



AALBORG UNIVERSITY

STUDENT REPORT

Electronics and IT
Aalborg University
<http://www.aau.dk>

Title:

Decentralized Identity Verification System for International Students Academic Degree Attainment

Theme:

Identity Access Management Using SSI Concept

Project Period:

10th Oct 2021 - 28th February 2022

Project Group:**Participant(s):**

Mohammad Sayeem Chowdhury

Supervisor(s):

Henning Olesen

Copies: 1**Page Numbers:** 89**Date of Completion:**

February 28, 2022

Abstract:

A school database protects data. Most of these resources are inaccessible without interoperability. Students' opportunities are hampered by lack of academic control. An open self-sovereign protocol field for students is proposed. Personal data and identity control online is enabled by a set of technology standards and community-supported concepts. The SSI design system also gives students more control over their academic records. SSI also checks academic records. Its growing popularity may also help institutions recruit qualified international students. The verifiable credential has also raised student rights and privacy awareness. We have always prioritized user privacy. International universities benefit from SSI technology concepts that expose system flaws. The SSI system concept can also handle data over-release and record blocking. This report addresses the issue by demonstrating SSI standards and technologies. Adopt and test findings after considering specific principles and technologies. This report will also look into individual data control. Individuals and users refer to students seeking an internationally recognized degree.

The content of this report is freely available, but publication (with reference) may only be pursued due to agreement with the author.

Contents

1	Introduction	3
1.1	Report Motivation	3
1.2	A Synopsis of the Situation	4
1.3	Scenarios as a Tool for Communication	5
1.4	Classification of forgeries	5
1.5	Reputational damage	7
1.6	Complications in the global verification system	7
1.7	Forgeries: Internal and External	9
1.8	Lack of trust	10
1.9	Problem Formulation	11
1.10	Delimitation	12
1.11	Methodology	12
1.11.1	Research Developments: Requirement Specification	13
2	Evolution of Identity Management in the Digital Age	15
2.1	Identity management issues in the digital age	15
2.2	Identities	17
2.3	Digital identity management development phases	18
2.3.1	Centralized identity	18
2.3.2	User-oriented identity	20
2.3.3	Federated identity	21
2.3.4	Self-Sovereign Identity: a new way to manage identity.	22
3	State of Art: Recent Developments	27
3.1	Standardization of technology and establishment of technical foundations	27
3.1.1	Verifiable Credentials	27
3.1.2	Verifiable Credential Data Model	29
3.1.3	Verifiable Credential Proof Mechanisms	31
3.1.4	Comparison between Linked data proofs and JSON Web Tokens	32
3.1.5	Advanced proof mechanisms	33

3.1.6	Zero Knowledge Proof and BBS+ Signatures 2020 Draft Specification	33
3.1.7	Decentralized Identifiers	35
3.1.8	Distributed Ledger Technology (DLT)	36
3.1.9	DIDComm	38
3.1.10	Decentralized Verifiable Data Registries	39
3.1.11	Comparative study of credential hosting services	39
3.1.12	Privacy-preserving Credential Status	40
3.1.13	Digital Wallet	41
4	Questionnaires and Analysis	43
4.1	How SSI can apply to design an IdM	43
4.2	Benefits of using SSI for verification system	44
4.3	Scenario-based SSI	45
4.4	Discussions with Experts: Q&A	47
4.4.1	Questionnaire formulation	47
4.4.2	Surveys purpose: Inquiry-based methods	48
4.4.3	Q&A: Analysis	49
4.5	Existing admissions procedures in foreign institutions	50
4.6	Expected risk of using existing verification system and responses . .	51
4.6.1	Expected Risk	52
4.6.2	Discrimination	53
4.6.3	Manipulation	54
4.6.4	Over Disclosure	54
4.6.5	Tracking	55
4.6.6	Vendor Lock-In	55
4.7	Response Analysis	56
4.7.1	Verifiable Credentials	56
4.7.2	Decentralized Identifiers	56
4.7.3	Decentralized Verifiable Data Registries	57
4.7.4	Privacy-Preserving Credential Status Check	57
4.7.5	Personal Data Stores	57
4.7.6	Selective Disclosure	58
4.7.7	Elective Computation	59
4.7.8	Progressive Disclosure	59
4.7.9	Embedded Identity Proofing Attributes	60
4.7.10	Data Minimization	60
4.7.11	Information Fiduciaries	61
4.7.12	Governance Frameworks	61
4.8	Security Challenges	61

5	Conceptual Design Proposal	63
5.1	Stage one: Using DID to establish identity	63
5.2	Stage two: Channel between institution and student	64
5.3	Stage three: Presenting academic records in credential form	66
5.4	SSI's Functional aspects and interaction between entities	68
5.5	Setting up Scenario to create confidence between entities	70
5.6	SSI for Student's Academic Record System	71
6	Conclusion	73
	Bibliography	75
A	Questionnaires	83
B	Experts' Talk	85
B.1	Conversation with Eva Marie Althoff Schäfer	85
B.2	Conversation with Mr. Ziarat Hossain Khan	86
B.3	Conversation with Mohammad Tanvir Hossain	88

Chapter 1

Introduction

Students' records are secured within their institution's proprietary database system. The majority of the time, these documents are inaccessible and non-portable due to the lack of an interoperable standard. Students lack control over their records and diploma achievement, resulting in less access to utilities, fewer choices, and diminished equity.

1.1 Report Motivation

The report focuses on developing a management system for verifying international students' domestic degree attainment and on the establishment of a field of open self-sovereign protocols for learners. The term self-sovereign is derived from self-sovereign identity (SSI) [87], a set of technological standards and community-supported principles that enable greater online control over an individual's personal data and identity [58]. The SSI design system enables institutions to examine and restructure their existing systems in order to make them more collaborative and interoperable and to give students greater control over their educational records. Simultaneously, SSI ensures the veracity of the current academic credential. The increased importance of the SSI system may give students a greater degree of control over their degree credentials and advance institutional initiatives for selecting appropriate international students for admission [91]. As a result of Covid-19, interest in portable, interchangeable, and verifiable credentials has increased significantly [66]. Not only that, but the immune credential has also drawn attention to the importance of adequately protecting students' privacy and rights. While SSI is not a panacea for all problems, users' rights and privacy have been a primary focus of SSI since its inception [21], [72]. SSI technology concepts assist by providing critical and valuable insights into system flaws and aid in the improvement of the verification system for students seeking admission to foreign universities. Not only that, but the SSI system concept can also be sufficiently

present to address the issue of disclosing more information than necessary and preventing record tracking [73]. To improve the overall system and mitigate the associated risk, stakeholders should implement these system concepts and apply the ICT tools and principles discussed throughout the report.

- A **verifiable credential** is a mechanism that verifies the cryptographical reliability of a credential issued by any institution. Institutions or asserting parties stand behind the statements contained in it and reserve the right to revoke or suspend the credential's validity status if necessary.
- **Decentralized Identifiers:** Establishing an identity serves as a conduit between institutions and students that is free of interference from centralized parties.
- **Privacy-Preserving Credential Status:** monitoring the credential's current status without disclosing additional information about an individual's personal information.
- **Selective Disclosure:** allows an individual to share only a portion of the complete information.
- **Data Minimization** is a technique for requesting the bare minimum amount of information necessary to complete a transaction.

This report details how implementers and stakeholders can begin utilizing the technical details of the SSI standards and technologies mentioned previously to address the problem outlined in the problem formulation. Before applying and testing for findings and sharing with the broader SSI community, implementers of the SSI management system and other stakeholders must consider these principles, technologies, and guidance. Additionally, this report will discuss the risks, opportunities, and community guidance for achieving individual data control. It is critical to emphasize here that the terms 'individual' and 'learners' refer to students in the context of this report or to any individual life-long learner attempting to obtain an internationally recognized degree by simultaneously presenting self-controlled academic records to multiple institutions, frequently as a learner or as a career instructor in foreign universities.

1.2 A Synopsis of the Situation

Each year, thousands of international students travel abroad to pursue higher education, and they submit educational documents from their home countries through an application portal. All documents were scanned manually, and the only identity they verify prior to traveling abroad is the individual's citizenship via their

passport at the immigration offices. However, there is no (circle of trust) or Identity Provider to authenticate students' accomplishments in support of the relying party's assertion that the local educational degree or qualification is valid. According to research, the majority of applications from numerous large students are frequently embellished with extra activities, features, and forgery [88]. As a result, thousands of international students worldwide are admitted to the renowned university and quickly processed through the immigration and admissions systems based on transcripts, educational records, and recommendation letters from institutions that lack authenticity. Australia and the United Kingdom are grappling with admissions fraud and have taken steps to reform the traditional system in recent years [3]. At the moment, the United States of America and Canada are both dealing with diploma forgery [28]. Another statistic demonstrates that the English language proficiency test score is highly unreliable and utterly useless in some cases [59]. Additionally, the data indicates that students are willing to pay a high price, ranging from 20,000 USD for the LSAT required for admission to a US law school to 60,000 USD for access to an Indian medical school [13], [43]. According to evidence, it costs \$1,000 to provide forged documentation for visa applications in Canada and Australia [62].

1.3 Scenarios as a Tool for Communication

To help students achieve their goals, this report describes one user scenario that demonstrates the value of interoperable, individual academic records to various institutions and job market. The scenario first outlines how verifiable and interoperable academic records can be used to identify meritorious students for domestic and international admissions. [Figure: 1.1] This facilitates students' integration into academic institutions and enables them to establish satisfaction with their degree attainment.

Through the use of scenario it was also demonstrated how students can obtain employment in both the public and private sectors by presenting these unique academic records. For employees, it fosters collaboration among coworkers and accelerates progress toward a more satisfying work experience. Again, it directs employers' advance power toward finding efficient applicants.[Figure: 1.1]

Using the scenario as a guide, this report discusses how SSI initiatives can help ensure the ongoing verifiability of students' academic records while also empowering them to manage their own data.

1.4 Classification of forgeries

The rise of fraud over the last decade can be classified into four critical factors.

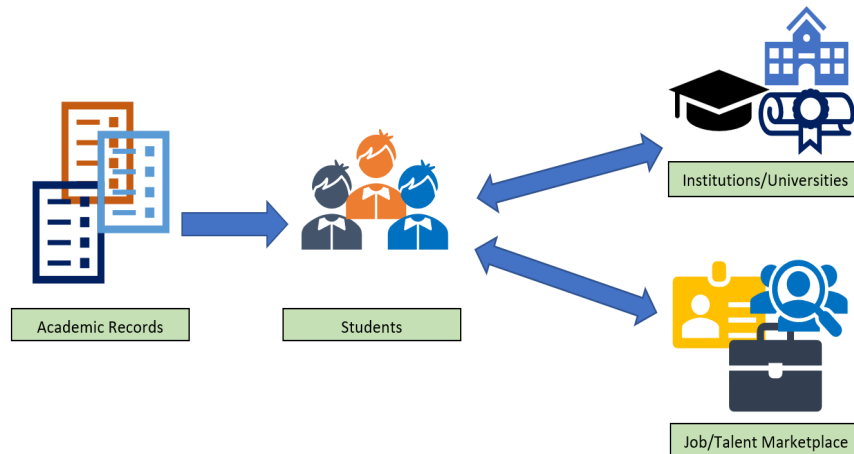


Figure 1.1: Using scenarios to portray academic records to third-party stakeholders

- **First**, the high demand for higher education study spaces creates an imbalance in educational quality, motivating students to increase their chances of admission to education spaces through illegal means. This behavior is more visible in the case of international students because it enables them to validate their accomplishments, which motivates them to win the prize.
- **Second**, as Asia's and, more recently, Africa's economies grow, applicants from populous countries generate high application forgery and admission behavior rates. And the manner in which fraud is infiltrating the mainstream of international education.
- **Third**, the widespread availability of web-based tools and content, combined with the assistance of mobile technology, significantly reduces the transactional constraints on fraudulent behavior. Using Photoshop to create papers that are sold online and used in smartphones for fraud testing and other wireless technologies encourages students and applicants to commit fraud. This also raises awareness and prompts institutions and testing agencies to take countermeasures.
- **The final and fourth drivers** are based on tacit agreements with specific stakeholders who place a premium on the economic contribution of international students over the integrity of their educational profiles, admissions systems, or institutional reputation and brand value. The incentive is reasonably self-explanatory - money.

1.5 Reputational damage

Another critical component is to examine test results for evidence of fraud or fraudulent activity. Those recruited to take the test, deploy technological devices, or participate in large-scale memorization of illegally obtained test documents, resulting in identity fraud or a breach of the company's internal testing system. As a result, language test results in several Asian countries have developed a reputation for being notoriously inaccurate. Language tests must typically be retaken to review students once they arrive on campus at most reputable universities. This list could include anything from cheating in class to manipulating study visas in order to enter a country solely for the purpose of finding work [17]. Generally, the primary motivation for committing fraud outweighs the ordinary penalties. It is frequently viewed as a necessary act for the purpose of entering specific countries. When diploma forgery becomes more prevalent, the long-term consequences must be considered or addressed. This is because, in the end, the outcome is always a loss for everyone. To elaborate on that point, students who cheat their way into foreign programs frequently face an insurmountable amount of work that exceeds their ability, resulting in unmeasurable and significant fraudulent activity to complete their degree, which is not properly educated. Ultimately, this harms employers who place a high premium on the quality of specific programs. Additionally, tutors and institutional education providers frequently face challenging situations when dealing with cases of unequal treatment of students. The latter of the two causes is rapidly spreading through the media, creating unease among faculty members due to numerous conflicts. Based on anecdotal evidence, employers frequently respond negatively to international students' lack of quality during the task procedure of getting hired. When universities and institutions that provide statements about students (certification or recommendation letter) fail to address the fraud risk adequately, they frequently put themselves in the position of jeopardizing the brand reputation they built a century ago and continue to build.

1.6 Complications in the global verification system

Without any identity providers in most developing nations' present local educational system, some testing service providers give additional lip services that compromise identification and engage in fraudulent conduct, putting them at odds with the educational system. When educational institutions seek new verification schemes, they overlook these companies' existing unreliable offerings. If they have not already done so, local and national education systems will lose their credibility and reputation. Many students sending countries from Africa to Asia have placed little trust in their portfolios' legitimacy. On the other hand, Australia and the United Kingdom were early adopters of complicated policy frameworks to

combat visa and immigration fraud [20]. Now, the focus has shifted to Canada's and the United States' governmental and institutional responses [26]. Regrettably, there is no simple solution to the problem of admissions fraud in the international educational system. Several facts are associated with it, including the economic imperative and motive of stakeholders, a loss of control over the handling of technical measures of fraud, a lack of ICT tools for mapping and measuring fraudulent activities, an abundance of opportunities for forgery, and cheating on admission by manipulating existing mechanisms. Previously, specific actions were taken periodically. Stakeholders agreed that forgery is the spread of a word, and the failure to act harms a person's reputation and merits. It is also applicable to institutions of higher education that maintain relationships with employers and alumni. Due to the wide variation in culture and the economic situation between countries and institutions, a more comprehensive and unified measure of cross-campus action is necessary to address the impact of fraud. Additionally, educational institutions and language test providers must work cooperatively to prevent documentation forgery and quantify fraudulent activity to design effective countermeasures. Without adequate justification, there is a risk of admitting a student with insufficient documentation. Additionally, chances occur as a result of an institution refusing to accept a student who submits an authentic, official credential. Neither the international admissions recruiter nor the academic credential evaluation specialist wishes to promote or reward academic credential fraud. They must be fair, ethical, and adhere to sound policies that prohibit the use of deception.

The question that needs to be answered is

- How we can all learn about the international educational system?
- What academic credentials a student receives upon completing secondary education? or
- How a local student can enroll in a foreign university outside of their country?
- How would the verifier know what an academic credential looks like in Mozambique, Bangladesh, or Nepal?
- When the certificate is presented, what official language does it contain?
- Is the resource current with the educational course being submitted by the student?
- Has the foreign university established a human resource department and a global network to assist them in the event of a problem?

1.7 Forgeries: Internal and External

Today, gathering verifiable information is critical, but maintaining current and accurate information is more critical than ever. Forgery can occur on both the **internal** and **external** sides.

Dishonest behavior by an internal employee who already possesses a trust identity from the academic institution occurs on a small to large scale. Even so, when it occurs, it has a ripple effect throughout the institution. When information about identity fraud from an institution becomes public, it tarnishes the institution's good name. Not only that, but it also jeopardizes the genuine students who have graduated from that institution and are not involved in that heinous activity. Once one's reputation has been tarnished, it takes a long time to rebuild the public trust required to maintain Memorandums of Understanding (MOU) with the outside world and foreign universities. Modifiable credentials are available through the internal admissions office. Several examples include the incident at Touro College in New York City [16]. Numerous academic members accepted bribes from students to alter their grades and then sold the credential to outsiders under the institution's name. Finally, the fraud was reported and the involved students' and outside buyers' credentials were revoked. Such incidents in local institutions also result in significant losses for foreign institutions when students or non-students acquire credentials through other illegal means and are admitted to higher institutions to obtain a professional degree or to work in the country. Both ways, when forgery is discovered after the admissions process, the academic year is lost, and foreign universities do not receive proper students who have the merit and all authentic credentials to study for higher achievement in their field. As a result, many developing countries annually lose intellectual productivity from their bright students. Another incident occurred at LA Southern University in Baton Rouge [2]. Students paid the admissions office for eight years to change their grade and educational history to conform to the application's requirements. So that they may apply for admission to a higher degree program at another institution. That incident impacted a total of 2500 individual grades.

External fraud is more common than internal fraud. The fraudster does not require additional resources such as professional printing equipment to create forged documents with the aid of internet tools and modern graphics technology. Nowadays, the internet enables the creation and printing of a variety of documents for diploma certification and student records while maintaining the institution's name. Additionally, some providers send the counterfeit documents in an envelope bearing the institution's name as the return address, which gives the counterfeit documents a more authentic appearance. Numerous fraud providers even provide additional verification methods to justify the documentation they provide in order to ensure its authenticity. Counterfeiters use the name of a local educational in-

stitute to offer documentation and records to students and create a website based on the institution's information in order to deceive the verifier on a primary level. Any document, including student records, that is printable can also be modifiable and available for sale. The recent expulsion of a large number of Chinese international students from Stony Brook University exposed the scam that lures many students in exchange for a guarantee of admission to the country's top graduate schools in exchange for thousands of dollars. According to a Statesman investigation [40], seven students were expelled from Stony Brook University after submitting a forged transcript with their graduate school application. However, these students claimed that their records and testimonials were forged without their consent by outside firms promising to secure their admission to their desired graduate school. On the contrary, Stony Brook officials stated that they had no intention of investigating outside firms when students visited them voluntarily. Following that incident, one of the actions taken was to educate students about academic integrity and how to avoid becoming vulnerable in a similar situation in the future [15].

Employing consultants to assist with college and university admissions is also quite common in developing countries. According to a 2011 survey conducted by the University of Iowa, nearly 87 percent of students from South Asia who come to the United Kingdom, the United States of America, and Australia for higher education use a consultancy firm to assist them with their application in accordance with the university requirements [9]. While many of these consulting firms work on behalf of students to provide legitimate services such as matching students with the appropriate universities based on their profiles and scheduling interviews with admissions offices. Others obtain the result through deception and forgery. They prey on students with a lower grade point average and promise them admission to a top-tier foreign university regardless of whether they meet the university's admission requirements [12].

