Self-Sovereign User Scenarios in the Educational Domain

Gerd Kortemeyer, ETH Zurich

February 10, 2022

1 Introduction

Self-Sovereign Identity (SSI) is a break from the traditional client-server model of user interaction with institutions and their online services [1, 2]. Today, in most cases, a user's client machine connects to a server machine via IP-addresses. The server stores all relevant user data for the service. Authentication for user sessions is either handled by service-specific username-password combinations or increasingly by Single-Signon (SSO) identity providers, either within institutions, within federations of institutions (e.g., Swiss edu-ID), or world-wide by third parties (e.g., Google, LinkedIn, or Facebook).

In contrast, SSI is build around connections instead of sessions. Entities, be it users or services, connect via Distributed Identities (DIDs) instead of IP-addresses, and these connections remain persistent across what traditionally might be called sessions. These DIDs are specific to the connection and pseudonymous, which makes the entity behind the DID untraceable across connections with different entities. The end-points of the connections are called Agents, and may be on an individual's personal device ("Edge Agent") or in the cloud ("Cloud Agent").

Data is stored with the user; where necessary, the integrity of this user-hosted data is verifiable against a crypto-secured Ledger via Verifiable Credentials (VCs) [3]. Alongside their verifiable content (hopefully based on an agreed-upon data model), VCs have a verifiable Issuer — whoever generated the VC — and a verifiable Holder — whomever the VC was made out to. The Ledger, frequently a blockchain[1], can be out in the open, and copies are typically widely distributed — this is possible, since the Ledger does not include any information that is useful beyond cryptographically verifying a VC. Holders can present VCs to other entities, who can independently verify the authenticity against the Ledger — in SSI-lingo, the recipient of a VC or other cryptographic proof is then called the Verifier. VCs can be presented as a whole or in part to provide Proof for Claims (credentials that they "claim" to have, e.g., "I have 3 credits for Calculus 1 at XYZ University in FS21 with a grade of 3.5"). Particularly intriguing are Zero-Knowledge-Proofs, where an entity proves that it holds certain data, but does not reveal what it is[2]. VCs can have expiration dates or be revoked.

The main impetus is to enable free movement and commerce in an educational ecosystem without the ever-looming and sometimes paralyzing concerns of data privacy and security. SSI enables users to take control of their own data and only reveal information on a need-to-know base, including their own real-life identity. Services, on the other hand, are not responsible for the protection and longterm security of user data, which reduces their vulnerability to disasters, cyber-attacks like ransomware or data breaches, and resulting potential lawsuits — for a Service,

[1] This does not have to be a public blockchain like BitCoin or Ethereum, which require an energy-devouring and expensive Proof-of-Work, but in fact, for an educational ecosystem would more likely be a Federated Blockchain, which instead requires a consensus-based Proof-of-Stake

[2] "Excuse, do you know what time it is?" - "Yes."

Figure 1: Analogy of a wallet and safe-deposit box in a self-sovereign user model.

being responsible for identifiable user information can be a liability rather than an asset. Notably, the academic records of major US-American universities represent billions of dollars in user-invested tuition. In some aspects, a self-sovereign ecosystem is a move back to the likes of a pre-digital age, being responsible for the management of their own paper-based credentials and paying with untraceable cash.

2 Users

A user is the Holder of their own data: VCs and other files, such as portfolios or logs. Their "digital twin" consists of a Wallet, where typically VCs are stored and managed, and a Data Pod in the cloud, where typically larger files are stored and managed — the latter is the equivalent of a safe-deposit box. Wallets can usually be found on personal devices, such as smartphones, and connect through Edge Agents. Data Pods are typically hosted at so-called Agencies and connect through Cloud Agents (in an extension of VCs, files in the Data Pod could be verifiable through storing hashes of the write transactions (full or incremental) [4]); a possible implementation for Data Pods may be found in an extension of Solid [5]. Figure 1 illustrates this digital twin.

Preliminary versions of this paradigm have already been rapidly taking hold over just a couple of years; examples are payment systems such as Apple Pay, electronic boarding passes on airline applications, SwissPass, COVID certificates, etc. However, while already implementing several components of this new ecosystem, these mechanisms are not yet truly self-sovereign. For example, the airline still holds the authoritative copy of the flight booking — a fully self-sovereign implementation would mean that the booking only exists in the form of a VC under the control of the passenger. During the pandemic, restaurant guests still need to dig out some plastic ID-card to prove that they as an individual are indeed the Holder of their VC — a process called "Identity Assertion," which is still analog here. Finally, these VCs are still frequently scattered across proprietary wallet applications instead of being managed by the Holder within one Wallet of their choice.

