Deutscher Akademischer Austauschdienst
German Academic Exchange Service

Digitale Bildungsnachweise für Hochschulen (DiBiHo), FKZ: M534800

Requirements Engineering

Interim Report Version 1.0

by

Prof. Dr. Dr. Christoph Meinel
Alexander Mühle
Daniel Köhler
Katja Assaf

Prof. Dr. Hans Pongratz
Dr. Matthias Gottlieb
Ulrich Gallersdörfer
Felix Hoops

Alexander Knoth
Kathleen Clancy
Dr. Barbara Schwazwald
Leo Peters
Erwin Soldo

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Contents

1 Preamble

At the beginning of every successful project there is a phase in which the requirements, whishes and expectations for the project are formulated. In the traditional way of working, a requirements specification is often created and handed over by the client to the development team. Since we are aiming for a strongly user-centered system and are committed to an agile way of working, the formulation of requirements is not implemented by a static specification sheet but by the concept of user stories.

These user stories are created and verified directly in collaboration with stakeholders within the system. This intensifies the communication between developers and future users, thus ensuring that varying interests from different user perspectives are taken into account.

In addition to the direct communication with users, we are also taking the extensive related work on digital credentials in the education sector into account. This also includes general literature concerned with design paradigms for such systems. In this context of design paradigms, we are especially interested in the concepts of user-centric design as well as self-sovereign identity design. While user-centric design has been established for a number of years, self-sovereign identity is a more recent development. Fueled by increased public awareness of privacy and data sovereignity in the digital world these principles are experiencing growing interest.

The overall scope of a productive project runs beyondimplementing functional requirements. Rather, it additionally needs to fulfill non-functional requirements of the system, such as scalability and availability. For this purpose, we will supplement the user stories with a collection of system requirements derived from stakeholder and expert interviews as well as review of relevant literature. We will continuously involve stakeholders throughout the project while further refining and adding new user stories depending on the stakeholder feedback collected.

This document provides a first overview of the derived use cases and corresponding user-stories of the project. Thereby we present the identified requirements as well as the scope of our system. It is important to note that our use cases and user stories were developed as part of a complex project landscape with numerous ongoing related projects and efforts. Due to this complex range of projects, we will first present our own project scope and goals and then contextualise these with a brief overview of relevant related work.

2 Use Cases

In the following sections we will describe the use cases, which provide the main focus of the DiBiHo project. They are threefold and roughly correspond to the focus points of the three project partners. The HPI is closely related with the Massive Open Online Courses (MOOC) platform openHPI, which renders it a natural use case for the institution. The German Academic Exchange Service's (DAAD) core mission is the facilitation of worldwide student mobility via the issuance of scholarships which is reflected in our second use case. Last but not least the TUM as a large public university strives to digitise the issuance of academic degrees at scale traditional university degrees.

2.1 MOOC Certificates

Scenario In this scenario, our learner, Luis is continuously trying to familiarise himself with information technology, as well as wanting to increase their knowledge of this rapidly developing field via MOOCs, a common example of life-long learning. While applying for new jobs, he has started to realise that it appears to be benefical if he attaches relevant certificates awarded to him in previous online-courses. After some research, he identified an online course that would benefit his skill set. However, this course has entry requirements: another course has to be completed. Luckily, Luis recalls that he completed the entry course a few years ago. Providing the old certificate, he is able to participate in and complete the new course. The new certificate can be sent to the potential employer who - in return - has to verify its validity and correctness.

2.1.1 Verifiable Credentials

Course Certificate	Is used to verify the completion of the course
Passport / ID-Card	Is used to map the received certificates to the natural person applying for a job
(*Course*) *Entry Requirements*	Might be any credentials that confirm any criterium used to restrict entry to a course. Examples include: • Completion of a previous course • Employee of a certain company • Person of specific age • Specific citizenship

2.1.2 Special Requirements

It should be possible to generate Credentials for **Course Certificates** which have an expiry date. This ensures that they can properly represent scenarios in which retaking a course is necessary on a regular basis or after a specific time frame. Similarly, all other VCs for certificates from online courses shall not expire.

2.1.3 Diagramm of the Workflow

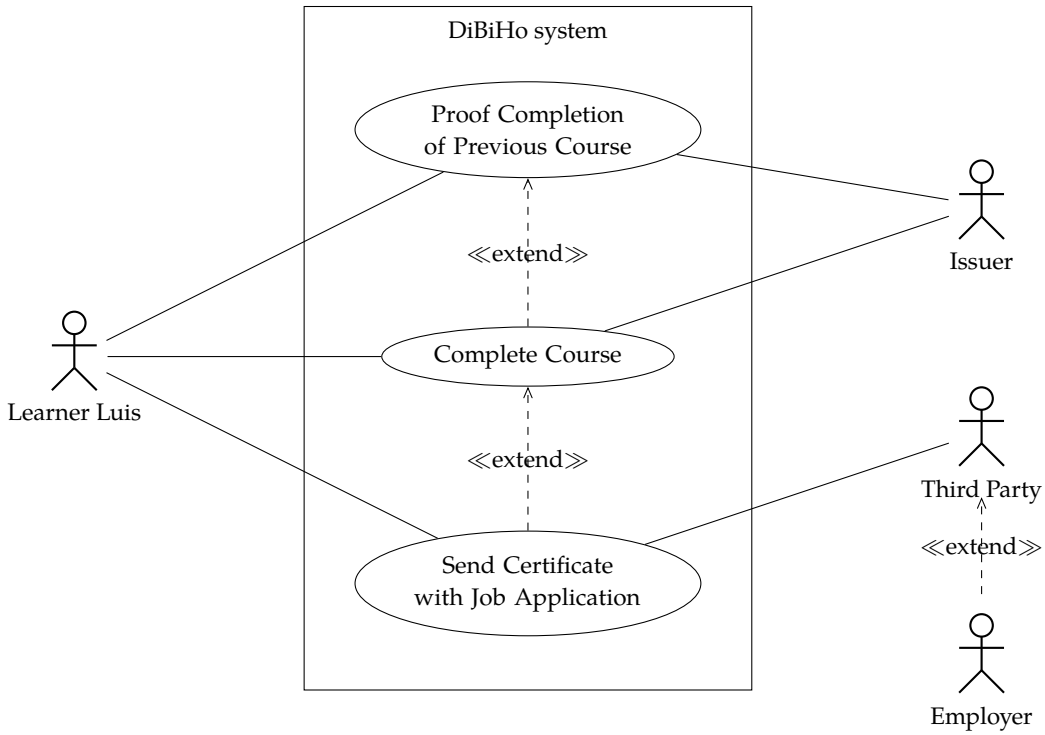

Figure 2.1: Use Case Diagramm: Learner Luis

2.2 Scholarships

Scenario The Learner Laia would like to apply to the DAAD for a scholarship to study for a Master's degree in Germany. To do so, she needs documents, including an expert opinion from the issuer Ignacio regarding an assessment of her abilities and the final certificate of her Bachelor's degree. If possible, these documents should be sent to the DAAD digitally, verifiable and with a receipt. The DAAD would like to check the documents as directly as possible through the scholarship administration system - without manual activities.

2.2.1 Verifiable Credentials

Transcript of Records	Is used to verify the courses taken and the grades obtained
Enrolment Certificate	Is used to verify that the respective person has studied at the university
Degree Certificate	Is used to verify the completion of the respective degree
Passport / ID-Card	Is used to map the received certificates to the natural person applying for a job
Expert Opinion Certificate	Is used for the expert opinion
Receipt Certificate	Is used for confirmation of documents received
Further documents	Depending on the scholarship, further documents are required

2.2.2 Special Requirements

It should be noted that the DAAD also awards scholarships to persons who are based outside Europe.