1.8 Lack of trust

Without identity access management, the credentials that a local institution issues to students for submission to a foreign university must undergo a rigorous examination process to determine the authenticity of the documents submitted manually or digitally. Several of these measurements include a check of the degree paper for that specific country, a check of the institutional stamps and seals for legitimacy, and a check of the time period for the embossed logo on the credentials if it changes. Other actions include verifying the signatures and seals on the degree certificate or recommendation letter and the vocabularies included in the credential, such as font, text layout presentation, and course title for the specified time period. To continue with the existing system's vulnerabilities, the report will examine the fundamentals - signed international admission documents and the stu-

dent's educational history — correlating biographical information with statements included in the educational diploma. Numerous academic credentials include the complete date of birth and, in some cases, the city of birth of the student, which can be analyzed to fill in the gaps of unexplained educational history. Additionally, it is critical to justify chronological academic history by ensuring that each degree or diploma awarded by the local institution follows the standard timeline for that system. It fills in any gaps in admission requirements caused by missing documents. However, trust is the primary issue. For example, understanding the students' home institution of study and the basic credential it provides is critical when admitting an international student to a higher degree program. What is the authenticity of the institution's name as it appears on the credential, given that the institution frequently changes its name? Numerous institutions in the former Soviet Union, for example, have changed their names. Additionally, many local institutions in China offer academic credentials that can be translated into English in various ways, all of which are acceptable in the region.

1.9 Problem Formulation

Learners have no control over their records and have no say over who has access to their data or when they can access them. There is no mechanism for learners and issuers to verify their identities online.

Therefore, the problem formulation is as follows:

How to design an identity management system for verifying International Students' domestic educational records submitted to foreign universities, emphasizing students exercising control over their credentials.

This project aims to describe the technical details of SSI standards and technologies to contribute to the development of forward-thinking technologies that protect students' privacy and control over their personal data records.

This research question has a number of subquestions, which are detailed in the section that follows. Each of these sub-issues/questions points to a significant location that aids in the formulation of the broader problem. Resolving the central research question also leads to a better understanding of the issues and problems that need to be addressed:

- How to decentralize identification for entities that use the credential throughout the VC lifecycle?
- How to build a bridge between an academic institution and a student to earn a graduation credential and use it?

- How to present academic credentials?

1.10 Delimitation

Beyond the scope of the SSI

Throughout this study, the broad phrase "SSI-based approaches" will be used to refer to critical SSI vocabulary and concepts. This is because, as mentioned in the State of the Art Chapter's "Short Introduction to SSI," the term "SSI" may refer to a collection of technologies and principles that are neither fully developed nor in use. This means that the term "SSI" should not be interpreted literally. Terminology is a problem since the breadth of SSI-based procedures is so broad that they do not provide full answers to a large number of queries. This study highlights the legislation that governs student privacy and access rights, as well as access to student academic records, by focusing on real-world implementations of student academic records. Other technology parties can help pilot project partners and implementers collect and disseminate this information in this area. These parties are detailed in the report, including a brief explanation of themselves and comparisons to other similar parties, in order to provide a full picture, and several of them are also used as bridges to accomplish the object goals specified in the problem statements.

1.11 Methodology

Section 1.1's stated objectives necessitate four steps: gathering theoretical background, devising solutions, building a conceptual layer and setting up an evaluation scenario (see Figure 1.2). According to Mark's study [10], a range of business and information systems engineering approaches were used to achieve this. As a result of reading published articles and books, a theoretical framework is developed as well as a foundation that may be used in all subsequent phases of research.

Research on the topic of self-sovereign identity, decentralization of identity, and verifiable credentials was conducted using Google Scholar and the Aalborg University Library Catalogue, as well as Van's [61] complex query "SSI-academic-student-degree-diploma-employment." and following subsequent queries:

("Self-sovereign identity" OR "SSI ").

OR (

("Decentralize" OR "ledger")

AND ("identity management system" OR "idm")

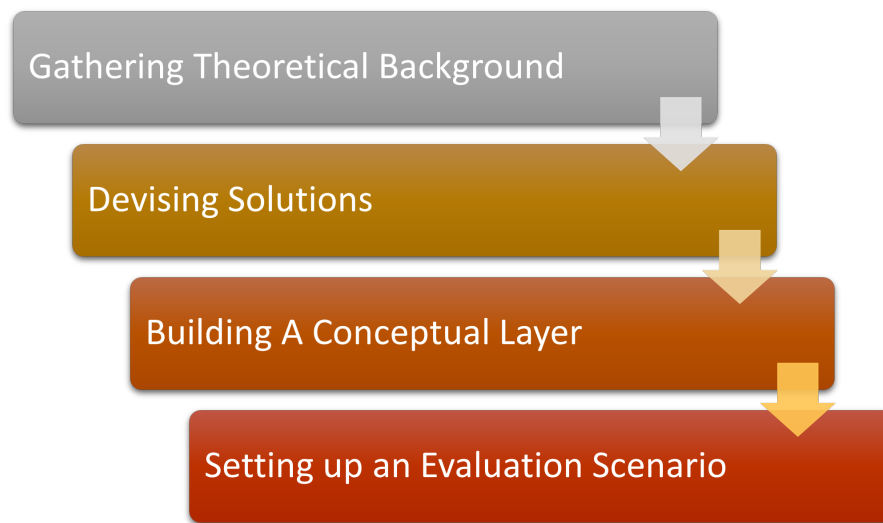


Figure 1.2: Method of investigation

AND ("solution" OR "design" OR "literature review" OR "poll" OR "questionnaire")

AND ("verifiable credentials" OR "did" OR "dvdr" OR "data registry")

)

In addition, data is gathered through cross-sectional research, typically in the form of expert surveys. Questions are used to evaluate not only the solution overview but also to establish what is needed to meet a student's specific needs. Learn more about the expert selection process and questions in Chapter 4. The structural design is created using a combination of reference modeling and prototypes. Both allow for the production of a design prototype that accurately depicts a specific problem and can be used in conjunction to find new knowledge. This is a fascinating thought to ponder when it comes to designing the evaluation scenario. The [14] has defined the term "real-world artifact" as a component of design science, and this thesis falls under that definition.

To summarize, the subsequent research topics represent a synthesis of the previously disclosed studies and methodologies that have been utilized. Listed in the form of separated sub-questions, they follow the problem formulation.

1.11.1 Research Developments: Requirement Specification

Initial project milestones include a "Technical Requirement Specification" and "Evaluation of the Existing Situation." For this, one needs first obtain high-level "Analytical" - domain knowledge - understanding and comprehension before evaluating

the current state of the art. A thorough examination of the fictitious system's fundamental capacities is required here, in particular one will be able to evaluate the current state of the art in the field by examining each of the study questions provided in Section 1.9. This work is all about gathering and assessing important information that can help solve research problems.

The 'Collecting requirements for participating entities' phase can be started after what is practicable is determined, and this should lead to the construction of an initial definition of the participating entities' entity requirement. The development approach will be guided by user scenarios and past study on how the projected system will be utilized. Potential students are prohibited from participating since the advantages are so minor. Based on these circumstances, the system's usefulness could also be limited.

Chapter 2

Evolution of Identity Management in the Digital Age

The identity of a person, whether digital or analog, is composed of a sequence of individual identities. If a user requires Internet access, he or she may do it through the use of one or more partial identities. There is a possibility that some of the information contained in each partial identity overlaps with that contained in other partial identities [see figure 2.1]. These partial identities are frequently employed in daily life, necessitating the usage of a mobile digital identity, compatibility with several systems, and user maintenance of the partial identities. The name, home address, and academic credentials of an individual all contribute to their job identity. It is conceivable to own multiple distinct partial identities. A person may assume a variety of distinct partial identities depending on the circumstances [6].

2.1 Identity management issues in the digital age

Due to the exponential growth of digital interactions in the digital age, identity management is critical. Physical systems are only partially or completely digital. It is critical to adapt physical identity management systems' advantages to their digital counterparts. Through digital identity management solutions, users can share their identities with third parties (DIMS) [6]. In the analog world, identity is routinely verified via an ID card, passport, or driver's license. In today's digital age, this is impossible [67]. Historically, physical identification certificates were protected by difficult-to-forge qualities and photographs. Traditionally, users' online identities were managed through the creation of domain-specific user accounts that were accessible via username and password. This is not always true. Each user account requires its own unique username and password. Due to the ease with which password management may be accomplished, it is fundamentally unsafe. For instance, each of the twenty accounts [67] uses six or seven different passwords.

Often, a single password can be used to access many services. As a result of the identification, third parties are more likely to profit from it. Password organizers and notes can assist you in keeping track of several passwords. Using numerous passwords makes access control more difficult. In either instance, the user must spend considerable effort or be very aware of the security concerns associated with the assaults. Internet-based identity-related data cannot be used across domains. Registration with multiple service providers is time consuming and costly. As a result, users' identities are limited to the context of the program they are currently using. Frequently, the data and information obtained are irrelevant or useless [29] outside of the context in which they were collected and thus cannot be used.

Access to basic essentials such as health care, social security, education, and financial services is taken for granted in the Western world. Despite this, over 1.1 billion individuals worldwide lack identification and are unable to access essential services. Individuals can participate in society on a more equal basis using digital IDs, which could help remedy this problem [46]. Today's international students require more than the current generation of digital IDs [89]. These issues were classified into four categories:

- 1.Ownership and Governance of Academic Credentials
- 2.Authentication with a password
- 3.Identity Data in Selective Form
- 4.Forgery of Credentials and Identity Fraud

Students lack control over their academic credentials as a result of not possessing them. Recruitment agencies and consulting organizations benefit from this by amassing data on students in order to customise advertising space on connected markets. Additionally, a lack of control implies that agencies, corporations, and local institutions have the ability to refuse students access to their credentials at their discretion. Password-based authentication presents a security risk as well, owing to the widespread usage of weak passwords, which might result in identity theft. To avoid academic records being misused, students must create unique and complicated passwords for each of their credentials, which is difficult without the use of a password manager. Dashlane study indicates that the typical client manages 147 passwords [34]. While such tools simplify password management, they may fall short of adequately protecting users against security concerns[evaluation, adapt, defenses]. One-time passwords, which enable users to sign in to many services using their Google account, can help alleviate this issue, but they also create dependency and centralization. Third, identifying data is dispersed across multiple agencies and identity suppliers, complicating maintenance. Duplication, mistakes, and out-of-date data sets are widespread as a result. Additionally, the absence of

open standards impedes interoperability between providers, which might be used to retrieve, relocate, or delete sensitive data. These programs, which have been ongoing for more than four years [22], [25], [81], are being accused for further lagging small competitors [48], [89].

2.2 Identities

What is a human's essence? That person's name, gender, home town and occupation are likely to be mentioned, as well as philanthropic and political affiliations. In his work Identity management and its support for multilateral security, Sebastian [6] explains that a person's identity is made up of many partial identities. So, depending on the situation, it takes one of its many partial identities, each of which symbolizes the individual as a human being. For example, a partial identity for health care includes medical history, but a partial identity for work includes certificates. Some information may overlap, therefore these distinct components of identity are not usually addressed individually. Notably, an individual choose whatever information to share with which party and when. Figure 2.1 depicts a person named Alice as an example of partial identity.

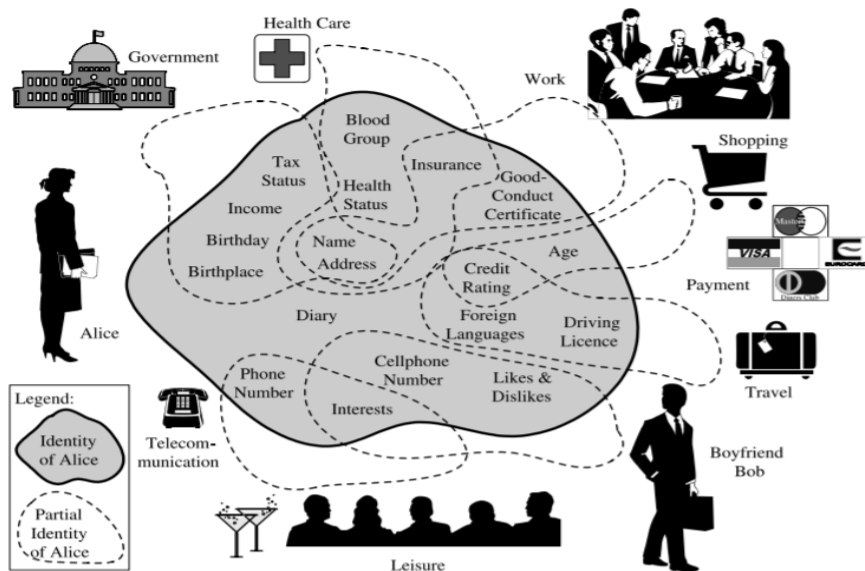


Figure 2.1: Partial Identities (Source: [6])

It is critical to strike a careful balance between maintaining confidentiality and delivering necessary information to the other side. While kiosk merchants should not request personal information for water purchases, age verification is a valid justification for giving personal information for liquor transactions. While official

evidence, such as a state identification card, is usually used to verify an individual's identity, non-official documentation, such as a customer card, may also be used. Due to the fact that the documents are in the user's possession, they can be shown only to the individuals they choose, at their discretion. Additionally, official identification documents are developed and standardized to assure the best possible level of security and interoperability. Other countries can authenticate the authenticity of these documents simply by inspecting them, without contacting any authorities directly. The verifying party's belief in the issuing authority is what provides them with confidence in the data's legitimacy [90].

Numerous procedures have been migrated to the digital sphere as a result of the rising digitization of many parts of our life. Digital services are increasingly relying on digital identities, which are theoretically identical to physical ones. They enable entities, like as persons or things, to verify their identity online through the use of unique characteristics [19], [23]. Kim [11] defines digital identity in greater depth as "a collection of statements made by a digital subject about itself or another digital subject." Claims, which are defined in this context as "An assertion of something's truth, typically one that is contested or contested," can be used to express the aforementioned characteristics of a digital subject, which is defined as "A person or thing represented or existing in the digital realm that is described or dealt with." The issue is that analogue identities and their associated documentation frequently lack or lack widely accepted digital representations suitable for use as digital identities [8], [33]. As a result, the patchwork of unique identities discussed in this chapter is distinct from digital identities based on the originals. For the convenience of the reader, the study detailed the various stages of developing a digital identity below [24], [90].

2.3 Digital identity management development phases

In today's digital world, there are numerous methods for managing one's identity. Allen's work has been cited in over 200 titles [24], according to a Google Scholar user query based on his work [24]. Allen believes that since the inception of the Internet, the evolution of online identities, or digital identities, has been a four-stage process. Self-sovereign identities evolved as a result of the following developments: centralized identities, user-oriented identities, federated identities, and self-sovereign identities [24], as depicted in the Figure: 2.2

2.3.1 Centralized identity

Administrators, for example, are responsible for unified identities that span the entire system. Their true identities are inextricably linked to that of the user. Only the appropriate entity has the ability to delete an identifier, which complicates user



Figure 2.2: Development phases of digital identities

monitoring and increases the risk of misuse. Interoperability is often threatened when relying on a single institution. Due to the impossibility of sending the user's identity, another service must generate it. Additionally, the central organization can track users' interactions with the system. Data storage is redundant since it is not synchronized and hence may become out of date fast.

A centralized identity is one that is produced and maintained by a single organization or institution (see figure 2.3). In 1988, the Internet Assigned Number

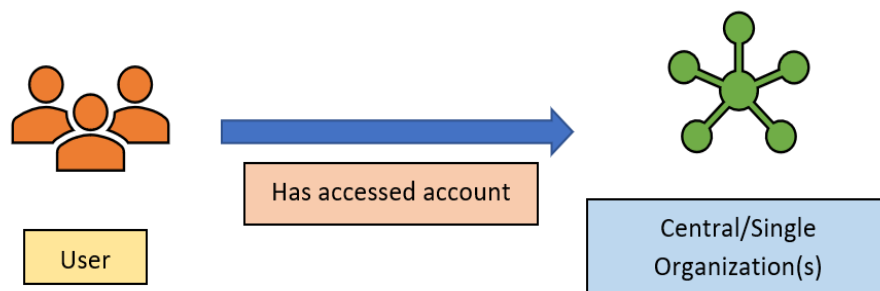


Figure 2.3: Identity in a centralised context (Source: [86])

Authority was established; in 1998, the Internet Corporation for Assigned Names and Numbers was formed; and in 2000, the Certificate Authority (CA) was formed to monitor SSL certificates. The hierarchical structure of an SSL certificate is readily seen in a browser, particularly the latter. To illustrate, the root authority enables another organization to govern its structure while yet exercising complete command and control. This is critical for a multitude of reasons. The identity of a person can be entirely controlled, with the power to delete or create a false one at anytime. As a result, either intentionally or inadvertently, a hack may result in the latter. Recent incidents [18] have demonstrated the vulnerability of central authority and, by implication, the entire hierarchy (chain of trust). Due to the absence of an identity layer, all internet-based services have centralized their operations. A fantastic illustration of this is the amount of accounts necessary to access various

services by a typical internet user. Personal information is once again out of the public's reach [24].

It's not just passwords that the user has to remember. Although this is a problem for the services, they are required by law to safeguard a vast amount of personal information. However, this has advantages in that the services can operate more autonomously and without third parties while maintaining complete control over their data [90].

2.3.2 User-oriented identity

The term "user-oriented identity management" was coined to address the shortcomings of traditional, centrally administered identity systems. Users have complete control over their access to a range of services (and thus their partial identities). However, passwords can be used for a variety of purposes, and account information may be difficult to transfer to other websites, posing security and usability concerns. Individual identifying characteristics (such as a legitimate job or driver's license) must be established on a regular basis for each service. Due to a local application that collects and manages access data for many services, users can use a single password to access several services (or authentication step). On the other hand, the supplier maintains a record of the attributes of their fictitious identities. They can also be used in other online services due to their shared nature [24], [29].

As a part of user-centric identification, the goal is to eliminate the need for federations and give users the ability to take control of their identities across a wide variety of organizations [24]. This is made possible by eliminating the need for federations and integrating an online identity directly into the design of the Internet, as Allen [7], [24] points out. People's digital identities were at the heart of their mission. As part of their digital identity, people have the power to choose what data is collected and who gets access to it. Microsoft Passport and Liberty Alliance Project were too business-oriented and focused on information privatization for Jordan's preference in 2003, he said [7]. They feel their digital identities should be a public good rather than a private benefit since private corporations' financial aims may be different from those of society.

Many new organizations and activities have been born out of these ideals. The Internet Identity Workshop (IIW), a major player in this field, was founded in part because to the efforts of the Identity Commons and the Identity Gang. User-centric identification is defined by the IIW community, which is represented by open standards such as OAuth (2010), OpenID Connect (OIDC) (2014), and OpenID 2.0 (2006). User permission and interoperability, ideas that were either absent or impossible to achieve in earlier models, are summarized by Allen [24]. As a result of the rise of social logins from firms like Facebook and Google, these

approaches have also proved successful [86]. The basic concept of user-centric identities couldn't be expanded upon. They have complete and entire control over the system because the SSO providers who register them have the identification data. Here's an example of how an IDP user operates as a go-between for other companies and the IDPs they're trying to access (see Figure 2.4). An example of a

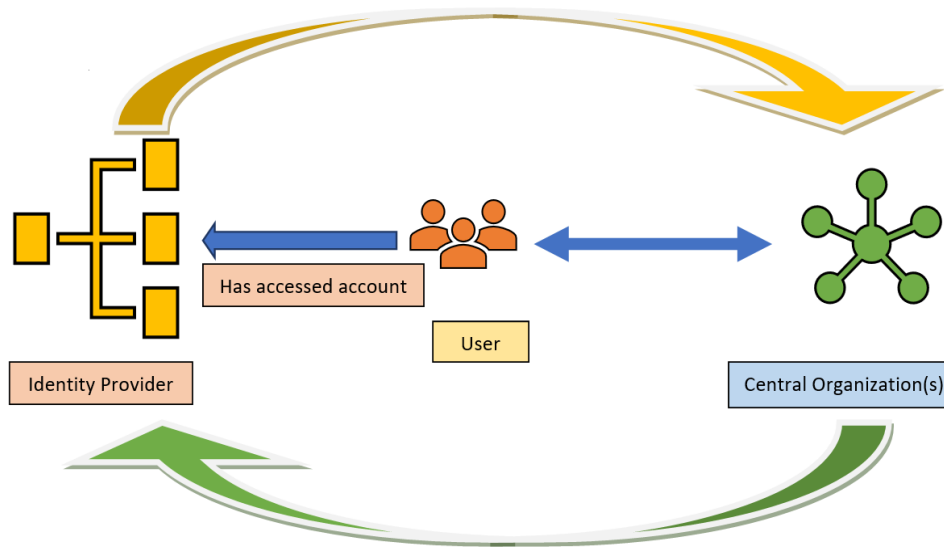


Figure 2.4: Identities centered on users and their relationships (Source: [86])

system that allows users to set up their own OpenID provider is OpenID, which Allen [24] points to as an example. However, this strategy is rarely used in practice due to its complexity. It is because of these issues that user-centric identities are unable to address the basic concerns for which they were designed. Despite the fact that user-centric identities are now merely interoperable, some literature fails to make the distinction between federated and user-centric identities [24], [86].

