, as called for in [111].

Distributed Authority In the same sense as the above international collaborative effort, the authority for VC schemas regarding edu-ID could be distributed all across participating countries' NRENs. However, in the end, each of them can decide for their own data format, or extensions thereof as compared to other countries. Therefore, SWITCH can decide how affiliations look in the edu-ID ecosystem for Switzerland. Universities and their services then stick to the schema, which is why they should be first-class citizens in the discussion for establishing SSI as a new standard. For all these reasons, edu-ID is distributing its authority over a number of organizations, and it already tries to be consistent with European schemas without SSI, so this interoperability could continue to be the case in the SSI world.

High Volume Students access educational services such as Moodle almost every day and people subscribed to a library also go there periodically to borrow new books. On top of that, employees of higher education institutions can also use edu-ID for logging into their portals, which connects back to life-long learning, since edu-ID enables numerous services with its identity provision.

Authorization-Granting In that sense, edu-ID grants access to online services, and it could continue to do so with libraries enabling translations from VCs to OIDC claims. Moreover, it could also serve as an electronic means to enter buildings in universities or participating institutions.

Time-Limited In the current implementation of SWITCH edu-ID, a sliding window of 5 years keeps the identity active, as explained in [10]. However, such a varying expiration date is probably hard to implement with SSI by nature, so it is probably best to avoid limiting edu-ID VCs in time.

[35] Universities marked as "migrated" are those who rely on edu-ID for all their online services instead of their own IdP. Orthogonally, all of them are providing SWITCHaai IdPs, which are the relevant ones for establishing affiliations.

Revocable If credentials for life-long learning are not meant to expire, they should at least be revocable. For instance, affiliations are currently renewed every day, and they become "former affiliations" once they are no longer verified. In the context of SSI, such a daily verification system would become obsolete, since revocation could take care of disabling affiliations.

User-Centric The idea of SWITCH edu-ID is to be user-centric, and SSI would empower the user even more by giving them sovereignty over their verifiable credentials. However, as explained in Figure 1.2 and Figure 1.3, the difference is that there is not identity provider as an intermediary in the authentication process. Instead, verifiable credentials can be shared directly in the form of cryptographic proofs from the holder to the verifier.

Human Trust The idea of human trust is to replicate the processes of the physical world as closely as possible in order to facilitate adoption, since users understand how the information flow is happening. In the case of an educational identity that is already digital, this means involving the same actors as in the existing situation. Therefore, if universities and SWITCH continue to issue credentials in a similar way as hey are doing now, the process would keep human trust as expected.

Identity-Specific SWITCH edu-ID accounts are strongly linked to identity and some attributes can even be verified (such as email addresses and phone numbers, as described previously). Moreover, once an eID ecosystem is in place, it could be coupled with edu-ID in a similar way as explained in the analysis for the user-centric requirement in the diploma use case (*cf.* section 7.2).

Takeaways on edu-ID as VC In the light of the current requirements, this use case is very promising next to a state eID, even though some questions remain open. In particular, the cross-sector requirement is not strictly established as we speak, but gradual adoption will probably broaden the application range; and the fact that multiple issuers have equal rights to contribute to edu-ID credentials further distributes power and trust across the ecosystem.

Speaking of further use cases, an edu-ID as VC can also constitute the base for more applications, such as access control in university buildings when a student has the right affiliation. Additionally, in the sense of the ambition level targeting a digital ecosystem of trust, VCs can be combined with each other, and it could be practical to combine VCs about eID, edu-ID and diplomas in the same proof for instance. For all these reasons. the edu-ID based at SWITCH is the use case of choice for a sandboxed implementation in chapter 8.

7.4 Other Outlines of Requirements Analyses

For the sake of brevity, the remainder of this chapter will not cover all use case analyses echoing chapter 4 in detail, but a condensed form of the most relevant discussions is provided in this last section. For a more complete study, the SSI matrix in Appendix B can provide an overview of the requirements to consider.

7.4.1 Existing Use Cases

ID Wallet The idea of the ID wallet is to provide an AAI environment for German citizens with a growing set of VCs around their base identity. At the moment, crossing sector borders is envisioned, through use cases such as hotel check-in or driving license verification. In principle, this use case is very similar to the eID ecosystem that is planned for Switzerland, but it needs to be developed and tested thoroughly before being officially released. Indeed, it has been published in "production" mode without a scalable ledger underneath, which quickly resulted in security problems. As a result, it may be revisited in the future, but it should also take interoperability with other countries into account. In particular, since Germany is part of the EU, it would make sense to either bind the existing project to an euID.

Digital Staff Passport (DSP) The DSP in UK hospitals has been developed with mobility for health employees in mind. Since patient's lives are at stake, it is probably better in the everyone's interest that as much information as possible about the capabilities of a hospital staff member be known to their employer. However, private data should absolutely be kept confidential to comply with the idea of SSI. Since the use case is contained in the health sector, it probably only involves authorities from there, thus compatibility issues could occur when trying to bind it to another ecosystem, when it comes to enlarging the scope to *e.g.* opening bank accounts. In principle, it would have been best to wait before implementing this use case until SSI becomes more widespread, but due to the emergency of the COVID situation, it came at the right time with a moderate scope.

7.4.2 Possible Use Cases for Single VCs

Immunity Certificates Now that the COVID situation is hopefully over, we won't need immunity certificates as much, but they could be useful for other proofs of vaccination when traveling. Indeed, if we ignore the fact that restaurants do not usually have access control, then the human trust factor is relatively well-respected (*e.g.* immigration offices asking for certificates). Moreover, immunity VCs can make use of zero-knowledge proofs to avoid disclosing one's identity or which kind of vaccine one has. Consequently, this use case would would have matched with SSI requirements well, but it happened a tad too early, as a result of which we still used physical ID cards. But, since we have gathered some experience with such certificates, they could serve as a good base for experimental VCs in a sandbox.

Medical Prescriptions As in the digital staff passport above, it is important that health professionals can learn information about a patient who trusts them. In the case of prescriptions, specialists and pharmacists could leverage some internal communication channel such as the *Electronic Patient Record* (EPR) [45]. However, such a patient-centric platform relies on an existing electronic identity which is provided by some external IdP. In other words, it leverages an existing user-centric identity stored in a company's database and not within the health sector. As a result, one may well decide to keep one's data private *via* SSI. This would generate positive evolution with the support of revocation for *e.g.* a doctor that finds out soon enough that they have made a mistake. However, SSI may be out of scope for now, since its main goal is to provide a digital identity or eID, on which the EPR system could rely directly in a first step. Later, it could be interesting to use SSI for more fine-grained credentials once it is more established, so as to link other use cases to existing ones.

Employment Status In this use case, one may want to disclose whether or not they are employed and possibly additionally the name of the employer as well. What is more, unemployment allowances are sent out for a maximum period of a couple of months, which hints at expiration dates, while employment is often unlimited, which should use revocation. However, just like what we said about medical prescriptions, this does not directly link to identity checking, so it is probably better to wait until SSI is more established in other sectors for combining it with more use cases.

Public Transportation Tickets Depending on whether examiners are collecting statistics or checking ticket validity, one may want to disclose different information. Moreover, both a company itself and an online booking proxy should be entitled to issue (sell) and revoke (refund) tickets. However, this use case remains within the sector of mobility, which does not unravel the full potential of SSI, even though such tickets are usually non-transferrable and thus identity-specific. Hence, it looks promising for SSI, but not immediately, because "manual" face recognition based on profile pictures works "well enough". When an eID ecosystem is in place though, mobility VCs can become a sensible addition to one's digital wallet.

7.4.3 Possible Use Cases for SSI Interactions

Transportation as a Service (TaaS) The TaaS use case links technicians, lawyers, police officers and driving teachers, covering several sectors at once. More and more, it becomes important to share means of transport instead of owning a car, so TaaS will also grow gradually. However, roles are not clearly defined yet, since this use case combines several others, and it may well be contained in CarDossier. Ultimately, it could be interesting to leverage existing credentials when SSI is established, and build TaaS on top of them.

CarDossier As alluded to before, different issuers and authorities are involved in the establishment of VC schemas for CarDossier. Since these VCs are car-centric, there is no single user at the center; but entity-centric VCs can be rightfully delegated to a holder. In that case, it is important that users understand precisely what is going on in the sense of human trust. As such, this use case is probably not well-aligned with current SSI efforts, since there is no way to verify a car's identity with biometrical factors, but it could become an interesting application of delegation and portability once an SSI ecosystem is up and running.

Student Matriculation and Family Allocations The matriculation use case could benefit from selective disclosure and ZKPs for minimality. However, since multiple sectors are involved, these should cooperate towards supporting common VC schemas. For instance, VC lifetime can be an issue: either the matriculation is a snapshot to be renewed periodically, or it waits for revocation to avoid additional burden once the flow has been set up. This use case could also very well lead to adoption of SSI among students, which can later be useful for diplomas. Nevertheless, it may include some verification about the family status, to check that a student is indeed a child of their parent, which is a bit blurry at the moment using SSI.

Certificate of Residence and GA Travelcard Since two sectors are involved in this use case, they should collaborate to make sure each of them sets/gets what they want. Notably, the credentials are "multi-user-centric", since different holders have to create a single proof together, which is not documented in stone for SSI; and may thus require one family member to collect all VCs at one place *via* delegation. Other than that, this use case is quite simple and could become one of the early PoCs for SSI in the new Swiss eID ecosystem.

8 Proof of Concept Implementation of the edu-ID Use Case

"For lifelong learning to work, students must own their educational data"
— Gerd Kortemeyer [69]

8.1 Design Choices for an SSI Sandbox

Putting the previous analysis into practice, we will now describe a very preliminary approach to implementing edu-ID verifiable credentials in order to log into educational relying parties in the Swiss academical sector. In fact, there are usually three stages in the introduction of a new service:

- **Demonstration**: This is a good place to test a system in the form of a *proof of concept* (PoC) implementation in order to find out how it could look like with fake data or a carefully restricted scope;
- **Pilot**: This is where some people get involved and try out the product, a bit like an alpha test, so that the scope still be quite narrow, but with a focus on real users' feedback to improve usability;
- **Operational**: This last step is where a stable product is released to the public, which usually takes a few years to happen starting from the pilot project.

In our case, we will stick to a basic PoC demonstration with a simple wallet application holding a basic edu-ID credential. With this goal in mind, we will describe in this chapter which design choices were determinant for the implementation in the light of the threat model from chapter 6, as well as how we set up an SSI sandbox to issue edu-ID as a VC; all that followed by a discussion on the analysis and demonstration.

8.1.1 SSI and Decentralization

First of all, one of SSI's building blocks is the principle of decentralization (*cf.* subsection 2.1.2), according to which data is never centralized at a single place. Indeed, the long-established PKI solution for digital signatures and encryption schemes suffers from the issue of a centralized IdP which gets all the information about someone's login credentials. This may be alright for most users who are "not aware of data collection" [60], but actually computers never forget information, as opposed to human brains. In fact, digital protocols have side effects that may lead to massive information leaks, for instance in case an IdP is not careful in its implementation. To solve this issue, also reflecting the threat of an intrusive authority, SSI can store VCs directly on users' devices and provide minimal disclosure of private data, while relying on decentralized VC schemas that are globally available. This is why decentralization is so important in the context of SSI, and thus also in the implementation of the current proof of concept.

8.1.2 Database vs Distributed Ledger

Second, now that decentralization is established, we have to choose some type of storage system to hold our system together. In particular, we consider two possibilities:

- **Distributed database**: In a distributed database, data is either replicated over several nodes or localized at one specific node according to some criterion. Operations include both reading and writing, which provides flexibility, but these are typically not so efficient due to the step where the system has to figure out where the data is located.
- **Distributed ledger**: A distributed ledger limits these inefficiencies by replicating the state across all nodes and ensuring immutability of the stored data. As a result, modifications are not allowed, which simplifies the consensus mechanism to an agreement over new transactions, for instance in the context of blockchains.

While not all blockchains are efficient, both in terms of speed and energy, those relying on proof-of-authority (PoA) can find a good balance between trust and efficiency. Indeed, a set of validator nodes are operating the entire chain while playing the role of trust anchors, which may not be so problematic if they are enough for trust to be distributed without possibility for a majority to attack the system by misbehaving in their task. Thus, such a PoA blockchain mitigates the blockchain influencer threat effectively.

When it comes to regular users of such permissioned PoA blockchains, read access comes for free and write access incurs some costs. In order to participate, individual users therefore need to set up a cryptocurrency wallet with a pair of private/public keys that they generate on the spot[36]. However, in the SSI world, one does not typically need to write on the decentralized network as a holder, because VCs are stored on one's device (as opposed to VC schemas, which are publicly available on the ledger).

Due to the more decentralized consensus approach taken by distributed ledgers, as well as the secure way of storing one's access to the network, we choose to leverage a PoA blockchain for our PoC use case. More precisely, since the hyperledger Indy project has been specifically designed for identity purposes related to SSI, we use this project's software for setting up an SSI sandbox.