A challenge is that while hopefully COVID certificates and typically flight tickets only need to be cryptographically secure for a few months, VCs associated with lifelong learning need to preserve integrity for maybe sixty years: from entrance into kindergarten to retirement, and

possibly even beyond in a "second act." Advances in computing (in particular quantum computing) may render encryption algorithms obsolete, and the non-traceability of DIDs may be compromised by vast correlation analyses.

If lifelong learning starts in kindergarten, learners start out as minors. This means, the technology platform of the ecosystem will need to implement key delegation and guardianship mechanisms. These mechanisms are provided for in SSI-models, but add complexity.

Finally, this new ecosystem should not lead to the next wave of a Digital Divide. While users should be free to choose their agencies, which may include for-profit offerings, some basic agency functionality needs to be offered for free by local governments or the Federation.

3 Services

For the purposes of this paper, "Services" encompasses all entities that a learner might interact with during their lifelong learning journey. These may be traditional grade schools and universities, schools of continuing education, test administration companies, and training providers, but also ancillary cloud services like online homework engines, collaboration tools, interactive worksheets, etc. Also, government agencies, publishers, and employers may participate in this ecosystem. An important strength of an SSI-ecosystem compared to some monolithic "education platform" is, that it accommodates existing and emerging services in a scalable and future-proof fashion; most of these Services do not need to change the way they do business or re-invent themselves, they simply need to accommodate a different way of connecting with customers. This is similar to a bakery providing a payment terminal to accommodate customers paying with their smartwatches — the business still makes and sells bread.

These service entities would be represented by Cloud Agents, and learners may typically establish connections between their agent and service's agent by scanning QR-codes from a welcome screen instead of making accounts and logging in. Typically, at least when first connecting, the Service may request certain VCs or other Proofs, which the user can selectively provide or deny.

4 Governance

Crypto-technologies are only half of what makes an SSI-ecosystem work; Figure 2 illustrates the necessary layers for such a system. Unfortunately, the fourth layer, Governance, is easily forgotten in favor of focussing on the technology, but the ecosystem will not work without it. In a global society, where benevolence cannot be assumed, deciding whom to trust within an ecosystem is a challenging task. A likely form of organization will be an international federation with national sub-federations. There are already national governing bodies, e.g., swissuniversities [6], the German Kultusminister Konferenz [7], or US-American Regional Accrediting Organizations [8]. In fact, many of the necessary governing bodies already exist in most any nation in analog form.

Within national contexts, entities such as SWITCH [9] or the Deutsches Forschungsnetz [10] will be essential partners; these have traditionally been the provider of similar services in the education sector, including central identity services such as SWITCH edu-ID [11]. These organizations are already networked — in more than one meaning of the word! — with the computing centers at the universities.

On the crypto-utility layer, open-source will be an essential component to build trust in academic environments. These security-relevant layers need to be open for inspection. It is important to note that "open-source" is not necessarily "free software," and that "free software" means "free as in speech," not "free as in beer" [12] — developing, operating, and maintaining this

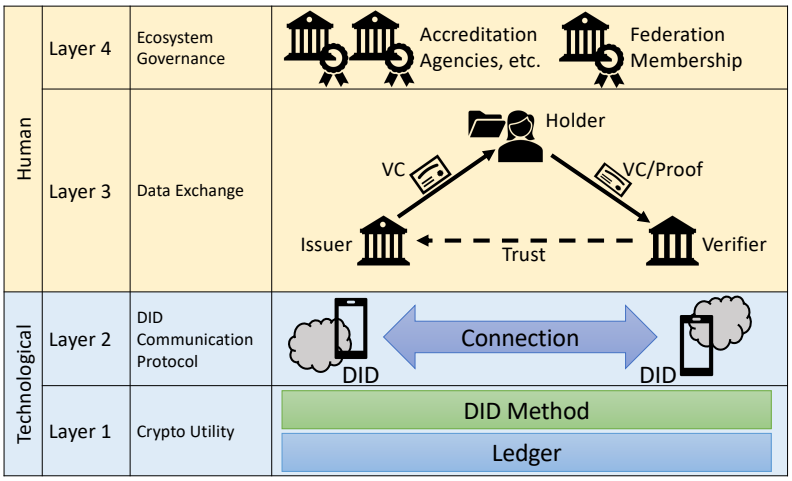

Figure 2: The layers of a self-sovereign ecosystem.

utility layer will incur real cost and might be handled by commercial companies or public-private partnerships. Germany already has a long tradition of juggling this balance act in academic environments through CampusSource [13].