2.3.3 Federated identity

When it comes to digital identity, federated identity management is the next logical step in the process. Users can share their partial identities with other service providers by logging into a centralized log-in point. Single sign-on (SSO) is the corporate term for this notion, which is widely provided by companies and social networks like Facebook and Google. By using single sign-on (SSO), users can quickly and simply change their identities across several services. Data transfer is required to maintain a connection to the central log-in service. The disadvantage for the user is the reliance on the log-in service as the source of identity. Additional to this, the central log-in server is responsible for all partial identities and is always

able to track which services are visited by users logged in via partial identities. The risk of identity theft increases significantly if unauthorized individuals obtain access to the central login service's access data. Access to all linked partial identities may be granted as a result of the service's existence. A lack of interoperability and reliance on third-party vendors have resulted in the present systems for managing digital IDs. Today's identity management systems and user needs have not yet been addressed by a widely adopted solution.

As part of the second phase of growth, federated identities were developed to eliminate power structures built around a single authority. Multiple business groups came up with this approach for dispersing control among federated authorities. It was Microsoft's Passport project, which debuted in 1999 and offered a federated identity that could be used across several sites, that paved the way in this area. Even so, Microsoft's control over the federation was compromised in order to achieve this uniformity. Liberty Alliance Project, which was launched in 2001, aimed to build a genuine Federation of many companies that shared control. As a result of this totalitarian system, users lost all control over their data. In the end, the sites' authority was preserved [24]. Using digital identification eliminates

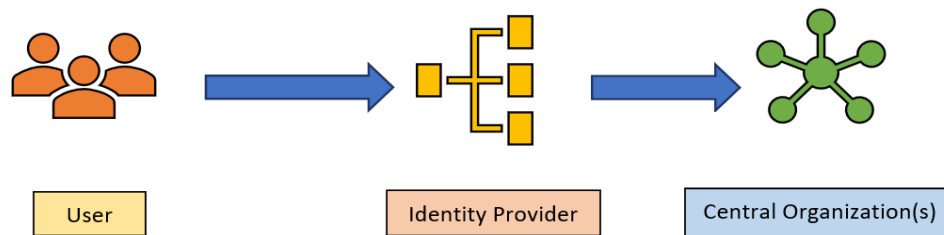


Figure 2.5: Identity in a federated management context (Source: [86])

the need for users to manage several identities and accounts for various services, while also reducing the administrative costs for businesses. Logging onto another federation service requires users to first get in touch with their data's issuer and owner, an identity provider (such as Microsoft). As a result, the user has no control over their data and is completely reliant on the identity provider's continuous existence (see Figure 2.5). IDPs collect data from numerous sources to develop profiles of its users, which can cause a slew of issues [75].

2.3.4 Self-Sovereign Identity: a new way to manage identity.

SSI has evolved in recent years to address the issues outlined in the preceding chapters and others. SSI has been dubbed the "next generation of digital identities"

due to its ability to address the shortcomings and limitations of existing digital identity management systems. Despite this, many individuals, particularly in the current period, continue to be perplexed by the phrase and its implications [41]. Tobin and Reed (2017) [29] define the SSI stage as the final stage in the development of a digital identity. Digital identity management is a critical component of this initiative, which also encompasses security and mobility. Prior identities, according to Allen(2016) [24], are a component of a user's core identity, and vice versa. As a result, consumers' independence and control over their identities must be maintained across a broad range of services. To be useful, an SSI must be both replaceable and transportable. Before user assertions about their identity may be accepted, they must be validated by a third party. Third parties must be able to verify someone's identity in order for it to be validated. Comparing SSI with other identity management systems to illustrate the basic notion.(See Figure 2.6) According to Allen [24], self-sovereign identity (SSI) is the next and most advanced

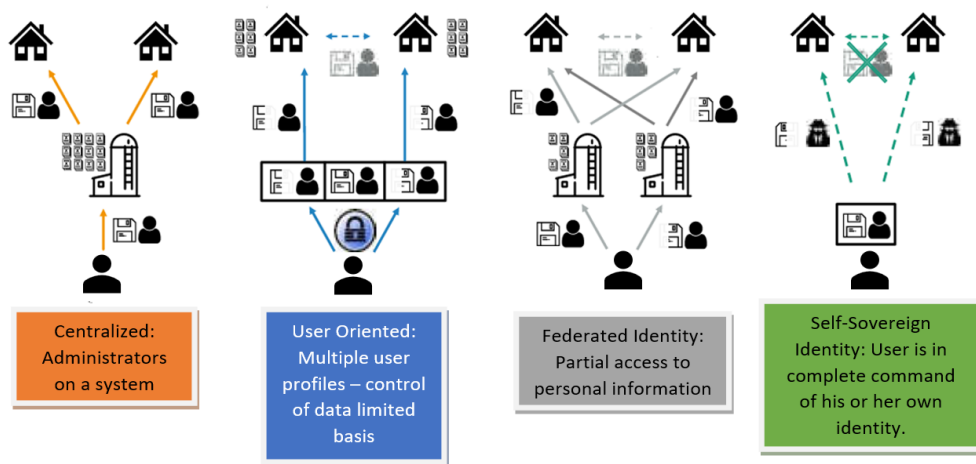


Figure 2.6: Comparative analysis of several identity management systems (Idea: [24], [29], [86])

level of digital identities available today. When users participate in identity-related operations, they should have total control and management over their personal information. Alex and Reed(2021) [86] define this as a "[...] transfer of power from the network's core [...] to its periphery [...]" in which all users communicate directly as peers in a self-sovereign manner. Figure 2.7 illustrates this mechanism in motion. One can find the new element register, which acts as a decentralized public key infrastructure [86], here. Chapter 3 goes into greater information about this. As detailed in Allen's ten principles [24], the system is based on Kim's [11] research into the "Laws of Identity," which distinguishes SSI from other identity management systems.

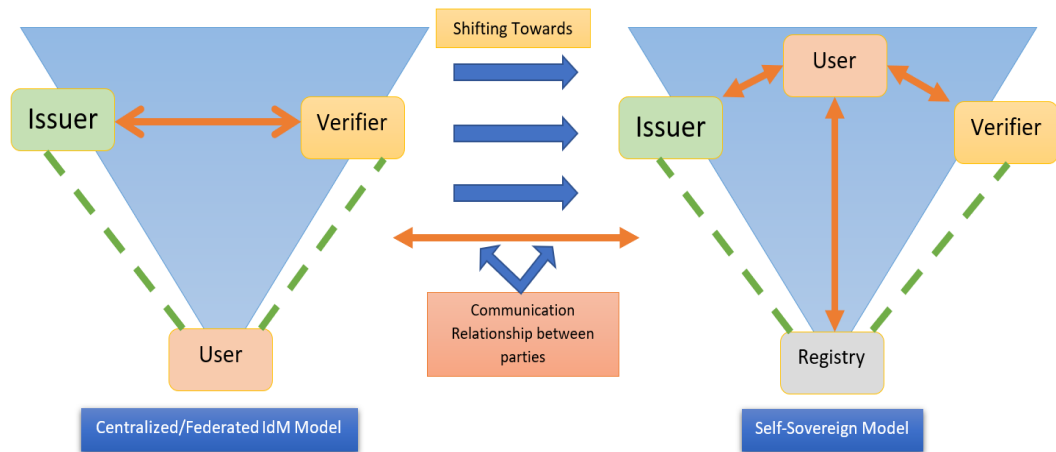


Figure 2.7: Control shifting in favor of SSI

Allen's [24] ten principles of SSI

- 1. Existence - Users must be self-sufficient. In the end, self-sovereign identity is predicated on the ineffable "I." There will never be a fully digital world. This must be the core of one's self-sufficiency. Having a self-sovereign identity merely makes some limited components of the "I" visible.
- 2. Control - Users must retain control over their data. Users have the final say on their own identification, as long as they follow established protocols that verify their claims are genuine. As a result, they should always be able to update or delete information. Users may make statements about another user, but these should not be considered part of that person's identity.
- 3. Access - Data privacy is a fundamental right. A user's identification must be easily available at all times. Gatekeepers and obfuscated information must be abolished. However, users should be aware that they cannot go back and amend all of their identity claims. No one else's data is in the same place because users only have access to their own.
- 4. Transparency - Transparency of systems and algorithms is vital. A network's governance and management systems must be accessible to anyone. The method's operation should be obvious to all users because it is open-source, well-known, and unrestricted by architecture.
- 5. Persistence - Identity requires longevity to build and maintain. Ideally, users should be able to retain their identities indefinitely. Privacy and data integrity are not compromised. We should try to maintain our identities as

long as possible until new identification systems emerge. Users' "right to be forgotten" cannot be violated; users should be able to delete their identities if they so desire, and claims should be updated or removed as needed. This needs a clear distinction between identity and the assertions made in support of it.

- 6. Portability - Identity data and services must be transferable. The identity should not be kept by a single third-party entity, even if it is trusted and considered to act in the user's best interest. The issue is that things can vanish, and this is true of most things on the internet. Consumers may relocate if their existing regime is abolished. The user retains control of their identity regardless of the circumstances.
- 7. Interoperability - Identifiers should be used as widely as possible. An identity is worthless if it only serves a small group. A 21st-century digital identification system's purpose is to make identity information publicly available globally without compromising individual autonomy. Due to persistence and autonomy, these publicly available identities can last indefinitely.
- 8. Consent - For this to happen, the user must provide authorization. An interoperable system makes it easy to share identities and claims. Before sharing any data, users must give consent. An employer, credit reporting agency, or close friend can make claims on behalf of a user, but the user must still approve the claim before it is valid. Not all consent is mutual, but it must be fully informed and understood.
- 9. Minimalization - Claims disclosure should be kept to a minimal. Only essential information should be supplied to complete the task at hand. Keep in mind that if a specific age is required, the exact age should not be revealed. Selective disclosure, range proofs, and other zero-knowledge techniques may support this hypothesis, although non-correlation is difficult (if not impossible) to achieve.
- 10. Protection - Users' rights must be safeguarded. When individual liberties and rights collide with the network's interests, identity networks must prioritize individual liberties and rights. Identity verification must be decentralized, censorship-resistant, and force-resistant.

This abbreviation stands for "Self-Sovereign Identity," which is derived in 2012 from [60] as "Sovereign Source Authority," according to Allen [24]. Marlinspike makes the point throughout this book that severe political systems violate the human right to self-determination. He desired for people to have greater control over their digital identities via Patric Deegan's Open Mustard Seed. He embarked on the endeavor in 2013 with a specific objective in mind. This approach resulted in

the Windhover Principles (2014) and the concept of Self-sovereign Identity, both of which have since been refined [30], [35]. Since then, SSI and blockchain technology have been at the forefront of much discussion within the IIW community. Since then, various government bodies have attempted to conduct additional research on the subject. The IIW's scientific and technology concerns were addressed in a 2015 document produced by the Homeland Security Department's division of science and technology. Countries such as China and South Korea, for example, have taken advantage of the chance. Standards authorized by the World Wide Web Consortium (W3C) have been created to make Self-Sovereign Identity (SSI) a reality. They will be discussed in greater detail in the next chapter [86].

Chapter 3

State of Art: Recent Developments

In order to apply SSI, it is necessary to adhere to the ten principles. Because of this, it is essential to know how to implement an SSI solution on a technical level in addition to the ten SSI principles. An understanding of which SSI's core components may be implemented utilizing already accessible technologies and, when integrated, constitute an SSI solution can be gained from this research. Because of this, this chapter demonstrates the various core components and underlying technologies.

SSI along with many other standards rely on Decentralized Identifier and Verifiable Credentials, thus this section goes into deeper detail about those two foundational standards.

3.1 Standardization of technology and establishment of technical foundations

An explanation of the standards and technologies used by SSI is provided in this section in order to help implementers and stakeholders (such as universities, educational institutions, and organizations for recruiting) get started with the implementation of the solutions described here. Other topics covered here include potential research and development projects that could help create cutting-edge tools to protect students' personal data and give them greater access to it.

3.1.1 Verifiable Credentials

Its standard, lightweight data model for presenting statements of verifiable authenticity, is a critical enabler of interoperability. This tool can represent a wide range of data standards.

W3C Verifiable Credentials Data Model [49] defines a verifiable credential (VC) as one that can be confirmed and is not tampered with. Verifiable credentials (VCs)

are used to store and deliver an issuer's content. A VC can also be used to convey a driver's license, a degree, a certificate of completion of an online course, job records, and other information. They can be linked to competency definitions and additional credential information, allowing for digital and semantic interchange. These capabilities enable student-focused solutions like the students' personal vault to safely store credentials for international students (such as passwords).

Consider the VC as a container that can serve multiple functions. It facilitates the packaging and evaluation of content information by providing an interoperable framework. These tools and services ensure that data is managed in a consistent manner. Example: A user's wallet may save and show record type metadata for the purpose of categorizing and searching records [49], [50].

Verifiable credentials can be used in favor of physical certificates that contain the same information. Digital signatures and other tamper-evident technology can be used to get more dependable verified credentials.

They may build presentations and distribute them to verifiers to demonstrate their confirmed credentials.

According to studies [49], [78], verifiable credentials and validated presentations are more important than their physical counterparts when it comes to generating trust online.

VC's Terminology Overview

This section demonstrates how the critical actors in a paradigm where credential verification may be beneficial interact and perform their assigned duties (Figure: 3.1). A role abstraction can be constructed in a variety of ways. The assignment of responsibilities identifies future standardized interfaces and protocols. The following jobs will be introduced as a result of this standard:

- **Holder** When an entity possesses one or more verifiable credentials and produces verifiable presentations based on those credentials, it is said to be fulfilling a job function. Holders include students, employees, candidates, and customers, to name a few examples [49], (See Figure: 3.1)
- **Issuer** Credentialing entails making assertions about a subject or subjects, developing a verifiable credential from those assertions, and distributing the verified credential to the proper recipient. Businesses, universities, trade associations, governments, and individuals are all issuers [49], (See Figure: 3.1)
- **Subject** A claimant is a person who is the subject of a claim. Humans, animals, and objects are all examples of subjects that can be written about. Occasionally, the individual possesses a credential that is easily verifiable, but this is not always the case. Consider the following scenarios: a parent

(the holder) may possess verifiable credentials on behalf of his or her child (the subject) [49], (See Figure: 3.1)

- **Verifier** An organization's function in accepting and processing verified credentials, which may or may not be presented in a verifiable manner. Verifiers include employers, security people, international organizations, and websites [49], (See Figure: 3.1)
- **Verifiable Data Registry** These are just a few examples of data needed to implement verifiable credential schemes. A system can help generate and verify data by acting as a middleman. Relative IDs are sometimes required. The term "verified data registry" describes trusted, decentralized, and distributed data registries. Many systems store data in multiple reputable data repositories [49], [78].

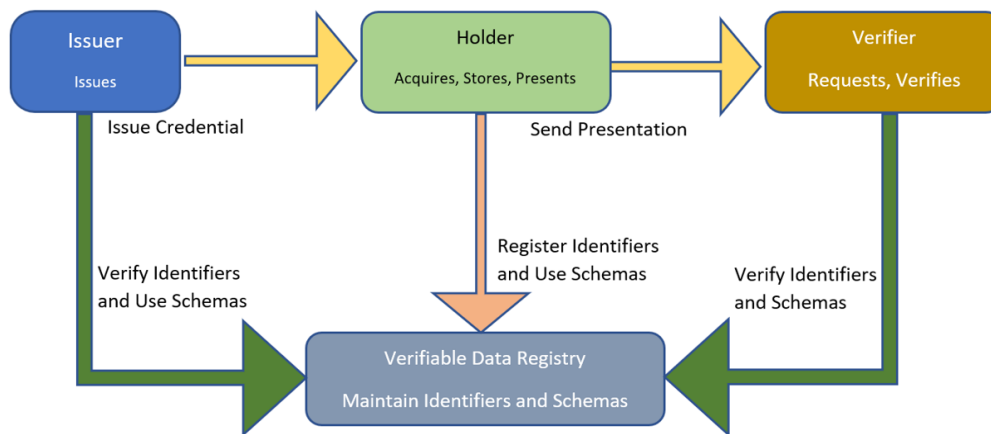


Figure 3.1: The roles and data flows that underpin this specification [49]

3.1.2 Verifiable Credential Data Model

A verifiable credential can be used to illustrate the following:

- A standardized collection of credential-related metadata
- A container for the credential's content
- Flexibility in terms of format/encoding

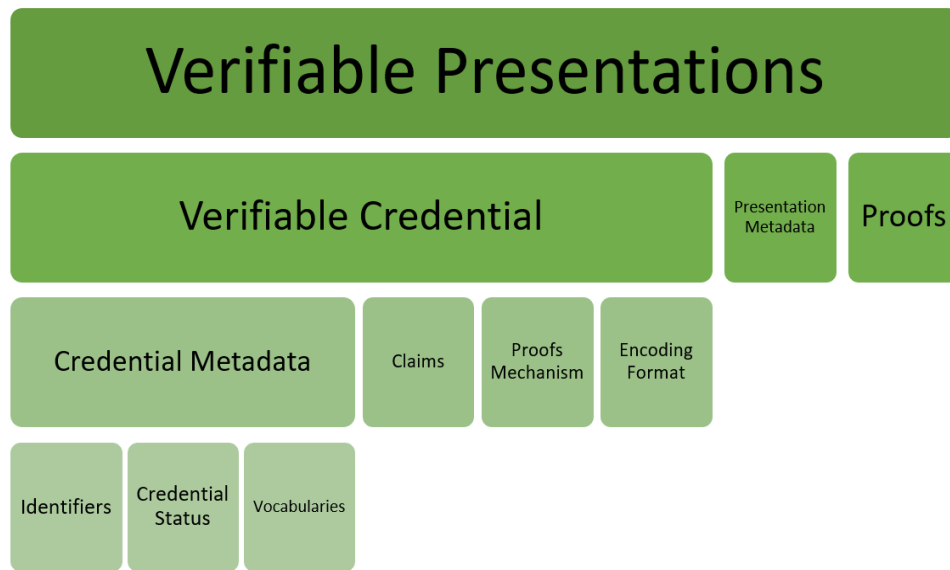


Figure 3.2: Verifiable Credential Data Model.(Source: [51])

Claims

Claims are statements made on a specific subject. Something can be considered a subject when one can make claims about it. Claims are expressed through the usage of subject-property-value relationships [49], [50], [78].

Credentials

When an individual makes one or more claims, the term "credentials" is used. Additional metadata may exist to describe the credential's characteristics, such as the holder's name, the credential's expiration date/time (and possibly the method of revocation), and an identifier, such as an alphanumeric code or an alphanumeric string. The issuer may sign the metadata. A verified credential includes tamper-evident assertions and metadata that demonstrate who issued it [49].

Presentations

One or more verifiable credentials are used to obtain data that is presented in a manner that allows the data's authorship to be established. When credentials are directly presented, they become verifiable presentations [68]. It is also possible to have verifiable presentations that are cryptographically verifiable but do not contain verifiable credentials [49].

Most presentations have a lot of data about the same topic, but from a variety

of sources. A person, organization, or entity's attributes are typically reflected in this data aggregate.

3.1.3 Verifiable Credential Proof Mechanisms

The Verifiable Credentials Data Model is extensible in order to support a diverse array of established and emerging proof systems. The "Verifiable Credentials Implementation Guidelines" [49] are an excellent resource for those interested in learning more about these procedures (Guidelines). Rather than substituting for the Guidelines, this section will provide additional discussion and recommendations about the current state of these techniques.