8.1.3 Blockchain and Privacy

As has been alluded to in the SSI requirements, privacy is of major concern when implementing a use case. However, privacy is subject to various dimensions, as shown on Figure 8.1:

- **Attributes**: which attributes are shown to a verifier depends on selective disclosure, the fewer the better;
- **Identifiers**: how to uniquely identify an identity in a VC proof can range from complete anonymity to public DIDs;
- **Re-identification**: whether it is possible to reverse an identifier to an identity can be possible or impossible for competent authorities.

[36] In order to recover one's private key in case it gets lost, one gets a list of 12 seed words, which are simply English words that, put together in the specified order, can recover the generated private key. Therefore, these 12 words should be stored in a physically secure place upon creating the wallet.

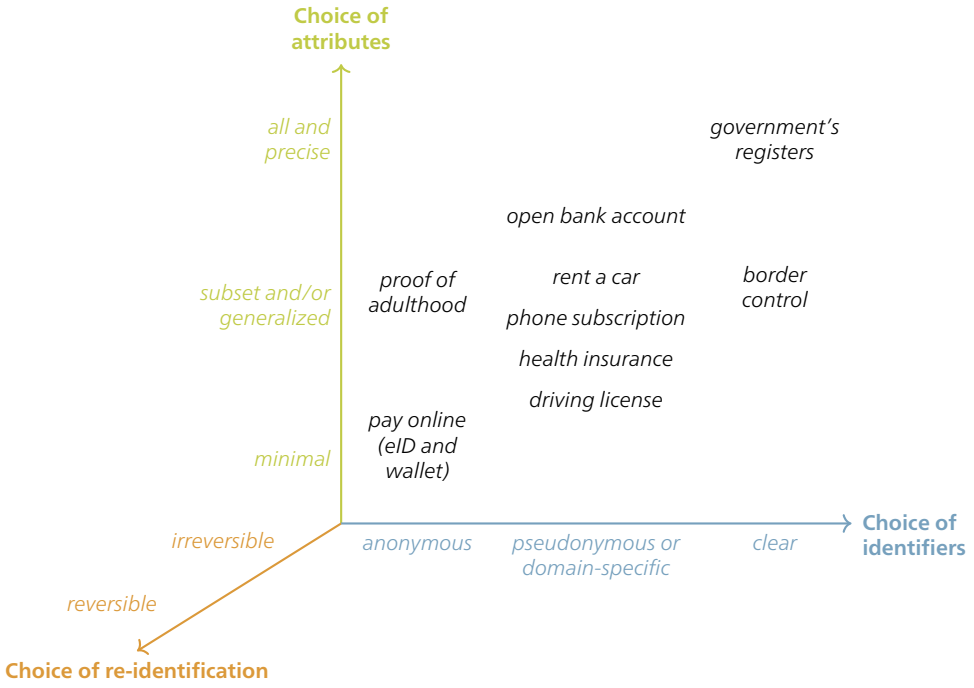


Figure 8.1: Privacy Dimensions of VCs (adapted from [60])

On this figure, the closer we get to the origin, the more privacy-friendly we become. When it comes to attributes, holders will choose to disclose a minimal subset every time they access a service. What is about identifiers, the most logical domain-specific identifier, namely `swissEduPersonUniqueID`, can be used for edu-ID VCs, but it would typically be reversible for SWITCH, *i.e.* they could re-identify a student based on their identifier, because they hold existing such identifiers on their IdP for edu-ID. As a result, one could simply use a different DID for each connection and combine VCs directly from one's wallet.

In particular, since some users are unconscious and do not care about privacy, VCs should never be written to the blockchain altogether; not only because this would not scale at all, but also because even in the form of hashes, certain correlations about a VC owner can be made by a blockchain explorer (*cf.* chapter 6) unless every single transaction uses a new DID. Therefore, only VC schemas necessary for everyone are published on the blockchain, and it can be enforced that issuers follow them.

Regarding domain-specific identifiers, unlike what is done in the US, where people's social security number is their all-in-one identifier, the situation with a unique student identifier is a bit different. However, there is no reason why this should be the only identifier provided to the holder of an edu-ID VC. In fact, such a credential could be linked to some generated custom pseudonymous identifier, or to an existing eID identifier, depending on which information is being disclosed in the proof. As such, holders have the freedom of choosing whether they want to be identified and by which entity.

An example of such domain-specific identifier is the *pairwise pseudonymous identifier* (PPID), which establishes a different identifier for each tuple (IdP; RP), so that correlation becomes much harder across relying parties (RPs). Additionally, hyperledger Indy supports such domain-specific identifiers and its VCs can be translated into OIDC claims, which bridges the gap between the existing system and SSI.

8.2 SSI Sandbox Setup

With these design choices, SWITCH is participating in a project building an SSI sandbox along with three other verifier nodes. The resulting network is a small-scale PoA blockchain running on hyperledger Indy, with the purpose of experimenting around with some first SSI use cases.

Next the the local verifier node, two nodes without consensus authority are connected, so as to distribute power against threats: the administrator node and the issuer node. Thus, in total, there are three *virtual machines* (VMs) based at SWITCH at the moment, for each of which the setup is documented in [20]:

- **Validator node**: this is the one replicating the Indy blockchain along with the three other participating validators and its goal is to avoid DDoS authorities;
- **Administrator node**: this node has full power over the blockchain with the "steward" role in the Indy jargon and it has to carefully prevent corrupt and spoofing issuers;
- **Issuer node**: this last VM has got the "endorser" role and can thus create VC schemas and issue VCs to any connected holder wallet.

For a better overview, Figure 8.2 depicts the SSI sandbox architecture in detail, especially with respect to the nodes operated by SWITCH.

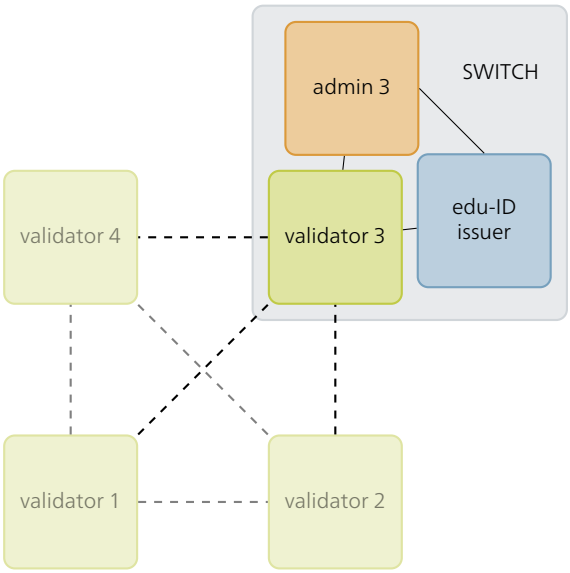


Figure 8.2: SSI Sandbox Architecture

In order to interact with the underlying hyperledger, the Indy-CLI tool is installed on each of the three nodes described previously. In particular, three steps are necessary for setting up the environment:

- Create the genesis file with all four trustees/stewards in the transaction pool and copy it to other nodes;
- Start the Indy ledger from the validator node to open it for transactions and connect the other two nodes to it by referencing the genesis file;
- Create an endorser DID to give the edu-ID wallet issuer capabilities and register it on the ledger.

8.3 SWITCH edu-ID as VC

Once the SSI Sandbox infrastructure is ready for use with Indy-CLI, another hyperledger projects enters into the implementation, namely Aries. More precisely, we use a library called *hyperledger Aries Cloud Agent – Python* (ACA-Py) [6], which provides an abstraction layer above Indy through an *application programming interface* (API) that directly communicates with Indy-CLI. Strictly speaking, ACA-Py simply runs in a Docker container, but actually it provides a whole web interface called Swagger, with which we interact in order to register VC schemas and credential definitions, and to issue credentials after connecting it to a wallet. This user interface is reproduced on Figure 8.3 from the project on [6] with a synoptic view that contains only the functionality that we used in this demonstration.

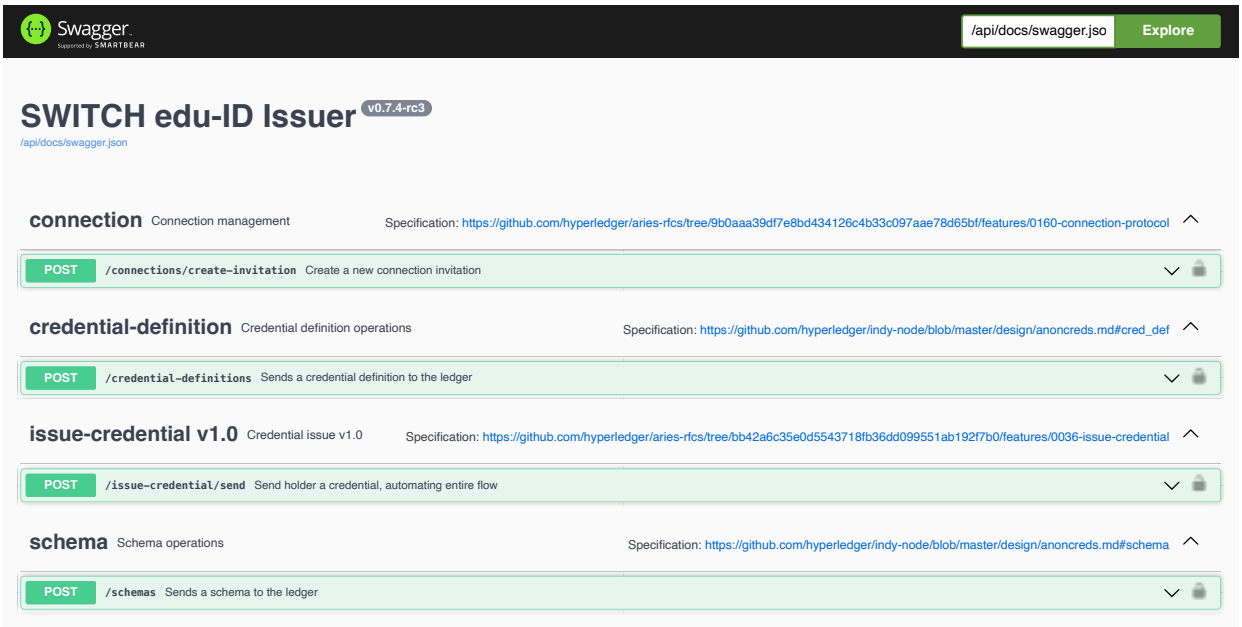


Figure 8.3: Swagger User Interface in ACA-Py

Posting a schema Since this implementation is a PoC, the exact VC schema does not matter for interoperability yet. Therefore, we try to establish a simple one that contains a small subset of edu-ID attributes, a bit like so-called OIDC scopes [46] by grouping several OIDC claims, as shown on Figure 8.4. In our case, we choose to enclose the basic information that is listed in Table 8.1. In particular, we depict affiliations to higher education institutions and a minimum age category which enables proving more minimal information than a birthdate.

User-Friendly Name	Computer-Friendly Name
Given name	`givenName`
Surname	`surname`
Email	`mail`
Linked affiliations	`swissEduIDLinkedAffiliation`
Minimum age category	`swissEduPersonMinimumAgeCategory`

Table 8.1: Attributes for PoC VC Schema

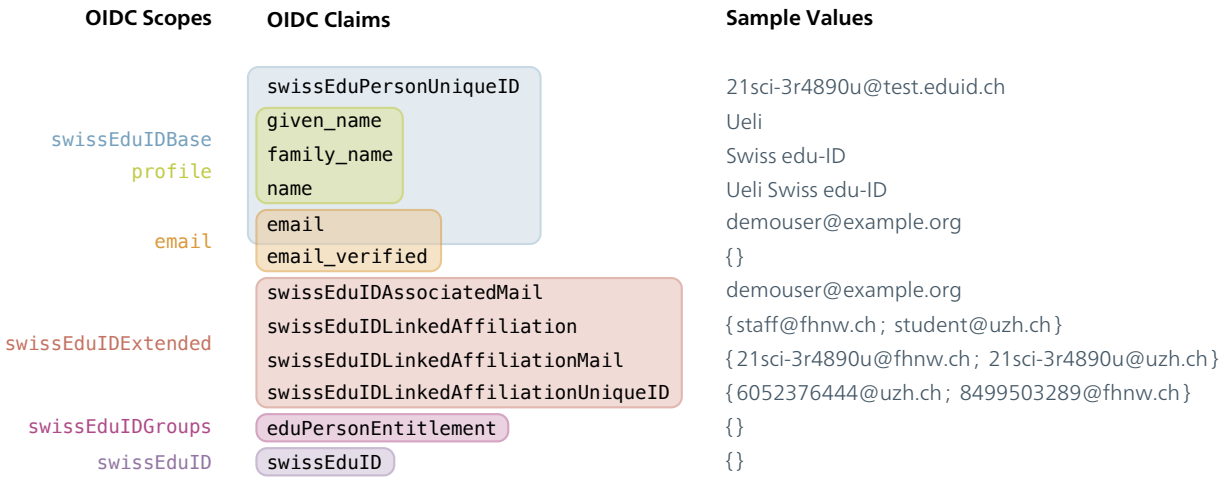


Figure 8.4: Relevant OIDC Scopes in SWITCH edu-ID Grouping Multiple Claims

In the ACA-Py web interface, we create a sample edu-ID schema by entering all attribute names, as well as the VC schema name and version, as shown on Listing 8.1. Under the hood, this schema is written on the Indy ledger under some schema ID, which can be used subsequently to reference it.

```
{
  "attributes": [
    "Given name",
    "Surname",
    "E-mail",
    "Linked affiliations",
    "Minimum age category"
  ],
  "schema_name": "edu-ID Attributes",
  "schema_version": "1.0"
}
```