2.2.3 Diagram of the Workflow

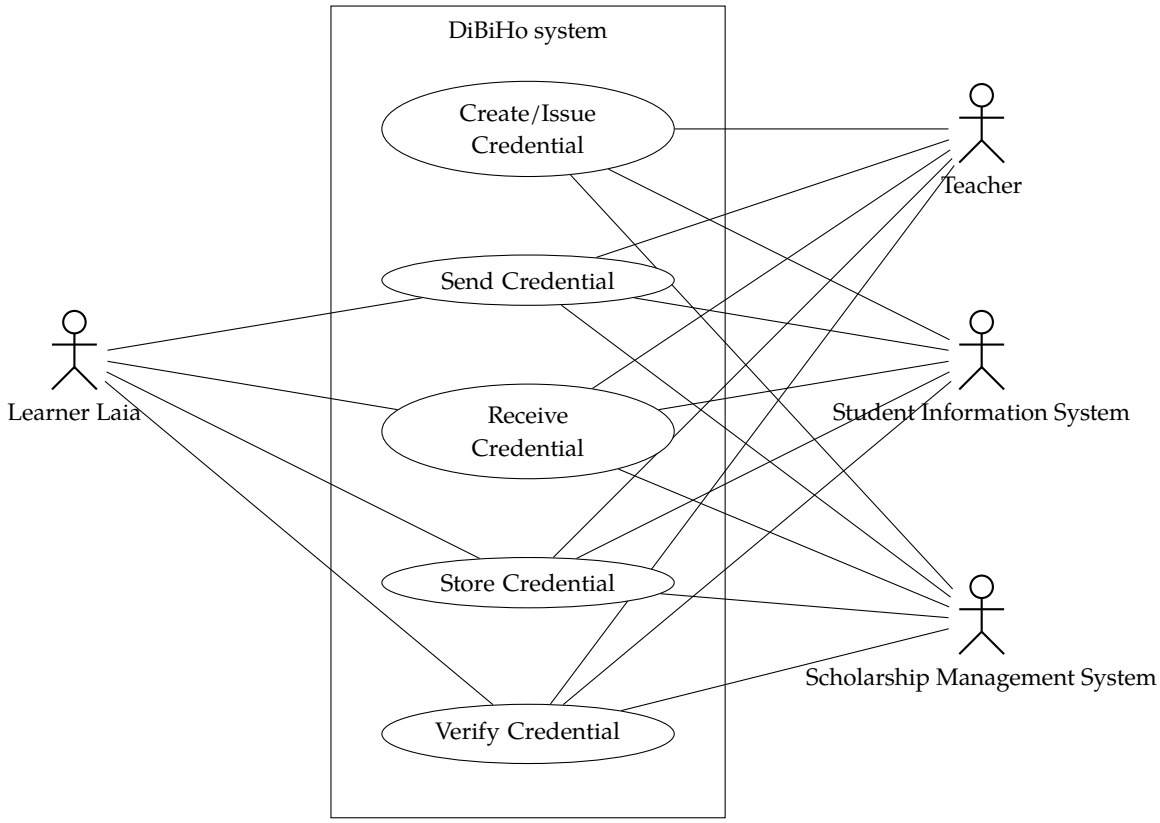

Figure 2.2: Use Case Diagramm: Learner Laia

2.3 Diploma

Scenario In this scenario, our learner, Lucas, is currently finishing his B.Sc. in Economics. He is on his way to the top of his class and will graduate with honors. With his Bachelor's degree, he wants to apply to leading universities in Europe and abroad. As he would like to apply to multiple universities, he needs an easy, cheap and safe way to hand in his certificates. The renowned universities he is applying to, accept his credentials and verify its validity and correctness.

2.3.1 Verifiable Credentials

Transcript of Records	Is used to verify the courses taken and the grades obtained
Enrolment Certificate	Is used to verify that the respective person has studied at the university
Degree Certificate	Is used to verify the completion of the respective degree
Passport / ID-Card	Is used to map the received certificates to the natural person applying for a job

2.3.2 Special Requirements

It should be possible to generate human-readable documents out of VCs in case the receiving party has no means to verify the correctness.

2.3.3 Diagram of the Workflow

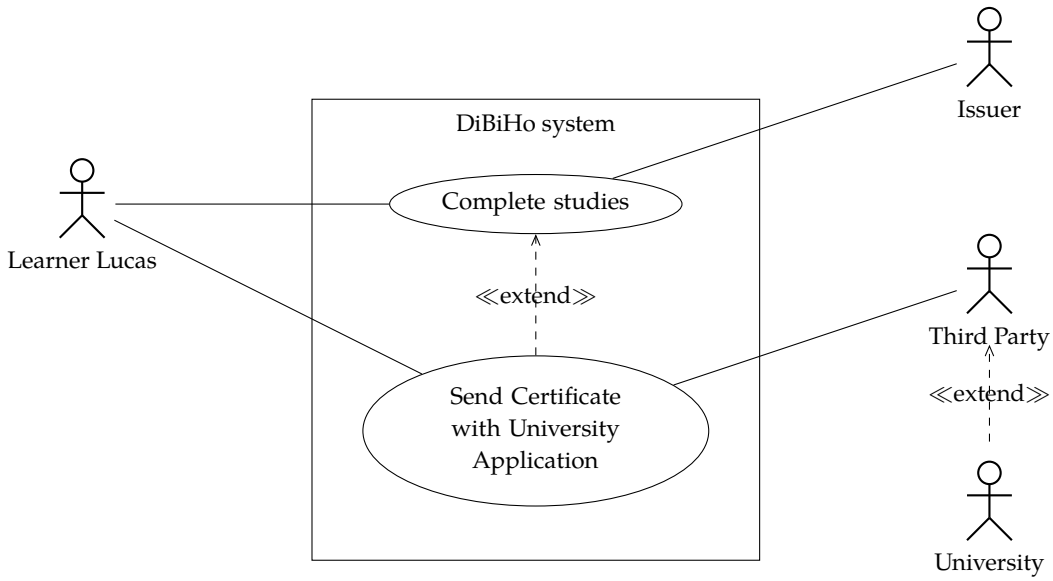

Figure 2.3: Use Case Diagramm: Learner Lucas

3 Requirements Solicitation

This Chapter provides an overview of the different approaches that were taken during the requirements engineering phase to enable a holistic view of the system from a user's perspective in terms of needs for the system.

3.1 Literature Review

The field of digital credentials, especially in the context of educational credentials, has seen a large amount of interest from a broad variety of actors. Both industry as well as academic projects have tackled the issue with different focuses and perspectives.

In order to capture the previous work of projects aiming to provide a credential issuance system we have performed a literature review and summarised or extracted the requirements relevant to the area. These are listed in more detail in Appendix A.1.

They are subsequently matched to our user stories in Chapter 4. The overlap with and distinction from our user stories are discussed in Chapter 6.

Initially, documents of the following national and international projects were reviewed:

- Digital Credential Consortium [1]
- QualiChain [2]
- Blockchain4Education [3]
- EBSI/ESSIF
- Europass Digital Credentials Infrastructure (EDCI)
- EDSSI

Not only have there been projects implementing and piloting such systems but there has also been an academic grappling with the topic of digital credential issuance in education which we have taken into consideration:

- Dimitrijević et al. [4]
- Caldarelli et al. [5]
- Keck et al. [6]
- Carey and Stefaniak [7]

Domain knowledge in the areas of governance and qualifications frameworks was extracted from these publications:

- Ozga et al. [8]
- Ossiannilsson et al. (ICDE) [9]

- Ben Williamson [10]

Finally, as we are aiming to design a user-centric system following the design principles of Self-Sovereign Identity we have also reviewed papers tackling the general definition of this paradigm:

- Christopher Allen [11]
- Andreas Abgraham (EGIZ) [12]
- Satybaldy et al. [13]
- Ehrlich et al. [14]

3.2 Expert Interviews

In addition to a literature review we performed expert interviews with users and administrators of interconnected HEI systems. Thereby being be able to identify the user's needs and transform the systems into requirements for our system. These requirements were specifically selected to provide a deeper insight into our selected use cases and lay a foundation for pilot applications.

3.2.1 MOOCs

The openHPI MOOC platform was selected to be our focus and later serve as a pilot platform. For this purpose we conducted an interview with Thomas Staubitz, the head of the openHPI platform. Before the interview we had access to the openHPI system in the roles of learner and teacher (role: issuer). We used our first impression to formulate concrete questions e.g. about the usage of openBadges or the availability of aggregated statistical data.

During the interview, our expert lead us through the workflow using the views of different personas:

- **Learner** - How is the platform accessed?
- **Issuer, Administrator** - How is the platform administered?
- **Issuer, Teacher** - How and which credentials are assigned and issued upon a learner's completion of a course?
- **Relying Party, HR-Departement** - How can the course credential of a candidate be verified?
- **Relying Party, University** - How can the quality of a teaching offer be ensured when a student wants to be credited ECTS-points for an online course?

During our conversation with the expert, requirements for a potential new system were outlined. These concern mainly aspects of credential types and identity management. Regarding identity management, the way a user logs in and authenticates himself on different platforms turned out to be of particular interest. Requirements for the corresponding identity management systems in regard to privacy, security and usability were named as well. These requirements are formalised in more detail in Appendix A.1.16. Additionally, the topic of scalability was brought up and the following user statistics were given to us to

estimate potential load on the system. Other scalability benchmarks were peak events such as the openWHO system experiencing rates of 50.000 new learners per day during the beginning of the COVID-19 pandemic.

	Users	Enrol ments	Certificates
openWHO	2.385.356	5.356.628	1.366.371
openSAP	1.187.951	5.262.408	561.847
openHPI	274.303	959.919	106.685
mooc.house	63.084	99.748	15.611
lernen.cloud	17.625	26.800	771
KI-Campus	4.838	6.219	14
Total	3.933.157	11.711.722	2.051.299

Table 3.1: Statistics of the HPI-operated Online Learning Platforms

3.2.2 Scholarship

The DAAD's future use of digital credentials within DiBiHo pertains to its scholarship programs for individual mobility. In principle, the process of awarding a scholarship can be divided into three phases:

- Preliminary phase (application, preparation)
- Scholarship phase (while the student is holding the scholarship)
- Post-scholarship phase

In the preliminary phase of the scholarship, the potential scholarship holder applies to the DAAD for a specific scholarship. For this purpose, the potential scholarship holder has to provide different documents (see Use Case). After the acceptance by the DAAD, the potential scholarship holder must declare the acceptance and thereby becomes a scholarship holder in terms of the role. Further documents, such as the confirmation of the university, can be provided after the start of the studies.

During the scholarship period, the scholarship holder receives performance records and evaluations from the university, which are to be forwarded to the DAAD. Should unforeseen problems arise, further communication artifacts will be forwarded to the scholarship holder by the DAAD and, if necessary, answered by the scholarship holder.