There must be at least one proof mechanism and the details necessary to evaluate that evidence in order for a certification or presentation to be verifiable.

External proofs and embedded proofs are the two types of proof techniques mentioned in W3C specification [49]. For instance, a **JSON Web Token** can be considered an external proof because it comprises a self-contained description of the data model. An embedded proof, in the context of data security, is a system that embeds the evidence inside the data, such as a **Linked Data Signature**.

JSON Web Token

JSON Web Tokens (JWT) continue to be a popular way for two parties to convey claims. Existing systems and libraries can participate in the system described in Section 3.1.1 Terminology Overview by implementing a Verifiable Credentials Data Model for JWT. A JWT is a set of claims included in a JSON object [57]. It is contained in a JSON Web Signature (JWS) or a JSON Web Encryption (JWE). This specification does not cover the use of JWE.

Linked Data Proofs

Through Linked Data, URLs, JSON-LD, and other Web standards are used to publish information on the Internet. This presentation format simplifies the process of discovering new data and expanding the existing graph of knowledge [49], [70]. The decentralized structure of Linked Data eliminates impediments to large-scale integration. To ensure the security of this standard, Linked Data Proofs and Linked Data Cryptographic Suites must be used.

Verified credentials and presentations can be stored using the Linked Data Proofs format because no additional processing is required in comparison to JSON Web Tokens. Verified examples from this standard can be used to protect a verifiable credential or presentation using Linked Data Signatures.

3.1.4 Comparison between Linked data proofs and JSON Web Tokens

The most frequently used proof types in current verifiable credential deployments are Linked Data Proofs and JSON Web Tokens. Implementers may struggle to comprehend the relative merits of each. Thus, in order to summarize the Guidelines' tables, the following table summarizes the advantages of using both methods of proof.

Features that promotes JWTs

- Mature library in multiple languages
- Native platform toolchain (no extra libraries)

Features that promotes Linked Data Proofs

- Open Data Modeling
- JSON-based file sharing

Mature library in multiple languages

JWTs have robust libraries for a range of computer languages. Linked Data Proofs, on the other hand, are a more newer standard with less library support at the moment [49], [57].

Native platform toolchain

To contrast with JWTs, JSON-LD libraries are still in their infancy and are not usually included in the native platform toolchains for which they were designed [49], [57].

Open Data Modeling

JSON-LD By providing a "context" in which statements can be made, proofs enhance the open-world approach of linked data. Unambiguous claims can be made because of this [70]. For diploma records to be portable and interoperable, linked data approaches are needed since they allow academic qualifications to be mapped to competency framework, taxonomies, and ontologies.

JSON-based file sharing

Due to the normalization step that occurs before to signing and verifying the credential, it is feasible to save the signed credential as a JSON-native document. Historically, the capability of educational records with verifiable credentials to utilize common JSON tools following their issue has been considered as a positive

feature. This, however, may alter as the number of valid credential tool sets grows. Surprisingly, proponents of JWT claim that this level of growing phenomenon is bad because it lengthens and complicates the processing process [49], [70].

3.1.5 Advanced proof mechanisms

The above-mentioned proof formats are compatible with more advanced (and ever-evolving) proof procedures. Pilots that concentrate primarily on usage situations and fitness are needed to study the potential for enhanced privacy provided by these technologies in greater depth. With zero-knowledge proofs, a statement can be established without the need to provide additional details. Despite the fact that this method isn't widely used currently, interest in it is growing due to the enhanced anonymity it provides. There has been considerable interest in the BBS+ Signatures 2020 Draft Specification, which has been offered as a straightforward implementation method to zero-knowledge proofs.

3.1.6 Zero Knowledge Proof and BBS+ Signatures 2020 Draft Specification

BBS+

As described in the study, data reduction is essential for stakeholder implementation to be successful. Some of the anticipated dangers described in the analysis chapter can be addressed through the use of data reduction techniques. Allen's ten principles for SSI include the concept of "minimization," which says that the number of released claims should be maintained to a bare minimum in subsection 2.3.4 of the identity management development phases in chapter 2. Known as selective disclosures, this technique allows a user to conceal some attributes of a credential, similar to the blackening of paper in the analog world, while maintaining the rest of the credential's functionality. What is known as ZKP is the following step in this process; it is during this phase that the actual attribute isn't sent, but rather an assertion of a value that confirms what the verifier is looking for. For example, an age check does not require the verifier to know the subject's precise age, only that he or she is older than the age of majority in the country. Two of the most regularly used methods in the community are the Camenisch-Lysyanskaya (CL) signature and the BBS+ signature, which are both based on the BBS+ algorithm. Furthermore, the keys and credentials that came with them were quite large, which made them prohibitively expensive to generate [76], [77], [82]. Instead of a single signature for a single message, this signature is comprised of a collection of signatures for a variety of messages. The holder is then able to extract the signature, which can only represent a subset of the document's attributes because it is a subset of the signature. In contrast to Camenisch-Lysyanskaya signatures, the current

BBS+ implementations do not accept the usage of predicates for the purpose of implementing the ZKP in its entirety.

It is conceivable to receive such assistance, but it has not been the primary focus of research in cryptography up to this point. If the value of such predicates is included directly in the VC as a separate property, the issuer can choose to reveal it selectively or not at all, according on the circumstances. The W3C Credentials Community Group is currently in charge of an unofficial draft of the "BBS+ Signatures 2020" specification [77], which is currently being managed by the group [76].

Zero Knowledge Proof

Cryptographic techniques such as zero-knowledge proofs are used to demonstrate to other entities that they are aware of a given value, but without revealing the value itself [4]. In this context, it's used to denote that an object is aware of a specific value. An established institution may award an honorary degree on an individual without revealing the student's identity or any other personal information that may be contained on the degree itself. Zero-knowledge proof approaches allow a holder to do the following tasks:

- Combine several verifiable credentials from multiple issuers into a single verified presentation without disclosing the verifier's verifiable credential or the IDs used to verify the credentials. " Due to this, it becomes more difficult for the verifier to build an alliance with any of the credential issuers.
- A validator should be able to see just the claims in a verified credential without needing to provide a huge number of verifiable credentials to do so. Thus, the holder will be able to submit only the information requested by the verifier.
- As long as the verifier's data schema is followed, the issuer doesn't need to be contacted again to receive a derived credential that is prepared in accordance with that template. As a result, holders of verified credentials can use them in a variety of ways.

For the purpose of selectively disclosing private information, the W3C specification includes a data model that incorporates zero-knowledge proof procedures [52]. Holders of zero-knowledge verifiable presentations must ask an issuer to supply a verifiable credential so that the holder can generate a proof from the initially provided verifiable credential, allowing the holder to present information to a verifier while safeguarding the verifier's privacy. If the document has been signed by the issuer, it is possible for the holder to verify the authenticity of that signature without disclosing the values signed, or at least only a subset of the values signed.

Without divulging the presence of the signature, the standard approach is used to verify this. (Figure: 3.3)

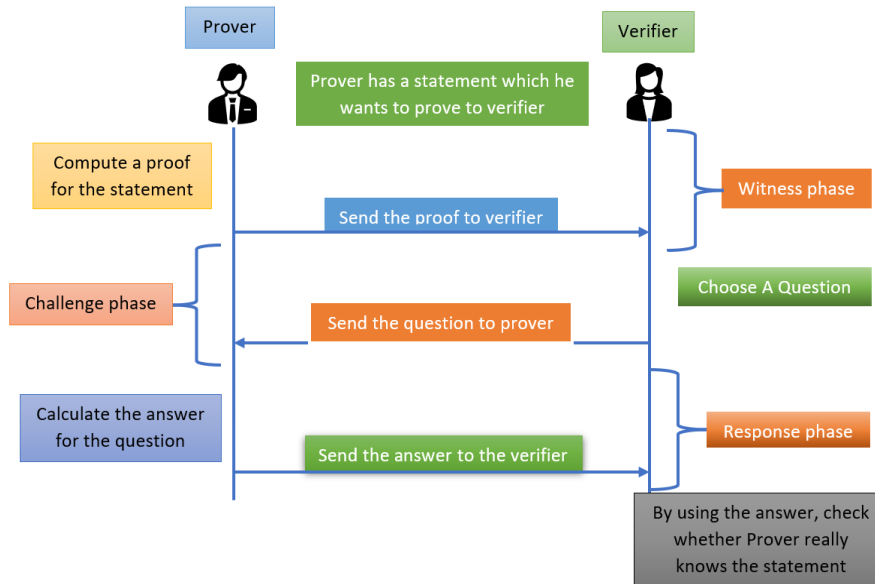


Figure 3.3: Zero-Knowledge protocol between parties [4]

There are two prerequisites for using verifiable credentials in zero-knowledge proof systems [1].

- In order for the holder to generate a verifiable presentation that shows only the information desired by him or her, the verifiable credential must include a proof that makes use of this capability.
- If a credential definition is to be utilized by all parties to perform various zero-knowledge cryptographic activities, it must be defined in the credential schema property.

3.1.7 Decentralized Identifiers

In verifiable credentials, URIs (Uniform Resource Identifiers) are used to identify the issuer and the learner (students/holder) [5]. A URL to an issuer profile is the most prevalent URI for an issuer profile in the current state of Open Badges v2 implementations (i.e. web addresses). One of the ways in which VCs can identify both the issuer and the student is by using this form of URI. Decentralized, long-term, and verifiable digital identities can be created by using a decentralised identifier (DID). Initially, DIDs were used in conjunction with VCs in order to gain control of a unique identity through the use of authentication procedures, signing

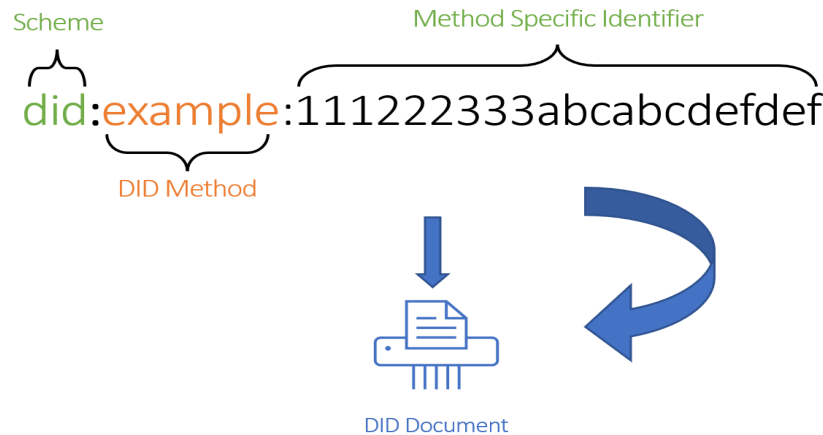


Figure 3.4: Decentralized identifier [74], [86]

keys and other secure methods of communicating with the individual. DIDs have the potential to dramatically increase the overall durability of public key infrastructure (PKI) management in theory by allowing for planned key rotation and recovery in the event of device loss or other catastrophic failures. Additional effort, both technically and, more importantly, usability-wise, will be required to realize these potential gains, which will require additional resources. According to the findings [36], [39], [44], studies of student-focused applications have demonstrated that we are only at the beginning of our understanding of how a student might effectively connect with this environment. Numerous DID implementations make use of blockchain technology. While this technology improves longevity and control, it also creates new technological dependencies. Numerous articles and research studies have argued in favor of more research and development in these potentially lucrative fields.

Interoperability "bridges" between digital identification systems that are centralized, federated, or distributed can benefit from the usage of DIDs. As an example, the `did:web` strategy advises that web-based DIDs be used to "bootstrap trust by leveraging the existing reputation of a web domain" in order to increase the use of DIDs on the internet [31], [71]. Blockchain-based DIDs have the advantages of this system without the uncertainty that comes with it. For example, when used to connect to contemporary authentication systems such as OpenId Connect, these DIDs can give the student with greater control and utility.

3.1.8 Distributed Ledger Technology (DLT)

To ensure that students' personal information is protected, one of our primary goals is to make as little personal information about them as possible available to the broader public. These two concerns emerge as a result of the application of this

rule: To begin, data must be made available to the general public in some instances. For example, include the issuing university's public identity and accompanying service endpoint in the DID document is quite fair. Second, not all credentials are valid for an unlimited period of time. As a result, credentials and the attributes linked with them must be revoked by the institution that issued the credentials and attributes. This is referred to as revocation in this context. Students who cheat on a test, for example, should be subject to having their degree certification taken away from them. In a legal sense, the student cannot be compelled to remove his or her VC. Therefore, the verification institutions must be able to track and monitor the development of the VC. According to theory, a verifying institution might contact the VC's giving university immediately and request that the VC's certificate be revoked. Making a service endpoint specifically for this purpose could be one approach to achieving this goal, for example. It is necessary to standardize data formats and protocols in order to deal with this situation effectively. This strategy, on the other hand, would compromise SSI's efforts to keep direct institutional interaction from occurring. Because of the uniformity and fail-safety that platforms provide, they may be a viable choice for some applications. These systems must include the following functionalities as a bare minimum [53]:

- DIDs should be published to make the institution known to as many people as possible, especially for institutional reasons.
- A revocation register is required in order to keep track of whether or not a Verifiable credential is still in use.
- An open release of credential schema definitions and their related schemas is necessary to facilitate semantic interoperability of verifiable credentials.
- Additionally, third-party authorization may be revoked as a result of the posting of third-party authorization.

It is almost probable that using a centralized platform will result in dependency on and lock-in to the platform in question. These challenges connected with a central platform can be avoided by using DLTs, or decentralized, distributed systems, which are capable of overcoming them. Blockchains, which are a subset of distributed ledger technology, are used in well-known SSI systems, such as Hyperledger Indy, to store and transfer information. Blockchains are distributed data structures that allow for the transparent, chronological, and tamper-proof storing of transactions grouped in blocks. Blockchains are used to store financial transactions [69]. When used in conjunction with an SSI architecture, distributed ledger technologies (DLTs) and blockchains provide a number of benefits, including:

- There are no single points of failure in the distributed ledger because of the redundant, decentralized design.

- It is impossible to reverse a transaction or alter the data linked with it once it has been recorded on a blockchain.
- All network participants have equal access to all transactions. It is possible for all members of the network to see the most recent status change, such as the assignment of a new identity.
- Every transaction has to be authorized and signed by the person who started it. Thus, it is possible to track the origin of data in a transaction back to a specific participant.
- A linked list of transactions is created as a result of the blockchain's block architecture, which cryptographically ties individual blocks together. Individual transactions are automatically arranged in chronological order as a result of this rule. For example, a revocation register's content can be easily checked for accuracy and timeliness thanks to this.

Although there are advantages to implementing a blockchain solution as part of an SSI solution, there are also disadvantages to consider. For example, to prevent any potential bottlenecks, it is recommended that as little data as possible be stored on a distributed ledger system. Furthermore, no personal information should be recorded in plain text on a (distributed) ledger of this nature. Even the secure storing of personal information on a distributed ledger is fraught with danger. Future technological advancements (for example, quantum computing) may allow asymmetric encryption to be broken, even if it is still regarded safe for the foreseeable future [83]. Article 16 GDPR - Right to rectification and deletion, 2018) also mandates that personal data be updated or erased if a person requests it. In light of the intrinsic attribute of cryptographic tamper resistance that blockchains possess, personal data should not be stored on the blockchain from a legal standpoint.

3.1.9 DIDComm

Asynchronous, secure, and asynchronous peer-to-peer communication protocol based on the DID standard, DIDComm, also known as DID communication, is used by agents to communicate with one another. It is the responsibility of the Decentralized Identity Foundation's DID-Comm Working Group to monitor the effort [84][maomie], which is a direct product of the Hyperledger project's operations [55]. This means that any current protocol can be utilized because messages are not dependent on the medium over which they are transmitted. When a standard is centered on machine-readable communications, it opens the door to a greater range of application scenarios in which anybody or any entity can send any type of encrypted communication [86].

3.1.10 Decentralized Verifiable Data Registries

Decentralized verified data registries (DVDR) are used to maintain credential status, such as whether a credential has been revoked, as well as identify management for DID discovery and authentication [63]. Blockchains [42] are often used to do this, although distributed ledgers such as the InterPlanetary File System(IPFS), which is a distributed ledger system, can also be used to accomplish this [45]. By using one of these methods, the issuer can keep the information required for credential verification up to date without requiring verifiers to engage directly with the issuer, resulting in time and money savings for both parties.

3.1.11 Comparative study of credential hosting services

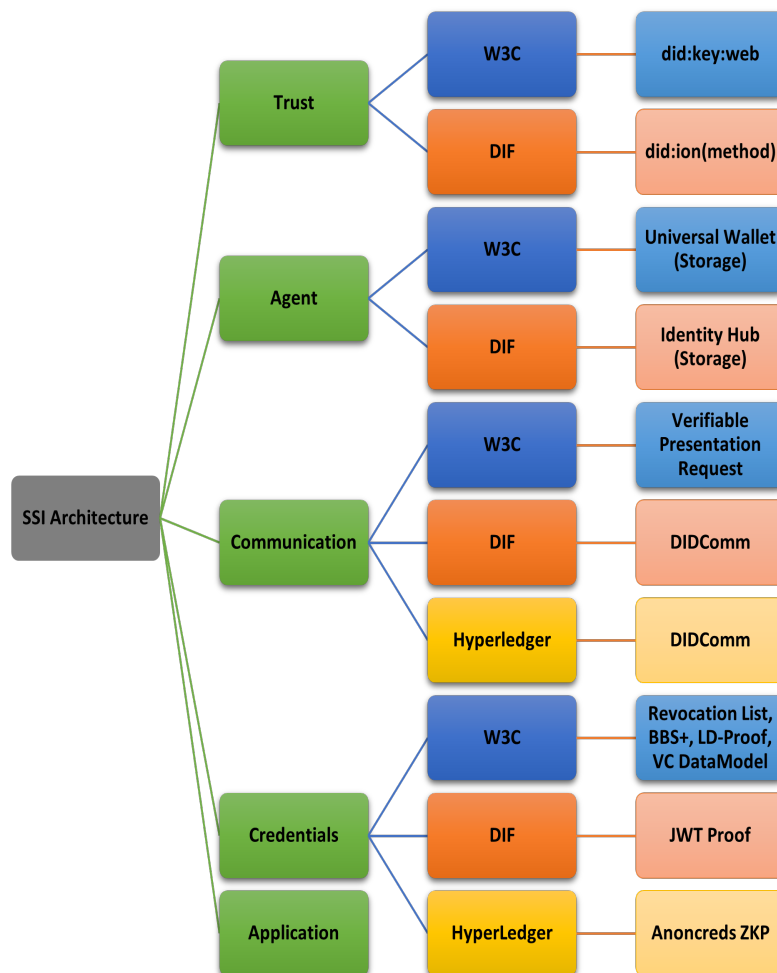


Figure 3.5: ssi stack

As illustrated in Figure 3.5, SSI's technical stack is divided into five tiers and three organizations. The W3C, DIF, and Hyperledger are just a few of the organizations driving a deluge of open-source projects and standards. This comparison is based on research conducted previously by organizations such as the Trust over IP group and the Decentralized Identity Foundation (DIF) [53], [80], [92]. One of the most noticeable changes in this situation is the separation of the communication layer from the agent layer. Apart from the fact that it is utilized by agents, it is a distinct collection of communication technologies that may be used to communicate by any entity and is not a component of the agents themselves. The public trust layer serves as the foundation for all following levels. This project's objective is to establish a public trust registry that contains DIDs and their associated DID procedures and so functions as a public key infrastructure. In view of the above, a blockchain or decentralized file system may be required in the future. In did:web, one such centralized alternative, all method-specific activities including the DID document are dependent on a centralized web server. The communication layer is at the bottom of the stack, and it is responsible for controlling how data is sent between agents. This includes, but is not limited to, transit, envelope, and credential exchange standards and protocols. At the fourth level, the credential layer contains all of the standards and technologies utilized in the data model of credentials, such as formats, proof types, disclosure, and revocation of credentials. The application layer, as the highest level of abstraction, builds user applications based on the implementation of specific use cases in the underlying layers. Along with the actual data models for credentials, this contains the app's business logic and technology [53], [80], [86], [92]. Also with establishing the overall structure and elements of the layers, these standards and community activities also create the technological groundwork for the layers. This section detail the concrete activities taken by the three largest organizations operating in this field. To minimize confusion, keep in mind that the material offered here is not exhaustive, but rather serves as an illustration.

