Issue se2021
2021

A Model for Lifelong Learners' Educational Records and Identity in a Next Generation Learning Management System

Gerd Kortemeyer
gerd.kortemeyer@let.ethz.ch

ETH Zurich
Educational Development and Technology HAD G11
8092 Zurich, Switzerland

Stefan Dröschler
stefan.droeschler@inf.ethz.ch

ETH Zurich
Department of Computer Science (D-INFK) UNG G14
8092 Zurich, Switzerland

Peter Riegler
p.riegler@ostfalia.de

Ostfalia University of Applied Science
Salzdahlumer Str. 46/48
38302 Wolfenbüttel, Germany

Nick Koslowski
n.koslowski@ostfalia.de

Ostfalia University of Applied Science
Salzdahlumer Str. 46/48
38302 Wolfenbüttel, Germany

urn:nbn:de:0009-5-52672

Abstract

The need to be competitive in a fast-changing global job market will likely lead to an increased demand for “just-in-time” educational experiences. Parallel to developments in the medical sector with virtual patient records, the paper presents a model for storing and managing educational data gathered along a lifelong learning journey, such as transcripts, artifacts, and performance analytics. Using the concept of Social Linked Data (“SOLID”), the learners instead of the educational institutions would have sovereignty over their own data, while transactional fingerprints would be used to guarantee data integrity using a federated blockchain.

Keywords: e-learning; LMS; educational data; learning management; social linked data; self-sovereignty; federated blockchain

1. Introduction

In August 2020, participants from Austria, Germany and Switzerland discussed the features and properties of a Next Generation LMS in a workshop organized by CampusSource, the research focus project D2L2 at FernUni Hagen, and ETH Zurich. A strong emphasis was put on nontraditional, lifelong learners, who carry their own data from institution to institution, where they “plug into” the local campus systems. The issue is going to gain in importance, as even traditional universities increasingly aim to attract these migrant learners (Gartner, 2021). This paper proposes a corresponding user model as one of two large-scale models needed for a Next Generation LMS. The second model is for the handling of educational content resources, which needs a separate effort and will not be discussed here.

2. Status Quo

Currently, learner data are highly distributed, duplicated, and redundantly stored: academic records are traditionally held by the respective institutions that the learner attended. Within those institutions, some data are in institution-wide databases, while other data are stored in particular learning platforms like course management systems, and they are frequently associated with particular courses (Kortemeyer, 2017). The result of the status quo is a lack of verifiability, coherence, and personal, user-centric data sovereignty (“data self-sovereignty”) of educational data.

2.1 Verifiability and Sustainability

Users usually receive paper copies of their certified transcripts (showing earned course credits) and degrees (which admittedly look decorative when framed), and they need to make photocopies or scans of those documents to transmit their credentials to other institutions or potential employers. Not surprisingly, fraud abounds, particularly in an increasingly global education and work space. In fact, there are several companies with names like phonydiploma.com, diplomacompany.com, and diplomamakers.com, who openly advertise services to generate fake transcripts and diplomas; the authors did not try to employ these services (or so they say), so no guarantees regarding their efficacy can be given.

To provide higher levels of verifiability, several efforts are underway:

- A growing number of institutions offer proprietary mechanisms to make authoritative versions of academic data available to others. These “callback” mechanisms create a token, that can be used by other educational institutions or employers to retrieve the record directly from the source (as verified by the underlying Transport Layer Security (TLS)).

- Other approaches store a hash (“fingerprint”) of the institution-provided PDF documents (not the underlying structured data per se) in an independently verifiable way (e.g., SWITCHverify, 2021, and TrustCerts, 2021).
- Yet other approaches market the ability for institutions to generate their diplomas, certificates, and transcripts in a verifiable electronic format (e.g., Hyland, 2021), which goes back the Digital Certificates Project (MIT Media Lab, 2015).

In all of these examples, the credentials need to be verified through third parties, either the issuing institution or other “notarization” entities; an open question is what to do when this verifier vanishes – a lifelong learner requires decades of stability. This is outside the control of the learner, as the mechanism used depends on the issuing institution.

Finally, there are end-to-end confidential data like letters of recommendation for scholarships, awards, and potential employers. A unique feature of these data is that the learner should be able to manage the distribution of these letters, but not be able to see their content. Waving the right to read these letters is often expected by authors (who could otherwise simply refuse to write a letter) and recipients (who put much higher weight on letters with the “waiver”). The letter may also not be replaced with a (potentially) more favorable one. A small sector of industry has developed around managing the workflow of soliciting and distributing these records, for example Interfolio (Interfolio, 2021).