After the scholarship has been awarded, the scholarship holder receives proof of funding and, if necessary, further documents that can be forwarded by the scholarship holder, for example, to the tax authorities, potential employers or other research and/or educational institutions.

We conducted two expert interviews in order to obtain knowledge on the varied scholarship options and their distinctive requirements for issuance and verification. All experts were presented with the same questions.

- Nicole Berners, Head of Section "Scholarship Policies"
- Dr Katja Lasch, Director of the DAAD Regional Office New Delhi, India

After a short project introduction, specific questions on types of scholarships, the current issuance and verification process, problems and possible future changes were posed. We asked the interviewees to answer each question reflecting on the preliminary phase, scholarship phase, and post-scholarship phase. The questions are listed below:

- What types of scholarships are awarded by the DAAD? (subject, degree)? How many are awarded?
- In which aspects (roughly) do the individual scholarships differ with regard to the process? How much effort is required by DAAD staff for each aspect?
- Which documents do applicants have to provide at which stages, and which of these are issued directly by universities/research institutes and/ or their staff (e.g. teachers)? Are these submitted as digital artifacts? If so, which ones?
- Are these documents verified by the universities? If so, in what way?
- Which documents are given to the scholarship holder, that can be presented to a university or research institute at a later time? Are these provided as digital artifacts? If so, which ones?
- Are the DAAD documents verified? If so, in what way?
- Does the DAAD have any previous experience with issuing or verifying of digital certificates or credentials?
- What is troublesome about the current process of scholarship application and award? Are there any problems?
- How would you like to structure the application process in the future? What would you change about the current process if you could?

Our findings on current scholarship issuance and (credential) verification processes within the DAAD can be summarized as follows:

- The DAAD issues around 6.000 individual scholarships per year, as many of these scholarships run for more than a year, this means the DAAD supports around 20.000 scholarship holders as part of its individual mobility programs.
- The application and selection processes differ widely according to the type and length of scholarship and the applicant's home region.
- The DAAD has no past or current experience issuing or verifying digital credentials.
- All application documents are submitted via an online application portal (SAP/-MOVE API), except for any references from third parties. These must be sent to the student in a sealed envelope, the student then forwards this sealed envelope to the DAAD headquarters via post. The online application portal is currently being adapted to include an option for the external reviewer to upload the reference directly.
- Submitted documents are currently verified "manually" by DAAD staff, which is very time-consuming. No formal authentication or check for fraudulent documents takes place, statistical records on fraud do not exist. The DAAD often relies on the universities or academic test centers for the formal authentication of documents.

- The DAAD does not communicate directly with the university. The application for a place at university is solely the applicant's responsibility. A scholarship is only ever awarded, if a university place is granted, thus the scholarship is "subject to approval for study in Germany."
- DAAD documents are currently issued in a PDF format using Escriva, the bundle of documents is then sent to the applicant via the online application portal. Documents that are issued by the DAAD are not inspected by the university. Some German embassies abroad (e.g. in Nigeria, Ethiopia, Congo) do not accept digital scholarship awards and require a separate stamped list from the DAAD headquarters.
- Media continuity is identified as problematic throughout the application process.
- The following documents are submitted by the applicant or issued by the DAAD during the three phases of scholarship award:

  Preliminary phase: Verified documents: application form, CV, letter of motivation or intent, research description, reference by external reviewer, academic certificates and transcripts (can be submitted at a later date, if degree has not yet been obtained), language certificates. If documents are not in the national language, a certified translation must be included.

  Issued documents: Letter of Award (includes name, university, field of study, program of study, funding period, information on scholarship amount, travel allowance and type of insurance), contract "Your DAAD scholarship", contract conditions

  Scholarship phase: Verified documents: In some cases: declarations of additional income, application for additional allowances

  No issued documents.

  Post-scholarship phase: No verified documents.

  Issued documents: In some cases: confirmation of scholarship for tax reasons or the calculation of retirement benefits, final reports

3.2.3 Campus

To verify our assumptions and experiences that we have by being HEI graduates and further deepen our understanding of university degree issuance, we conducted an expert interview with Carina Fritzsche, head of TUM's central examination office at the campus Garching. Our semi-structured interview was focused on establishing the details of the current issuance process and capturing important metrics. The rough outline of our interview was as follows:

1. **Project Introduction** - We started out by introducing ourselves and the project for some background.
2. **Our Understanding** - What we already know or assume establishes a base for the rest of the interview and helps to catch possible misconceptions early in the interview.
3. **Current Issuance Process** - How are degree certificates issued and who is involved where and when?

4. **Specific Questions** - Finally, we had some specific questions prepared in advance to stimulate the conversation if necessary and steer it towards topics we deem relevant.

At any point during this interview, we encouraged our partner to talk about anything related coming to mind and proceeded to further inquire about interesting details ourselves whenever the option presented itself. As a result of this interview, we set a number of requirements which are recorded in Appendix A.1.18.

In addition to hard requirements, we gained some more insights. Degree issuance currently takes about 2 to 4 weeks due to the amount of different parties having to physically sign documents. A fully digital system could eliminate the time loss incurred by moving physical documents and decrease this issuance time significantly. It also solves the other major problem currently encountered, which is documents accidentally creasing and having to be replaced during the issuance process, as digital documents cannot crease.

While this is not a hard requirement, we were advised that the simultaneous issuance of physical and digital documents is deemed infeasible due due to the fact that the central examination office is already working at capacity. Also we established that it would make a lot of sense to allow students to request a signed Transcript of Records at any point during their studies. As this is part of the final degree, this functionality could be used as a proof-of-concept for digital university degree issuance.

During our interview we obtained some key figures wich are essential to designing a future-proof digital system. To make sure that we had numbers representative of a typical university, we contacted some other universities. The following table shows our results.

	Degrees p.a.	Revocations	Degree Documents	Signatures	Signers
TUM	10.000	$\approx$ 10%	5	5	3
Uni-Göttingen	5.000	rarely	3	3	2
UDE	6.000	rarely	4	4 to 5	2 to 3

Table 3.2: University degree issuance numbers of contacted universities

4 User Stories

After reviewing literature, consulting experts/stakeholders and eliciting their requirements we formulated user stories to reflect functionality that our system should support. To allow for more transparency and traceability we noted which sources have formulated similar requirements.

Furthermore we divided the requirements into two categories. First is the core functionality that any system such system needs to provide as a basis. Second are additional user stories that are more specific to our project, tailored and elicited from our expert interviews as well as domain specific literature.

4.1 Core Functionality

4.1.1 Learner

DiBiHo-1 As a learner, I want to authorize relying parties to receive and verify my credentials so that I don't need to send them a certified copy of the original.
realizes: Allen-2 , EGIZ-3 , Ehrlich-5 , Satybaldy-1

DiBiHo-3 As a learner, I want to manage (request, present, delete, recover, store) my credentials in a usable and secure way, so that I have full control over my data, can access it at all times, can use the system and have trust in the system.
realizes: Allen-3 , B4E-5 , B4E-6 , Caldarelli-3 , Carey-2 , DCC-6 , Dimitrijevic-5 , EGIZ-1 , ICDE-2 , Keck-3 , Satybaldy-8

DiBiHo-4 As a learner, I want to tie my identifier to my reallife identity, so that I can identify myself.
realizes: EGIZ-3 , Ehrlich-7 , openHPI-5

DiBiHo-5 As a learner, I want to restore my keys, so that I can still use my credentials after having lost my keys.
realizes: Satybaldy-4
Note: *This requirement is necessary if the learner lost their key or the key is compromised. The above requirement does include either the recovery of keys or the regeneration of keys.*

DiBiHo-6 As a learner, I want to create a new account, so that I can have digital credentials assigned to me.
realizes: EGIZ-1 , Ehrlich-6

DiBiHo-7 As a learner, I want to choose a client freely, change to another client or even implement one myself, so that I can choose the client which suits my needs best.
realizes: Allen-6 , Carey-2 , DCC-2 , EGIZ-1 , Ehrlich-2 , Keck-8 , Satybaldy-6

DiBiHo-8 As a learner, I want to choose my storage location, so that I can switch to the storage best suiting my needs of accessibility, privacy, security.
realizes: DCC-7 , EGIZ-1 , Keck-4 , Keck-8 , Satybaldy-6

DiBiHo-50 As a learner, I want to have all information related to me available in my wallet, so that I have full control.
realizes: Allen-3 , Allen-6

DiBiHo-100 As a learner, I want to be able to own multiple identifiers, so that I can have full control over how my data is connected.

4.1.2 Issuer

DiBiHo-9 As an issuer, I want to issue a digital credential, so that I can confirm the claim about a specific learner.
realizes: B4E-3 , Dimitrijevic-1 , QFR-3

DiBiHo-10 As an issuer, I want to be able to revoke credentials, so that they cannot be verified any more.
realizes: B4E-4

DiBiHo-11 As an issuer, I want to delete the learners information, so that I can comply with e.g. DSGVO.

DiBiHo-12 As an issuer, I want to authenticate a learner, so that I can be sure that the subject of the presented digital credential is the same (or authorized) as the receiver of the digital credential.
realizes: DCC-8

DiBiHo-48 As an issuer, I want to log the events when issuing or revoking a credential, so that I can audit the events to determine proper system behaviour.
realizes: DCC-10

DiBiHo-101 As an issuer who is a university, I want to authenticate a learner at the time of enrollment and establish a known identifier for that student, so that I can be sure that subsequently issued credentials are securely bound to that natural person and cannot be passed on.