3.1.12 Privacy-preserving Credential Status

The Verifiable Credentials Data Model emphasizes that issuers must be able to update the status of credentials, for example, by reporting that a credential has been revoked, and that this should be done in a manner that promotes privacy as a desired ecosystem quality. For example, no extra information about the student should be revealed during revocation checks. Additionally, the Verifiable Credential Data Model advises against adding revocation status checks that alert the issuer (or comparable parties) to the fact that a verification check on a particular credential (or learner) was done.

This can be accomplished through a variety of means. Certain techniques make

available a list of revoked credentials' hashes. Verifying a particular credential is as simple as computing the (well-known) hash, retrieving the current list, and checking to verify if the hash of the credential in question is included in the list, as mentioned above. Along with the preceding recommendation, this list should be decentralized.

3.1.13 Digital Wallet

The development of a personal wallet can begin with a common students degree record wrapper data model, such as the one offered by VCs, but additional standards work is required to facilitate credential storage and exchange. Student-facing tools must be intuitive to use and purpose-specific, as they present entirely new methods of interacting with one's data. Thus far, efforts to build student-centric credential management solutions have encountered considerable criticism. For instance, a Georgia Tech research on the usability of the Blockcerts program found that students struggled with the application's experience, method, and even concepts. This raised concerns about the new method's security and provenance. Additionally, students expressed fear that the risk would be passed to them because, under the existing system, they can seek assistance from the school rather than being held accountable.

In addition to improving usability, additional work on standards is required. For example, as the number of digital credentials issued to students continues to grow, common access patterns, indexing, and encryption will become increasingly important in the development of solutions to manage credentials. The World Wide Web Consortium and the Decentralized Identity Foundation are now in the early phases of developing these new standards and protocols, which are critical for preventing lock-in and attaining interoperability.

Chapter 4

Questionnaires and Analysis

As an example, this chapter describes and evaluates an existing scenario by highlighting flaws in the current system and procedure in order to demonstrate why it is necessary to develop a new system capable of resolving existing obstacles that students and educational institutions face when evaluating academic degree credentials, the author uses the example of a hypothetical situation. As an additional advantage, this chapter examines questionnaires completed by professionals in the field of evaluating degree verification processes and draws on their knowledge and experience to restructure the scenarios and lay the groundwork for incorporating the proposed design concept into the evaluation criteria.

4.1 How SSI can apply to design an IdM

It is a technique for managing digital identities that is based on concepts and technology with the goal of handing control to students via the usage of self-sovereign identity (SSI). At its most fundamental level, self-sovereign identity (SSI) is a set of rules that regulate how identity and personal data should be preserved on digital networks. SSI's core concepts include identity management, distributed computing, blockchain or Distributed Ledger Technology (DLT), and cryptography [85].

These concepts are frequently referenced in the web article *The Path to Self-Sovereign Identity*. The content suggests a new relationship between individuals and their digital identities based on ten fundamental principles [74]. The desire to minimize vendor lock-in regarding data transfer and interchange is one of the aspirational goals for individual rights in connection to data collected about them.

As we consider how to make academic records more accessible and participatory, the architecture of SSI-type systems serves as a lens through which we can consider how to make such systems more egalitarian, allowing students greater access to and control over their academic records while still ensuring data integrity.

These initiatives have the potential to improve student identification and empowerment while also enhancing educational institutions' ability to educate and businesses' ability to recruit qualified workers through the use of SSI-based techniques.

This article focuses on the user scenario, illustrating the importance of interoperable, individual-level data in improving student outcomes. The scenario illustrates how verifiable academic credentials might be presented to a foreign university in order to get admission to a higher degree program. Additionally demonstrates how verifiable and inter-operable academic records (together with future diploma training) can result in more exact talent matching in subsequent public or private sector employment. Service members who are students benefit from a more rapid integration into the workforce and greater levels of job satisfaction in this case. As a result, organizations' capacity to recruit qualified candidates improves. The purpose of this study is to demonstrate how SSI techniques may assure the ongoing verifiability of students' records while also allowing students to manage their own records and academic records.

While this study concentrated on SSI components relevant to students' academic records, the findings should not be regarded as a comprehensive map of the SSI terrain. The "Comprehensive Guide to Self-Sovereign Identity" [79] covers the history, objectives, and present political climate of SSI.

4.2 Benefits of using SSI for verification system

When SSI-based technological solutions are implemented, a slew of significant benefits flow to students, institutions, and the broader ecosystem:

- The institution grants students the ability to control who has access to their academic record(s), including specific components of their records, and when they have access.
- Credentials are confirmed and accessible regardless of the condition of the originating organization (academic institutions) at the moment of authentication, as authentication is cryptographically secured, which is often done on distributed ledgers.
- It is possible to verify students and local institutions online in a secure and timely manner.
- When it comes to validating non-traditional accomplishments, verifiable credentials might be advantageous because they demonstrate learning across a variety of contexts.

4.3 Scenario-based SSI

Using the Identity Management System for academic credential prioritized user scenario described above, we can describe each position and the experience of a student named Mohammad in an SSI environment when verified credentials are utilized, as follows:

- **Mohammad is a Bangladeshi college student who recently transferred from a small coastal metropolitan area's high school to a national college. He is a student enrolled in a next-generation (digital curriculum) school. He enrolled in an IT program to round out his education and get a sector-recognized network management certification. He sought and was admitted to a university certificate program the following year, which included an internship and industry certification. He recently earned a certification as a result of completing his university degree, which included an internship. Outside of Bangladesh, his current interests include postgraduate studies and employment opportunities in the fields of network administration and cybersecurity.**

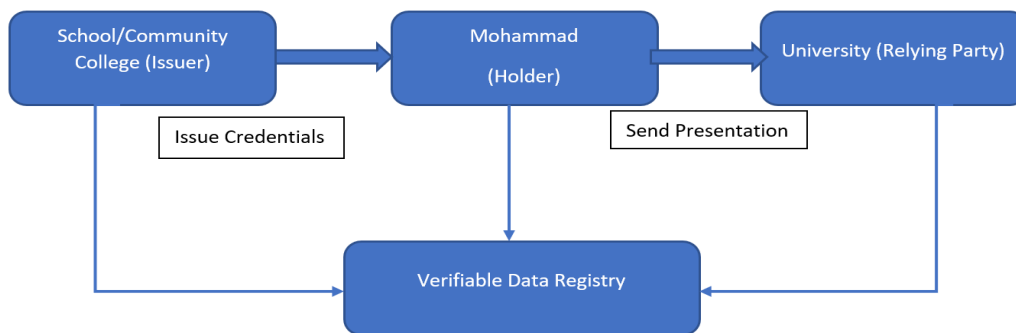


Figure 4.1: VC Presentations for application to university programmes

The roles and interactions inside an SSI ecosystem are referred to as the "trust triangle" because to the way it develops. Confidence in the credentials' issuer instills trust in them, just as it does in the real world. This triangle is seen in Figure 4.1, but it also illustrates how roles and VCs interact, which is why the Verifiable Credential Lifecycle is frequently referred for the VC's data model [52], [86]. The lifecycle diagram of a Verifiable Credential illustrates the numerous steps it goes through, as well as the roles that execute specific activities at each level. The method is described below in terms of a Verifiable Credential that serves as a substitute for a college diploma. The issuer is a university, the holder is a student, and the verifier is a university's admissions recruiter.

Educational institutions (issuers) begin issuing credentials to Mohammad (subject/holder) using an SSI-based system. Mohammad can store this information and access it from any device using his mobile or web-based credential wallet/application. By sending credentials along with metadata from his wallet to the local national college, he ensures that his academic credentials have not been tampered with, are real, and are in good standing. This is accomplished through the use of a verifiable data registry. Mohammad's application for enrolment has been authorized following the national college's assessment of his credentials. Mohammad would receive accreditation from the national college after successfully completing tasks such as finishing a course or earning a certification, one of which would be in Information Technology. This certification, along with a few other carefully selected academic qualifications, is added to Mohammad's credentials wallet, which he organizes. Finally, Mohammad applies for a university program that will recognize his qualifications using the same approach he used to obtain this certification. While the secondary school may be a member of a different verified data registry than the national college, each registry's objective is the same. Mohammad maintains a

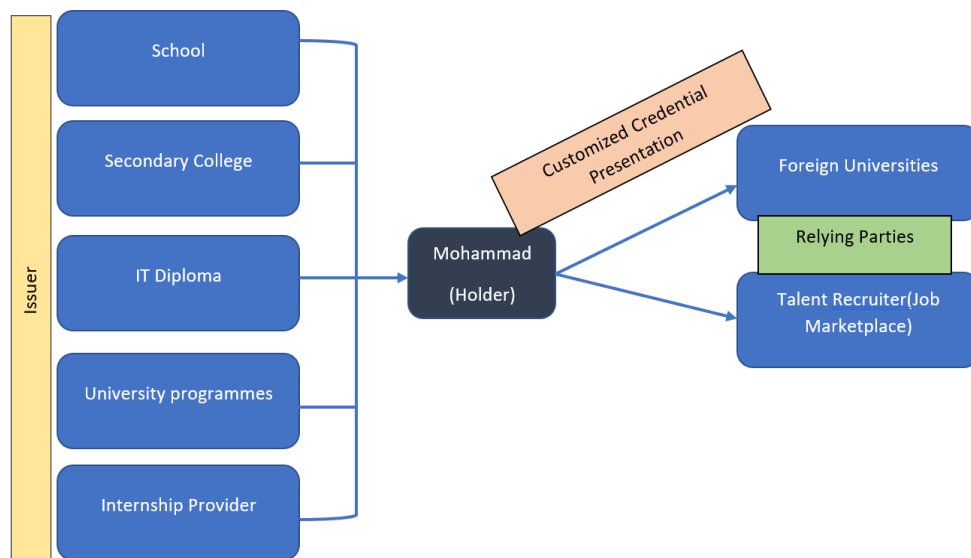


Figure 4.2: Customized VC's Presentation with Selective Disclosure to different Relying Parties.

personal credential record wallet that contains a variety of verified credentials, including his school and college records, a computer technology industry certification (along with other industry certifications), internship records, and a certificate from an accredited university program (see figure: 4.2). He can use his interoperable credential wallet to create customised presentations of his credentials, which he can utilize to apply to worldwide institutions and career markets. Except for the

presentation of credentials, the two potential verifiers/relying parties (foreign university / talent recruiter) would follow the same verification procedure as national colleges and universities.

4.4 Discussions with Experts: Q&A

Apart from establishing theoretical groundwork, this section establishes a framework for future research into the proposed design and evaluation approach. This division is in charge of developing, administering, and analyzing a survey of educational sector specialists. This strategy lays the groundwork for the subsequent chapters. The following part will go into greater detail on how to put together the questionnaire.

4.4.1 Questionnaire formulation

A questionnaire of experts is used to ensure that the work and its artifacts are not based on speculation or guesswork, but on actual experience and expert judgment. Along with emphasizing the User/Stakeholder Role Experience, it is critical to include a list of verified SSI solutions as a secondary objective. Additionally, the following factors should be considered: whether the solutions are suggested, what selection criteria should be used, and whether components of the solutions are currently underrepresented in the market.

Prior to conducting the interview, an exhaustive literature review was conducted [37], [38], [47], [54], [56], [60], [61], [64], [65] and a search on GitHub for the terms "verifiable credentials" and "self-sovereign identity." This proved to be a challenging endeavor, given that the literature typically discusses legacy or SDK-free solutions, and occasionally even mixes in SSI networks. As an example, Sovrin was frequently placed in the same side of the table as uPort as a Hyperledger network [37], [47], [64], [65]. This may be perplexing for those interested in incorporating SSI into their systems or service offerings. As a result, initiatives that could be implemented in collaboration with particular organizations were initially rejected. Following that, it was determined which stages of the verifiable credential lifecycle [52] each solution might cover. This is critical for determining the feasibility of offered solutions. This was accomplished by an analysis of the various alternatives' websites and documentation, which frequently lack sufficient information.

A more in-depth look at the issue of expert selection is provided once the first basic material has been covered in this section. With the author's supervisor's help, author was able to learn about the GAIN perspective in the SSI community through his supervisor's recent participation in a workshop, which was really helpful. The GAIN viewpoint on the SSI program, as well as subsequent technical discussions, highlighted field professionals as possible participants. In order to compile a list

of all the professionals who took part in the survey, author used this table along with information gleaned from LinkedIn and other sources.

Name	Organization	Position
Eva Marie Althoff Schäfer	Aalborg University	International Co-ordinator
Mr. Ziarat Hossain Khan	American International University-Bangladesh	Office of Students Affairs
Mohammad Tanvir Hossain	Renata Pharmaceutical Limited-Bangladesh	Senior Officer-HRD

4.4.2 Surveys purpose: Inquiry-based methods

It was determined that the questionnaire should be used based on the project's analytical progress. Given that the problem statement was analyzed based on the roles played by entities that would use the system rather than on the technical development of the identity management system, experts were selected based on their roles as individuals who were responsible for evaluating students' academic records and performance.

While the project was analytical in nature and centered on the application of the new SSI concept, technical standards were thoroughly defined in order to develop the scenario based on the conceptual design offered in the design chapter.

The meanings of the questions are based on the essential concepts introduced at the outset of this section. In addition, just a small number of questions were selected in order to speed up the process of answering them. It was because of this, that the following question emerged:

- 1. What is the title of your position/job?
- 2. Are you currently working on anything that would alter the management system used to verify international students' domestic degree completion?
- 3. What value would you place on the existing system's toolkit and flexibility for successfully implementing new technology?
- 4. What additions or modifications would you make in light of previous incidents?
- 5. Which solutions would you choose and why if you were in charge of a company looking to integrate verification systems into their products?

- 6. Which ones would you choose not to utilize, and why?
- 7. What factors do you believe are critical when evaluating a system for implementing Verifiable Credentials/academic records?
- 8. What do you believe are the most prevalent issues that today's institutional solutions face?
- 9. Is there anything more you wish to say?

Following completion of the preparations, the defined questions were forwarded to the specialists on the list, who responded swiftly and competently. The following section will discuss the administration of the questionnaire and the receipt of responses.

4.4.3 Q&A: Analysis

The questionnaire was meant to be completed by email or video conference to suit busy individuals. The high response rate was attributed to qualified candidates for expert roles. Through open-ended inquiries, participants can express themselves freely. We received three comprehensive responses after contacting each of the four individuals. Eva Marie Althoff Schäfer, Ziarat Hossain Khan, and Mohammad Tanvir Hossain were among those present. Appendix A enlisted the questions together where Appendix B summarizes the responses of each participant, including the following:

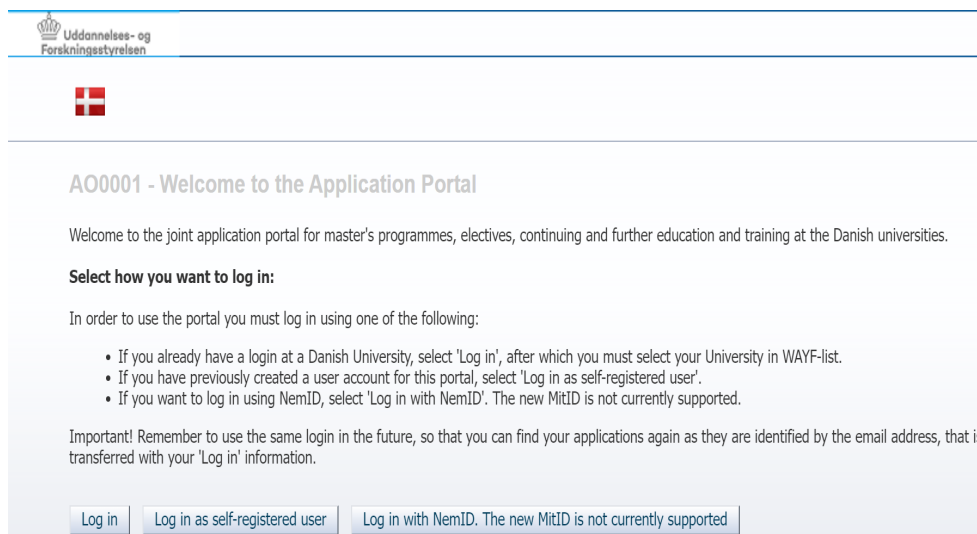
- 1. *What is the title of your position/job?* International Coordinator, Human Resource, Admission Controller.
- 2. *Are you currently working on anything that would alter the management system used to verify international students' domestic degree completion?* Government projects, adaptation, new field of technologies.
- 3. *What value would you place on the existing system's toolkit and flexibility for successfully implementing new technology?* public registry, trust, collaboration.
- 4. *What additions or modifications would you make in light of previous incidents?* control, record, database, attestation, verification.
- 5. *Which solutions would you choose and why if you were in charge of a company looking to integrate verification systems into their products?* UKNaric, online verification, direct collaboration between organization, major player, stakeholders.
- 6. *Which ones would you choose not to utilize, and why?* Paper based record, attesting method, translated certificate.

- 7. *What factors do you believe are critical when evaluating a system for implementing Verifiable Credentials/academic records?* Universal system and record, interoperability between entities.
- 8. *What do you believe are the most prevalent issues that today's institutional solutions face?* vast amount of application, time, justification method.
- 9. *Is there anything more you wish to say?* flexibility, interoperability, international collaboration.

4.5 Existing admissions procedures in foreign institutions

Universities in Denmark have an administrative system that enables students to conveniently register for classes, view exam results, and generate multiple transcripts. The university's administration included all pertinent study information for students on that page. Students can easily obtain printed academic transcripts, but they must contact the study secretary if they need the transcripts confirmed for employment purposes. In the case of personal data, information such as an address or a contact medium that has been retrieved from the Danish National Registration Office can be revised only if the relevant information is updated in the Danish National Registration Office. That facility provided the system with a student's personal information without altering the student's identity. However, the report once again concentrates on academic credentials, which have little impact on the Danish National Registration Office. Additionally, international students interested in pursuing a higher degree in Denmark must use the Danish Agency for Education and Research's Application Portal to create a profile and apply to graduate programs at various education institutions in Denmark. International students were required to provide documentation of past educational degrees and records without going through any verification process. However, once a student has enrolled in a course, his or her educational record is shared with NemID-CPR. One method of verifying the degree holder is through the use of the degree holder's Civil Registration Number. However, it is not internationally recognized because CPR has limited value to a student studying in a different country.

When looking at the Scenario from this perspective, , Mohammad is a Bangladeshi student with no unique identifying number other than his passport, which verifies his citizenship. Additionally, his passport number may be utilized to facilitate visa processing in accordance with international regulations and identification verification, but claiming to own an academic diploma is unjustifiable. According to the illustration, Mohammad graduated from a university approved by the local government, which may be verified by cross-checking university registration information with that of the local government. However, Mohammad's civic identification information remains absent.



Uddannelses- og Forskningsstyrelsen

AO0001 - Welcome to the Application Portal

Welcome to the joint application portal for master's programmes, electives, continuing and further education and training at the Danish universities.

Select how you want to log in:

In order to use the portal you must log in using one of the following:

- If you already have a login at a Danish University, select 'Log in', after which you must select your University in WAYF-list.
- If you have previously created a user account for this portal, select 'Log in as self-registered user'.
- If you want to log in using NemID, select 'Log in with NemID'. The new MitID is not currently supported.

Important! Remember to use the same login in the future, so that you can find your applications again as they are identified by the email address, that is transferred with your 'Log in' information.