2.2 Coherence

The learner leaves behind a breadcrumb trail of educational data across platforms and institutions, which – due to data protection laws – the prior institutions might even need to purge after certain amounts of time. In addition, due to political or financial instability, educational institutions can vanish over the lifetime of a learner.

Besides transcripts and degrees, there are transactional data (e.g., clickstreams or formative assessment results) from learning platforms, which can be useful for recommender systems, analytics, and quality control. Before making these data useful, they frequently need to be extracted, processed, and compiled from various sources. In any case, as these data are scattered across platforms, no one platform “gets to know” the user.

While a perfect human tutor or mentor would accompany a learner over an extended amount of time and get to know him or her, the status quo is that any kind of AI-mentor would be rather scatter-brained and frequently suffering from memory-loss.

2.3 Self-Sovereignty

Currently, the learner basically has very little control over his or her data, i.e., lacks sovereignty. The main idea behind the user model presented here is that the learner’s educational experience is one contiguous, lifelong journey, and that the data gathered along the way gets added to one continuous transcript (“ledger”) of achievements, credits, certifications, and degrees, and that the user builds up learning analytics data which enables him or her to take better advantage of each station along the educational journey.

These data should be under the control of the user, i.e., he or she should have data self-sovereignty, except in areas where limitations to that control are in his or her advantage to establish trust.

2.4 Being a Lifelong Learner

As a result of these challenges, being a lifelong learner is a cumbersome endeavor, as one needs to get just-in-time training and education from a variety of institutions, and needs to proof those credentials to one's current or potential employers. In the social media realm, some commercial companies are stepping in to give users some way of consolidating credentials and experiences, most notably LinkedIN, which offers brokerage of continuing education and certifications (LinkedIN Learning, 2021) – currently from mostly non-traditional institutions. Targeting more traditional institutions, the concept of a Lifelong Learning Passport was developed (Gräther et al., 2018) – the user model presented here takes a related approach.

3. Players

There are several players to consider when building a user model:

- **User:** this is a lifelong learner, who carries his or her data from educational institution to educational institution, and who makes data selectively available to the other players.
- **Federated platform:** federated systems in which users and content interact with each other as part of educational experiences.
- **Federated educational institution:** a school, college, university, or training program, which would be member of some larger federation. On an administrative level, federation members acknowledge course credits and certifications (subject to mutually agreed-upon pairwise equivalency rules). On a technical level, the federated institutions build on a common infrastructure.
- **External educational institution:** an educational institution that is not federated, but which a user might want to apply to, and where a user might participate in educational experiences.
- **External stakeholder institution:** a non-educational external organization as a "consumer" of educational data, for example a potential employer, a scholarship organization, or some other funding agency.
- **External stakeholder user:** a person, system, or employer who contributes additional educational data or artifacts, such as letters of recommendation, internship evaluations, reviews, etc.
- **Service providers:** these may be external providers of data storage or cloud computing, including third-parties running campus IT systems, etc.

4. User Data

A user accumulates the following kinds of education-relevant data:

- **Personal data:** name, date-of-birth, basic demographics, student ID number or numbers (some countries like Switzerland have lifelong student IDs), etc. These data needs to be disclosed or opened up in whole or in part to any other player that the user interacts with.
- **Certified transcript data:** academic credentialling, for example course credits or degrees. Currently, these data need to be transferred between educational institutions, where “the next chapter” of the learner’s education is written (as evidenced by terms such as “transfer student” or “transfer credit”), but in principle, this is one continuous, ledger-like record of the learner’s accomplishments.
- **Transactional data:** data routinely produced while interacting with learning platforms, which are potentially useful for personalization and guiding of learning (Kortemeyer & Dröschler, 2021), analytics (Verbert et al., 2013), and content metrics (Kortemeyer, Dröschler, & Pritchard, 2014). This is where the system “gets to know” the user.
- **Portfolio data:** a collection of artifacts generated during educational experiences, such as presentations, posters, artwork, compositions, videos, CAD-files, etc., which may be useful for applying for admission to other educational institutions or employment.
- **End-to-end confidential data:** Letters of recommendation, reviews, and the like, which a user needs to hand over from the author to the recipient without him- or herself being able to see them or to switch them out.