DiBiHo-102 As an issuer, I want to be able to attribute every credential signature to one specific delegate, so that I can have accountablity in the case of mistakes or malicious

behavior.

DiBiHo-103 As an issuer who is a university, I want to be able to archive all issued degrees, so that I can comply with my legal obligation.

DiBiHo-107 As the issuer's IT department, I want to have an easy-to-integrate REST API that provides all the necessary functions for issuing, transporting, verifying and withdrawing a verifiable credential, so that I can quickly and easily connect these functions to my backend systems.

DiBiHo-108 As an issuer, I want to provide at least one service, so that I can validate and revoke digital credentials.
realizes: DAAD-12

4.1.3 Relying Party

DiBiHo-13 As a relying party, I want to verify a credential, so that I can be sure that the contents of a presented credential are trustworthy.
realizes: DCC-9 , Keck-1

DiBiHo-14 As a relying party, I want to authenticate the issuer of a presented digital credential, so that I can be sure of the identity of the issuer, as well as their authorization to issue, and therefore the validity of the credential.
realizes: DCC-9 , Keck-2

DiBiHo-55 As a relying party, I want to verify a credential without the direct involvement of the issuer, so that I am not dependent on the issuer's infrastructure especially when the issuing party does not exist anymore.
realizes: DCC-3
Note: *We presume that it is not possible to support revocation functionality without the issuers involvement. However, a verification of credentials shall be possible even if the issuer ceased to exist.*

4.1.4 Governance Authority

DiBiHo-15 As a governance authority, I want to express my assertion about an issuer, so that relying parties and users can trust them.
realizes: Caldarelli-7 , Williamson-1

4.1.5 Overall System

DiBiHo-16 As the user, I want to have the standard widely applied, so that I can use it in many different ways.

Note: *The applicable standards will be identified in the next project phase.*

DiBiHo-17 As the user, I want to have the choice of using the UI in my country's official language, so that I have better usability.
realizes: DCC-20
Note: *The supported languages for the first version shall be English and German.*

DiBiHo-109 As a learner, I want to be able to read the structured claim with a default text editor, so that I have human readable credentials.
realizes: DAAD-5

DiBiHo-110 As a user, I want to know how the vc was created, so that I can verify the vc.
realizes: DAAD-7

4.2 Additional Functionality

4.2.1 Learner

DiBiHo-18 As a learner, I want to disclose only the minimal set of credentials to an RP, so that I keep full control over my data.
realizes: Allen-9 , DCC-4 , Ehrlich-1 , Keck-7 , Satybaldy-2

DiBiHo-2 As a learner I want to authorize issuer to create new credentials for me and store them in a trusted data registry so that I can receive new credentials and reject unwanted credentials.
realizes: Allen-2 , Allen-3 , Allen-8 , DCC-1 , Dimitrijevic-3 , EGIZ-1 , Ehrlich-5
Note: *This is a MOOC specific requirement.*

DiBiHo-19 As a learner, I want to delete credentials, so that I can get rid of unwanted credentials.
realizes: Dimitrijevic-5 , Satybaldy-4
Note: *Especially in the MOOC environment where a significant amount of credentials are generated the deletion of credentials is necessary to make the credentials manageable. This does not necessarily mean that all traces of the credential have to be wiped from an issuer's storage and the trusted data registry, but rather that the credentials are not shown in the user's client anymore.*
Note: *Please be aware of the difference between the user controlled deletion and the issuer controlled revocation.*

DiBiHo-20 As a learner, I want to make my credential verifiable for a limited amount of time and/or limited amount of times, so that I keep full control over my data.
realizes: Satybaldy-1

DiBiHo-49 As a learner, I want to be able to hide my identity when presenting a credential to a relying party, so that I can use applicable services under a pseudonym.
realizes: Allen-2 , openHPI-4

DiBiHo-21 As a learner, I want to generate a human-readable version from a verifiable credential, so that I can add it to an application or print it to hang it on my office wall.
realizes: Dimitrijevic-6 , Keck-6

DiBiHo-105 As a non-expert user, I want to be notified of security implications, so that I can use the system securely, even if I am not a security expert myself.

DiBiHo-106 As a learner, I want to export a chosen subset of my credentials into a single PDF, so that I can present the PDF during an (external) application process.

4.2.2 Issuer

DiBiHo-22 As an issuer, I want to administer who is allowed to manage credentials in my organisation, so that I can delegate credential management.
realizes: DCC-10

DiBiHo-23 As a MOOC provider, I want to compare the image of a test taker with the verified image of a learner, so that I can prevent cheating on an exam.
realizes: openHPI-5
Note: *This is a MOOC specific requirement.*

DiBiHo-51 As an issuer, I want to be compatible with Campus Online (TU Graz) and the Move System (DAAD), so that I can easily integrate into existing issuer systems.
realizes: DCC-17

DiBiHo-52 As an issuer, I want to support several different credential types, so that I can use the system as flexibly as possible.
realizes: openHPI-2

DiBiHo-56 As an identity issuer, I want to create a digital credential for a user from their existing identity data, so that I can support self-sovereign identity systems.

4.2.3 Relying Party

DiBiHo-24 As a relying party, I want to authenticate a learner, so that I can be sure that the subject of the presented digital credential is the same (or authorized) as the sender of the digital credential.

DiBiHo-25 As a relying party, I want to integrate the information inside a digital credential in my digital processes, so that I can use it in my further workflows.

realizes: Keck-6 , QFR-22

4.2.4 Governance Authority

DiBiHo-26 As a governance authority, I want to inspect the issuers and access key metrics, so that I can make informed decisions for governance.
realizes: Ozga-1 , Williamson-2

4.2.5 Qualification Framework

DiBiHo-27 As a qualification framework, I want to define the structure of applicable digital credentials during issuance, so that credentials can easily comply with my framework.

DiBiHo-28 As a qualification framework, I want to communicate the requirements for a course, so that the issuer can appropriately identify the skill level of the learner.
realizes: Carey-1 , ICDE-1
Note: *This is a MOOC specific requirement.*

DiBiHo-29 As a qualification framework, I want to be able to review the offered courses associated with digital credentials using my qualification framework, so that I can perform quality assurance.
realizes: ICDE-3
Note: *This is a MOOC specific requirement.*

4.2.6 Overall System

DiBiHo-30 As the user, I want to use the system regardless of my disabilities, so that no learner is excluded.

DiBiHo-53 As the user, I want to use different login methods, so that I can reuse what I am accustomed to.
realizes: openHPI-3

5 Non-Functional Requirements

This Chapter provides an overview of the non-functional requirements that are imposed on our system. Just as the user stories, we note which sources have formulated similar requirements or have informed our decision.

Open Standard And International Use

DiBiHo-31 The DiBiHo system shall be non-restrictive regarding who can participate in the system.
realizes: Allen-7 , Caldarelli-5 , DCC-5 , EGIZ-3 , Ehrlich-4 , Ehrlich-6
Note: *This is necessary to enable a wide range of users from all participant roles e.g. learner, issuer, relying party. Being able to connect with as much people or institutions as possible is a main factor for attractiveness and user acceptance for the new DiBiHo system.*

DiBiHo-32 The DiBiHo system shall be designed in such a way that users cannot be tracked by a third party.
realizes: DCC-5 , EGIZ-2 , Ehrlich-1 , Ehrlich-5
Note: *This includes protection of users metadata.*

DiBiHo-33 The DiBiHo system shall be free-of-charge for learners.
Note: *Primarily, this ansures that no learners will be unable to use the system because of monetary issues. Further, a free-of-charge system enhances anonymity of the user as there is no need to provide payment information. Enabling this brings a wide variety of users to increase the attractiveness of the system.*

DiBiHo-34 The DiBiHo system shall be documented in a way so that any third party might connect their own client.
realizes: Allen-4 , DCC-16 , EGIZ-4 , Ehrlich-3 , Satybaldy-5

DiBiHo-35 The DiBiHo system PoC shall be open source.
realizes: Allen-4 , DCC-16 , EGIZ-4

DiBiHo-36 The DiBiHo system shall consider differences in national jurisdictions during its architectural phase.
realizes: DCC-20 , Satybaldy-6
Note: *The US still has an embargo on certain cryptographic protocols. Further, intellectual property rights might apply only to certain countries.*

DiBiHo-37 The DiBiHo system shall consider differences in national school systems during its architectural phase.

realizes: DCC-20 , Satybaldy-6

Efficiency and Scalability

A number of projects in the relevant literature have been concerned with scalability issues such as Satybaldy [13] and Carey [7]. In our expert interviews the topic of system scale and requirements for scalability were brought up and more concrete numbers established.

The scale of the systems of the HPI and TUM can be observed in Tables 3.1 and 3.2. The resulting goals for this prototype system have been layed out below.