Listing 8.1: Schema Creation Request

Posting a credential definition At this point, hyperledger Indy enforces an additional level of indirection, which is the one of a credential definition. Indeed, once a schema is on the ledger, an issuer still has to decide to issue VCs according to it and whether they want to support revocation. Therefore, we define such a "family" of credentials as in Listing 8.2, after which it also gets a `credential_definition_id`.

```
{
  "schema_id": "LJS2vPSCPZiQiFoNpjCZ5v:2:edu-ID Attributes:1.0",
  "support_revocation": false,
  "tag": "v1.0"
}
```

Listing 8.2: Credential Definition Request

Creating a new connection The last step before issuing an actual VC consists in connecting ACA-Py with some wallet application. For the example in this PoC, we use the *Trinsic Wallet* on an iOS platform, but it is noteworthy that about a dozen such applications exist on stores for various mobile operating systems, including also *esatus Wallet*, *Lissi Wallet* or *MyID*, to cite only a few. That being settled, we use the ACA-Py API in order to create a connection invitation, which is shown on Listing 8.3. Note that in this code, we use the endpoint IP address that has been associated with the issuer VM, but this varies depending on the setup. Upon this request, the response Indy sends back contains an invitation URL, which may look for instance as in Listing 8.4.

```
{
  "metadata": {},
  "my_label": "SWITCH edu-ID",
  "service_endpoint": "http://86.119.39.73:8000/"
}
```

Listing 8.3: Connection Invitation Request

```
{
  "connection_id": "ef1b10c0-4242-4e6a-8a9d-47d860ce9dcb",
  "invitation": {
    "@type": "did:sov:BzCbsNYhMrjHiqZDTUASHg;spec/connections/1.0/invitation",
    "@id": "54b378ba-c586-494f-a3bf-8ef5f281f6c2",
    "label": "SWITCH edu-ID",
    "recipientKeys": [
      "4swgsYTEpMeApfVCNmARmRkDf6xuwM3DDB3v7S3hsHyR"
    ],
    "serviceEndpoint": "http://86.119.39.73:8000/"
  },
  "invitation_url": "http://86.119.39.73:8000/?c_i=eyJAdHlwZSI6ICJkaWQ6c292OkJ6Q2
     JzTlloTXJqSGlxWkRUVUFTSGc7c3BlYy9jb25uZWN0aW9ucy8xLjAvaW52aXRhdGlvbiIsICJAaWQiOiAiNTRiMzc4
     YmEtYzU4Ni00OTRmLWEzYmYtOGVmNWYyODFmNmMyIiwgImxhYmVsIjogIlNXSVRDSCBlZHUtSUQiLCAicmVjaXBpZW50S2V
     5cyI6IFsiNHN3Z3NZVEVwTWVBcGZWQ05tQVJtUmtEZjZ4dXdNM0REQjN2N1MzaHNIeVIiXSwgInNlcnZpY2VFbmRwb2
     ludCI6ICJodHRwOi8vODYuMTE5LjM5LjczOjgwMDAvIn0="
}
```

Listing 8.4: Connection Invitation Response

Lastly, the invitation URL can be pasted in some QR Code Generator, which generates a QR code to be scanned by the Trinsic wallet application. This opens a pop-up window asking whether the application should indeed connect with the "SWITCH edu-ID" issuer, which can be approved by the user to add a new connection to the wallet.

Issuing a credential To finally use all of the previous steps for issuing a VC, one can browse to the 'issue-credential v1.0' section in the ACA-Py interface, of which the `send` method can issue a credential to a connection that has been established before. On can for instance use the sample values from Figure 8.4, and reference the schema and definition created earlier, as done on Listing 8.5.

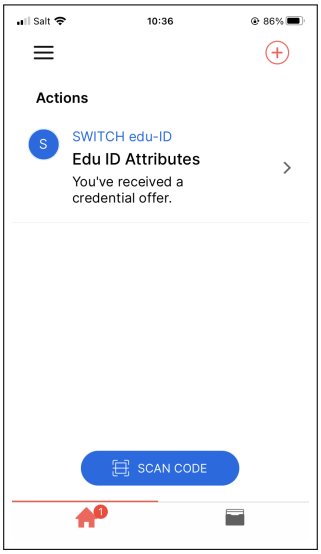
When executing this request, the wallet application receives a credential offer, as illustrated on Figure 8.5a, which one can open and accept as shown on Figure 8.5b.

```
{
  "auto_remove": true,
  "comment": "",
  "connection_id": "ef1b10c0-4242-4e6a-8a9d-47d860ce9dcb",

  "cred_def_id": "LJS2vPSCPZiQiFoNpjCZ5v:3:CL:15:v1.0",
  "credential_proposal": {
    "@type": "issue-credential/1.0/credential-preview",
    "attributes": [

      {
        "name": "Given name",
        "value": "Ueli"
      }, {

        "name": "Surname",
        "value": "Swiss edu-ID"
      }, {
        "name": "E-mail",

        "value": "demouser@example.org"
      }, {
        "name": "Linked affiliations",
        "value": "staff@fhnw.ch; student@uzh.ch"

      }, {
        "name": "Minimum age category",
        "value": "18"
      }

    ]
  },
  "issuer_did": "LJS2vPSCPZiQiFoNpjCZ5v",
  "schema_id": "LJS2vPSCPZiQiFoNpjCZ5v:2:edu-ID Attributes:1.0",

  "schema_issuer_did": "LJS2vPSCPZiQiFoNpjCZ5v",
  "schema_name": "edu-ID Attributes",
  "schema_version": "1.0",
  "trace": true

}
```

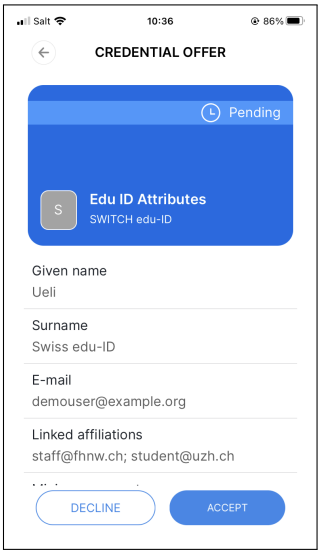

Listing 8.5: Credential Issuance

Proving credential attributes Once a credential has been accepted, it is listed in the wallet under one's credentials. Thus, by clicking on it, one can view the attributes again and, among other options, select "Share with connection" (if a connection has been established with a verifier before), which is illustrated on Figure 8.6a. As a result, a new window appears, as shown on Figure 8.6b, allowing the holder to choose which information they actually want to share with their verifier. However, as notified by the application, disclosure[37] is still a beta feature and it does not work in a stable way yet.

[37] Regarding the cryptographic "magic" that enables selective disclosure, [47] explains that several options are possible, but the simplest one consists in the issuer signing each attribute separately, so that a series of proofs can be shown by the holder.

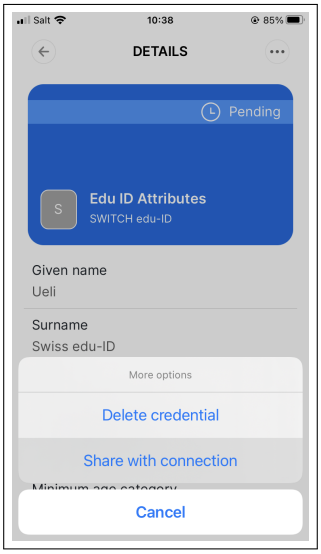


(a) **Receive Credential**: The credential reception triggers a notification and the home overview of the application now lists a new action to view the credential offer (other flows for issuance are also possible, *e.g.* where the wallet sends a credential request to ACA-Py)

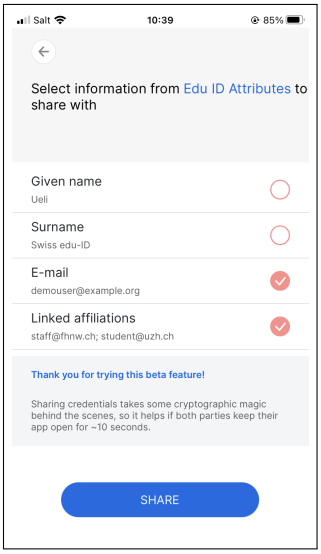


(b) **Accept Credential**: Upon viewing the pending credential offer and its attribute values, one can decide to either accept it or decline it (this part is not yet working properly, since accepting the credential triggers an error; however, one can decline the offer and keep it in the wallet)

Figure 8.5: Screenshots of Trinsic Wallet (iOS v3.2.0) during Issuer-Holder Flow



(a) **Share Credential**: By clicking on the extended options on the top right of the screen, one gets to share the stored credential with a connected wallet application (this can be ACA-Py itself or a different wallet application, for instance on another smartphone)



(b) **Disclose Credential**: The final screen enables selective disclosure, so that one can choose which attributes will be included in the cryptographic proof to the verifier (however, this is a beta feature and we have not been able to make it work as expected for the time being)

Figure 8.6: Screenshots of Trinsic Wallet (iOS v3.2.0) during Holder-Verifier Flow

8.4 Discussion and Analysis

To wrap up this experimental part of the project, we discuss the approach taken and provide some high-level insights about the requirement analysis.

8.4.1 Takeaways from the edu-ID Demonstration

First of all, it is directly noticeable that some wallet functionality did not work as expected. In fact, we tried several wallet applications listed in section 8.3, but only the *Trinsic Wallet* was able to receive VCs correctly from ACA-Py and at least display them in a human-readable way. Among other points, here is a short list of issues that we encountered while trying to implement the edu-ID PoC:

- **Attribute labels**: According to the schema creation, attributes can only be described by their displayed name, which may contain spaces, because it is meant for humans to read. Therefore, some JSON structure should be created for entering computer-friendly attribute names as well, without affecting user experience in a negative way.
- **Automating issuance**: Ultimately, the goal would be to issue VCs on-demand from the edu-ID IdP, but they have to be crafted manually at the moment. To this end, the API could be bound to an automatic issuer service.
- **Issuing credentials**: Indy originally had a JSON format for issuing credentials (v1.0), but they later released an update with more configurability (v2.0). However, we were unable to even receive credential offers with the latter version (on all tested wallets), which is why we used the former one in section 8.3.
- **Accepting credentials**: It was unclear why credentials could not be accepted in the intended way, even after an offer was successfully received. This may be related to the credential issuance protocol or to an incomplete configuration of the underlying ledger, so the functionality could be improved.
- **Multi-valued attributes**: When sharing credential attributes *via* selective disclosure, one can only select a flat structure of attributes due to the AnonCreds approach taken by Indy [3]. As shown on Figure 8.5 and Figure 8.6 for instance, linked affiliations have to be encoded with a manual semicolon in between different values, because arrays are not natively supported as in JSON-LD [40].
- **Proving credentials**: Showing credentials to a verifier should also display some information on their wallet/verifier application, which does not work at the moment, either because the credential is still marked as "pending" since it could not be accepted, or because of some issue in the beta implementation of the functionality. Thus, we could not try to mitigate threats on verifiers, either.

For all these reasons, it becomes quite apparent that SSI is not yet a mature technology, since different wallets coexist and have different functionalities. However, it is precisely through this approach of trial-and-error that the ecosystem will evolve and eventually become stable. Moreover, when it comes to the edu-ID approach, requirements were matched and it would be sensible to develop such educational credentials for a more self-sovereign approach in life-long learning, because intrinsic motivation is precisely what makes it happen.

In that sense, we also provide an outlook on further development of SSI use cases, as well as some discussion about the requirements that led to this work in the first place.

8.4.2 Research on Open Questions

With these points in mind, SSI is evolving in the right direction, because it is constantly getting challenged and tested. As a result, a number of open questions for future research arise, specifically regarding storage/backup/recovery mechanisms on wallet applications, as well as support for data migration and delegation of credentials.

Additionally, the trust and identity role of NREN organizations such as SWITCH is also unclear in a world where IdPs are no longer needed. For instance, [105] raises a set of suggestions for replacing/complementing IdPs, be it through issuance of VCs, support for a helpdesk environment, assistance for recovery or migration, or maintenance of a DLT infrastructure. In any case, SSI would initially come in parallel of existing solutions in order to establish itself on a wider scope through a transition time.

Next to that, research can focus on participating in various projects working on SSI use cases, such as the identification of educational blockchain opportunities, the future of edu-ID or even the preparation of an interoperable eID ecosystem, for which a consultation is currently in progress. Of course, it is also sensible to tackle the challenges related to wallet applications, since these should be made compatible with each other as well.

8.4.3 Some Perspective on SSI Use Case Requirements

Finally, we come back to the requirements for SSI use cases as listed in chapter 5. Originally, multiple ways of displaying such a use case analysis were envisioned, but the matrix representation was the most practical one, because it did not bake in any logic that would introduce dependencies between different requirements. Nevertheless, analyzing each requirement separately enables some discussion that helps taking decisions. Indeed, oftentimes the answer is not a strict yes/no, but rather an open door to interpretation.