All of these data will need agreed-upon data formats, which is going to be a challenge that is outside the scope of this user model. It is clear, though, that these will need to be structured, clear-text data formats (which could be represented for example in JSON) with possible binary attachments (e.g., images, PDFs, etc.).

5. Transactions, Risks, and Trust

The next stage would be to define transactions for different types of data to be stored, retrieved, and processed by the players, mediated by the Next Generation LMS. An allimportant ingredient in these transactions is trust to mitigate risks.

In our proposed user model, the default trust relationship between players is “trust nobody” – we have to assume that by default, any player might manipulate, fabricate, omit, or abuse data. Short of chiseling the data on stone tablets and physically locking them up in a Swiss bank vault, and any transaction only happening in person with proper identification and witnesses, we would then need to define who must trust whom for particular transactions, and how to ensure that this trust is justified. In analogy to a firewall, we need to start with “block everything” and then selectively open up, rather than “allow everything” and selectively block.

Table 1 shows some use cases, as well as the associated transactions and necessary trust relationships. This table would need to be extended, and it will evolve over time.

Use case	Transaction	Risks	Trust
User completes a course at a federated institution, gets credit and a grade.	Institution adds an entry to the continuous transcript of the user.	User manipulates entry; entry does not get added correctly and user loses credit.	User gives the institution append-access to his or her transcript.
User applies for a degree program at a federated institution and needs to provide transcript.	Institution reads the continuous transcript of the user.	User delivers manipulated transcript, e.g., modifies, adds, or hides entries.	User gives the institution read-access to his or her transcript.
User is taking a course at a federated institution and generates analytics-relevant data.	Institution adds clickstream and formative assessment data to user's transactional data repository.	User is unable to understand the data that is collected and unable to gauge the consequences of these data on future learning experiences.	User gives the institution write-access to his or her transactional data repository.
User is taking a course at a federated institution and asks for recommendations or remedial interventions.	The LMS at the institution combines content usage data ("dynamic metadata") and user transactional data to make recommendations or construct learning paths.	User transactional data becomes public; user cannot reconstruct decision processes and potentially misses out on learning opportunities; user is subject to AI-prejudice.	User gives the institution read-access to his or her transactional data repository.
User applies for a degree program at a federated institution and needs to provide an end-to-end confidential letter of recommendation.	User selects the letters he or she wants to submit and makes them available.	User can read or manipulate the letter; the letter becomes public.	User gives the institution open read-access to the letter.

Table 1: Use case, transactions, risks, and trust relationships

6. Technologies

The user model presented here is a tall order. Fortunately, there are some existing technologies to possibly enable implementation. The technologies listed here are the ones explored for the prototype of openLCMS, which is a project at ETH Zurich.

6.1 OpenID Connect

When dealing with different players, first of all their identities need to be verified. A highly promising technology is OpenID Connect (OpenID Connect, 2021), which builds on the popular OAuth (OAuth, 2021). OAuth 2.0 is foundational to the increasingly-adopted SWITCH edu-ID (SWITCH edu-ID, 2021), which provides lifelong educational identity management for Swiss educational institutions. OpenID Connect is already in use for the ambitious SwissID project (SwissID, 2021). There are some open questions about the privacy of OpenID Connect, which are currently being researched and addressed at ETH Zurich (Hammann, Sasse, & Basin, 2020). Also, the interplay with the concept of decentralized identities needs to be further explored.

6.2 Social Linked Data

Social Linked Data (SOLID) is a concept of storing data with the user instead of the application or service, under the control of the user (Mansour et al., 2016; SOLID Project, 2021). The user gets to choose which data they release to which platforms, i.e., the user has self-sovereignty over his or her data.

In particular, learner data would not (at least not permanently) be stored in the Next Generation LMS. The user would need to provide their own data “pods,” in which his or her data are stored. Pods can be hosted anywhere on the web under the control of the user; in particular, companies offer hosting of “pod space,” but this function could also be carried out by non-profit organizations or tech-savvy users themselves (e.g., from a server in their basement).

SOLID is not so much a “technology,” since it relies on standard webserver functionality, but rather a philosophy with associated protocols. It is key to the user model proposed here, but for the user, it is not limited to that – they could also use their pods to plug into online stores or social media, if the associated applications or services talk SOLID. On the SOLIDified web, the pods are the users, with which they would buy groceries and take courses. Considering the next generation of learning management systems, when a user applies to or enrolls at an institution, he or she makes their own educational data selectively available, and the platform would start interacting with the data inside the pod.