DiBiHo-38 The DiBiHo system shall be able to register 100.000 learners/day.
realizes: openHPI-1 , TUMCEO-3

DiBiHo-39 The DiBiHo system shall be able to issue 1.000.000 certificates per day.
realizes: openHPI-1 , TUMCEO-3

DiBiHo-40 The DiBiHo system shall be able to verify 100.000 credentials per day.
realizes: openHPI-1 , TUMCEO-3

DiBiHo-41 The DiBiHo system shall be able to support 10.000.000 learners.
realizes: openHPI-1 , TUMCEO-3

DiBiHo-42 The DiBiHo system shall be able to support 10.000.000.000 certificates.
realizes: openHPI-1 , TUMCEO-3

DiBiHo-104 The DiBiHo system shall be able to revoke 1.000.000 certificates per day.
Note: *There are extreme cases where widespread revokation becomes necessary. In a worst-case scenario the system must be able to revoke as fast as it can issue. Regular operation should stay drastically below these figures in terms of revocation volume.*

Fault Tolerance and High Availability

DiBiHo-44 The DiBiHo system shall be designed in such a way that there is no single point of failure.
realizes: Satybaldy-3

DiBiHo-45 The DiBiHo system shall be designed in such a way that it is highly available (99% availability).

Longevity

DiBiHo-46 The DiBiHo system shall be designed with an upgrade strategy.
realizes: Allen-5 , DCC-14 , DCC-15 , Satybaldy-4

Note: *This ensures the longevity of the system by enabling outdated components (e.g. cryptographic protocols) to being upgraded.*

Sustainability

DiBiHo-47 The DiBiHo system shall be designed to be sustainable.
realizes: Caldarelli-4 , DCC-15
Note: *This includes needing the minimal amount of resources. Sustainability is required to enhance the user acceptance of the system.*

Further Requirements

DiBiHo-54 The DiBiHo system shall not interfere with existing processes.
realizes: openHPI-6
Note: *Although, we are convinced that digital credentials can replace classical credentials in almost every use case. The PoC does not support all necessary functionality to do this.*

6 Requirements Tracing

In this section we will analyse how the requirements from similar projects are covered by requirements posed to the DiBiHo system. Therefore, we have chosen a subset of our input requirements as identified and described in Chapter 3 3.

The DCC input requirements [1] have been considered, as DiBiHo is closely coupled with the initiative and subscribes to the same main principles.

Additionally, we consider the 10 principles of Self-Sovereign Identities as identified by Allen in [11]. Although some other literature has subsequently expanded on these principles, Allen's seminal work is still widely considered the basis to the design princple of Self-Sovereign Identity, which makes it a good first gauge on the adherence to the principles.

Last but not least, we check the coverage of the requirements we elicited via our expert interviews 3.2.1 3.2.2 3.2.3 as they are closest to our own use cases.

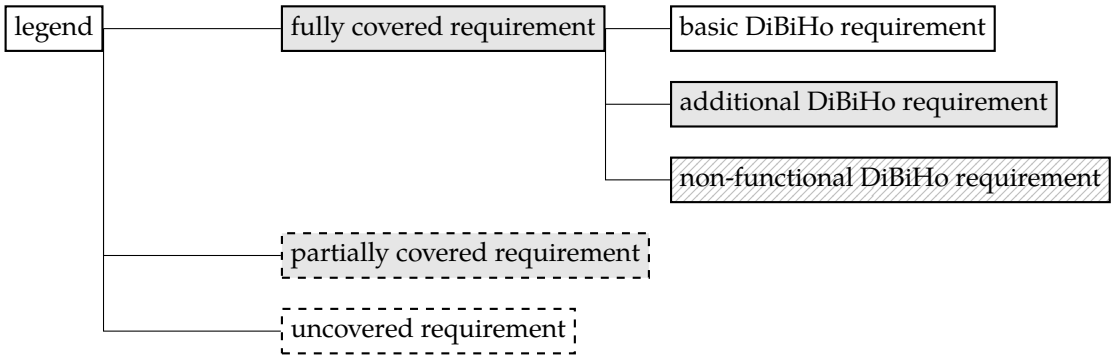

Figure 6.1: Legend

6.1 DCC: Tracing and Coverage

As visualized in 6.2 we do cover most of the DCC requirements. However, some requirements identified by the DCC are either not applicable or not feasible for our project.

- DCC-2 is concerned with lock-in effects and privacy of the learner, which DiBiHo covers. However, DCC is also considering how a learner handles their data after they deceased. This is not explicitly captured by the DiBiHo project since it falls into the wider range of what happens to accounts and data after a person is deceased. We do not foresee any technical measures to support this use case and assume that the heirs are informed about the password of the account through other means. This is sufficient since the digital credentials in our use cases are assumed to not hold much value to the heirs.

- DCC-11 describes the necessity to support a human verifier with easily understandable visual cues. We do not consider the client / application design in such depth in this document.
- DCC-12 describes the necessity to support many different sources and types of credentials. Since we need to restrict ourselves to a subset of inputs due to the project size, this requirement will not be fully covered. The decision which sources and types of credentials will be supported will be taken during the design phase of the PoC.
- DCC-17 refers to the integrability of the system into existing solutions. Due to the size of the project we will only show the integrability into the systems Campus Online (TU Graz) and the Move System (DAAD) as a PoC.
- DCC-18 refers to the preferred trust model of the DCC which is centred around the members of the initiative. Here we deviate from the DCC project as we plan a more open approach where governance authorities may vouch for their issuers as it is currently handled in the non-digital world, where every country might grant any of their institutions the right to issue a master's degree or Ph.D.
- DCC-19 describes the availability of their solution. Although we are planning a publicly available documentation and PoC we cannot, due to the size of our project, ensure to support diverse Use-Cases.

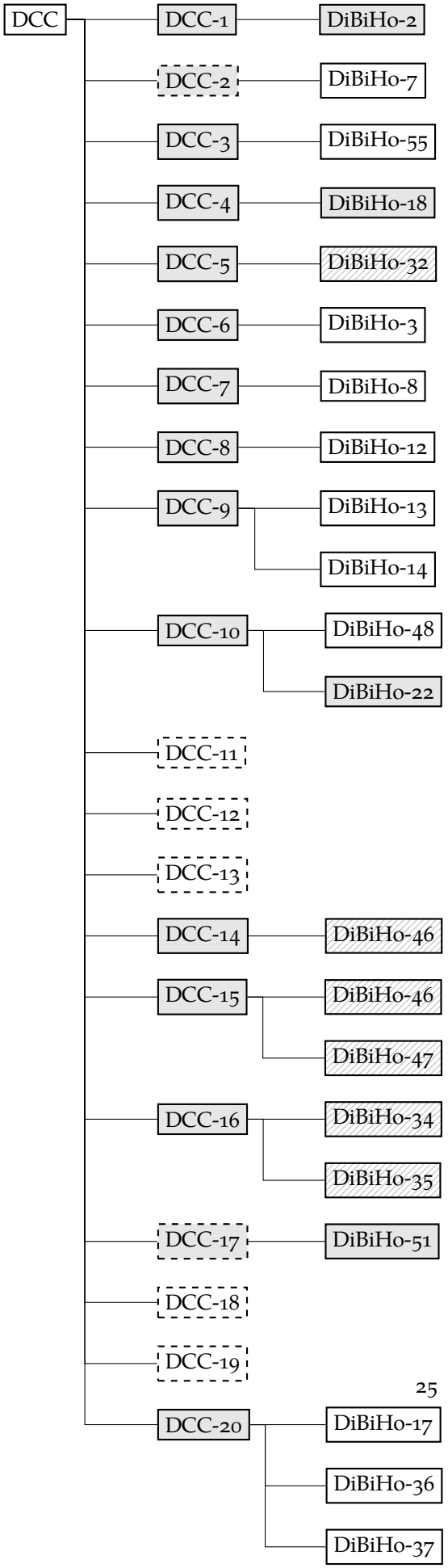

Figure 6.2: Tracing and coverage of [1]

6.2 Allen's 10 Principles: Tracing and Coverage

As visualized in 6.3 we cover or at least consider all of Allen's 10 principles of Self-Sovereign Identities.

- Allen-1 refers to the "I" behind the digital identity. We consider that a rather philosophical question. Additionally, it is rather hard to ensure by technical means that an identity is connected to a physical entity.
- Allen-2 refers to the necessity that the user keeps full control over their own data. This includes amongst other things the right to be forgotten, which is also explicitly mentioned later in the persistence principle A.1.13.
  We consider this covered by the proposed system since all data is stored in the learner's wallet, where the learner has full control. If the issuer or any relying party holds a copy the right to be forgotten is ensured - at least in the EU - by juridical means e.g. GDPR.
- Allen-10 refers to the protection of user's rights. We assume that we cover this requirement by following certain regulations e.g. GDPR and best practices e.g. open source, testing. Although we do not link this requirement since it is to vague to ever be fully covered.