Finally, the Federation needs mechanisms for Identity Assertion, to, where necessary, associate DIDs with real-life individuals (which may be the case less often than one might guess!). Due to the high level of international mobility in the academic sector, insular solutions relying on only one national type of government-issued digital ID-card will be insufficient; instead, the Federation needs to decide which digital ID-cards are valid to uniquely associate an individual with their private cryptographic keys, similar to the way passports are acknowledged internationally. Within an academic federation, university registrars might be trusted to provide Identity-Assertion VCs if the learner shows up in person with their passport.

5 Use Cases

The following subsections describe examples of existing educational use cases and how they would map into a self-sovereign model. New use cases may develop due to the existence of the ecosystem, but those are not described here.

5.1 A learner earns a degree

This is the most classic case of using VCs, but also the most coarse-grained. A learner might receive a degree, for example a B.Sc., from an accredited institution. The institution issues the VC and registers it to the Ledger, the learner adds it to their Wallet; this is illustrated in the

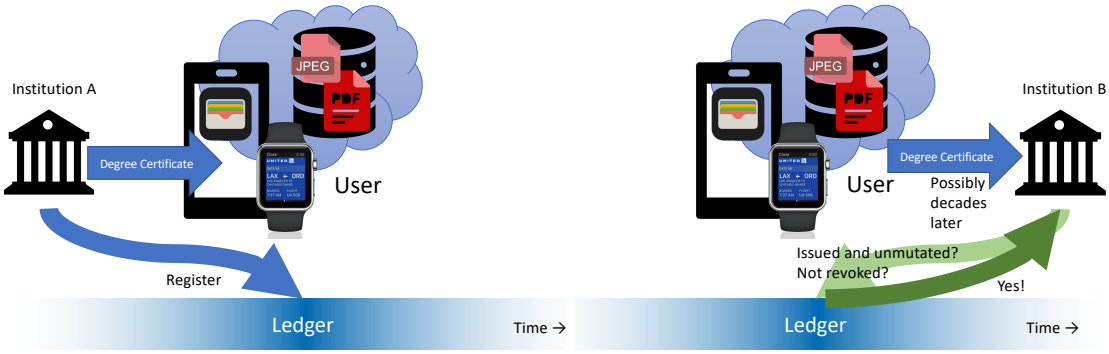

Figure 3: A learner receives (left panel) and presents (right panel) a degree certificate.

left panel of Figure 3. While VCs are of course machine-readable, making sense of them in an automated way requires a data model; efforts toward such a data model are under way for degrees [14] or the non-traditional concept of badges [15].

In addition to the VC, the learner might receive a decorative certificate as a PDF, which they can print, frame, and put on the wall. This PDF would go into the Data Pod, and a hash of the PDF might go into the Ledger to prove its authenticity. Within the Federation, though, the machine-readable VC will be used.

5.2 A learner earns course credit

On a more fine-grained level, a user might receive credit for a course. Again, the institution would issue a VC for the course. A constant challenge are course equivalencies — while different universities offer large numbers of basically equivalent courses (think "Calculus I"), this is a complex task, as these not only have different titles but also different flavors. In the United States this is done partly by crowd-sourcing of university registrars [16], while in Europe, the European Credit Transfer and Accumulation System (ECTS) is essential [17]; for the purpose of issuing automatically transferable course VCs, the Federation needs to make use of these or similar structures.

5.3 A learner needs to get a foreign degree acknowledged

An ecosystem like this cannot be implemented from one day to the next — historical or "foreign" (in the sense of created-outside-the-ecosystem) credentials need to be taken in as users are onboarded. In the analog world, there are already entities that assist in this process, for example the Swiss SERI [18] and the German anabin [19]. Services like these could evaluate paper-based documents and issue corresponding VCs. Alternatively or complementary, university registrars could acknowledge these degrees as transfer degrees and issue corresponding VCs.