Authentication and identity management in SOLID is handled using OpenID Connect. The possible creation of fake identities (particularly problematic in countries like Germany where some exams can be “failed for life”) will need to be addressed at this level, in the same way as it is increasingly addressed today. Data access authorization is handled within the data pods and thus under the control of the learner.

SOLID provides some data formats, but mostly aims to develop application-specific formats as a community effort, using the concept of “vocabularies” (SOLID Vocabularies, 2021). For educational data, a new vocabulary (basically an ontology) would need to be developed.

Unfortunately, only the personal and portfolio data are immediately compatible with the SOLID concept: personal information falls into the realm of OpenID Connect, and portfolio data falls exactly into the class of data that SOLID was designed for: identifiable, non-confidential, and usually not subject to fraud short of plagiarism. For other types of educational data, however, the control of learners over their data – also in their own interest – needs to be limited: some of it they should not be able to modify themselves (e.g., bestow a Ph.D. on themselves or change their grade in Calculus 1), and some of it they cannot even see (e.g., end-to-end confidential letters of recommendation). Thus, the user should only have control over who can access their data and how, but not necessarily over the content of the data. Other technologies need to be used to accomplish this apparently impossible feat: establish trust in an inherently untrustworthy environment. Particularly with a server in their own basement, learners could otherwise easily read and manipulate anything.

6.3 Federated Blockchain

To establish trust, the second key technology in this user model is that of a federated blockchain. Combining Personal Data Storage and blockchains has been suggested previously (e.g., Yan, Gan & Riad, 2017) to serve as “notary,” Blockchains are usually associated with cryptocurrencies, energy-consuming Proofs-of-Work, and global entities like Ethereum (Ethereum, 2021), but none of that is needed here; a federated blockchain, for example using Hyperledger Fabric (Cachin, 2016), and simple Proof-of-Stake will do.

Educational institutions would be the peers in this federation, each holding copies of the blockchain. While “federating” a number of schools, colleges, and universities might seem like herding cats, in a small country, like for example Switzerland, with mostly non-competing institutions, this just might be possible. While on the one hand, at least initially, there might be too few peer nodes to form a minimum effective blockchain, on the other hand, initially mutual distrust among institutions might not yet be an issue.

It is important to emphasize that not all educational institutions that a learner visits need to be part of the federation; actually, that would be illusionary. Thus, the list of “Players” in Section 3 includes external educational institutions. It is crucial, however, that there is a trust relationship between the external player and the federation: the external institution would need to trust the federation to guarantee (“notarize”) trustworthy records, and the federation would need to allow the external institution to register and record transcript data. This, however, is no different from current trust relationships when it comes to accepting transfer credit or conducting study abroad or study away programs.

The learner’s transcript itself should not be in the blockchain, since not all peers in the federation should have access – that access would be selectively granted by the learner (as expected by the SOLID paradigm). Instead, the blockchain stores the fact that a learner received a new transcript entry and the cryptographic hash of that entry.

Table 2 shows an example of a simplified transcript for a user Carlos, as it would be stored in his data pod. In a real application, institutions and users would have unique IDs, and data might be structured rather than in table format, and it may have attachments, such as a PDF version of certificates. As in a ledger, the entries are time-ordered, where later entries supersede earlier ones. For example, in Table 2, the 2000 grade in “Intro to Biology” replaces the failing 1999 grade. However, just like in normal transcripts, past entries are never deleted.

The entries in this transcript have IDs, and the user-ID and hash of the entries (including possible attachments) are stored in a blockchain, which is hosted by the federated institutions; Table 3 shows an example. Thus, at any point in time, all federated institutions can verify the correctness and completeness of a transcript which a learner made available to them, but cannot see or reconstruct a transcript that the learner did not give them access to. The mechanism is robust against an institution dropping out of the federation.

In order to attend an institution, the learner also must give that institution the right to add to his or her transcript, at which point also new entries are added to the federated blockchain. The requirement of “write permission” might be perceived as an infringement on data selfsovereignty, but it is necessary particularly in countries and university systems where examinations can be failed “for good” – the completeness of the record needs to be guaranteed for better or worse. In a variation or extension of the user model, whenever an entry gets added, the current blockchain could be copied to the user’s pod – this would, in principle, allow every user for themselves to verify their own transcript and the integrity and completeness of the blockchain (in case they do not trust the federation).