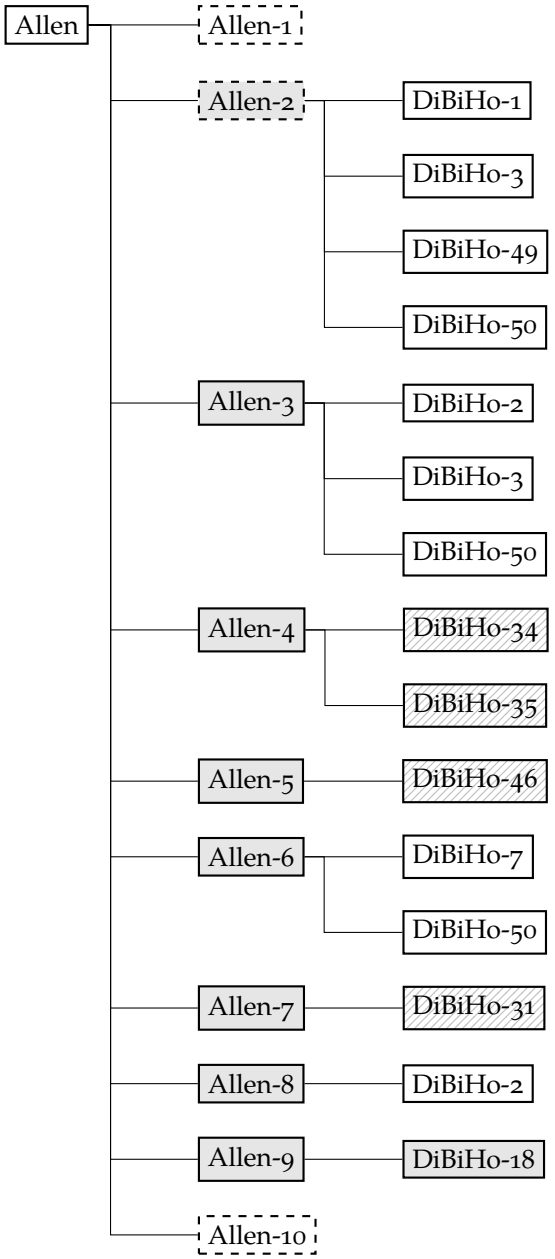

Figure 6.3: Tracing and coverage of [11]

6.3 Expert Interview MOOC: Tracing and Coverage

We cover all requirements which we deducted during or expert interview with openHPI. Only the test coverage is not considered yet.

- openHPI-7 refers to a high test coverage, which we do not consider during the current phase of the project.

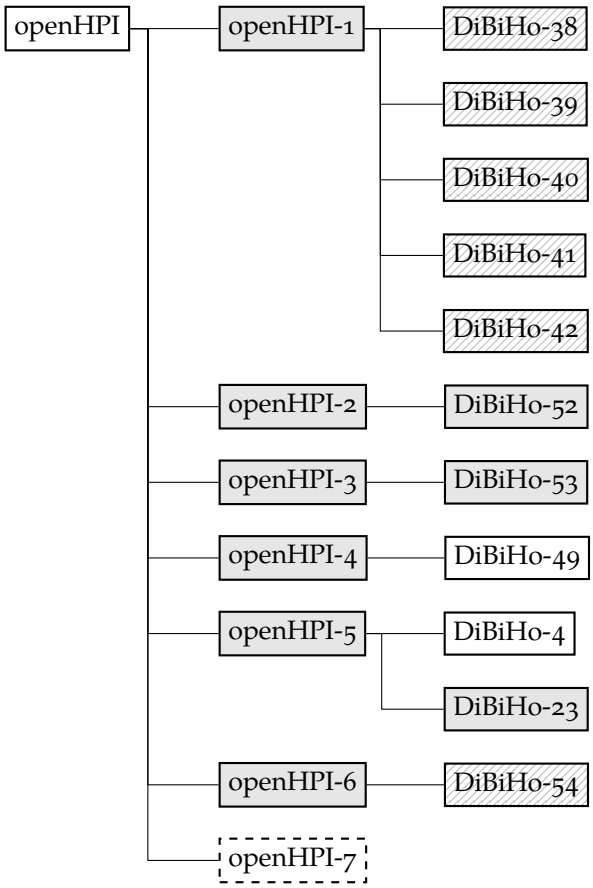

Figure 6.4: Tracing and coverage of 3.2.1

6.4 Expert Interview Campus: Tracing and Coverage

We cover almost all requirements which we deducted during or expert interview with the TUM central examination office (CEO). Only exception is TUMCEO-7, which is covered partially. Credential reissuance is difficult to guarante as we cannot guarantee that an issuer is still in operation at every point in the future. Given our other requirements, especially referring to archiving (DiBiHo-103), re-issuance would be possible if an issuer wishes to implement an appropriate mechanism. For the purpose of this document, we choose to focus on preventing loss of credentials instead.

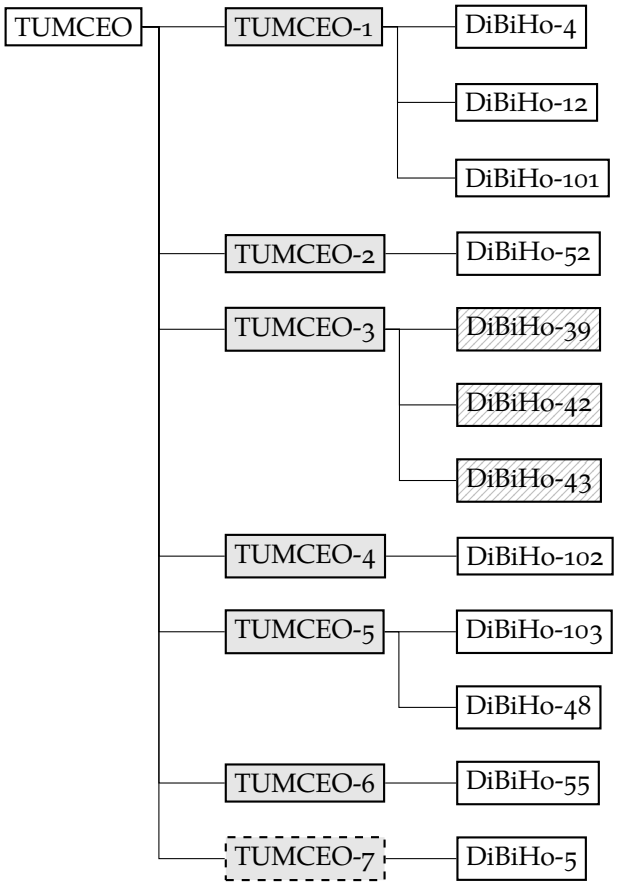

Figure 6.5: Tracing and coverage of 3.2.3

6.5 Expert Interview DAAD: Tracing and Coverage

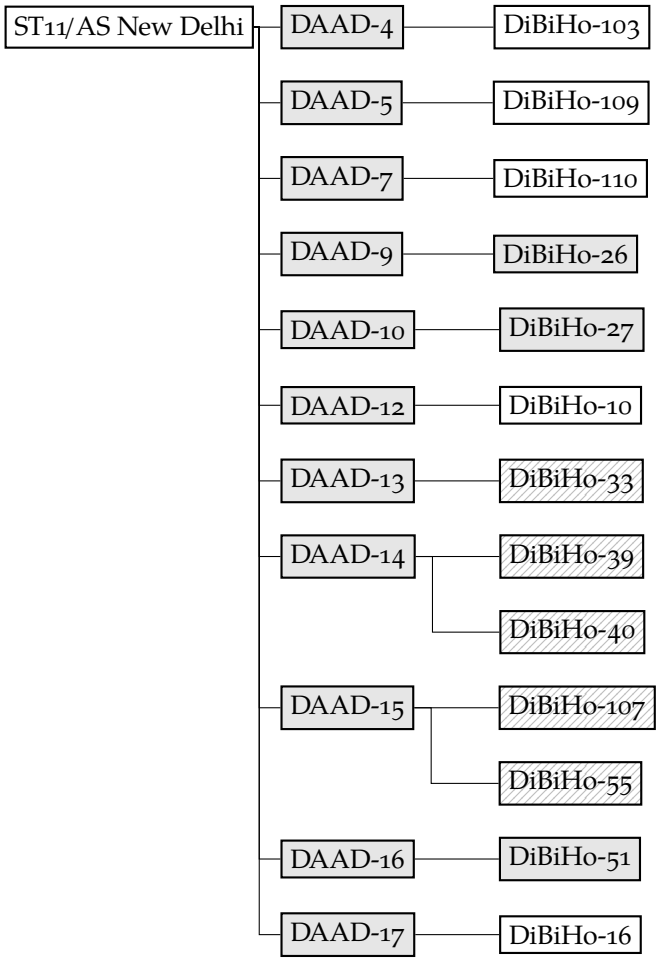

Figure 6.6: Tracing and coverage of 3.2.2

7 Digital Credentials Landscape

The Digital Credentials Landscape worldwide is diverse and highly active. Both government-directed approaches to regulation and infrastructure development as well as a projects and platforms driven by universities, private sector companies, or diverse consortiums contribute to this. While several projects worldwide focus on solutions on a national scale, international cooperation in this area is driven by the European Commission as well as networks such as the Groningen Declaration Network and standardisation bodies such as the W3C.

In this Chapter we will provide an overview related projects that are working in a similar direction as DiBiHo. For this reason, we have listed currently active and related projects that deal with the digital credentialing process chain: "Issue, Transport, Store, Verify, Archive" and not those that are primarily concerned with infrastructure (e.g. EDSSI, EMREX, PIM). This is aimed to give context to the reader and help them distinguish our project from other similar efforts.