One possibly blurry aspect lies in the distinction between functional and non-functional requirements. Indeed, this dichotomy may instill some false impression of inequality. However, it is important to note that both kinds of requirements are equally relevant, and that the functional ones really focus on the way a user interacts with their VCs, whereas non-functional ones navigate around the ecosystem surrounding SSI interactions. Therefore, considering them distinct enables a better decision-taking process, for instance by checking whether it is the ecosystem around a use case or its functionality factor that match with SSI better. Nevertheless, such a granular analysis has admittedly not been performed.

As a closing remark, while similarities and differences between use case requirements and SSI principles have been clarified in section 5.4, some principles are covered more extensively than others by the set of formal requirements, leading one to think that these are more important than others. In fact, while it is true that most discussions emphasize on certain principles more than on others, it also holds that some principles are not considered enough in the analysis. For instance, delegation, which is part of the more general idea of agency, is not being referenced enough in the context of the established requirements, even though it is of primary importance in the context of human trust and several use cases heavily rely on it. Alternatively, one could imagine checking all SSI principles one by one for each use case, but this would not provide a complete picture of the use case's feasibility. Consequently, it could be possible to periodically insert requirements into the provided list as the landscape evolves, and then reassess use cases that are being developed.

9 Related Work

"Any sufficiently advanced technology is indistinguishable from magic."
— Arthur C. Clarke [27]

Self-sovereign identities have been around for a couple of years, and their exploration is not completely new. However, it is a technology that is not mature yet and thus it has not reached the point where it simply works "auto-magically". Consequently, research has been focusing on making it evolve by looking at different aspects of its applications. In particular, similarly to this project's goal, there exist publications that have tackled the problems of finding SSI use cases, settling requirements for their relevance, modeling potential threats on them, as well as implementing them using distributed ledgers. This chapter will make a survey of these papers and articles, without claim for completeness, but with a wide overview on these different points that loosely relate to the chapters of this report.

9.1 Use Cases of SSI

First of all, while SSI is strongly linked to identity by definition, electronic identities are not the only use cases for verifiable credentials [15]. Indeed, as alluded to in [77], VCs can be seen as containers for any kind of payloads, including:

> - *Consent, permissions, votes, opinions*
> - *Tests, procedures, results, prescriptions, diagnoses*
> - *Balances, totals, deficits, ranges, statistics, source data*
> - *Statements, agreements, contracts, invoices, sources*
> - *Confirmations, acknowledgments, attestations, assertions, affidavits*
> - *Date, time, location, speed, trajectory, weight, temperature*
> - *Laws, regulations, statutes, rules, orders, decrees, declarations*
> - *Photos, videos, music, messages*
> - *Software code, hashes, files, the state of a database at a given point in time*

While some of these items may not require SSI in a strict sense, they can be seen as enablers for a range of possible use cases of SSI. In fact, there exist numerous publications about SSI and its potential applications. In this section, we look at the most important ones gravitating around electronic identities, blockchain-specific use cases, educational applications, as well as entity-centric credentials.

9.1.1 Electronic Identity Ecosystem

First of all, [74] provides an overview by world regions about where the world is standing (as of 2021) regarding eIDs. For instance, in countries where there is little existing infrastructure, eIDs actually develop faster than in those with existing federations, specifically when they directly rely on emerging technologies such as blockchains. Indeed, many countries still offer a central portal for managing digital identities, which is part of some *e.g.* OIDC federation, which needs to remain functional in parallel of any new system. When it comes to SSI in particular, there exist various projects for eIDs around the world, including in Germany, the Netherlands, Sierra Leone, South Korea, British Columbia, the US and Brazil. These projects are still at an early stage of development, but they will continue to unfold as SSI is maturing.

In the Swiss landscape, the eID is being shaped actively as we speak, which was not yet the case when the previous paper was written. In the mean time, [2] has been written as a discussion input for the development of the Swiss eID. More precisely, it articulates some ideas of use cases regarding the "ecosystem of digital credentials": diplomas, identity cards, customer cards, credit cards, subscription cards, *etc.* Additionally, it explicits how different sectors are entangled in order to identify opportunities for cross-sector use cases.

> *For example, the agriculture authority (one entity) could issue sustainability and organic processing certificates to farmers (another entity) who sell yogurt (another entity) to food companies (another entity).*

What is about further use cases related to identity, [99] proposes a new model for access control called *SSI-based access control* (SSIBAC), which can provide *identity access management* (IAM) within and across organizations. In the proposed scenario, the verifier is coupled with an access control engine, so that authorizations can be granted on-demand upon checking digital proofs. A similar use case could also be included in a cross-sectoral ecosystem such as the one envisioned for Switzerland.

9.1.2 Blockchain-Based Applications

Many publications about emerging technologies can still be found in the form of articles or blog posts, as is the case for instance with [55], which is a hitchhiker's guide to the blockchain. In this online article, several use cases for blockchains are discussed from a critical viewpoint. These are not specific to SSI, but could in fact be implemented using it, which is why they are presented here.

The first opportunity is the one of digital elections, which is especially interesting because it has been on hold in Switzerland for several years due to security issues in the technical system. While the author does not advocate in favor of using blockchains for storing individual votes, there is potential in using SSI for eVoting, for instance by leveraging self-issued credentials, which can then be trusted by the government if they satisfy a certain amount of criteria.

Other proposed use cases include certificates of provenance/origin, so that one can verify the entire supply chain of a product, or degree certificates for students in the academic sector, which can be of diverse nature. This last possibility leads us to the next subsection, where educational use cases are explored further. Later, more ledger-based implementations will be described in section 9.4.

9.1.3 Educational SSI Credentials

As alluded to already, educational use cases of SSI are being actively pushed by discussion groups all over Europe – and probably also in other continents. This encompasses not only digital diplomas, but more generally all kinds of digital academic credentials [101], which also includes professional VCs, certificates for some online course, or even educational login credentials. For instance, [105] proposes two use cases for an edu-ID: one where the student already has an eID that can be linked to it and one where they do not have one available but are still willing to use some service that requires an edu-ID. In both of these scenarios, the service should work, but only one of them will be provisioned with the state eID.

When it comes to academic documents such as diplomas, [58] proposes to leverage SSI for university admissions, supplements to paper documents, student (inter)national mobility and even "eInternships", which can actually enable a sensible combination of academic and professional credentials. This is also what is suggested in [14], where very fine-grained VCs about education are envisioned.

On the European scene, the EBSI project is gaining momentum in the area of academic VCs as well, as demonstrated in [16], where life-long certificates such as diploma VCs or social security VCs are explored, with an emphasis on interoperability across the EU. For instance, one of the considered scenarios proposes to "combine identity credentials with educational credentials for student mobility".

Education and SSI is thus an idea that will endure for some time, as cited also in [19] among other use cases such as mobile providers, state portals in the US, as well as eGov purposes in various countries. Such applications of SSI all provide a user-centric experience, which can link various sectors of our society, be it in state identity, education or telecommunications to cite a few (*cf.* Figure 4.2).

9.1.4 Entity-Centric Perspective

According to [113], the user-centric aspect of SSI does not account for all use cases. Indeed, it considers the holder's perspective as one of the main credential "dimensions", next to their schema format, JSON rendering, correlation possibilities and payment options. More precisely, it distinguishes the subject and the holder of a VC, because while they are often the same person, they may actually be distinct, or there could be multiple subjects for a single holder.

For instance, the employee-centric model that we have seen in [15] enables staff movement around hospitals in the UK by providing all participating employees a digital staff passport in the form of a VC, of which both the holder and the subject are the employee themselves.

On the other hand, the car-centric model from CarDossier [42] unites several credentials about a car in the wallet of an "external" holder, namely its owner. Actually, [112] has established most of the architectural basis for the CarDossier ecosystem, including the choice for hyperledger Indy when it came to the implementation. Alternatively, there exist other systems such as Affinidy, which can manage driving license credentials [88] as well.

These two examples advocate for a model that is rather entity-centric than user-centric, where an entity can be any generic instance which has one or more DIDs. This opens an even wider door to use cases that account for the agency principle of SSI, where some delegation takes place to shift the responsibility for VCs to where it makes the most sense.

9.2 Searching for SSI Requirements

Next to the search for SSI use cases, the key goal of this project is to formulate a set of requirements to analyze these use cases in a systematic way. In fact, there are some other publications that tackled this question, although in a slightly different way. This section presents two viewpoints on requirements: first, how one can visualize them in a clear way; and second, which requirements should actually be used.

9.2.1 Requirement Visualization

When it comes to depicting requirements graphically, one should take great care on how the visualization impacts the clarity and precision of the analysis. For example, [119] proposes (on page 42) a flow diagram for checking whether blockchain use cases make sense or not. The diagram proposed in this book is not SSI-specific, but it provides a good intuition on how databases often make more sense than blockchains, thus considering the latter as over-engineering for most use cases. This flow diagram approach had originally been taken for the current work, but it led to considering fewer requirements per use case, which eventually made the analysis evolve towards the actual matrix that has been presented.

Another way to look at requirements for SSI is used in [63], where three solutions for SSI implementations are compared: Sovrin, uPort and Civic. This approach is not directly use case oriented, but it performs a comparative analysis based on criteria such as ownership, user control, trustworthiness, privacy, interoperability, portability, sustainability, user experience, recovery and cost. For each of these elements, each system is analyzed in the form of a table, which also inspired the matrix visualization in the current work.

9.2.2 Alternative Requirements

As we have seen in the previous subsection, the criteria for use case analysis may not only vary in their form but also in their content; and indeed, several publications have tried to list requirements for SSI use cases.

To begin with, [101] focuses on academic credentials and lists a range of "core requirements" for said SSI use case. Notably, this includes emphasizing learner agency through consent, flexibility and privacy; preventing tracking by verifying minimal data without involving the issuer; and finally ensuring sustainability with both an energy-efficient infrastructure and open standards to prevent vendor lock-in. As such, these requirements are rather non-functional, but they describe the interface to the system very well, especially when it comes to linking requirements with SSI principles, as done in section 5.4.

When it comes to the Swiss eID project, [2] lists several requirements (on figure 3), which are not specifically named as such, but correspond to a similar spirit as what we unveiled in chapter 5: "user-controlled, reusable, instantly-verifiable, secure, tamper-proof, privacy-preserving and digitally-watermarked".

What is about other use cases of SSI, we can also look at [82], where requirements specific to health applications are identified and described in further detail: "trust, transparency, ease of use, security, rights and access, compliance, added value, efficiency, awareness and patient-centred". As stated in the paper, satisfying these requirements will ease "SSI adoption in healthcare". Notably, the patient-centric approach can be related to the entity-centric concept introduced in subsection 9.1.4, since healthcare is about patient's health in priority.

9.3 Threats to SSI Systems

Threat modeling involves identifying challenges of some system, listing its components and then abstracting the most threats one can think of. This approach has been taken in various papers, with a focus on SSI or wider, and they are presented in this section, according to the different steps of establishing a threat model.

9.3.1 Identifying Possible Weaknesses of SSI

SSI is not perfect, as it faces a number of challenges. For instance, [74] cites two publications identifying technical and non-technical issues, including key storage for distributed ledgers, compatibility with "legacy systems" and immaturity of SSI as opposed to PKI, thus possibly degrading user experience. In the end, it seems that the biggest bottleneck is the user themselves, because their behavior is unpredictable and their trust may be misplaced in entities that are not trustworthy.

More precisely, [59] identifies a series of challenges of SSI that build on top of this idea of "trusted *vs* trustworthy". For instance, the quality of authentication with an eID depends largely on the issuer of the corresponding VC. Additionally, wallets can be a source of confusion, since backups should enable recovery, which leads to the possibility of holding VCs of other people in one's wallets. What is more, this is even expected in the context of delegation, which requires authentication and proper authorization. The last important point that is made in this article is the one of phishing, whereby SSI credentials could be stolen by sharing a proof with the wrong verifier.

At this point, it is hard to tell which challenges can be solved and which cannot, although OIDC seems to provide mitigations to some of them [59]. In any case, there seems to be a large focus on the human trust, which is also corroborated by [104], which provides a critical ethical perspective on SSI that questions the right for digital sovereignty and true decentralization of the web. Of course, this issue is much larger than SSI itself, but it enables attacks and threats that are worth considering.

9.3.2 Modeling Threats on SSI Components

To begin with the threat model, one should start by identifying the different components of the system under analysis. In this spirit, [117] identifies different components of an SSI system, including functionality such as identification and authentication, but also elements like verifiable claims and public storage, which are both essential in the ecosystem for digital credentials. In particular, it displays a graphical representation similar to Figure 6.1 to clarify who does what in an SSI interaction.

Towards modeling threats, one then has to consider various kinds of attacks, as well as decide which of those attacks are actually relevant for the system. In that regard, the white paper on the *Decentralized Privacy-Preserving Proximity Tracing* (DP3T) [108] provides a good overview on how threats can be modeled appropriately. In particular, this document distinguishes different kinds of users of the system: regular user, "tech-savvy user", state-level adversary and so on. While this paper is not related to SSI in any way, it describes different possible user behaviors and it is with this approach in mind that the threatening actors have been modeled in section 6.4.