Transcript of User Carlos

EntryID	Time	Institution	Type	Code	Name	Credit	Grade
3125412	03.05.1999 23:55	Bob College	Course	MAT103ss99	Calculus 1	4	4.0
3242414	10.12.1999 15:55	Alice College	Course	FS99_BIO101	Intro to Biology	4	1.0
4243217	10.12.1999 15:58	Alice College	Course	FS99_BIO131	Cell Biology	3	4.0
…							
4331412	04.05.2000 16:40	Alice College	Course	SS00_BIO101	Intro to Biology	4	3.0
…							
5541594	05.05.2002 09:13	Alice College	Degree	BScBio	B.Sc. Biology		3.27
6415042	08.12.2002 15:58	Charlie University	Course	F2002eng503	Biochemical Engineering	3	2.5
8435235	08.12.2002 15:58	Charlie University	Course	F2002phy560	Thermodynamics	3	3.0

Table 2: Simplified example of a transcript, stored in the data pod

EntryID	User	Hash
…		
3125411	Frank	g45pxquiRs41f4qq
3125412	Carlos	tD4h9qH43K4RY17b
3125413	Erin	Se7p98e41J485122
…		
3242414	Carlos	r4dGxq8LFs4bf47b
…		
6415042	Carlos	uIh8q63p5R1vn7o7A
…		

Table 3: Blockchain with hashes of the entries in Table 2.

6.4 Encryption

If authors could be expected to own data pods, confidential recommendation letters would most easily be stored with them. A mechanism would then need to be implemented for the user to release the letter to others. However, such a mechanism would be very much in conflict with the philosophy of SOLID to control one’s own data: both for the user, who could for example not delete the letter, and for the author, who would need to grant another user the right to release data from his or her own pod – rightly so, SOLID has no protocols for that.

Thus, to stay within the philosophy of SOLID, the letter should be inside the pod of the user, but undecipherable and unalterable for him- or herself. In keeping with SOLID, the user can selectively grant access or even delete the letter, but without knowing its content. That pod, however, is pure data storage with access control; it cannot carry out any computational tasks, like for example establish encryption keys – and even if it could perform encryption computations, one could not trust the results, since the pod is completely under the control of the user.

As a consequence of these limitations, encryption needs to be handled by the learning management system. Having only one actor as a central clearinghouse means that a lot of trust has to be bestowed on this platform, but also that it makes no sense to deploy overly complicated encryption mechanisms. The process clearly has vulnerabilities, for example the user somehow managing to send the letter to themselves, but this is similar to the vulnerabilities of currently deployed systems.

7. Discussion

The model differs from the Lifelong Learning Passport in two ways: all data is stored with the user, and there is no third party as certifier, as the federated institutions themselves run the learning management system and associated blockchain. A weakness of this model is that it requires a federation to be implemented, and any SOLID pod established by learners will likely be the first one they own – not unlike the concept of the Lifelong Learning Passport, it may take some explaining to bring about such a paradigm change, and at least initially, the pods may need to be hosted by a not-for-profit in purely educational context. However, if the concept of SOLID takes root, service providers will spring up – in the 80s, it took effort to get an email address, while now a new address can be established in minutes.

Most institutions already run some traditional course management system, as well as an ecosystem of historically grown databases, back-office applications, and web frontends. In some universities, these decades-old databases represent billions of dollars in tuition investments. Generally, these systems, some of them implemented in COBOL on System/370 mainframe emulations, are highly robust and reliable. All of this existing infrastructure is designed around the paradigm of local and proprietary user data storage. There is no way to move to the model presented here from one day to the next. Thus, the switchover would have to happen gradually, where the identity management and data pods are first emulated locally or by a trusted provider. Also, data destined for pods might have to be mirrored for a while as a fallback.

Another concern is that the learners themselves might be overwhelmed by managing the plethora of data presented in Section 4. Currently available interfaces to SOLID pods (SOLID Tools and Libraries, 2021) at times appear to be more geared toward developers than actual users, however, it is expected that common usage paradigms across domains, including online shopping and social networking, will develop.

The user model, as well as a content model, are currently being prototyped within the openLCMS project at ETH Zurich. The hope is to have open-source prototypes in place by 2023.

8. Conclusions

The changing reality of our global society in general, as well as workplaces and higher education in particular, due to digitization may demand a new model of what a user is. This proceedings paper of the workshop Next Generation LMS attempted to outline approaches for supporting lifelong learning journeys, giving learners control and sovereignty over their various forms of educational data – which is the necessary consequence of one of possible futures of our understanding of personal data. Several of the necessary technologies are already in place, and connecting them is an engineering effort, but deploying this model will require a political effort.