7.1 DiBiHo

Running: Dec 2020 – Dec 2022
Partners: Technical University of Munich (TUM), Hasso Plattner Institute for Digital Engineering (HPI), German Academic Exchange Service (DAAD)
Information: DiBiHo - TUM IT - CIO

The aim of the project "Digital Credentials for Higher Education" (DiBiHo), funded by the German Federal Ministry for Education and Research (BMBF) under the funding code M534800, is to explore a **trustworthy**, **distributed** and **internationally usable infrastructure standard** for **issuing**, **storing**, **displaying** and **verifying** academic certificates and educational credentials in a national and international context. Thus, the project serves as a target definition for digital credentials for German higher education institutions that are independent of specialised process manufacturers.

The basis for this is, among other things, the work of the Digital Credentials Consortium (DCC): In 2018, twelve leading international universities, including MIT, Harvard, UC Berkeley, TU Delft, HPI and TUM, founded the Digital Credential Consortium to investigate forgery-proof credentials using blockchain technology and to design and build a global standard for a trustworthy infrastructure for the exchange of digital credentials and academic performance records.

The starting point for the project is the DCC white paper, which aims to develop university-driven infrastructures for digital credentials. As the project partners TUM and HPI are DCC founding members, the results will be incorporated into the future work of the DCC on an international level.

DiBiHo's project work takes into account crucial preliminary work and findings, for example from the "Platform for International Student Mobility" (PIM) and European projects such as EMREX with the ELMO data schema, Europass, European Blockchain Partnership (EBP), European Self-Sovereign Identity Framework (ESSIF), European Student Card Initiative, W3C Verifiable Credentials (VC)/Decentralised Identifier (DID) and from the Groningen Declaration Network (GDN). Essential European data standards from the areas of Single Digital Gateway (SDG), Online Access Act (OZG) and XHochschule (XHEIE) and the eIDAS Regulation, among others, will also be included.

Building on this groundwork, a proof-of-concept will be carried out for various use cases at German universities. This includes the specification of a reference architecture and the data model as well as the development of prototypes and operating, operator and support models. Modelprocesses for generating, storing, transferring, verifying and cancelling (in case of error or revocation) digital academic certificates are to be specified and evaluated.

The project focuses on Self-Sovereign Identity (SSI) as a new paradigm. SSI has emerged in recent years as a complement to user-centric design. It aims to give the user better control over their digital identity and the associated digital assertions. DiBiHo places the user's digital sovereignty at the centre of the system design. To implement this ideal, various approaches are available. For a user-centred requirements analysis, the project investigates three use cases (i) MOOC Certificates, (ii) Scholarships and (iii) Diplomas deriving customised user stories by means of expert interviews.

The project provides a basis for possible operators. It is characterised by a vendor-independent target definition, which considers international standards, taking into account national preparatory work and standards, and examines these for possible interoperable aspects. The project enables further fields of application outside the project focus of universities, for example, vaccination certificates, driving licences or third-party providers of certificates such as evening schools or the German Association for Technical Inspection(TÜV).

Main strategic objectives:

- Independent and technology-agnostic evaluation of existing concepts, data formats and standards for digital, international data transfer.
- Increase of educational mobility through the use of common data standards and increased international compatibility
- Data sovereignty and control for learners based on the principle of Self-Sovereign Identity.
- Unambiguous attribution of individuals to their associated data
- More flexibility in the recognition of academic achievements, especially with regard to skills acquired outside of formal higher education or internationally.
- Achieve more transparency and efficiency gains for universities through the digitalization of organizational processes
- Successful networking of the digital credentials community and continuation of networks beyond the funding period

7.2 Related Projects

The many initiatives related to the research field of digital credentials are listed below according to their geographical reach; at the EU-level alone, there are many projects that are directly related to our area of interest and touch upon relevant topics such as self-sovereign digital identities, verifiable credentials, technologies for data storage and data communication.

7.2.1 National

7.2.1.1 Digitales Schulzeugnis (Germany)

Started: 2019
Partners: Federal Printing Office of the Federal Republic of Germany, govdigtal
Information: Bundesdruckerei Website, DIGIZ Website

The digital Schulzeugnis is a solution of the Federal Printing Office (Bundesdruckerei) for digital high school diplomas. The diplomas are offered both in paper and as PDF documents, whose hash is stored on a private blockchain hosted by the governmental entities forming the govdigital collective. It is currently piloted in NRW, Rheinland-Pfalz and Bremen together with the hochschulstart.de and several universities integrating the verification process into their university admission processes. It is intended to be rolled out nationwide in 2023.

7.2.1.2 Cert4Trust (Germany)

Started:: 2020
Partners: Bavarian State Ministry for Digital Affairs, Chamber of Commerce and Industry for Munich and Upper Bavaria, Chamber of Trade for Munich and Upper Bavaria
Information: Cert4Trust Website

Cert4Trust is a Blockchain based solution to store and verify digital certificates for completed apprenticeships. Its public permissioned blockchain is based on Ethereum and the issued certificates are PDF documents and only offered in combination with traditional paper certificates.

7.2.1.3 Blockchain for Education / DigiCerts (Germany)

Started: 2018
Partners (BfE): Fraunhofer FIT, Fraunhofer Academy, Fraunhofer AISEC Additional Partners (as Blockchain Allianz DigiCerts): TH Lübeck, RWTH Aache, kiron, g.a.s.t., oncampus GmbH, iMoox (Austria), EQASCE
Information: Blockchain for Education, DigiCerts Website

Blockchain for Education is a project to develop an open platform based on blockchain technology to issue, store and display digital credentials. It displays the certificates based on the OpenBadges standard and uses its own Blockchain solution. Its initial prototypes focus

on Fraunhofer Personnel Certification. The project has since expanded as the DigiCerts Blockchain Alliance and conducted some prototypes to integrate digital certificates based on the Fraunhofer Blockchain and on Ethereum into TH Lübecks Moodle Platform.

7.2.1.4 EduCTX (Slovenia)

Started: 2019
Partner: Blockchain Lab:UM, University of Maribor (Slovenia)
Information: EduCTX Website

EduCTX is a private blockchain-based solution for student's certificate management including a web verification portal. The technology uses the Ethereum platform in combination with the Metamask Wallet for Authentication. It is currently in use or prototyped by a small number of universities, namely Brno University of Technology, University of Sarajevo and FH Bielefeld.

7.2.1.5 SURF Edubadges (Netherlands)

Started: 2016
Partners: SURF (Netherlands)
Information: Edubadges Website

Edubadges is a project by SURF, a cooperative association of Dutch educational and research institutions, to bring a unified digital certificates platform for the Dutch education community. It is based on Badgr, which uses the Open Badges standard, and included pilots with 16 HEIs from the Netherlands examining different approaches to use Badged Micro-Credentials (regarding target groups, goals etc.).

7.2.1.6 DUO (Netherlands)

Started: 2012
Partner: Dienst Uitvoering Onderwijs (DUO), Dutch Ministry of Education, Culture and Science (Netherlands)
Information: DUO Website
The Dutch platform DUO is a central student service platform by the Dutch Ministry of Education, Culture and Science. It includes a central diploma service for most Dutch Higher Education institutions that lets students in the Netherlands request a digital extract of their diploma in form of a PDF document with a digital certificate.

7.2.1.7 UNIT/Vitnemålsportalen (Norway)

Started: 2017
Partners: UNIT Directorate for ICT and Joint Services in Higher Education and Research, Norwegian Ministry of Education and Research (Norway)
Information: UNIT Website
The Norwegian Diploma Registry (Vitnemålsportalen) is a Norwegian service established in 2017 by the Norwegian Directorate for ICT and Joint Services in Higher Education and

Research, commissioned by the Norwegian Ministry of Education and Research. It is part of the Norwegian central student service platform UNIT. The main goal of the Diploma Registry is to help individuals collect their results from higher education and share them with potential employers, educational institutions, and other relevant recipients. It is also connected to the Emrex Network.

7.2.1.8 eDiplomas (Greece)

Started: 2019
Partners: Gunet (Greece)
Information: eDiplomas Website

EDiplomas is a web portal for Greece HEI degree verification, that lets the student share their degree information full or in part with interested third parties and currently in its Beta phase, with four out of the 25 member registering their Bachelor diplomas through the platform.

7.2.1.9 DiploMe (Italy)

Started: 2019
Partner: CIMEA (Information Center on Academic Mobility and Equivalence)
Information: CIMEA diploME Website

DiploMe is a blockchain based degree and qualification service using a permissioned Ethereum blockchain with Smart Contracts. It revolves around the diploMe wallet service and allows HEI and other qualification issuing institutions connected to it to issue certificates to learners using the diploMe wallet service. It also includes certifying organisations (like CIMEA itself) as issuers of certificates.

7.2.1.10 DigiLocker NAD (National Academic Repository) (India)

Started: 2017
Partner: University Grants Commision (UGC), Ministry of Education India
Information: https://nad.gov.in/NAD Website

The National Academic Repository is India's nationwide digital degree credential service. It is integrated into India's DigiLocker System, a citizen's wallet that is also used for use cases such as driver's licenses or vaccination certificates.

7.2.1.11 National Student Clearinghouse (USA)

Started: 1993, Electronic Transcript Delivery introduced in 2010
Partner: EAB (Education Advisory Board), Ellucian, Naviance by Powerschool, iQ4, NCCEP (National Council for Community and Education Partnerships), Paradigm, Wiley Education Services, Xello
Information: https://www.studentclearinghouse.org/Student Clearing House Website

The National Student Clearinghouse verifies enrolment, degrees and attendance certificates for nearly all colleges in the USA as well as High School Diplomas via a centralised Web Service. However, its structured as a paid service for schools and students.