Log in Log in as self-registered user Log in with NemID. The new MitID is not currently supported

Figure 4.3: Application Portal Denmark

In Germany, applying for higher degree admissions follows a similar procedure as in the United States. International students applying to German universities from other countries must send their application materials via postal or air mail. In the same way, a credential does not provide any clarification on the identity of an individual in terms of his civil identity.

When Mohammad was admitted to a university program in Bangladesh upon completion of higher secondary school, he was required to surrender his original academic transcript to university officials in exchange for a four-year hold. This was because he was required to withdraw from all other educational programs while enrolled in one.

4.6 Expected risk of using existing verification system and responses

To demonstrate how SSI can alleviate some of the issues associated with student academic record systems, the following user scenarios are examined: Beginning with an assessment of potential dangers to a student's agency and progressing to areas where these issues may result in regulatory considerations, employment opportunities and foreign university entrance should be pursued. Numerous risk reduction approaches are also provided, including technical, legislative, and architectural techniques.

The User Scenario details Mohammad's experience as a university graduate transitioning from a science background. Along with looking for jobs in his own country, Mohammad is exploring options to study at international universities in

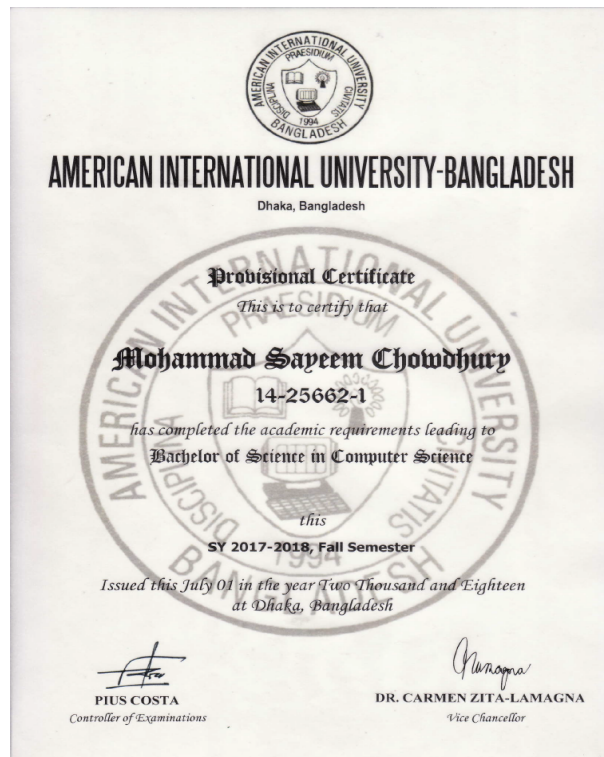


Figure 4.4: Academic Credential without Civil Identification

a more specialized topic. Mohammad holds a bachelor's degree in science and is currently enrolled in a university-level certification program. He is responsible for connecting with a number of systems, utilizing his academic credential record to track his successes and determine which ones to share with other schools. Numerous instances of such systems are as follows:

- Tools for navigating career
- System(s) for Recruiting/Applicant Tracking
- System(s) for Assessment
- System(s) for Background Checks
- System(s) for Human Resource Information System
- System(s) for Data Collaboration

4.6.1 Expected Risk

This report examines the dangers Mohammad may face as a result of his usage of these technologies, including discrimination, manipulation, excessive disclosure,

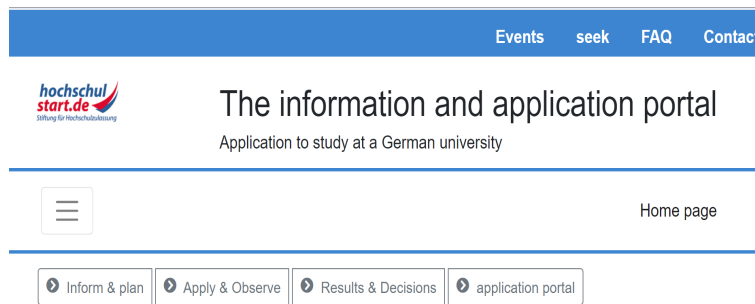


Figure 4.5: Application Portal Germany

tracking, and lock-in/lock-out. Case studies are used to illustrate the findings. The report's objective was to provide plausible responses to each risk segment utilizing both the SSI and privacy-focused frameworks, which are then outlined in detail in the next section.

Generally, the most effective method of mitigating these hazards in the conventional learning environment is through legislation and regulation. Family Educational Rights and Privacy Act (FERPA) and the General Data Protection Regulation (GDPR) are two examples. Decentralized approaches are preferred over centralized approaches in the field of SSI. The SSI approaches are not designed to replace regulations or the rule of law, but to supplement them by providing relief in instances where the rules are not consistently enforced.

4.6.2 Discrimination

In the scenario outlined above, service providers such as academic institutions and labor market firms have access to sensitive information. As a result, they are able to discriminate on the basis of gender, ethnicity, age, and other legally protected characteristics.

Examples include machine learning algorithms that perpetuate biases inherent in training data, frequently without the well-intentioned authors of such optimization algorithms being aware of it. Offering "tailored recommendations" to students also means excluding those who do not meet the criteria for the customised offer, which may result in unintentional bias and illegal discrimination on the part of the institution. For example, when Scandinavian graduates are awarded higher management or academic positions, they are reaffirming the privileges of graduates of Scandinavian schools while discriminating against groups that are underrepresented among Scandinavian graduates. While the term "Scandinavian graduate" is never mentioned explicitly in the training data, machine learning algorithms might "learn" to favor Scandinavian grads.

As a result of systems that are not built to be inclusive from the beginning, discrimination might arise, as well. Accessibility, usability, and inclusivity are all

listed as crucial concerns by the World Wide Web Consortium (W3C) [27] when evaluating how users will interface with websites and services.

Responses

- Selective Disclosure
- Data Minimization
- Governance frameworks
- Embedded identity proofing attributes

4.6.3 Manipulation

For firms that create job exploration tools, student welfare may be a secondary consideration. They will need to upgrade their system to better serve paying consumers if their business model is based on the interests of third parties, as is the case with the various international organizations outlined in the case section of the introduction chapter. If the majority of customers are advertising and recruiting firms, the system may evolve to favor the interests of the customers. If left unchecked, algorithmic decision making may provide features and designs that enrich tool manufacturers at the expense of students.

Responses

- Elective Computation
- Information fiduciaries

4.6.4 Over Disclosure

When information is sought or shared, there is always the risk of revealing more than is necessary. When a driver's license with a person's address is used to purchase a product that can only be purchased by persons who are at least eighteen years old. As an alternative method of demonstrating mastery, students may submit an unedited transcript of their educational history, which often includes the entirety of their courses at the institution they are applying to.

Responses

- Selective Disclosure
- Progressive Disclosure

- Embedded identity proofing attributes
- Data Minimization

4.6.5 Tracking

It is typical to contact the original submitter of the request to ascertain the status of the request. A police officer, for example, may conduct real-time data comparisons of a driver's license to data stored by the Department of Motor Vehicles during a traffic stop. Similarly, businesses can contact the awarding body (or any reputable third party) to ascertain whether candidates have successfully finished their degrees or certificates. Coordinating a student's application to a foreign college necessitates collaboration with the student's home university in order to validate academic qualifications.

Contacting the original issuer to ascertain the most recent status is not unreasonable, and may even be required by legislation or industry standards if done in this manner. Privacy concerns have arisen as a result of an over-reliance on systems that query a single central database, as records become more accessible via digital technologies. Educational institutions and service providers are not required by law to know where students post their academic achievements. Students run the risk of their actions being detected by unauthorized individuals if a solution requires the school to validate their accomplishments.

Responses

- Verifiable credentials
- Decentralized identifiers
- Decentralized verifiable data registries
- Privacy-preserving Credential Status

4.6.6 Vendor Lock-In

Along with the fear of being tracked by centralized verification systems, students face the potential of being unable to utilize their credentials once obtained. Students and other parties relying on credentials lose their value if the process of confirming credentials is dependent on unavailable third-party services. Additional hazards associated with relying on digital credentials include the credential being lost or the student being unable to utilize the credential successfully due to a name change.

Responses

- Verifiable credentials
- Decentralized identifiers
- Decentralized verifiable data registries
- Privacy-promoting credential status checks
- Personal data store
- Governance frameworks

4.7 Response Analysis

4.7.1 Verifiable Credentials

Verifiable Credentials, with their standard, lightweight data architecture, are a critical enabler of interoperability, as they provide a declaration of verifiable authenticity. Depending on the conditions and the particular scenario, a diverse range of data standards can be represented.

When utilizing Verifiable Credentials, one can rely on flexible proof (verification) methods to ensure that cryptographically secure credentials are produced and that the issuing institution stands behind the credentials' declarations. There are a variety of credential status methods available that enable institutions to suspend or revoke credentials on an as-needed basis. For example, both selected disclosure and zero-knowledge proofs can be used in both minimum and progressive disclosure systems, as well as hybrid disclosure systems.

Verifiable credentials data models benefit all processes in this case of user scenario because they enable the expression of credentials in a single format, ease portability and interoperability between systems, and aid in the prevention of lock-in.

4.7.2 Decentralized Identifiers

DIDs(Decentralized Identifiers) enable academic institutions and students to build their identities independently of a central, trusted third party, which is one of their key objectives. When a school declares bankruptcy or consolidates, certain kinds of decentralized identification continue to be utilized even after the institution ceases to exist. Individuals may benefit from the ability to preserve their educational records for the remainder of their lives if the cryptographic material establishing

ownership of an identifier is updateable. Individuals and institutions alike may independently verify the encryption of their decentralized IDs, which is a significant benefit.

As a result, students can maintain their privacy and flexibility across platforms by employing DIDs rather than a single, unique identity.

4.7.3 Decentralized Verifiable Data Registries

When employing decentralized verifiable data registries, such as revocation lists, to broadcast the status of suspended or revoked credentials, there is no need to contact the original issuing authority. There are numerous approaches to decentralize an SSI system through the use of blockchains (or distributed ledger technologies, such as DLT). When this strategy is employed, a single point of failure is less likely to occur; for example, the value of the information may stay intact even if the institution that provided the credentials goes out of business or if the system that produced them goes offline as a result.

In the user scenario, by plotting decentralized verifiable data registries credentials can be examined by the recruitment manager, foreign recruiter, or international admission coordinator, thus improving trust in the process of advancing the candidate to an on-site interview.

4.7.4 Privacy-Preserving Credential Status Check

A credential status check that safeguards personal information is used to ascertain the current state of a credential without disclosing any personal information to the credential's original issuer. The most popular method of determining the authenticity of a credential ID is to contact the issuer directly, which is a simple yet widely used alternative. As a side effect, the issuer receives information about the subject's identification, which is frequently in the form of a reference to a background check firm or institution.

According to a student's academic context, this means an education institution is certain that a specific student is making inquiries about verification requests, which means that the institution can reveal which colleges and companies the student has been communicating. In order to avoid this problem, privacy-enhancing checks allow verification to take place without the disclosure of any identifying or personally identifiable information (PII). The following chapter focuses on a variety of different implementations.

4.7.5 Personal Data Stores

The personal data store of an individual is a collection of data repositories that can be accessed and shared only by the individual who has access to them. Individuals

may preserve complete control over these repositories or they may be disclosed in such a way that the individual retains control. Personal blogs, for example, are frequent data repositories with limited storage space. Individuals have created writings that have been published publicly and privately. On the other hand, social networking sites (such as Facebook and Twitter) are highly structured, ad hoc data storage services such as Dropbox and Google Drive.

Maintaining credentials and accessing them is critical, regardless of where they are stored, for students. This might be a centralized service that gathers credentials from a variety of sources and provides a graphical user interface for curating and showing many representations of the same information to the user. In addition, it is probable that many services (including those supplied by enterprises and academic institutions) provide common APIs that allow employees and students to dynamically export certain accomplishments via a URL on a digital résumé, allowing them to stand out in the crowd.

The usage of personal data stores in the user scenario allows Mohammad to give verifiable application data with the least amount of duplication of effort.

4.7.6 Selective Disclosure

By utilizing cryptographic or structural techniques, an individual can selectively disclose a subset of a much larger data collection. This is referred to as "selective disclosure." For example, selective academic records permit students to disclose information about their academic standing, start and end dates, but not about their courses or tuition payments. Again, a student's selective disclosure employment record enables him or her to identify their employment position, start and end dates, and experiences without disclosing job responsibilities or salary... One way to achieve selective disclosure through technology is to issue a series of oversampled, fine-grained statements from which a student can choose which facts to reveal, using techniques ranging from advanced techniques (such as zero knowledge proofs and redaction signatures) to the brute-force method.

While presenting information selectively does not prohibit later questions, it is critical to keep in mind that additional information may be asked from the student. Rather than requiring the subject of the information to engage in an all-or-nothing interaction, such as revealing the entire driver's license when just the age information is necessary, it allows the subject of the information to choose which data to reveal and which to remain private. Minimal disclosure regulations compel students to supply only the bare minimum information; in exchange, students use selective disclosure to disclose only the information requested.

Mohammad can disclose only the information requested by the admission recruiting/applicant tracking system at the moment of disclosure while employing selective disclosure in the user scenario.

4.7.7 Elective Computation

The term "elective computation" refers to the procedure through which a person desires that their personal information be processed on their behalf. These "automated" enhancements frequently contradict this notion by adopting an unethical paternalistic attitude toward customers' "best interests." Google's search results are an example of elective computation, as they are determined by explicit user requests rather than machine learning. For the majority of individuals, seeing relevant results on the current search results page is expected. Everything is now evident. In other words, it is the objective. Consider how an individual feels when they are "retargeted" with advertisements for things they previously viewed on other websites as a result of ubiquitous advertising technology.

Mohammad must specifically direct the career navigation tool and admissions website to conduct this search for roles and courses that meet his background in the situation outlined above. If not handled effectively and responsibly, the combination of professional and educational aims may result in privacy violations such as discrimination.

4.7.8 Progressive Disclosure

The progression of disclosure involves disclosing less and less information as the value proposition becomes clearer, the connection deepens, and the parties' trust grows. When it comes to internet shopping, the vast majority of firms do not require membership or a credit card to conduct business. People rarely begin by informing a business of their requirements, but they routinely click on links and enter search phrases indicating an interest in particular products. When a buyer is ready to purchase something, he or she must provide payment and shipping information. As a result, the vast majority of internet businesses default to progressive disclosure.

This means that regardless of where Mohammad attended school, the grades he earned, or the dates they were earned, the information shared with applicant tracking and admission portal systems would initially be limited to the bare minimum—for example, attestation of Mohammad's completed degree in a specific field or certifications earned. Mohammad may be required to make more disclosures throughout the application process as he feels more comfortable with the procedure. Personal data gathering can be delayed until later in the hiring or recruiting process, and in certain cases, until after an offer of employment or admission has been extended, "until additional documentation is obtained," if necessary. Individuals can avoid discrimination by concealing personal information such as their name, age, and even their school attendance.

4.7.9 Embedded Identity Proofing Attributes

Even if advanced selective disclosure techniques are available, a credential may be essential and appropriate for exposing personally identifiable information (PII). By examining the document itself, a human observer can assess whether or not the individual presenting the document is the same person who has been issued it in the first place. Additionally, in addition to the holograms and microprinting on the ID card, a person can validate an individual's photo, age, eyes, hair, and other "soft" biometrics such as fingerprints.

When employers and admission recruiters incorporate identity proofing characteristics into a given credential and combine them with limited and selective disclosure, employers and admission recruiters can more easily associate the credential with a new employment or admittance offer. By law, students must submit their full legal name, as well as any supporting documentation, when completing admissions and employment paperwork. If the embedding qualities are disclosed selectively and requested only when absolutely necessary (minimal exposure), as in a progressive disclosure information exchange method, it is permissible to compare one's own name to the name of a credential.

When the approach is employed in the user scenario, it is possible to conduct efficient background checks inside the same credential exchange operations as before.

4.7.10 Data Minimization

Data minimization, as the name implies, is the practice of seeking only the information essential to complete a transaction. Without requiring the customer's age, pizza orders can be placed over the phone; nevertheless, the clerk will need to know the customer's location. When service providers request more information than is necessary, consumers become locked in a vicious circle, unable to use the service or agreeing to an unacceptable risk of harm. This emphasis on requiring only the bare minimum information at each point of the connection is synonymous with progressive disclosure in that it emphasizes the importance of requiring only the bare minimum information at each stage.

Encryption and data security concerns associated with storing personally identifiable information (PII) that may be "exposed to unauthorized access or use" are noted as critical privacy considerations in NIST's "Digital Identity Guidelines: Enrollment and Identity Proofing" [32]. Limiting data collection "encourages confidence in the identity proofing process," thereby mitigating this vulnerability.

By limiting the amount of data collected, Mohammad from the user scenario can safeguard his privacy while still establishing trust in the system.

4.7.11 Information Fiduciaries

Informatics fiduciaries are individuals who are legally bound to act in the best interests of others when it comes to the acquisition, processing, and distribution of personal information. Those who are legally required to collect, store, and disseminate personal information are referred to as data controllers. To assist pupils in comprehending knowledge that is too difficult for them to grasp, analogous to the fiduciary obligations that increase society's trust in professionals such as doctors, lawyers, and accountants. Career navigation software vendors and admission portal providers could form a fiduciary relationship, pledging to put students' interests ahead of their own. As a result, there would be less concern about service misuse, such as scope creep, which sometimes favors marketing and paying clients (such as recruiters) at the expense of individual students' rights and interests. Fiduciaries are not a panacea for dishonest actors; lawsuits alleging wrongdoing are made for a reason. For persons who, like students, rely on the good faith of professional service providers to look out for their best interests, the use of fiduciaries to resolve conflicts of interest is well established.

4.7.12 Governance Frameworks

The structures, roles, and rules of an organization or government are frequently referred to as the "governance framework." Due to the cross-domain application of SSI techniques, governance frameworks are frequently used to bridge trust gaps across educational institutions, government organizations, and financial institutions. Governing frameworks contribute to the reduction of failure points by ensuring that records are kept in interoperable formats, are available to students, and adhere to privacy and other best practices to avoid bias throughout the application process.

4.8 Security Challenges

Security audits, threat assessments, and privacy and data protection impact assessments, to name a few, are required for any new technical stack, among other things. Existing threats are subject to being displaced by new ones in the near future. For example, in a setting where the issuer is not required to be consulted, issuing-side threats may be permissible under certain circumstances. Solutions based on purpose-built blockchains may offer whole new security issues that have not yet been addressed. When it comes to new threat models and mitigation measures, stakeholders should proceed with extreme caution.

Chapter 5

Conceptual Design Proposal

A credential is a collection of claims (or statements about a subject) issued by an issuer. It is a foundational SSI concept. A credential may take the form of a diploma or certificate, as well as a license or digital badge, but is not limited to these. The SSI strategy, on the other hand, is based on the convergence of standards and encryption, distributed ledgers, and front-end applications that enable computers to authenticate credentials on their own. We'll discuss how credentials are verified in an SSI environment in the following section, including the roles and human experience that are required.

This chapter covers the design model for the identity management system, which is based on the SSI concept and is intended to provide a means for verifying students' academic success in foreign institutions as well as in the labor market. A student must first enroll in an academic program at his or her selected university in order for this to occur. In this case, both the institution and the students play key roles in the establishment of their digital identities through the use of a decentralized identity management system. It was as a result of this that the design process was separated into three discrete stages (see Figure:5.1).

5.1 Stage one: Using DID to establish identity

A decentralized identifier has been devised to meet the needs of an SSI system's IDs in a draft proposal from the World Wide Web Consortium. They can be generated independently of a centralized authority by students and institutions, and they can be controlled through the use of cryptographic evidence to establish their legitimacy. These IDs are globally unique and are not location-specific.

The advantages of acquiring DID are discussed in the following paragraphs [86]:

- DIDs do not need to be updated because they do not have a lifecycle or expiration date.