References

Cachin, C.: Architecture of the hyperledger blockchain fabric. In: Workshop on distributed cryptocurrencies and consensus ledgers, Vol. 310, 2016, No. 4. https://www.zurich.ibm.com/dccl/ (last check 2021-04-13)

Ethereum: https://ethereum.org/ (last check 2021-04-13)

Gartner, L.: Public colleges are going after adult students online. Are they already too late? The Chronicle of Higher Education, Feb. 10, 2021. https://www.chronicle.com/article/public-colleges-are-going-after-adult-students-online-are-they-already-too-late (last check 2021-04-13)

Gräther, W.; Kolvenbach, S.; Ruland, R.; Schütte, J.; Torres, C.; Wendland, F.: Blockchain for education: lifelong learning passport. In: Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET). https://dl.eusset.eu/handle/20.500.12015/3163 (last check 2021-04-13)

Hammann, S.; Sasse, R.; Basin, D.: Privacy-Preserving OpenID Connect. In: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, 2020, pp. 277-289. https://doi.org/10.1145/3320269.3384724 (last check 2021-04-13)

Hyland: https://www.hylandcredentials.com/education (last check 2021-04-13)

Interfolio: https://www.interfolio.com/products/dossier/ (last check 2021-04-13)

Kortemeyer, G.; Dröschler, S.; Pritchard, D. E.: Harvesting latent and usage-based metadata in a course management system to enrich the underlying educational digital library. In: International Journal on Digital Libraries, 14, 2014, 1-2, pp. 1-15. https://www.springerprofessional.de/harvesting-latent-and-usage-based-metadata-in-a-course-managemen/11672798 (last check 2021-04-13)

Kortemeyer, G.: The Spectrum of Learning Analytics. In: eleed, 12, 2017, 1. urn:nbn:de:0009-5-45384 https://eleed.campussource.de/archive/12/4538 (last check 2021-04-13)

Kortemeyer, G.; Dröschler, S.: A user-transaction-based recommendation strategy for an educational digital library. In: International Journal on Digital Libraries (online first), 2021, pp. 1-11. https://www.springerprofessional.de/a-user-transaction-based-recommendation-strategy-for-an-educatio/18777642 (last check 2021-04-13)

LinkedIN Learning: https://www.linkedin.com/learning (last check 2021-04-13)

Mansour, E.; Sambra, A. V.; Hawke, S.; Zereba, M.; Capadisli, S.; Ghanem, A.; ...; Berners-Lee, T.: A demonstration of the solid platform for social web applications. In: Proceedings of the 25th International Conference Companion on World Wide Web. 2016, pp. 223-226. https://doi.org/10.1145/2872518.2890529 (last check 2021-04-13)

Nazaré, J.; Hamilton, K.; Schmidt, P.: Digital Certificates Project, MIT Media Lab, 2015. https://www.media.mit.edu/projects/media-lab-digital-certificates/overview/ (last check 2021-04-13)

OAuth. https://tools.ietf.org/html/rfc6749 (last check 2021-04-13)

OpenID Connect. https://openid.net/connect/ (last check 2021-04-13)

SOLID Project. https://solidproject.org (last check 2021-04-13)

SOLID Tools and Libraries. https://solidproject.org/developers/tools (last check 2021-04-13)

SOLID Vocabularies. https://solidproject.org/developers/vocabularies (last check 2021-04-13)

SwissID Project. https://www.swissid.ch (last check 2021-04-13)

SWITCH edu-ID. https://projects.switch.ch/eduid/ last check 2021-04-13)

SWITCHverify. https://www.switch.ch/de/verify/ (last check 2021-04-13)

TrustCerts. https://www.trustcerts.de (last check 2021-04-13)

Verbert, K.; Duval, E.; Klerkx, J.; Govaerts, S.; Santos, J. L.: Learning analytics dashboard applications. In: American Behavioral Scientist, 57, 2013, 10, pp. 1500-1509. https://doi.org/10.1177/0002764213479363 (last check 2021-04-13)

Yan, Z.; Gan, G.; Riad, K.: BC-PDS: protecting privacy and self-sovereignty through BlockChains for OpenPDS. In: 2017 IEEE Symposium on Service-Oriented System Engineering (SOSE), 2017, April, pp. 138-144. DOI: 10.1109/SOSE.2017.30 (last check 2021-04-13)