9.3.3 Threats and Attacks on SSI

Risks associated with the use of SSI depend largely on the identified assets, which goes from the underlying infrastructure through the wallet applications to the user's behavior, exposing a large attack surface. In that context, [21] provides a description of a series of risks related to "processes". For instance, in the process of obtaining a wallet application, the software could be malicious or the installation could wake up some attack on the device it is being run on. Likewise, similar risks are possible while a proof is being shown (*e.g.* with a replay attack), VCs are being issued (*e.g.* when an issuer is not trustworthy), authentication is in progress (*e.g.* through a person-in-the-middle) or there is some interaction with the data registry (*e.g.* by publishing private data without regard for confidentiality). Other than that, there may be functional issues, when parts of the system is unavailable or corrupted, which also prevents users from properly interacting with SSI, which practically limits their data sovereignty, as expressed in [86]. The paper on trust [21] stays very theoretical though and does not give concrete examples where such attacks have happened.

When it comes to performing attacks, [102] reports a set of experiments on the Sovrin network [118] that relies on hyperledger Indy [39]. In particular, security updates have to be applied fast to prevent attacks within the authorized update window. Additionally, the "board of trustees" may not be selected in compliance with international regulations, which could create legal issues. Therefore, different kinds of adversarial behaviors are possible, such as randomized fuzzing, replay/amplification attacks and non-privileged modifications; some of which have been acknowledged and fixed by the Sovrin foundation since [103].

9.4 Distributed Ledger Implementations of SSI Use Cases

As we have settled, a blockchain is a particular kind of distributed ledger. Since SSI use cases are likely to rely on some distributed ledger, blockchains can help implementing them directly. Indeed, the Sovrin white paper [118] goes as far as saying that "the starting point must be a public blockchain", because it can "replace trust in humans with trust in mathematics". However, blockchains are not the only resort for SSI, as [86] expresses very well:

> *Other systems, such as distributed databases or directory services, can also be suitable for implementing the data registry.*

Nevertheless, blockchains have been around for more than a decade, and their use has been documented in a number of publications for the time being. Among other use cases, it has been explored for identity-related applications, both without SSI in a first step, and then with SSI in a second step.

9.4.1 Blockchain without SSI

Since we have focused on the digital diploma use case, it is worth mentioning that experiments had been run on blockchains directly, without the additional SSI "layer". Indeed, [61] describes how one could use blockchain technology to store digital diplomas. More precisely, this paper reports on exploratory research of companies involved in blockchain development, including IBM, Alibaba or Mastercard, and how this technology can be used for storing university diplomas. In the end, it describes functionality similar to SWITCHverify [50] or CERTUS [26], which have been introduced in subsection 4.4.2.

9.4.2 Blockchain with SSI

There is no standard yet when it comes to implementing SSI on a blockchain, but several papers have tackled the idea. For example, [78] has implemented secret sharing on a blockchain using smart contracts, which enables distributed storage without credential disclosure as well as automated recovery in case of a loss.

When it comes to the technical aspect, [62] explores how a blockchain can hold an immutable registry at the bottom-most layer of the SSI stack. In that sense, it discusses how keys can be rotated in DID documents using cryptography and how using instances of hyperledgers such as Besu or Indy prevents incentives "to accept faulty transactions like there is for Blockchain or Ethereum, as no active mining takes place to generate income". As a result, the overall scalability of SSI on a blockchain is considered very good.

Regarding interactions between SSI and its underlying ledger, [72] proposes to set up three *smart contracts* (SCs): an identity SC for storing unique identifiers, a recovery SC to account for losses *via* multi-signature transactions (*cf.* subsection 3.1.2) and a "service" SC which is able to deploy the previous two. The implementation leverages Ethereum directly, by writing SCs in Solidity and estimating transaction fees in terms of Gas expenses. Overall, the authors consider their scheme secure, controllable and portable, unlike other existing system like uPort, ShoCard or Sovrin.

With the idea of estimating fees comes an interesting possibility for VCs that is described in [113]: credentials do not all have the same payment model: "some may be issued and used for free; others may be purchased; still others may incur a fee with every use". In a world where identity can be linked to payment, one could get paid for disclosing information, going to an interview or even just studying at a university.

However, as we have seen, there exist hyperledger projects which were built specifically for identity, *e.g.* Indy. Here, the focus lies primarily on security and privacy concerns instead of the economic model of the ledger. More precisely, [100] proposes to use mitigations against people-in-the-middle attacks and reputation scales for issuers. Most interestingly though, it analyzes so-called *sensitivity scores* for VC attributes, ranging between 0 and 1. For instance, one's name is estimated at a 0.025 sensitivity, while one's social security number is assigned a 1.0 sensitivity. This last example applies mostly to the US though, since this attribute is used virtually everywhere and cannot be changed over one's lifetime, making it particularly sensitive to public disclosure.

More generally, VC data should not be disclosed on a public blockchain, since that would break user sovereignty altogether, even though some information is usually published in newspapers or sent by email in the "analog" world. Indeed, as stated in [86]:

> *ledgers do not generally provide technical means to delete any data once it has been stored, but keeping outdated information is usually unnecessary and requires a large storage capacity*

At the very least, when non-public data has to be recovered, it needs to leverage multi-signature smart contracts, which could wait for, say, two parties out of three. In the Swiss academic world, these three entities could be the student themselves, the issuing university and *e.g.* SWITCH as a trusted third party. This links back to the edu-ID use case that we have demonstrated in this project, and thus closes the overview on related work.

10 Conclusion

"A better labeling of the SSI movement, in our opinion, is 'self-sovereign credentials' (or, to be more accurate, 'self-sovereign verifiable credentials'), but alas, SSI is the entrenched term, and we shall proceed with that nomenclature."
— Mary Lacity and Erran Carmel [15]

In a way, SSI is the most natural way to digitalize our identity. Indeed, there are no copies of physical identity cards lying around in some private company's basement and nobody is notified, even for statistics purposes, when one is showing it for identity checks when checking in to a hotel. Likewise, verifiable credentials enable a truly user-centric approach to the missing identity layer in the internet and beyond. In this report, we have covered the basics of SSI, evaluated some of its main use cases and implemented a proof of concept VC for the educational sector. To conclude, we will look at the four main takeaways of this project:

1. SSI enables a new era for many use cases of digital identity, which makes it difficult to navigate one's way through;
2. Nevertheless, we should target a high ambition level, so as to enable both trust and identity in the new ecosystem;
3. Therefore, the process will take time and adoption will happen on a gradual scale rather from one day to another;
4. Finally, it helps to settle a set of formal requirements in order to clarify what to implement and where to start.

10.1 A New Era for Digital Identity

Digital identity is a long-established concept that loosely follows a set of models. Thus, over the years, we have seen centralized identities, federated identities and user-centric identities, all of which relied on an identity provider which stored information about its users to enable access control. In the new world of self-sovereign identity, this role is taken over by the users themselves, which enables more privacy-friendly data handling, but also comes at the cost of great responsibility. In particular, if all information about a person is stored exclusively on their smartphone or even smartwatch, they are at a high risk of losing access to their data if anything unpredictable happens to their device.

In parallel of this rising consciousness, SSI has become a hot topic in the community of trust and identity, as it is often the case with such paradigm-altering ideas. In fact, countless blog posts, articles and papers have emerged on the internet over the past year alone, and will continue to appear in the foreseeable future. This enthusiasm reflects a very creative process of crafting use cases that could benefit from self-sovereignty over any kinds of data containers.

10.2 A High Ambition Level

Indeed, SSI is not only targeted at identity credentials, but rather at very general verifiable credentials holding structured data about some holder. This raises a number of issues regarding the scope of this new identity model, since some people may not want to redesign the entire public domain of a country (or larger). Nevertheless, the truth is that technically speaking, it is totally possible to implement a large number of information flows *via* SSI in order to give more freedom to the end-users of a service.

With this idea in mind, the Swiss eID project is targeting a high level of ambition, *i.e.* by first focusing on a base identity and then opening the floor to arbitrary VC schemas monitored by anyone willing to participate in the ecosystem. In that sense, SSI use cases will no longer be strictly related to identity, but also enable a country-wide trust domain – and more, thanks to discussions that are taking place with international actors.

10.3 A Gradual Adoption Process

As we have unraveled by trying to implement an educational use case in the form of a demonstration, we are still in the early days of SSI, even though it has been around for a few years already. From the experience we have made, it is clear that it is not ready for production use at a large scale. However, a series of pilot projects have been carried out with the goal of judging how well people interact with the system.

Based on the current situation, it seems that narrow-scoped projects are working well, which sounds promising for future adoption of SSI in a more global setting. But this process will take time, because research is often ahead of reality and even researchers are still figuring out the details of SSI implementations.

10.4 A Clear Set of Requirements

Consequently, this work has identified a set of twelve requirements that enable analyses of use cases, covering both non-functional principles such as privacy or decentralization, as well as functional ones like authenticity or verifiability. After analyzing all these requirements for a use case, one gets a much clearer picture of how the situation looks in SSI's perspective. Henceforth, these requirements provide a good basis to find out what to do in an SSI ecosystem and, more importantly, when to start doing it.

In particular, regarding the three use cases that we selected for a deeper assessment, it is fully justified to start with an eID provided by the state as a starting point. After that, it would be appropriate to integrate sector-specific identities such as an edu-ID, which provide access to more siloed services. Finally, other use cases such as the one of digital diplomas would fit nicely in an existing ecosystem of interoperable trust, because they would enhance user experience in their everyday life. And, in the end, helping our fellow humans is a common objective for all of us.

Figures

Listings

Tables

Bibliography

[1] Claudio Allocchio, Bartłomiej Idzikowski, Yehuda Afek, Mihály Héder, Andrea Detti, Giulio Sidoretti, Pierpaolo Loreti, Renato Lo Cigno, Lorenzo Ghiro, Aiden Valentine, Jurjen Braakhekke, Michiel Schok, Victoriano Giralt, David Groep, Emanuele Raso, George Parisis, Ludovico Funari, János Mohácsi, and Guido Aben. ***GÉANT Innovation Programme 2021 - showcase***. GÉANT, 2022. URL: https://wiki.geant.org/pages/viewpage.action?pageId=408715377.

[2] Vitus Ammann, Graeme Entwistle, Christoph Graf, Raffael Knecht, Marius Matter, Frank Michaud, Stéphane Mingot, Tim Weingärtner, Reinhard Riedl, Andreas Schneider, and Jan Friedli. ***Building a Swiss Digital Trust Ecosystem***. Digital Switzerland, 2022. URL: https://digitalswitzerland.com/wp-content/uploads/2020/04/Building-a-Swiss-Digital-Trust-Ecosystem_digitalswitzerland_April2022_vF.pdf.

[3] Stephen Curran, Hakan Yaldiz, Sam Curran, and Victor Martinez Jurado. ***AnonCreds Specification***. AnonCreds WG, 2022. URL: https://anoncreds-wg.github.io/anoncreds-spec/.

[4] Sam Curren, Tobias Looker, and Oliver Terbu. ***DIDComm Messaging***. DIF, 2022. URL: https://identity.foundation/didcomm-messaging/spec/.

[5] EPFL. ***GASPAR***. 2022. URL: https://gaspar.epfl.ch.

[6] Hyperledger Foundation. ***Hyperledger Aries Cloud Agent - Python***. GitHub, 2022. URL: https://github.com/hyperledger/aries-cloudagent-python.

[7] Frédéric Gerber. ***SSI for Future-Proof Digital Wallets***. GÉANT, 2022. URL: https://indico.geant.org/event/1/contributions/67/attachments/12/98/final_slides.pdf.

[8] Christoph Graf. ***A secure path to the new E-ID***. SWITCH, 2022. URL: https://www.switch.ch/stories/a-secure-path-to-the-new-E-ID/.

[9] Lukas Hämmerle. ***700'000 reasons to celebrate***. SWITCH Identity Blog, 2022. URL: https://identityblog.switch.ch/2022/06/07/700000-reasons-to-celebrate/.

[10] Lukas Hämmerle. ***The life of an edu-ID account***. SWITCH Identity Blog, 2022. URL: https://identityblog.switch.ch/2022/02/02/the-life-of-an-edu-id-account/.

[11] Patrick Herbke. ***ELMO2EDS***. GitHub, 2022. URL: https://github.com/TUB-SSI-Edu/ELMO2EDS.

[12] Federal Office of Justice. ***Consultation relative à la loi sur l'e-ID***. Swiss Confederation, 2022. URL: https://www.eid.admin.ch/eid/fr/home/e-id-gesetz/vernehmlassung.html.

[13] Gerd Kortemeyer. ***Next Generation Education Ecosystem (maybe)***. ETH Zürich, 2022. URL: https://www.eduhub.ch/export/sites/default/files/EduHubWebinar.pdf.

[14] Gerd Kortemeyer. ***Self-Sovereign Identity User Scenarios in the Educational Domain***. EDUCAUSE, 2022. URL: https://er.educause.edu/articles/2022/4/self-sovereign-identity-user-scenarios-in-the-educational-domain.