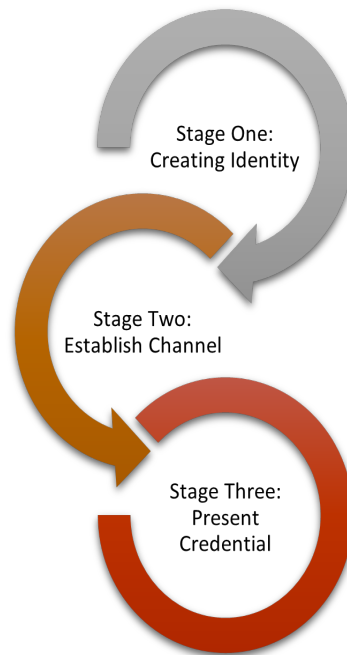


Figure 5.1: Procedural stages of design

- By resolving DIDs, additional information can be retrieved.
- DIDs can be demonstrated to be under the control of their owners at any time through cryptography. Using a public and private key pair, this can be done.
- Without the help of a central authority, a DID can be issued or produced.

Figure 5.2 displays the DID architecture in its entirety, including all of its components and relationships, to show how DIDs work between the institution and the student.

5.2 Stage two: Channel between institution and student

By utilizing a Decentralized Identifier, we can establish a connection between the local institution and the student.

In the figure 5.2 at the top, the DID subject is denoted by the DID, which can be a student. The 'did:example:190392-4841' is an example of a three-part DID. First, the identifier schema is described, followed by an example of how to use the DID method. Finally, the third section, '190392-4841,' is an identifier for students specific to the DID method that can be used to resolve the DID document in this case - a verifiable credential for academic records using the DID method." Because

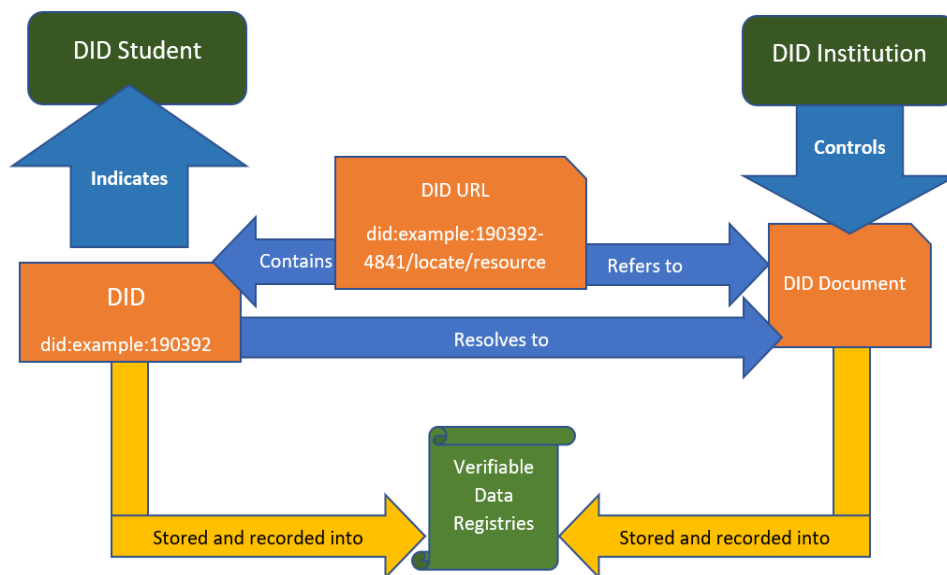


Figure 5.2: Establishing a trustworthy link between the school and the student in order to obtain academic qualifications

of their location independence, DIDs can be stored in a variety of Verifiable Data Registries, including blockchains, decentralized file systems, and even web servers. Create, resolve, update and deactivate DIDs and their relevant DID documents (credential records and location) in a specified data registry using the DID method (did:example). For DID methods that don't require a Verifiable Data Registry, such as did:key or DID-URL, the public key that can be used to derive the DID document is wrapped in a cryptographic wrapper [86]. For DID methods that use blockchains or layers built on top of them as a Verifiable Data Registry, however, the public key is wrapped in a cryptographic wrapper as well. Various academic records linked with DID-Students are described in the DID document, which also specifies how students can interact with verification methods, public keys, and service endpoints (such as a local database of University Record files). Users can be directed to specific resources inside a DID document using DIDs linked to routes. DID URLs are a type of URL. The accompanying figure 5.3 depicts a sample DID document [74]

The presentation concludes with Figure 5.2, which illustrates an academic institution's DID controller. This organization has been authorized to modify the DID document. This is not always the case, though. Generally, the DID controller and subject are the same individual (parent-child relationship) [74]. The World Wide Web Consortium's adoption of the DID standard enables the use of decentralized



Figure 5.3: Documents in the DID format

IDs in SSI situations. It is possible to use DIDs and verified credentials to represent a degree credential to a foreign university or talent market, as well as to act as the foundation for an SSI.

5.3 Stage three: Presenting academic records in credential form

When used in conjunction with DIDs, a data model is necessary to reflect a student’s academic record consistently, despite the fact that DIDs were formed as distinct and independent students. To accomplish this, the World Wide Web Consortium (W3C) developed the Verifiable Credential (VC) standard (see chapter 3). VCs can be used to protect the integrity and validity of academic institutions by representing them in a tamper-evident manner. The three basic components of a VC are depicted in Figure 3.2, each of which is written in JSON-LD format [52].

When it comes to credential information, factors such as location, expiration date, type of degree issued, and revocation process can be defined. These elements can be utilized to identify whether or not the status of a credential has been revoked. As a result, the school may define a set of claims, which may include assertions regarding the student’s academic qualifications. Degree certificates can be verified using cryptographic proof such as JSON Web Tokens or JSON Linked

Data, which can be used to prove their legitimacy [52].

```

1 {
2   "@context": [
3     "https://www.w3.org/2018/credentials/v1",
4     "https://www.w3.org/2018/credentials/examples/v1"
5   ],
6   "type": [
7     "VerifiableCredential",
8     "Higher School Certificate DegreeCredential"
9   ],
10  "issuer": {
11    "id": "did:key:american_international_university123456"
12  },
13  "issuanceDate": "2019-07-01T09:45:32.893Y",
14  "credentialSubject": {
15    "id": "did:key:msch19@aiub.edu123456789",
16    "type": "BachelorDegree",
17    "name": "Bachelor of Science in Computer Science"
18  },
19  "proof": {
20    "type": "Ed25519Signature2018",
21    "created": "2016-10-23T05:50:16Z",
22    "jws": "l1iKjnHy7GFHgFtgFgJhY6TrfHjGgF5R5fTgHJjkkkjhGyT6...",
23    "proofPurpose": "assertionMethod",
24    "verificationMethod": "did:key:
    kjNhYgTf5r4EyHyG7T6tFgVhBgY6T5rnJhBgYgT6Y7Yu8U..."
25  }
26 }

```

Figure 5.4: Degree records in credential form.

To fully comprehend this figure 5.4, it is critical to keep the following in mind: A context definition provides as a jumping-off point for the certification process's semantic terms. Degree certificates are included in this collection, together with the issuing institution's DID and date metadata. The "credentialSubject" object contains detailed information on the student's DID and degree status. Additionally, the DID and VC criteria are inextricably linked, as a DID that uniquely identifies an institution and its students serves as the foundation for the VC criterion. The proof that follows will rely heavily on the public-private key pair associated with the institution's DID. Due to its association with its DID, an institution can use its DID private key to authenticate the signature and credential associated with Linked Data.

Verifiable Presentations (VPs) are also a crucial part of the standard's architecture (see Chapter 3 and Figure 3.2). There will be no loss of cryptographic proofs

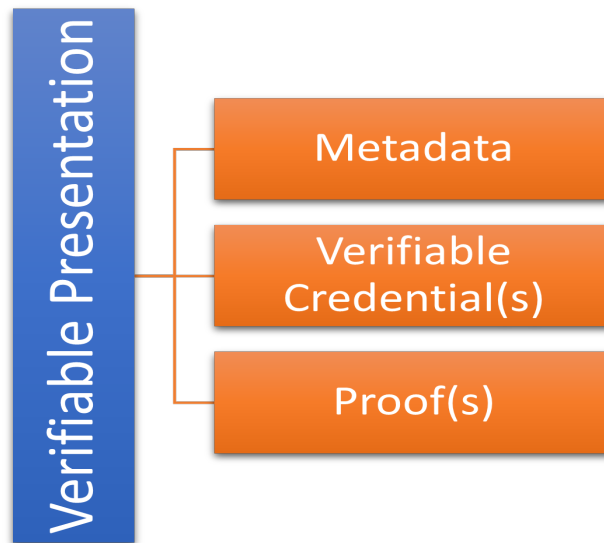


Figure 5.5: Credential presentation format to relying parties

when a student with a Verifiable Credentials(VCs) submits in a verifiable presentation form to a foreign institution or company. Using this method has a wide variety of advantages. Students, on the other hand, have the option of choose which credentials they wish to make public, and they are already demonstrating ownership by obtaining the credentials in the first place. Figure 5.5 shows the format of the Verifiable Presentation in a concrete manner [52].

A metadata attribute can have attributes such as context, type, and expiration time, just like in the previous two examples (see figure 3.2 and 5.5). This is followed by an alphabetical list of the degrees and certificates that will be conferred. Finally, the student's DID private key is used to produce a cryptographic proof. As well as guaranteeing that the credentials were provided by the correct DID student, this safeguards the presentation's integrity. An additional layer of protection against replay attacks can be provided by embedding aspects of the challenge and domain into the proof. This prevents an attacker from delivering the intercepted presentation to another verifier without their permission [52].

5.4 SSI's Functional aspects and interaction between entities

This section goes into greater depth on a number of the SSI's functional aspects. It is for this reason that the roles and interactions within an SSI system are outlined in detail. Participants in an SSI ecosystem can take on one of three fundamental

roles: issuer, verifier, or holder, each of which has its own set of responsibilities. Subsection 3.1.1 provides a high-level overview of these concepts, which are now incorporated into the VC standard.

In an SSI ecosystem, five critical functions exist: (see section 3.1.1)

- Holder
- Issuer
- Subject
- Verifier/Relying Party
- Verifiable Data Registry

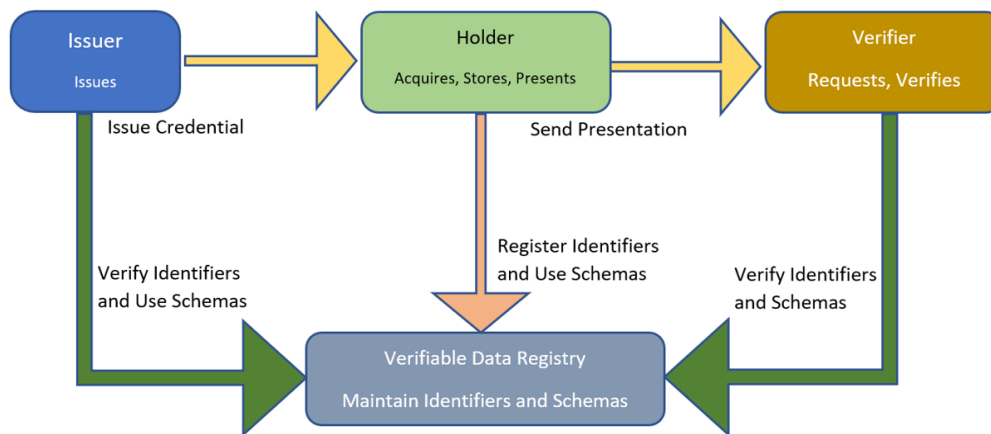


Figure 5.6: The roles and responsibility of SSI Ecosystem [49]

This form of ecosystem is based on the provision of independently verifiable credentials. A third party talent recruiter or foreign institution may rely on the student's credentials (in the form of a verified presentation). To verify credentials, one of the most prevalent scenarios is for the trusting party to employ a standard-based verification protocol (implemented by software/services). As a result, a verified data registry maintains information about both the degree record credential's state and the issuing institution's cryptographic keys. Issuers may control the lifecycle of a credential and demonstrate which credentials have been validated without relying on any third parties. Credential verification requires a paradigm shift to place the student at the center of the credential exchange process. This can occur in a variety of ways:

- It is the issuing institution authority's duty to establish a link with and benefit from the student/record holder.
- In an interoperable academic record wallet/app, a mobile or web-based unique identification (DID) is used to store the student's credentials. One of two things can happen: either the student or the degree holder presents or the relying party (employer or academic institution) requests a credential, either through a wallet, mobile app (or both) or using any portal.
- Following that, the dependent party aka foreign institution or talent recruiter must begin the verification procedure (through a code library or service provider).
- A third-party service may have tampered with the credential, which is determined (typically via a cryptographic signature).
- The legitimacy of the identification document is checked (i.e., confirms that the institution who provides the assertion for the student is a known party and credible for the assertions made in the claims). As an example, a certified data register (explained later section) can be used in this comparison.
- By comparing the credential to an instance of a reliable data registry, this check ensures its validity (that is, it has not been revoked).

Apart from third parties like as issuers and reliant parties, as illustrated in the SSI ecosystem diagram above (Figure: 5.6), credential holders often maintain complete control over how their credentials are maintained and shared. Credential hosting services are provided by a recognized issuer or third party (public or permissioned : detailed later section). Verification is now possible without contacting the issuing institution on a technical level. By utilizing a validated data registry during the verification process, a school authority can also keep control over the state of the credentials it offers (valid or revoked).

Using the trust model outlined above (figure 5.6), as well as recognized standards and technology (see chapter 3), this method is applied to the user scenario in the next section and results in the development of the proposed system that allows entities (local and international institution and organizations) to form trust through real-world interactions.

5.5 Setting up Scenario to create confidence between entities

The analysis chapter gave a scenario involving a student named Mohammad who has earned a degree in his home country and want to pursue a further degree

in a foreign university along with career opportunities in his field of study. This chapter discusses the design paradigm for how institutions and students interact (between entities : issuer and holder). Additionally, this section discusses how to convey an academic certification to another organization (institution or employment recruiter: Relying parties). With this knowledge, the scenario is described in which Mohammad obtains his transcript from his university/institution and, using the identical technique outlined below, submits his academic credentials to third parties.

If local and national institution A wishes to send a credential to Mohammad, a JSON message is generated and obtained from Mohammad's DID record. As a result, Mohammad's public key and a messaging endpoint are both required by institution A. Mohammad is the only person who can decipher the encrypted transcript, and this can only be done through the later approach. For further security, the private key generated by institution A is used to encrypt and sign the transcript. This method allows Mohammad to confirm the authenticity and provenance of the transcripts. Depending on the destination and route, the transcript can be sent in a single trip or spread out across several iterations. Various routing-specific information is incorporated into the standard to do this. When Mohammad uses his private key and the institution's (A) public key to decrypt and authenticate his academic transcript, he can now complete his degree. Even if Mohammad's first application was successful, the same method may be used for a second application to another foreign institution or employment market.

5.6 SSI for Student's Academic Record System

Of course, additional SSI lessons can be applied to students' academic record systems in order to assist them in improving their overall academic performance. This investigation identified potential dangers that might be minimized in part by the application of SSI approaches in a particular user context. The self-sovereignty notion seeks to develop an understanding of how current identity systems might be designed to respect an individual's innate dignity as a person. To implement the policy, there must be a constant interchange of ideas between the policy's architects, regulators, and administrators. While evaluating the principles of SSI for employers, educators, and institutions, students and recent graduates will undoubtedly gain new ideas and strategies. Existing systems, the paper states, will eventually include these concepts. By accumulating all of this knowledge, it is feasible to develop SSI-specific hiring procedures for both job markets and school admissions departments.

Chapter 6

Conclusion

A innovative approach to digital identity, "self-sovereign identity" has recently acquired prominence. Theses aim to offer an overview of the existing identity verification systems for students and their records of academic certificates in addition to developing a novel approach for the evaluation of these systems and their flaw identification. As a result, a conceptual design study was established to evaluate these ideas, and it was based on experts' interviews, real-world experience and the credential lifecycle. This work not only fills a void, but it also adds to the existing body of knowledge. Only a few notable exceptions to this rule have been found in the literature, which has traditionally focused on fundamental research, with little attention made to the practical challenges of existing solutions.

The Verifiable Credential lifecycle was also the subject of a poll of specialists in order to get an overview of the various results or solutions currently on the market and their suitability for dealing with it. Using a questionnaire, three experts from the institution and the talent market who engage with students to evaluate their achievement completed and provided comments for chapters 4 and 5. To ensure that the design proposal in the SSI field would be followed up on, it was helpful to have the support of a professional in examining and analyzing current solutions.

Based on expert advice and practical experience, a new user-oriented evaluation method was devised. It was necessary to seek the advice of experts in the field in order to identify the most crucial criteria for SSI solutions. Research and development of a proposed design model that incorporates three of the choices was also conducted. As a result, the five criteria of usability, adaptability, operability, resilience, and involvement were created. Every single one of these criteria can be used to answer a specific evaluation issue in the real world. This is the first time that a role-based approach has been used to investigate, design, and evaluate SSI solutions. However, while some solutions are ready for production, the field's lack of standards, as indicated by its infancy, continues to impede many of these solutions from being implemented.

Bibliography

- [1] A. De Santis, S. Micali, and G. Persiano, "Non-interactive zero-knowledge proof systems," in *Conference on the Theory and Application of Cryptographic Techniques*, Springer, 1987, pp. 52–72.
- [2] J. E. Van Tol, "Detecting, deterring and punishing the use of fraudulent academic credentials: A play in two acts," *Santa Clara L. Rev.*, vol. 30, p. 791, 1990.
- [3] H. Miller, "The state of the academic profession: An australia-united kingdom comparison," *Australian Universities' Review*, Jan. 1992.
- [4] O. Goldreich and Y. Oren, "Definitions and properties of zero-knowledge proof systems," *Journal of Cryptology*, vol. 7, no. 1, pp. 1–32, 1994.
- [5] R. Daniel and M. Mealling, *Rfc2168: Resolution of uniform resource identifiers using the domain name system*, 1997.
- [6] S. Clauß and M. Köhntopp, "Identity management and its support of multilateral security," *Computer Networks*, vol. 37, no. 2, pp. 205–219, 2001, Electronic Business Systems, ISSN: 1389-1286. DOI: [https://doi.org/10.1016/S1389-1286\(01\)00217-1](https://doi.org/10.1016/S1389-1286(01)00217-1). [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1389128601002171>.
- [7] K. Jordan, J. Hauser, and S. Foster, "The augmented social network: Building identity and trust into the next-generation internet," *First Monday*, 2003.
- [8] R. Riedl, "Rethinking trust and confidence in european e-government," in *Building the E-Service Society*, Springer, 2004, pp. 89–108.
- [9] E. Yoon and T. A. A. Portman, "Critical issues of literature on counseling international students," *Journal of Multicultural Counseling and Development*, vol. 32, no. 1, pp. 33–44, 2004.
- [10] D. Bouchlaghem, H. Shang, C. J. Anumba, M. Cen, J. Miles, and M. Taylor, "Ict-enabled collaborative working environment for concurrent conceptual design," *Architectural Engineering and Design Management*, vol. 1, no. 4, pp. 261–280, 2005.
- [11] C. Kim, *The laws of identity*, 2005.