5.4 A learner explores a possible study program

A learner may consider a study program at an educational service provider. The provider might make available adaptive recommender systems, but at this point, the user may choose to not yet connect using their asserted identity — they want to anonymously explore. The recommendation system may ask for information about the learner's educational history, where the quality and

usefulness of the recommendations will likely depend on how much the learner chooses to reveal. For example, a masters program will likely expect the learner to have earned the equivalent of a bachelor degree at some point in time, but the user may choose to only reveal that such a credential exists without disclosing the major or the grade.

At this point, the applicant may also decide to provide proof of previous course work (see Subsection 5.2) to see which credits may be acknowledged as transfer credit.

5.5 A learner applies for a study program

A learner may decide to apply for a study program at an educational service provider. At this point, they still might choose to not reveal their asserted identity, which in fact may be in the interest of the provider to avoid accusations of acceptance bias due to gender or apparent ethnic background of the applicant. However, the applicant now needs to reveal more information than in the exploratory scenario described in Subsection 5.4, for example, majors and grades become relevant. Also, VCs for transfer credit need to be provided.

As the right panel of Figure 3 shows, these credentials may be turned in several years later. The original issuer of these credentials does not need to exist anymore to verify these credentials, which is a large improvement over the analog scenario in case a university closed or somehow lost its records.

For programs in the design, musical, or fine-arts sector, the applicant at this point may also reveal sections of their Data Pod, which may contain portfolio artifacts such as audition recordings, scanned artwork, or digital media pieces.

5.6 A learner applies for graduation

As a learner applies for graduation, they will turn in all relevant course credits (Subsection 5.2) to the registrar's office for evaluation. A notable difference to the current method is that the user stores their credits, similar to the German concept of "Scheine," which actually used to be pieces of paper.

5.7 As part of course work, a learner needs to use an external service

Particularly due to the COVID crisis, it became apparent that a monolithic local learning management system (LMS) does not serve the needs of all instructors and learners anymore — instead, more and more instructors desire to use the plethora of cloud services that are available, such as Piazza, Miro, online homework systems, Slack, Google Docs, MS Teams, Quizlet, Kahoot, to name but a few. There are considerable privacy concerns, and learners complain about having too many usernames and passwords. In addition, performance information usually does not flow back into the campus LMS.

The current mechanism to overcome at least some of these challenges frequently is to use Learning Tools Interoperability (LTI) [20] in connection with SSO, as shown in the left panel of Figure 4. This usually entails at least some additional work in systems engineering, and it does not address data privacy and security concerns.

The self-sovereign equivalent is shown in the right panel of Figure 4. The learner connects to the service using a DID. As the learner works, artifacts may be stored in their Data Pod, and after completion of tasks, the service issues a VC. The learner subsequently turns in the VC to the local LMS.

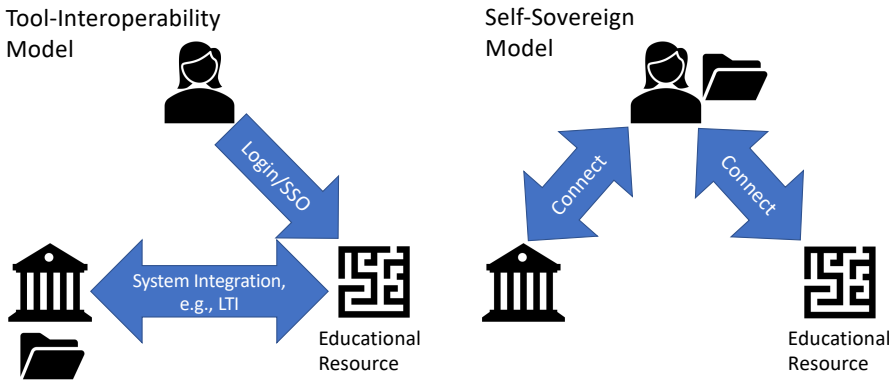

Figure 4: Learning Tool Integration (LTI) versus Self-Sovereign Identity (SSI) approaches to curricular inclusion of external educational resources. The folder icon denotes the location of the performance data.

5.8 A learner returns from a study abroad or mobility program

The learner may have spent a semester at another university and returns to their alma mater. This process requires no additional effort, as the hosting university would have issued course credit (see Subsection 5.2), which the learner would turn in when applying for graduation (see Subsection 5.6).