[15] Mary Lacity and Erran Carmel. ***Implementing Self-Sovereign Identity (SSI) for a digital staff passport at UK NHS***. University of Arkansas, 2022. URL: https://cpb-us-e1.wpmucdn.com/wordpressua.uark.edu/dist/5/444/files/2018/01/BCoE2022SS1FINAL.pdf.

[16] Maxine Lemm, Veronica Gaffey, Natalia Aristimuno Perez, Perrine de Coetlogon, Pierre Marro, João Frade, Saky Kourtidis, Daniel Du Seuil, Lluís Alfons, José-Manuel Panizo, Andrea Servida, Koen Nomden, Katrien Vanelven, Sebastiano Toffaletti, and Marc Tarverner. ***EBSI Demo Day***. European Commission, 2022. URL: https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/464979566/EBSI_Demo_Day.pdf?api=v2.

[17] Michael Lodder and Daniel Hardman. ***Sovrin DID Method Specification***. Draft. W3C, 2022. URL: https://sovrin-foundation.github.io/sovrin/spec/did-method-spec-template.html.

[18] Stéphane Mingot. ***Exploring the potential of Self-Sovereign Identity with representative use cases***. Adnovum, 2022. URL: https://www.adnovum.com/blog/exploring-the-potential-of-self-sovereign-identity-with-representative-use-cases.

[19] Monique J. Morrow. ***Making the Case for New Generation Identity Internet***. syniverse, 2022. URL: https://indico.geant.org/event/1/contributions/64/attachments/107/232/Monique%20Morrow%20Internet%20Of%20Trust%20Identity%20Keynote.pptx.

[20] Robert Ott and Frédéric Gerber. ***SSI Sandbox***. GitLab SWITCH, 2022. URL: https://gitlab.switch.ch/blockchain/ssi-sandbox.

[21] Nick Pope, Michał Tabor, Iñigo Barreira, Nicholas Dunham, Franziska Granc, Christoph Thiel, and Arno Fiedler. ***Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust***. European Union Agency for Cybersecurity, 2022. URL: https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust/@@download/fullReport.

[22] Haseeb Qureshi. ***Blockchains are cities***. Medium, 2022. URL: https://medium.com/dragonfly-research/blockchains-are-cities-564327013f86.

[23] Wojtek Rygielski, Matija Puzar, Mirko Stanic, and Richard Borge. ***The ELMO XML format***. EMREX, 2022. URL: https://github.com/emrex-eu/elmo-schemas.

[24] SWITCH. ***SWITCH edu-ID***. 2022. URL: https://www.switch.ch/edu-id/.

[25] SWITCH. ***SWITCHaai***. 2022. URL: https://www.switch.ch/aai/.

[26] ***CERTUS***. SICPA, 2022. URL: https://www.sicpa.com/solutions/digital-and-printed-documents-certification.

[27] ***Clarke's three laws***. Wikipedia, 2022. URL: https://en.wikipedia.org/wiki/Clarke%27s_three_laws.

[28] ***Diploma Verification***. EPFL, 2022. URL: https://www.epfl.ch/education/studies/en/diploma-verification/.

[29] ***Discover EBSI's USE CASES***. European Commission, 2022. URL: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Use+cases.

[30] ***Distributed Ledger***. Wikipedia, 2022. URL: https://en.wikipedia.org/wiki/Distributed_ledger.

[31] ***DRAGONFLY Mainnet***. Hexapods, 2022. URL: https://dragonfly.switch.ch/dashboard.

[32] ***eIDAS Regulation***. European Commission, 2022. URL: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

[33] ***Enhancing check-in using the COVID-19 NHS Digital Staff Passport***. NHS, 2022. URL: https://beta.staffpassports.nhs.uk/downloads/Case_Study_East_Lancs_VC.pdf.

[34] ***Foire aux questions numéro AVS pour particuliers***. 1.5F. Département fédéral des finances, 2022. URL: https://www.zas.admin.ch/dam/zas/fr/dokumente/Particuliers/FAQ%20Num%C3%A9ro%20AVS%20Particuliers%20-v1.3-fr.pdf.download.pdf/FAQ%20Num%C3%A9ro%20AVS%20Particuliers%20-v1.3-fr.pdf.

[35] ***Getting Started: Setting up an edu-ID Service***. SWITCH, 2022. URL: https://www.switch.ch/edu-id/docs/services/start/.

[36] ***How to Prepare Your Data | European Digital Credentials for Learning***. European Union, 2022. URL: https://europa.eu/europass/en/preparing-credentials-european-digital-credentials-learning.

[37] ***Hyperledger Aries***. Hyperledger Foundation, 2022. URL: https://www.hyperledger.org/use/aries.

[38] ***Hyperledger Besu***. Hyperledger Foundation, 2022. URL: https://besu.hyperledger.org.

[39] ***Hyperledger Indy***. Hyperledger Foundation, 2022. URL: https://www.hyperledger.org/use/hyperledger-indy.

[40] ***JSON for Linking Data***. JSON-LD, 2022. URL: https://json-ld.org/.

[41] ***Loi fédérale sur l'identité électronique et autres moyens de preuve électroniques***. Avant-projet. Swiss Confederation, 2022. URL: https://www.bj.admin.ch/dam/bj/fr/data/staat/gesetzgebung/staatliche-e-id/vorentw.pdf.

[42] ***Managing the life cycle of a car with blockchain technology***. cardossier, 2022. URL: https://cardossier.ch/.

[43] ***MANTIS Testnet***. Hexapods, 2022. URL: https://mantis.switch.ch/dashboard.

[44] ***Merkle tree***. Wikipedia, 2022. URL: https://en.wikipedia.org/wiki/Merkle_tree.

[45] ***My health information available online***. EPR – Electronic Patient Record, 2022. URL: https://www.patientrecord.ch/.

[46] ***Scopes and Claims***. SWITCH, 2022. URL: https://www.switch.ch/edu-id/docs/services/openid-connect/scopes/.

[47] ***SSI Essentials: Zero Knowledge Proof (ZKP) and Selective Disclosure, till death do us part?*** GATACA, 2022. URL: https://gataca.io/blog/ssi-essentials-which-selective-disclosure-protocol-will-succeed.

[48] ***SWITCH edu-ID Help***. SWITCH, 2022. URL: https://help.switch.ch/eduid/faqs/?lang=en.

[49] ***SWITCH edu-ID Participants***. SWITCH, 2022. URL: https://www.switch.ch/edu-id/about/participants/.

[50] ***SWITCHverify***. SWITCH, 2022. URL: https://www.switch.ch/verify/.

[51] ***The GA Travelcard for the whole family***. SBB CFF FFS, 2022. URL: https://www.sbb.ch/en/travelcards-and-tickets/railpasses/ga/families.html.

[52] ***Verifiable Diploma Schema***. EBSI Documentation, 2022. URL: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Verifiable+Diploma+Schema.

[53] ***What is EBSI?*** European Commission, 2022. URL: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi.

[54] TRID Team. ***Trust & Identity Meeting 2022***. SWITCH, 2022. URL: https://www.switch.ch/export/sites/default/edu-id/.galleries-orig/files/TRID_WG_2022.pdf.

[55] Marcel Waldvogel. ***Hitchhiker's Guide to the Blockchain***. Netfuture, 2022. URL: https://netfuture.ch/2022/04/hitchhikers-guide-to-the-blockchain.

[56] Jule Ziegler, Michael Schmidt, Niels van Dijk, Martin van Es, Lucie Kurečková, and Branko Marović. ***T&I Incubator Demo***. GÉANT, 2022. URL: https://events.geant.org/event/1202/.

[57] Lluís Arino. ***EBSI, Diploma Use Case and EMREX: Enabling a new paradigm for education in Europe while aligning efforts***. EMREX Meeting, 2021. URL: https://emrex.eu/wp-content/uploads/2021/12/EBSI-Diploma-Use-Case-and-EMREX-Llu%C3%ADs-Arino-Universitat-Rovira-i-Virgili.pdf.

[58] Guido Bacharach, Matthias Gottlieb, Jan Joost Norder, Hans Pongratz, Ramona-Denisa Steiper, Wolfgang Radenbach, Hermann Strack, and Arn Waßmann. ***Progress on Digitization of Higher Education Processes towards Standards EU & DE : status 1 Introduction and future perspectives***. 2021. URL: https://pim-plattform.de/wordpress/wp-content/uploads/2021/07/FINDE-03-EUNIS2021-full-2205.pdf.

[59] Damien Bod. ***Challenges to Self Sovereign Identity***. Software Engineering, 2021. URL: https://damienbod.com/2021/10/11/challenges-to-self-sovereign-identity/.

[60] Edouard Bugnion, Imad Aad, and Patrick Schaller. ***Swiss E-ID Privacy aspects***. EPFL, 2021.

[61] Alexandra Cernian, Elena Vlasceanu, Bogdan Tiganoaia, and Alin Iftemi. ***Deploying blockchain technology for storing digital diplomas***. 2021. URL: https://ieeexplore.ieee.org/document/9481034.

[62] Niels van Dijk, Bart Kerver, Harry Kodden, and Michiel Uitdehaag. ***Technical exploration Ledger-based Self Sovereign Identity***. SURF, 2021. URL: https://www.surf.nl/files/2021-05/technical-exploration-surf-ledger-based-self-sovereign-identity.pdf.

[63] Bahya Nassr Eddine, Aafaf Ouaddah, and Abdellatif Mezrioui. ***Exploring blockchain-based Self Sovereign Identity Systems: challenges and comparative analysis***. IEEE, 2021. URL: https://ieeexplore.ieee.org/document/9569821.

[64] gittaca. ***German ID Wallet app stopped after 1 day of public availability***. 2021. URL: https://github.com/molly/web3-is-going-great/issues/14.

[65] Christoph Graf. ***E-ID based on SSI – Needs for regulatory support***. DIDAS, 2021. URL: https://www.didas.swiss/2021/12/21/e-id-based-on-ssi-needs-for-regulatory-support/.

[66] Christoph Graf and Marco Dütsch. ***Diskussionspapier zum «Zielbild E-ID» - Stellungnahme SWITCH***. SWITCH, 2021. URL: https://identityblog.switch.ch/wp-content/uploads/2021/10/Stellungnahme-SWITCH-Zielbild-E-ID-final_sig.pdf.

[67] Christian Heimann. ***Discussion paper on the target vision for an e-ID***. Federal Office of Justice FOJ, 2021. URL: https://www.bj.admin.ch/dam/bj/en/data/staat/gesetzgebung/staatliche-e-id/diskussionspapier-zielbild-e-id.pdf.download.pdf/diskussionspapier-zielbild-e-id.pdf.

[68] Federal Office of Justice. ***Décision de principe du Conseil fédéral sur l'e-ID***. Swiss Confederation, 2021. URL: https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-86465.html.

[69] Gerd Kortemeyer. ***For lifelong learning to work, students must own their educational data***. Times Higher Education, 2021. URL: https://www.timeshighereducation.com/blog/lifelong-learning-work-students-must-own-their-educational-data.

[70] James F. Kurose and Keith W. Ross. ***Computer Networking – A Top-Down Approach***. Ed. by 2017. 7th ed. Pearson, 2021. URL: https://epfl.swisscovery.slsp.ch/discovery/fulldisplay?docid=alma9911670647310551 6&context=L&vid=41SLSP_EPF:prod&lang=fr&search_scope=DN_and_CI&adaptor=Local%20Search%20Engine&tab=41SLSP_EPF_DN_CI&query=any,contains,computer%20networking%20a%20top%20down%20approach&offset=0.

[71] Anthony Lusard, Arnaud Le Hors, Arun SM, Bobbi Muscara, Csilla Zsigri, David Bowswell, Hart Montgomery, Helen Garneau, Tracy Kuhrt, and Travin Keith. ***An Overview of Hyperledger Foundation***. Hyperledger Foundation, 2021. URL: https://www.hyperledger.org/wp-content/uploads/2021/11/HL_Paper_HyperledgerOverview_102721.pdf.

[72] Jianlin Niu and Zhiyu Ren. ***A self-sovereign identity management scheme using smart contracts***. 2021. URL: https://www.researchgate.net/publication/349317330_A_self-sovereign_identity_management_scheme_using_smart_contracts/fulltext/602e68864585158939b31d3f/A-self-sovereign-identity-management-scheme-using-smart-contracts.pdf?origin=publication_detail.

[73] Mathias Payer. ***Software Security: Principles, Policies, and Protection***. 0.37. HexHive Books, 2021. URL: https://nebelwelt.net/SS3P/.

[74] Daniela Pöhn, Michael Grabatin, and Wolfgang Hommel. ***eID and Self-Sovereign Identity Usage: An Overview***. MDPI, 2021. URL: https://mdpi-res.com/d_attachment/electronics/electronics-10-02811/article_deploy/electronics-10-02811-v2.pdf?version=1637131340.

[75] Alex Preukschat and Drummond Reed. ***Self-Sovereign Identity: Decentralized digital identity and verifiable credentials***. 9781617296598. Simon & Schuster, 2021.

[76] Chris Raczkowski, Drummond Reed, and Sankarshan Mukhopadhyay. ***Principles of SSI***. Trust over IP (ToIP) Foundation, 2021. URL: https://trustoverip.org/wp-content/uploads/2021/10/ToIP-Principles-of-SSI.pdf.