- [12] T. R. Ruge and A. D. Iza, "Higher education for undocumented students: The case for open admission and in-state tuition rates for students without lawful immigration status," *Immigr. & Nat'lity L. Rev.*, vol. 26, p. 383, 2005.
- [13] J. Hallak and M. Poisson, "Academic fraud, accreditation and quality assurance: Learning from the past and challenges for the future," *Report: Higher Education in the World 2007: Accreditation for Quality Assurance: What is at Stake?*, 2007.
- [14] A. R. Hevner, "A three cycle view of design science research," *Scandinavian journal of information systems*, vol. 19, no. 2, p. 4, 2007.
- [15] K. J. Nyitray *et al.*, "Responding to disruptions in the classroom-a guide for classroom instructors," 2007.
- [16] A. Ezell, "Recent developments with degree mills: Accreditation mills and counterfeit diploma and transcript operations," *College and University*, vol. 85, no. 2, p. 40, 2009.
- [17] D. M. West, "The costs and benefits of immigration," *Political Science Quarterly*, vol. 126, no. 3, pp. 427–443, 2011.
- [18] N. Van der Meulen, "Diginotar: Dissecting the first dutch digital disaster," *Journal of strategic security*, vol. 6, no. 2, pp. 46–58, 2013.
- [19] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *computers and security*, vol. 38, pp. 97–102, 2013.
- [20] M. Sumption and K. Hooper, "Selling visas and citizenship," *Migration Policy Institute Report*, 2014.
- [21] L. Deng, Y. Zhang, J. Li, and D. Dong, "Technology and application of ssi integration framework," *Journal of Zhengzhou University of Light Industry (Natural Science Edition)*, vol. 30, no. 1, pp. 46–49, 2015.
- [22] Y.-C. Lee, C. M. Eastman, and J.-K. Lee, "Validations for ensuring the interoperability of data exchange of a building information model," *Automation in Construction*, vol. 58, pp. 176–195, 2015.
- [23] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains," in *2016 USENIX annual technical conference (USENIX ATC 16)*, 2016, pp. 181–194.
- [24] C. Allen, *The path to self-sovereign identity*, Apr. 2016. [Online]. Available: <http://www.lifewithalacrity.com/>.
- [25] S. E. Chang, W.-C. Shen, Y.-T. Jang, and P.-F. Lee, "Building smartphone apps by using free cloud services from facebook, dropbox and google," in *Advances in Digital Technologies*, IOS Press, 2016, pp. 183–196.

- [26] A. Gopal, "Visa and immigration trends: A comparative examination of international student mobility in canada, australia, the united kingdom, and the united states," *Strategic enrollment management quarterly*, vol. 4, no. 3, pp. 130–141, 2016.
- [27] S. Henry, S. Abou-Zahra, and K. White, "Accessibility, usability, and inclusion: Related aspects of a web for all," *Retrieved October*, vol. 31, p. 2017, 2016.
- [28] S. A. Lee, Y. J. Ju, J.-Y. Shin, E.-C. Park, and H.-Y. Lee, "Readmission rate: Experience in usa, canada and uk," *Quality Improvement in Health Care*, vol. 22, pp. 29–37, Jun. 2016. doi: 10.14371/QIH.2016.22.1.29.
- [29] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *The Sovrin Foundation*, vol. 29, no. 2016, 2016.
- [30] A. Yasin and L. Liu, "An online identity and smart contract management system," in *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, IEEE, vol. 2, 2016, pp. 192–198.
- [31] M. Ali, R. Shea, J. Nelson, and M. J. Freedman, "Blockstack: A new decentralized internet," *Whitepaper*, May, 2017.
- [32] P. Grassi, J. Fenton, N. Lefkovitz, *et al.*, "Digital identity guidelines: Enrollment and identity proofing," National Institute of Standards and Technology, Tech. Rep., 2017.
- [33] P. Gunawong and P. Gao, "Understanding e-government failure in the developing country context: A process-oriented study," *Information Technology for Development*, vol. 23, no. 1, pp. 153–178, 2017.
- [34] S. Huber, S. Rasthofer, and S. Arzt, "Extracting all your secrets: Vulnerabilities in android password managers," in *Hack In The Box Security Conference*, 2017, pp. 1–50.
- [35] Z. Yan, G. Gan, and K. Riad, "Bc-pds: Protecting privacy and self-sovereignty through blockchains for openpds," in *2017 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, IEEE, 2017, pp. 138–144.
- [36] R. Arenas and P. Fernandez, "Credenceledger: A permissioned blockchain for verifiable academic credentials," in *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, IEEE, 2018, pp. 1–6.
- [37] P. Dunphy and F. A. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE security & privacy*, vol. 16, no. 4, pp. 20–29, 2018.
- [38] A. Grüner, A. Mühle, and C. Meinel, "On the relevance of blockchain in identity management," *arXiv preprint arXiv:1807.08136*, 2018.
- [39] M. Hori, S. Ono, K. Miyashita, *et al.*, "Learning system based on decentralized learning model using blockchain and sns," in *CSEDU (1)*, 2018, pp. 183–190.

- [40] R. Liebson and X. Luo, *EXCLUSIVE: Chinese international students caught up in admissions fraud scam*, en-US, Oct. 2018. [Online]. Available: <https://www.sbstatesman.com/2018/10/04/exclusive-chinese-international-students-caught-up-in-admissions-fraud-scam/> (visited on 11/10/2021).
- [41] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018.
- [42] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, "Blockchain-based, decentralized access control for ipfs," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, 2018, pp. 1499–1506.
- [43] V. Venkatraman Iyer, "Entering law students' ethical stigma: A proposal to introduce the mpre along with the lsat," *J. Juris*, vol. 36, p. 101, 2018.
- [44] D. Waddington, "Challenges of canada's decentralized education system.," *College Quarterly*, vol. 21, no. 2, n2, 2018.
- [45] Q. Zheng, Y. Li, P. Chen, and X. Dong, "An innovative ipfs-based storage model for blockchain," in *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, IEEE, 2018, pp. 704–708.
- [46] A. Beduschi, "Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights," *Big Data and Society*, vol. 6, no. 2, p. 2053951719855091, 2019.
- [47] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019.
- [48] O. Borgogno and G. Colangelo, "Data sharing and interoperability through apis: Insights from european regulatory strategy," *A modified version of the paper is forthcoming in Computer Law & Security Review*, 2019.
- [49] D. Chadwick, D. Longley, M. Sporny, O. Terbu, and D. Zagidulin, "Verifiable credentials implementation guidelines 1.0," *W3C Working Group Note*, Sep, 2019.
- [50] D. W. Chadwick, R. Laborde, A. Oglaza, R. Venant, S. Wazan, and M. Nijjar, "Improved identity management with verifiable credentials and fido," *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 14–20, 2019.
- [51] —, "Improved identity management with verifiable credentials and fido," *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 14–20, 2019.

- [52] W. W. W. 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.
- [53] M. Davie, D. Gisolfi, D. Hardman, J. Jordan, D. O’Donnell, and D. Reed, “The trust over ip stack,” *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 46–51, 2019.
- [54] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, “In search of self-sovereign identity leveraging blockchain technology,” *IEEE Access*, vol. 7, pp. 103 059–103 079, 2019.
- [55] D. Hardman, *Aries rfc 0005: Did communication*, 2019.
- [56] M. Kuperberg, “Blockchain-based identity management: A survey from the enterprise and ecosystem perspective,” *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1008–1027, 2019.
- [57] L. Lesavre, P. Varin, P. Mell, M. Davidson, and J. Shook, “A taxonomic approach to understanding emerging blockchain identity management systems,” *arXiv preprint arXiv:1908.00929*, 2019.
- [58] A. Othman and J. Callahan, “The horcrux protocol: A distributed mobile biometric self-sovereign identity protocol,” in *Selfie Biometrics*, Springer, 2019, pp. 355–377.
- [59] D. Roza, K. Kunci, and Guru, “The challenges and strategies in teaching toefl and ielts test preparation,” *J-SHMIC : Journal of English for Academic*, vol. 6, p. 2019, Sep. 2019. DOI: 10.25299/jshmic.2019.vol16(2).3067.
- [60] A. Satybaldy, M. Nowostawski, and J. Ellingsen, “Self-sovereign identity systems,” in *IFIP International Summer School on Privacy and Identity Management*, Springer, 2019, pp. 447–461.
- [61] D. Van Bokkem, R. Hageman, G. Koning, L. Nguyen, and N. Zarin, “Self-sovereign identity solutions: The necessity of blockchain technology,” *arXiv preprint arXiv:1904.12816*, 2019.
- [62] S. R. Ahmed, “Identity crime legislation in the united states, canada, australia and the united kingdom,” in *Preventing Identity Crime: Identity Theft and Identity Fraud*, Brill Nijhoff, 2020, pp. 252–542.
- [63] B. Alzahrani, “An information-centric networking based registry for decentralized identifiers and verifiable credentials,” *IEEE Access*, vol. 8, pp. 137 198–137 208, 2020.
- [64] M. A. Bouras, Q. Lu, F. Zhang, Y. Wan, T. Zhang, and H. Ning, “Distributed ledger technology for ehealth identity privacy: State of the art and future perspective,” *Sensors*, vol. 20, no. 2, p. 483, 2020.

- [65] O. Dib and K. Toumi, "Decentralized identity systems: Architecture, challenges, solutions and future directions," *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN, pp. 2516–0281, 2020.
- [66] A. Kalla, T. Hewa, R. A. Mishra, M. Ylianttila, and M. Liyanage, "The role of blockchain to fight against covid-19," *IEEE Engineering Management Review*, vol. 48, no. 3, pp. 85–96, 2020.
- [67] M. Kubach, C. H. Schunck, R. Sellung, and H. Roßnagel, "Self-sovereign and decentralized identity as the future of identity management?" *Open Identity Summit 2020*, 2020.
- [68] R. Laborde, A. Oglaza, S. Wazan, *et al.*, "A user-centric identity management framework based on the w3c verifiable credentials and the fido universal authentication framework," in *2020 IEEE 17th Annual Consumer Communications Networking Conference (CCNC)*, 2020, pp. 1–8. doi: 10.1109/CCNC46108.2020.9045440.
- [69] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, "Toward trust in internet of things ecosystems: Design principles for blockchain-based iot applications," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1256–1270, 2020.
- [70] D. Longley and M. Sporny, *Linked data proofs 1.0*, 2020.
- [71] M. Luecking, C. Fries, R. Lamberti, and W. Stork, "Decentralized identity and trust management framework for internet of things," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, IEEE, 2020, pp. 1–9.
- [72] N. Naik and P. Jenkins, "Uport open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain," in *2020 IEEE International Symposium on Systems Engineering (ISSE)*, IEEE, 2020, pp. 1–7.
- [73] D. Pöhn and W. Hommel, "An overview of limitations and approaches in identity management," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020, pp. 1–10.
- [74] D. Reed, M. Sporny, D. Longley, *et al.*, "Decentralized identifiers (dids) v1.0," *Draft Community Group Report*, 2020.
- [75] A. J. Zwitter, O. J. Gstrein, and E. Yap, "Digital identity and the blockchain: Universal identity management and the concept of the "self-sovereign" individual," *Frontiers in Blockchain*, vol. 3, p. 26, 2020.
- [76] N. Anaigoundanpudur Karthikeyan, "Cryptographic implementation of issuer policy for self sovereign identity systems," M.S. thesis, University of Twente, 2021.

- [77] P. Bolte, "Self-sovereign identity: Development of an implementation-based evaluation framework for verifiable credential sdks," 2021.
- [78] J. Garcia-Rodriguez, R. Torres Moreno, J. Bernal Bernabé, and A. Skarmeta, "Towards a standardized model for privacy-preserving verifiable credentials," in *The 16th International Conference on Availability, Reliability and Security*, 2021, pp. 1–6.
- [79] R. Garg, *Self Sovereign Identities*. Jul. 2021, ISBN: 978-620-3-92884-6. DOI: 10.5281/zenodo.1251191.
- [80] S. R. Garzon, H. Yildiz, and A. Küpper, "Decentralized identifiers and self-sovereign identity in 6g," *arXiv preprint arXiv:2112.09450*, 2021.
- [81] J. S. Koh, J. Nieh, and S. M. Bellovin, "Encrypted cloud photo storage using google photos," in *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, 2021, pp. 136–149.
- [82] P. S. Lapinski, "Information access and scholarly communication in post-publication peer review online social networks," Ph.D. dissertation, Harvard University, 2021.
- [83] K. Lemoie, "Determinants of behavioral intention to use a self-sovereign identity digital wallet: Extending the utaut with trustworthiness," Ph.D. dissertation, Fielding Graduate University, 2021.
- [84] N. Mohammadzadeh, S. Dorri Nogoorani, and J. L. Muñoz-Tapia, "Decentralized factoring for self-sovereign identities," *Electronics*, vol. 10, no. 12, p. 1467, 2021.
- [85] A. Preukschat and D. Reed, *Self-Sovereign Identity*. Manning, 2021, ISBN: 9781638351023. [Online]. Available: <https://books.google.dk/books?id=BfQ1EAAAQBAJ>.
- [86] A. Preukschat and D. Reed, *Self-sovereign identity*. Manning Publications, 2021.
- [87] M. Schanzenbach, C. Grothoff, H. Wenger, and M. Kaul, "Decentralized identities for self-sovereign end-users (dissens)," 2021.
- [88] D. Shah, D. Patel, J. Adesara, P. Hingu, and M. Shah, "Integrating machine learning and blockchain to develop a system to veto the forgeries and provide efficient results in education sector," *Visual Computing for Industry, Biomedicine, and Art*, vol. 4, Dec. 2021. DOI: 10.1186/s42492-021-00084-y.
- [89] R. Soltani, U. T. Nguyen, and A. An, "A survey of self-sovereign identity ecosystem," *Security and Communication Networks*, vol. 2021, 2021.
- [90] J. Strüker, N. Urbach, T. Guggenberger, *et al.*, "Self-sovereign identity: Grundlagen, anwendungen und potenzielle portabler digitaler identitäten," 2021.

- [91] P. Kavassalis, "Designing an academic electronic identity management system for student mobility using eidas eid and self-sovereign identity technologies,"
- [92] W. Song, R. N. Zaeem, D. Liao, *et al.*, "Self-sovereign identity and user control for privacy-preserving contact tracing,"

Appendix A

Questionnaires

The set of questions was enumerated here, and the expert responses are included in Appendix B.

- 1. What is the title of your position/job?
- 2. Are you currently working on anything that would alter the management system used to verify international students' domestic degree completion?
- 3. What value would you place on the existing system's toolkit and flexibility for successfully implementing new technology?
- 4. What additions or modifications would you make in light of previous incidents?
- 5. Which solutions would you choose and why if you were in charge of a company looking to integrate verification systems into their products?
- 6. Which ones would you choose not to utilize, and why?
- 7. What factors do you believe are critical when evaluating a system for implementing Verifiable Credentials/academic records?
- 8. What do you believe are the most prevalent issues that today's institutional solutions face?
- 9. Is there anything more you wish to say?

Appendix B

Experts' Talk

B.1 Conversation with Eva Marie Althoff Schäfer

After obtaining authorization from the other party to the conversation, a recording of the conversation between Eva Marie Althoff Schäfer and the Author was made and added to the report.

- 1. What is the title of your position/job?
- Ans: International Co-ordinator
- 2. Are you currently working on anything that would alter the management system used to verify international students' domestic degree completion?
- Ans: Yes and No, We continuously working on how to make more efficient the verification process and we are working as a team to process and handle and evaluate international students.
- 3. What value would you place on the existing system's toolkit and flexibility for successfully implementing new technology?
- Ans: We don't have any toolkit until yet, but we have been considering the fact that some other universities uses UKNaric a verification system for international students degree evaluation.
- 4. What additions or modifications would you make in light of previous incidents?
- Ans: We always want to make sure to find the right candidate. When we evaluate any degree certificate, we carefully look the identity attribute with relation to their passport and certificate and try to find any dissimilarity that contradict of what they say about themselves in the academic records.

- 5. Which solutions would you choose and why if you were in charge of a company looking to integrate verification systems into their products?
- Ans: Well, DTU uses UKNaric but we still until my knowledge not using any system but except based on our experience and skill we try to find best candidate for the study place.
- 6. Which ones would you choose not to utilize, and why?
- Ans: Sometimes when we are not sure of any institution in the following countries, we go back to their website and try to find something that we can rely but again it is based on experience but not with assurity.
- 7. What factors do you believe are critical when evaluating a system for implementing Verifiable Credentials/academic records?
- Ans: Name, date of birth and other identifiable attribute i think its important when evaluating.
- 8. What do you believe are the most prevalent issues that today's institutional solutions face?
- Ans: Time. It takes tremendous amount of time to evaluate one candidate.
- 9. Is there anything more you wish to say?
- Ans: We are trying to find a better solution day by day, sharing our thought with our colleagues to come up with new things that help us to easy our procedure to evaluate international students academic records.

B.2 Conversation with Mr. Ziarat Hossain Khan

- 1. What is the title of your position/job?
- Ans: Admission Controller
- 2. Are you currently working on anything that would alter the management system used to verify international students' domestic degree completion?
- Ans: No, but quite few of times we have a discussion about it, specially when it is time for admitting new students in the period.
- 3. What value would you place on the existing system's toolkit and flexibility for successfully implementing new technology?
- Ans: Well, at least something online that we can trust and check more easily without justifying for long.

- 4. What additions or modifications would you make in light of previous incidents?
- Ans: We had face some incidents about students enrolling two degrees at the same time in two different university, but after that the office decided that it is better if we kept students academic transcript to us until the student complete his degree from our university. But it is not the case with our university but most of university here Bangladesh do exactly the same. As because we believe students cannot enroll other program without representing his transcript.
- 5. Which solutions would you choose and why if you were in charge of a company looking to integrate verification systems into their products?
- Ans: Something like governmental records as in universal or at least us like people in academic institution, some kind of collaboration between institution, it can be through educational board ministry or understanding between universities that we can easily look up to students records.
- 6. Which ones would you choose not to utilize, and why?
- Ans: Calling in person of the other side. It is very difficult and timely matter.
- 7. What factors do you believe are critical when evaluating a system for implementing Verifiable Credentials/academic records?
- Ans: Most of the students come to us and ask recommendation letter that they request to make it in envelope with seal and closed so that the foreign university can open as a first time manner. Similarly sometimes we also have to attested or re modify the transcript in case of loss and go through entire record of the students that we believe need to change.
- 8. What do you believe are the most prevalent issues that today's institutional solutions face?
- Ans: Most of the time, forgeries are not that prevalent in our university, since it is not national/governmental university but private company so students here most of time have no competition to enroll except the money that they have to pay. The thing most of time we face is the query from students and other organization that seems to get answer back after long time since we are not enough staff to perform all activities beside our prioritize job.
- 9. Is there anything more you wish to say?
- Ans: We have been excited to see something changes in verification system, and also worried of how to adapt the system fastly when living with not yet but least technology we have.

B.3 Conversation with Mohammad Tanvir Hossain

- 1. What is the title of your position/job?
- Ans: I am in the HR department.
- 2. Are you currently working on anything that would alter the management system used to verify international students' domestic degree completion?
- Ans: We usually look through linkedin and some familiar recruiter also works for us when we need to hire fresh graduate or other employee. But the concept of SSI fascinate me, ofcourse.
- 3. What value would you place on the existing system's toolkit and flexibility for successfully implementing new technology?
- Ans: Something like coursera, so if the school provide something like that, our belief would become more strong and trustworthy.
- 4. What additions or modifications would you make in light of previous incidents?
- Ans: When we interview new students or other individuals, we specifically ask something about what he says in his portfolio and academic record. And we have to justify from that if we can find any disturbance.
- 5. Which solutions would you choose and why if you were in charge of a company looking to integrate verification systems into their products?
- Ans: If i had to choose, I would create a system that enlisted all record of a students like degree certificate we get from Udemmy online or coursera.
- 6. Which ones would you choose not to utilize, and why?
- Ans: the system that exist now. What I meant is that, we have to find the authenticity from a profile which seems to be very much true than it usually are.
- 7. What factors do you believe are critical when evaluating a system for implementing Verifiable Credentials/academic records?
- Ans: Trust problem, may be it seems very important to me. I have to find a way to trust some other company if they says something about an applicant.
- 8. What do you believe are the most prevalent issues that today's institutional solutions face?

- Ans: Making duplicate certificate from other sources that falsified what the applicant says about him. When we talk about background check with the help of our colleague who happens to also studied from the same institution runs a background check with his/her sources and if we are satisfied or not, I believe those are the critical issues that institution faces.
- 9. Is there anything more you wish to say?
- Ans: When hiring students we basically run a skill test and especially prioritize his skill development task record that are more easy to justify rather than qualification achievement.