5.9 A user applies for a job

The company's HR-portal allows applicants to connect and make available VCs and portfolio files, similar to the process of applying for a study program (see Subsection 5.5).

5.10 A company requires regular training from their employees

A company requires annual compliance training from their employees. The employees have a choice of providers. After successfully completing the training with one of these providers, the provider issues a VC with an expiration of one year. The employee then presents this VC to the company.

5.11 Academic fraud

Years after a person completed their M.Sc. with a university, it is detected that the thesis was plagiarized. After careful investigation and deliberation, the university decides to revoke the degree. At this point, a Ledger entry is made to revoke the VC associated with the degree. If the person subsequently attempts to present the VC to another university or potential employer, the VC will come back invalid (right panel of Figure 3). All transactions are cryptographically recorded and documented in case of legal disputes.

6 Conclusion

A self-sovereign educational ecosystem represents a major paradigm change in how the "education business" is conducted. It will take a concerted effort of the public and private sector, however, this does not make it insurmountable. As the introduction of electronic payment systems and COVID certificates showed, sometimes change can happen in the timeframe of a handful of years or — in case of COVID — even months, if there is sufficient political or commercial impetus. The introduction of SSI is also a large enough shift to give the opportunity to revise some of the historically grown and sometimes byzantine workflows, and it may be a catalyst for the more consequential implementation of the Bologna concept.

References

[1] Alex Preukschat and Drummond Reed. *Self-Sovereign Identity.* Manning Publications, 2021.

[2] Annett Laube and Gerhard Hassenstein. Self-Sovereign Identities. Technical report, Bern University of Applied Science for SWITCH, 2020.

[3] World Wide Web Consortium et al. Verifiable credentials data model 1.0: Expressing verifiable information on the web. `https://www.w3.org/TR/vc-data-model/?\#core-data-model`, 2019.

[4] Gerd Kortemeyer, Stefan Dröschler, Peter Riegler, and Nick Koslowski. A model for lifelong learners' educational records and identity in a next generation learning management system. *eleed*, 14(1), 2021.

[5] W3C Solid Community Group. Solid Protocol. `https://solidproject.org/TR/protocol`.

[6] swissuniversities. Recognised or accredited Swiss higher education institutions. `https://www.swissuniversities.ch/en/topics/studying/recognised-or-accredited-swiss-higher-education-institutions`.

[7] Stiftung Akkreditierungsrat. Accredited study programmes and higher education institutions. `https://www.akkreditierungsrat.de/index.php/en/accredited-institutions-higher-education-and-study-programmes/accredited-study-programmes-and`.

[8] U.S. Department of Education. Accreditation in the United States. `https://www2.ed.gov/admins/finaid/accred/index.html`.

[9] SWITCH.ch. SWITCH. `https://www.switch.ch`, accessed February 2022.

[10] German National Research and Education Network. DFN. `https://www.dfn.de/en/`, accessed February 2022.

[11] SWITCH.ch. SWITCH edu-ID. `https://www.switch.ch/edu-id/`, accessed February 2022.

[12] Richard Stallman. Viewpoint why "open source" misses the point of free software. *Communications of the ACM*, 52(6):31–33, 2009.

[13] CampusSource. Campussource e.v. `https://www.campussource.de`.

[14] World Wide Web Consortium Taskforce. Verifiable credentials for education task force. https://w3c-ccg.github.io/meetings/2021-11-08-vc-education/, accessed February 2022.

[15] IMS Global Learning Consortium. Open badges for education. https://www.imsglobal.org/activity/digital-badges, accessed February 2022.

[16] American Association of Collegiate Registrars and Admissions Officers (AACRAO). American transfer articulation database. https://www.aacrao.org/resources/transfer-articulation, accessed February 2022.

[17] European Higher Education Area. European Credit Transfer and Accumulation System (ECTS). https://education.ec.europa.eu/levels/higher-education/inclusion-connectivity/european-credit-transfer-accumulation-system, accessed February 2022.

[18] State Secretariat for Education, Research, and Innovation. Recognition of Foreign Qualifications. https://www.sbfi.admin.ch/sbfi/en/home/education/recognition-of-foreign-qualifications.html.

[19] Kultusministerkonferenz. Zentralstelle für ausländisches Bildungswesen. https://anabin.kmk.org/.

[20] IMS Global Learning Consortium. IMS LTI 1.3 and LTI Advantage. https://www.imsglobal.org/activity/learning-tools-interoperability.