[77] Timothy Ruff. ***Verifiable Credentials Aren't Credentials. And They're Not Verifiable In the Way You Might Think.*** Credential Master, 2021. URL: https://credentialmaster.com/verifiable-credentials-arent-credentials-theyre-containers/.

[78] Efat Samir, Hongyi Wu, Mohamed Azab, Chunsheng Xin, and Qiao Zhang. ***DT-SSIM: A Decentralized Trustworthy Self-Sovereign Identity Management Framework***. IEEE, 2021. URL: https://ieeexplore.ieee.org/document/9536956.

[79] Jacopo Sesana. ***Daily life with the Self-Sovereign Identity (Part 2)***. selfsovereignidentity.it, 2021. URL: https://www.selfsovereignidentity.it/daily-life-with-the-self-sovereign-identity-part-2/.

[80] Jacopo Sesana. ***Introduction to Self-Sovereign Identity and eIDAS (part 1)***. selfsovereignidentity.it, 2021. URL: https://www.selfsovereignidentity.it/self-sovereign-identity-and-eidas-part-1/.

[81] Jacopo Sesana. ***Introduction to Self-Sovereign Identity and eIDAS (part 2)***. selfsovereignidentity.it, 2021. URL: https://www.selfsovereignidentity.it/self-sovereign-identity-and-eidas-part-2/.

[82] Mohammed Shuaib, Shadab Alam, Mohammad Shabbir Alam, and Mohammad Shahnawaz Nasir. ***Self-sovereign identity for healthcare using blockchain***. ELSEVIER, 2021. URL: https://www.researchgate.net/profile/Mohammed-Shuaib/publication/350441465_Self-sovereign_identity_for_healthcare_using_blockchain/links/6115ec46169a1a0103f9578f/Self-sovereign-identity-for-healthcare-using-blockchain.pdf.

[83] Mohammed Shuaib, Shadab Alam, Mohammad Shahnawaz Nasir, and Mohammad Shabbir Alam. ***Immunity credentials using self-sovereign identity for combating COVID-19 pandemic***. ELSEVIER, 2021. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7983450/pdf/main.pdf.

[84] Jordan Singh. ***Benefits and use cases of SSI***. Condatis, 2021. URL: https://condatis.com/news/blog/benefits-and-use-cases-of-ssi/.

[85] Orie Steele, Manu Sporny, and Michael Prorock. ***DID Specification Registries***. W3C, 2021. URL: https://www.w3.org/TR/did-spec-registries/.

[86] ***A Brief Guideline on Self-Sovereign Identities (SSI) with special regard to the distributed ledger technology (DLT)***. Federal Office for Information Security, 2021. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/guideline_self-sovereign_identities.pdf?__blob=publicationFile&v=2.

[87] ***Brieftasche für Digitale Identitäten***. ID Wallet, 2021. URL: https://digital-enabling.eu/.

[88] ***Build a PoC with Affinidi in One Evening – Driving License as a Verifiable Credential***. Affindi, 2021. URL: https://academy.affinidi.com/how-to-implement-driving-license-use-case-using-verifiable-credentials-cef928222c92.

[89] ***Commission Implementing Decision (EU) 2021/1073 of 28 June 2021 laying down technical specifications and rules for the implementation of the trust framework for the EU Digital COVID Certificate established by Regulation (EU) 2021/953 of the European Parliament and of the Council (Text with EEA relevance)***. Official Journal of the European Union, 2021. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D1073&from=EN.

[90] ***Identity Theft and Your Social Security Number***. Social Security Administration, 2021. URL: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[91] ***Nachweise für die digitale Brieftasche***. Die Bundesregierung, 2021. URL: https://www.bundesregierung.de/breg-de/suche/e-id-1962112.

[92] ***Pilot hotel check-in project successfully launched***. Die Bundesregierung, 2021. URL: https://www.bundesregierung.de/breg-en/news/hotel-check-in-pilot-project-launched-1914992.

[93] ***SSI Essentials: Everything you need to know about Decentralized Identity***. GATACA, 2021. URL: https://gataca.io/blog/ssi-essentials-everything-you-need-to-know-about-decentralized-identity.

[94] ***Student eID Framework***. European Campus Card Association, 2021. URL: https://eidproject.eu/download/QlcHJlK2s2JC42FSxKWl5hRnItZVUnGhQGGTAwLi1-YGs6ciRsfy0qGzoSei8RC3JEaDx4VXldBwgMMTAuLX5gazhyJGx8OjcHNhJrUkJNNgwlYT1VeV0HCB88TX1rOjMlbiNUYXovKR4-FVJfJxojGzh8FVgmERIIBzsBByw_OSglNX1sI30jGDMULEpaCiUMJX8sFjsgBB0eMAopPQM_IG8PbjxuMiAGMANlLwgdPw4lfCgbChEYHw45DSI7A2h5OWEmPms5Z119HW8eH01qXC9hawo/european_student_eid_framework_proposal_november_2021.pdf.

[95] ***Thousands of fake Covid-19 certificates uncovered in Switzerland***. swissinfo.ch, 2021. URL: https://www.swissinfo.ch/eng/thousands-of-fake-covid-19-certificates-uncovered-in-switzerland/47214700.

[96] ***Verifiable credentials***. Wikipedia, 2021. URL: https://en.wikipedia.org/wiki/Verifiable_credentials.

[97] ***ZertES***. Wikipedia, 2021. URL: https://en.wikipedia.org/wiki/ZertES.

[98] Roman Zoun. ***Self-Sovereign Identity – a game changer regarding privacy***. 2021. URL: https://www.adnovum.com/blog/self-sovereign-identity-a-game-changer-regarding-privacy.

[99] Rafael Belchior, Benedikt Putz, Günther Pernul, and Miguel Correia. ***SSIBAC: Self-Sovereign Identity Based Access Control***. ResearchGate, 2020. URL: https://www.researchgate.net/profile/Miguel-Correia-13/publication/350453579_SSIBAC_Self-Sovereign_Identity_Based_Access_Control/links/6066dfe9299bf1252e21584a/SSIBAC-Self-Sovereign-Identity-Based-Access-Control.pdf?origin=publication_detail.

[100] Manas Pratim Bhattacharya, Pavol Zavarsky, and Sergey Butakov. ***Enhancing the Security and Privacy of Self-Sovereign Identities on Hyperledger Indy Blockchain***. 2020. URL: https://ieeexplore.ieee.org/document/9297357.

[101] James Chartrand, Stuart Freeman, Ulrich Gallersdörfer, Matt Lisle, Alexander Mühle, and Sélinde van Engelenburg. ***Building the digital credential infrastructure for the future***. The Digital Credentials Consortium, 2020. URL: https://www.researchgate.net/profile/Brian-Subirana-2/publication/342804022_Building_the_digital_credential_infrastructure_for_the_future_About_the_Digital_Credentials_Consortium_Founding_Members/links/5f06e90fa6fdcc4ca459ae1d/Building-the-digital-credential-infrastructure-for-the-future-About-the-Digital-Credentials-Consortium-Founding-Members.pdf?origin=publication_detail.

[102] Alexandre Délèze. ***Hacking Sovereign Identity***. EPFL DEDIS, 2020. URL: https://www.epfl.ch/labs/dedis/wp-content/uploads/2020/09/report-2020-1-Alexandre-Deleze-hacking_sovereign_identity.pdf.

[103] Alexandre Délèze. ***Updating a DID with a nym transaction will be written to the ledger if neither ROLE or VERKEY are being changed, regardless of sender***. GitHub, 2020. URL: https://github.com/hyperledger/indy-node/security/advisories/GHSA-wh2w-39f4-rpv2.

[104] Georgy Ishmaev. ***Sovereignty, privacy, and ethics in blockchain-based identity management systems***. Springer, 2020. URL: https://link.springer.com/content/pdf/10.1007/s10676-020-09563-x.pdf.

[105] Annett Laube and Gerhard Hassenstein. ***Self-Sovereign Identities***. 1.0. Bern University of Applied Sciences, 2020. URL: https://www.switch.ch/export/sites/default/about/innovation/.galleries/files/SWITCHInnovationLab_IDAS.pdf.

[106] ***European Blockchain Service Infrastructure: a new Building block, but not just another Building Block***. European Commission, 2020. URL: https://eidproject.eu/download/Uvbmx7NXUoOjAoCzJUREB-VGAze0s5BAoYBy4uMDNgfnUmbDpyYTM0BSQMZDEPFWxadiJmS2dDGRYSLy4wM2B-dSZsOnJiJCkZKAx1TFxTKBI7fyNLZ0MZFgEiU2N1JC07cD1Kf2QxNwAgC0xBOQQ9BSZiC0Y4DwwWGSUfGTIhJzY7K2NyPWM9Bi0KMlREEyIPN3o0ASoIBygUJBUGMys0O3ojdyNONCgKHgxxHQMuYz84fSIaFAAFERokAgY2MC04SiN3ImUvBF1xXiFeVS5gEDB3dUVpDQgZEmhLezIsZio/blockchain_and_diplomas_use_case_-_llus_alfons_ario_martn_201103_.pdf.

[107] ***NHS Staff completing a temporary move***. NHS, 2020. URL: https://beta.staffpassports.nhs.uk/staff/.

[108] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, Ludovic Barman, Sylvain Chatel, Kenneth Paterson, Srdjan Čapkun, David Basin, Jan Beutel, Dennis Jackson, Marc Roeschlin, Patrick Leu, Bart Preneel, Nigel Smart, Aysajan Abidin, Seda Gürses, Michael Veale, Cas Cremers, Michael Backes, Nils Ole Tippenhauer, Reuben Binns, Ciro Cattuto, Alain Barrat, Dario Fiore, Manuel Barbosa, Rui Oliveira, and José Pereira. ***Decentralized Privacy-Preserving Proximity Tracing***. EPFL, 2020. URL: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.

[109] eIDAS. ***Building trusted digital identity***. European Union, 2019. URL: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=61682.

[110] Otto C. Frommelt. ***Mobility in the Blockchain Series: Click & Drive***. Vol. Part 2. LinkedIn, 2019. URL: https://www.linkedin.com/pulse/frommelt-mobility-blockchain-series-click-drive-part-frommelt-1c/.

[111] Renato Furter. ***"But on <insert favourite service> I get <insert favourite feature> for free!"*** GÉANT, 2019. URL: https://www.youtube.com/watch?v=caYdoM4670o.

[112] Remo Glauser. ***Self-Sovereign Identities in Cardossier***. ETHZ DISCO, 2019. URL: https://pub.tik.ee.ethz.ch/students/2018-HS/MA-2018-34.pdf.

[113] Daniel Hardman. ***Categorizing Verifiable Credentials***. Evernym, 2019. URL: https://www.evernym.com/blog/categorizing-verifiable-credentials/.

[114] ***E-voting: current situation in Switzerland?*** ch.ch, 2019. URL: https://www.ch.ch/en/votes-and-elections/e-voting/.

[115] ***Estonia – GovChain***. GovChain, 2019. URL: https://govchain.world/estonia/.

[116] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco, and Jason Yellick. ***Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains***. EuroSys, 2018. URL: https://dl.acm.org/doi/pdf/10.1145/3190508.3190538.

[117] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. ***A survey on essential components of a self-sovereign identity***. SWITCH, 2018. URL: https://www.sciencedirect.com/science/article/abs/pii/S1574013718301217.

[118] Phil Windley and Drummond Reed. ***Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust***. The Sovrin Foundation, 2018. URL: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf.

[119] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. ***Blockchain Technology Overview***. NIST, 2018. URL: https://doi.org/10.6028/NIST.IR.8202.

[120] Andrew Tobin and Drummond Reed. ***The Inevitable Rise of Self-Sovereign Identity***. 2.0. The Sovrin Foundation, 2017. URL: https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

[121] Christopher Allen. ***The Path to Self-Sovereign Identity***. 1.0. Life With Alacrity, 2016. URL: https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

[122] Mike Hearn. ***Corda: A distributed ledger***. 0.5. corda, 2016. URL: https://www.corda.net/wp-content/uploads/2021/11/corda-technical-whitepaper.pdf.

[123] ***General Data Protection Regulation***. Official Journal of the European Union, 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[124] Roger Wattenhofer. ***The Science of the Blockchain***. 2016. URL: https://epfl.swisscovery.slsp.ch/discovery/fulldisplay?docid=alma9901059285702055 16&context=L&vid=41SLSP_EPF:prod&lang=fr&search_scope=DN_and_CI&adaptor=Local%20Search%20Engine&tab=41SLSP_EPF_DN_CI&query=any,contains,the%20science%20of%20blockchain&offset=0.

[125] Maximilian J Hartel, Lukas P Staub, Christoph Röder, and Stefan Eggli. ***High incidence of medication documentation errors in a Swiss university hospital due to the handwritten prescription process***. BMC Health Services Research, 2011. URL: https://bmchealthservres.biomedcentral.com/track/pdf/10.1186/1472-6963-11-199.pdf.

[126] Satoshi Nakamoto. ***Bitcoin: A Peer-to-Peer Electronic Cash System***. 2008. URL: https://bitcoin.org/bitcoin.pdf.

A Glossary

Abbreviation	Description	Context	Page
ACA-Py	Hyperledger **A**ries **C**loud **A**gent – **Py**thon		66
API	**A**pplication **P**rogramming **I**nterface		66
ATAD	**A**merican **T**ransfer **A**rticulation **D**atabase		35
CLI	**C**ommand-**L**ine **I**nterface		25
DID	**D**ecentralized **Id**entifier		15
DLT	**D**istributed **L**edger **T**echnology		21
DDoS	**D**istributed **D**enial-**o**f-**S**ervice		48
DP3T	**D**ecentralized **P**rivacy-**P**reserving **P**roximity **T**racing		77
DSP	**D**igital **S**taff **P**assport		28
EBSI	**E**uropean **B**lockchain **S**ervice **I**nfrastructure		26
eGov	**E**lectronic **Gov**ernment		26
eID	**E**lectronic **Id**entity		32
eIDAS	**E**lectronic **Id**entity, **A**uthentication and **S**ignature		32
EPR	**E**lectronic **P**atient, **R**ecord		60
ESSIF	**E**uropean **S**elf-**S**overeign **I**dentity **F**ramework		35
EU	**E**uropean **U**nion		32
Fedpol	**Fed**eral **Pol**ice		51
FINMA	**Fin**anz**ma**rktaufsicht		32
FOJ	**F**ederal **O**ffice of **J**ustice		32
FOSS	**F**ree and **O**pen-**S**ource **S**oftware		48
GA	**G**eneral **A**bonnement	Swiss public transportation	31
GA	**G**overnance **A**uthority	SSI role	46
GDPR	**G**eneral **D**ata **P**rotection **R**egulation		19
IAM	**I**dentity **A**ccess **M**anagement		74
IdP	**Id**entity **P**rovider		9
JWT	**J**SON **W**eb **T**oken		16
KYC	**K**now **Y**our **C**ustomer		32
LD	**L**inked **D**ata		16
L1	**L**ayer **1** Blockchain		24
L2	**L**ayer **2** Blockchain		24
NHS	**N**ational **H**ealth **S**ervice		28
NREN	**N**ational **R**esearch and **E**ducation **N**etwork		58

Table A.1: List of Abbreviations (1/2)

Abbreviation	Description	Context	Page
OIDC	**O**pen**ID** **C**onnect		12
PII	**P**ersonally **I**dentifiable **I**nformation		8
PKI	**P**ublic **K**ey **I**nfrastructure		33
PoA	**P**roof-**o**f-**A**uthority		24
PoC	**P**roof **o**f **C**oncept		62
PoS	**P**roof-**o**f-**S**take		24
PoW	**P**roof-**o**f-**W**ork		24
PPID	**P**airwise **P**seudonymous **Id**entifier		64
SAML	**S**ecurity **A**ssertion **M**arkup **L**anguage		12
SC	**S**mart **C**ontract		79
SSI	**S**elf-**S**overeign **I**dentity		12
SSIBAC	**SSI**-**B**ased **A**ccess **C**ontrol		74
SSN	**S**ocial **S**ecurity **N**umber		51
SSO	**S**ingle **S**ign **O**n		37
TaaS	**T**ransformation **a**s **a** **S**ervice		30
UK	**U**nited **K**ingdom		28
US	**U**nited **S**tates		35
VC	**V**erifiable **C**redential		16
VM	**V**irtual **M**achine		65
VDS	**V**erifiable **D**iploma **S**chema		55
W3C	**W**orld **W**ide **W**eb **C**onsortium		35
ZKP	**Z**ero-**K**nowledge **P**roof		16

Table A.2: List of Abbreviations (2/2)

B SSI Matrix

Requirements	ID Wallet	Digital Staff Passport (DSP)	Immunity Certificates	Medical Prescriptions	Employment Status	Public Transportation Tickets
Privacy-Preserving	✔	✔	✔	But keep in mind that pharmacy employees will learn information (unless it's all automated). But this may be okay due to human trust.	One needs to pay attention that the wrong people don't learn (un)employment information.	You don't want anyone to learn where you went and when.
Selectively Disclosable	✔	It is probably better in the interest of patients that as much information as possible about the capabilities of a hospital staff member be known to their employer. However, PII should absolutely be kept confidential.	✔	✔	You want to disclose whether you are employed and possibly the name of the employer.	Depending on whether people are checking for statistics or for your right to be there, you might want to disclose different information.
Cross-Sector	Not yet, but crossing sector borders is envisioned.	The use case could leverage better internal communication instead of relying on SSI; check out whether it is multi-issuer instead.	✔	One could leverage internal communication between the doctor and the pharmacy. However, this may become a mess (as it has with online consultations during COVID), so it should be okay if it is multi-issuer. Otherwise, it may become relevant again when SSI is better established.	This depends a bit on how such a credential would be used.	The use case remains within the sector of mobility, which does not really suit SSI perfectly. In the multi-issuer requirements, things look blurry as well.
Multi-Issuer	✔	✔	✔	✔	✔	I'm thinking about the case where proxies can issue tickets on behalf of the company (and of course inform it).
Distributed Authority	✔	Since the use case is contained in the health sector, it probably only involves authorities from there. If we wanted to adopt this use case elsewhere, compatibility issues could occur. So it would probably be beneficial to involve other stakeholders in the search for interoperability.	✔	✔	This holds especially when different sectors work together.	✔
High Volume	✔	✔	Now that the COVID situation is hopefully over, we won't need them as much, but it could be useful for other proofs of vaccination when traveling.	✔	✔	✔
Authorization-Granting	✔	✔	✔	✔	This could be linked with a use case where one gets unemployment allocations.	✔
Time-Limited	For driving license, not necessarily; for hotel check-in and eID yes.	They may, but I'm not sure it's good if someone can't perform a surgery just because of an expired credential; maybe some common sense is needed.	✔	✔	I think it's better if this kind of credential needs not be renewed periodically, it should use revocation.	✔
Revocable	Again, it depends on the credential.	✔	✔	Probably not the case now, but could trigger positive change: if a doctor realizes soon enough they made a mistake, they could revoke the prescription.	✔	If the person has asked for a refund of the ticket, then it should no longer be valid.
User-Centric	✔	✔	✔	✔	✔	✔
Human Trust	✔	The use case does not really exist without SSI, which is a good reason for introducing it.	If we ignore the fact that restaurants don't usually have access control, then yes...	✔	Depending on the exact use of such a proof, it should involve known actors only.	✔
Identity-Specific	✔	Your professional activity doesn't define your identity, but we're getting philosophical here. Though, a future eID can be linked to this DSP, which enables more use cases such as opening a bank account.	Unless one uses a zero-knowledge proof which doesn't disclose their identity.	SSI may be out of scope for now, since its main goal is to provide a digital identity. It could be interesting to come back once SSI is more established, to link other use cases to existing ones.	Just like what we said about hospital employees, this does not directly link back to identity checking. Come back once SSI is more established, to link other use cases to existing ones.	Such tickets/subscriptions are usually non-transferrable. And even if they are, the possibility of checking one's identity should be there, regardless of any credential like a picture (as it is currently done).
Takeaways	In principle good use case, but needs to be developed and tested thoroughly before being released out there.	I would have waited before implementing this use case until SSI become more widespread. The risk now is that the use case somehow becomes deprecated, but due to the emergency of the COVID situation, it came at the right time.	This use case would have matched with these SSI requirements well, but it happened a tad too early, so we still used physical ID cards. But we now have experience with immunity certificates, which can serve as a basis for experimentation.	This looks like a promising use case once SSI has established itself. For now, it is probably too broad and would require too many actors to test soon. Also, since real people's health is at stake, it's better not to risk problems due to SSI setup.	This is alone not a real use case, but use cases appear when sectors are combined, so it may be an interesting credential to implement once SSI is better accepted.	This use case looks promising, but not as of right now. However, it could be set up on a small scale sandbox with a small set of fake data.

Table B.1: SSI Matrix (1/2)

Requirements	Transportation as a Service (TaaS)	CarDossier	Student Matriculation and Family Allocations	Certificate of Residence and GA Travelcard	Electronic Identity (eID)	Digital Diploma Credentials	Life-Long Learning
Privacy-Preserving	✔	✔	At least, more so than now...	✔	✔	Depending on the information included in the diploma (fine-grained information), it's best if privacy is of concern. Otherwise, one could use document signing or public blockchains.	✔
Selectively Disclosable	✔	✔	It would be great to be able to select the fact that you're enrolled without telling at which university.	Maybe you want to state that you live all together, but not where.	✔	✔	✔
Cross-Sector	The TaaS use case links technical sectors building a car, legal sectors issuing documents, the police checking in and educational sectors teaching people how to drive.	Insurance, police and driving schools are from different sectors, right?	Education and finance	Population and mobility	✔	✔	This depends on the connected services. It could leverage internal communication if the service is directly related to the education sector. Otherwise, if it is multi-issuer instead, it should be fine.
Multi-Issuer	✔	✔	✔	✔	For people living in foreign countries, the embassy can do it. Locally, the cantons are responsible for issuing IDs. When it comes to linked use cases, eVoting could very well be multi-issuer, since every citizen should be able to be an issuer.	✔	Universities, SWITCH and the user themselves can be issuers.
Distributed Authority	✔	Depending on the different credentials that could be issued, different authorities could be involved in the schemas, even if they all come from the mobility sector.	Since two sectors are involved (education and finance), they should operate together to create credential schemas that are okay with both of them.	Since two sectors are involved, they'd better collaborate to make sure each of them gets/sets what is necessary.	If we want to have interoperability with other countries, we must involve their train of thought in the design of our schema.	✔	In the end, SWITCH decides how affiliations look and universities stick to the schema. But as of now, edu-ID kind of tries to be consistent with European schemas, which could continue to be the case in the SSI world.
High Volume	More and more, it becomes important to share means of transport instead of owning a car, so I would argue that transportation as a service will become gradually more frequent.	✔	✔	The more one travels, the higher the volume...	✔	I would say it could be useful more than once, even though not every day for sure.	✔
Authorization-Granting	✔	✔	✔	✔	✔	Depending on how the HR infrastructure can be made to participate, this can authorize a former student to get an interview. Otherwise, SSI is out of scope, and for disclosing data with integrity preservation, one can use digital signatures.	✔
Time-Limited	If credentials are not meant to expire, they should at least be revocable.	✔	✔	✔	✔	A diploma is given for an undefined period of time: in principle, once you have it, you keep it (unless it gets revoked upon discovery of academic dishonesty; but this is implemented using revocation).	If credentials are not meant to expire, they should at least be revocable. Having a sliding window of 5 years as is the case in edu-ID now may be hard to implement with SSI.
Revocable	✔	✔	The time-limited aspect mitigates this: at most one semester of validity, to be renewed.	Same as on the left, the time-limited aspect limits wrongly issued subscriptions to one year.	I don't see why not, although this may not happen often in practice.	✔	I think SWITCH is the authority here.
User-Centric	It depends a bit on the exact circumstances, but it may be that there are multiple holders. I think the roles aren't clearly defined. Maybe consider adapting the information flow, because this would specify the use case better and possibly make it suitable for SSI.	It is rather car-centric, which includes ownership transfer and multi-ownership (I guess). Thus there is no single user at the center, but it is entity-centric, which can be rightfully delegated to a holder by the SSI principles.	✔	It's multi-user centric.	✔	✔	The idea of SWITCH edu-ID is to be user-centric, and SSI would empower the user even more.
Human Trust	✔	It would work best if this were the case, but depending on the credential, it may introduce more bureaucracy. In that case, it is important that users understand precisely what is going on.	✔	✔	✔	✔	It would involve the same actors as in the digital world already.
Identity-Specific	SSI may be out of scope for now, maybe later.	It is related to a car, which needs to be verifiable; identity of a user is secondary.	It may include some verification about the family status, to know who is a child of who.	Since Swiss Passes for instance can partly be used as a means of authentication, I believe identity verification is key here.	✔	For checking the diploma itself no, but to make sure it belongs to the person presenting it yes. SSI may be out of scope for now, since its main goal is to provide a digital identity, but it could be interesting to come back once SSI is more established, to link other use cases to existing ones.	SWITCH edu-ID accounts are strongly linked to identity, and some attributes are even verified (such as email addresses, phone numbers, etc.) and could thus be used for identity linking.
Takeaways	This use case combines several others, and may well be contained in the CarDossier world. It is not yet very clearly defined, but I think if the roles are clear, it could be interesting to leverage existing credentials when SSI is established, and build TaaS on top of them.	This use case is probably not well- aligned with the SSI roles, since there is no way to verify a car's identity with biometrical factors, but it could become an interesting application of delegation and portability.	This use case is also very interesting and it could very well lead to adoption of SSI among students (which can later be useful for diplomas)	This use case is quite simple and could become one of the early PoCs for SSI in Switzerland.	The eID is probably the most relevant use case because it is general and corresponds exactly to an identity that can be represented with SSI. What needs to be clarified is interoperability.	The use case is not directly linked to identity checking, and may not be so private as expected, but overall it could be a good match with SSI. Maybe in a few years, when the ecosystem is more present in society...	In the light of the current requirements, this use case is probably the most promising other than eID, even though some questions remain open. Technically speaking, this use case can also constitute the base for other ones.

Table B.2: SSI Matrix (2/2)