7.2.1.12 Other National Diploma Verification Databases

A relevant number of countries in Europe and worldwide, big and small, maintain some kind of central diploma, degree or certificates database and provide a simple form of ID-based verification service for printed or digital (usually in PDF format) diplomas. This is most often based on a verification ID included on the diploma that is used to compare the certificates content with those stored in the central database. Some of those services are part of bigger service platforms, for example also allowing for evaluation of foreign certificates in the country. Examples include:

- EDEBO (Ukraine)
- SAQA NLRD (South Africa)
- ZAQAA QMIS (Zambia) (in development)
- Tartip (Kirgisistan)
- Verficarea Actelor de Studii (Moldova)
- FIS FRDO (Russia)

7.2.2 European Union

7.2.2.1 Europass Digital Credentials Infrastructure (EDCI)

Started: 2020
Partner: European Commission
Information: EDCI Website

Europass is a set of online tools for European citizens intended to help with learning and career management to enable career mobility in the EU single market. The Europass Digital Credentials Infrastructure consists of standards, services and software. It consists of a data model and several web services for issuers and learners allowing the issuance, storage, sharing, viewing, exporting and verification of credentials, as well as an accreditation database for institutions. Issuers can also interact with EDCI via implementation of an API.

7.2.2.2 Qualichain (EU Cooperation Project)

Started: 2019
Partners: National Technical University of Athens (NTUA) (Greece), Atos SE (Societas Europaea), Fraunhofer IAIS (Germany), Knowledge BIZ Consulting (Portugal), The Open University (UK), Leibniz Information Centre for Science and Technology (Germany), INESC-ID (Portugal), Agencia para a Modernizacao Administrative (AMA) (Portugal), Hellenic Parliament (Greece), Supreme Council for Civil Personnel Selection (ASEP) (Greece), Secretary of Health and Civil Protection (Portugal), UNINOVA (Portugal)
Funded By: EU Horizon 2020

Information: Qualichain Website

Qualichain is a research project conducting five pilots using blockchain technology to store, share and verify education and employment qualifications. It also focuses on modern data analysis of these qualifications, e.g. for course choice suggestions for learners or recruitment and personalized candidate notifications for open job offers. A special focus lies on the implications and impact of the use of these technologies (technical, political, socio-economic, legal and cultural).

7.2.2.3 Microbol/MicroHE (EU Cooperation Project)

Running: 2017 - 2020 (MicroHE), 2020-2022 (Microbol)
Partners (Microbol): Flemish Ministry of Education and Training (Belgium), Ministry of Education and Culture Finland, CIMEA (Italy), European University Association (EUA), European Association for Quality Assurance in Higher Education (ENQA), EQAR (European Quality Assurance Register for Higher Education)
Partners (MicroHE): DHBW Heilbronn (Germany), EDEN, Vytautus Magnus University (Lithuania), Institut Jozef Stefan (Slovenia), Tampere University (Finland), Knowledge Innovation Centre, Fondazione Politecnico di Milano (Italy), Knowledge 4 All Foundation
Funded By: Erasmus+ Key Action 3
Information: Microbol/MicroHE Website

MicroHE and MicroBol are two projects focused on analysing and improving the use of micro-credentials in the European Higher Education Area (EHEA) to increase access to continuous learning. Besides extensive surveys and research, MicroHE established a micro credentials clearing house (Credentify) to facilitate recognition of micro-credentials. The ongoing MicroBol project focuses on the question whether and how the existing EHEA tools can be used and/or need to be adapted to be applicable to micro-credentials and intends to propose policy recommendations to contribute to a common European Framework for micro-credentials.

7.2.2.4 ECCOE

Started: 2019
Partners: Fondation UNIT – AUNEGE (France), Knowledge Innovation Centre, Universidad Nacional de Education a Distancia (Spain), DHBW Heilbronn (Germany), Polictecnico di Milano (Italy), Vytautus Magnus University (Lithuania), European Association of Distance Teaching Universities (EADTU)
Information: ECCOE Website

The goal of the ECCOE (European Credit Clearinghouse for Opening up Education) project is the facilitation of open, online and flexible higher education by increasing trust in technology-enabled credentials. Planned actions mainly consist of policy and cooperation efforts like the development of quality descriptors for credentials and the development of Model Credit Recognition Agreement between HEIs, the development of an online catalogue of cross-institution recognisable modules and production and dissemination of

supporting documentation. But it also includes technological development of a system for issuing, sharing and validating digital credentials.

7.2.2.5 EBSI/ESSIF (EU)

Started: 2018
Partner: European Commission, European Blockchain Partnership
Information: EBSI Website

Information: ESSIF Website

The European Self-Sovereign Identity Framework (ESSIF) is part of the European Blockchain Services Infrastructure (EBSI). These EU initiatives aim to provide a framework for the use of verifiable credentials based on an EU-wide DLT infrastructure in combination with an SSI for different domains, including education. All necessary roles and processes are mapped for this purpose.

7.2.2.6 Other National Diploma Verification Databases

A relevant number of countries in the European union maintain some kind of central diploma, degree or certificates database and provide a simple form of ID-based verification service for printed or digital (usually in PDF format) diplomas. This is most often based on a verification ID included on the diploma that is used to compare the certificates' content with those stored in the central database. Some of those services are part of bigger service platforms, for example also allowing for evaluation of foreign certificates in the country itself. Examples include:

- Diplome (France)
- PravyDiplom (Czech Republic)
- LED (Belgium)
- Register of Graduate Students (Bulgaria)
- Virta (Finland)

7.2.3 International

7.2.3.1 Digitary Platforms (MyCreds, My eQuals, CHESICC, RECSIE) (Canada, Australia, New Zealand, China, Japan)

Started: 2005
Partner: Parchment
Information: Digitary Website

Digitary is a private service provider in the realm of digital credentials. They provide the technology for the national digital credentials platforms for Australia and New Zealand (My eQuals), Canada (MyCreds | MesCertif), and China (CHESICC), and are working on the national solution for Japan. While their platform itself is proprietary, they are working

together with Evernym to also offer their credentials aligned with Self-Sovereign Identity Principles using Hyperledger Blockchain technology. Digitary is also a signatory in the GDN. Since 2021, Digitary has formed a joint company with Parchment, another private service provider mainly serving individual universities and colleges in the USA.

7.2.4 Technical Standards

7.2.4.1 W3C Verifiable Credentials

Started: 2017
Partner: n/a
Documentation: Verifiable Credentials Data Model

The W3C Verifiable Credentials is a data model developed by the W3C Verifiable Credentials working group starting in 2017. It provides a general model for handling any (i.e. not just educational) verifiable claim to a person (drivers license, vaccine certificate, university degrees). It has become an official W3C Web standard (called a "Recommendation") in 2019. It has since been adapted or build on in other digital credentials projects, e.g. EDCI.

7.2.4.2 OpenBadges

Started: 2011
Partner: Open Badges IMS Global Leaning Consortium
Information: Open Badges Website
Documentation: Open Badges Standard

OpenBadges are a standard for learning credentials developed by the Mozilla Foundation in 2011 and maintained by the IMS Global Learning Consortium since 2017. It describes a method for packaging information about accomplishments, embedding it into portable image files as a digital badge, and establishing an infrastructure for badge validation. It is mainly used in the context of Micro-Credentials and has been adapted by successful platforms (Badgr, Accredible) and integrated into learning platforms like Moodle. It has served as a quasi-official standard for digital credentials in general with many projects and solutions building on it. OpenBadges 3.0 will combine OpenBadges with W3C Verifiable Credentials.

7.2.4.3 CASE and CLR

Started: 2011
Partner: Open Badges IMS Global Leaning Consortium
Information: CASE Website
CLR Website
https://www.imsglobal.org/activity/comprehensive-learner-record

The IMS Global Learning Consortium extended its digital credentials standards with CASE (Competencies and Academic Standards Exchange and CLR (Comprehensive Learning Record). CASE is a standard for competency definitions to define skills obtainable in learning or associated with degrees or courses. CLR is a a technical specification designed

to support traditional academic programs, co-curricular and competency-based education as well as employer-based learning and development, i.e. various digital credentials. It extends OpenBadges and is compatible with W3C Verifiable Credentials. Offical Documentation: CLR Standard, CLR general information, CASE Specification, CASE general information

7.2.4.4 ELMO

Started: 2015
Partner: n/a
Information: Information: Github Documentation

ELMO is an XML student data exchange format developed by the Emrex network to exchange student result information. It is an XML format for machine readable data that allows for the inclusion of .pdf attachments. It has been adapted in the many European projects, foremost EWP/EDSSI and EDCI.
Official Documentation: GitHub

7.2.4.5 EDCI Data Model

Started: 2019
Partner: European Commission
Information: Website
Website
Github Documentation The EDCI Data Model is an extension of the W3C VC standard and also aligns with the ELMO/Emrex Standard. See also Europass Digital Credentials Infrastructure (EDCI).

7.2.4.6 ESCO

Started: 2013
Partner: European Commission
Information: ESCO Portal
The ESCO (European Classification of Skills, Competences, Occupations and Qualifications) data model is a classification system for skills, occupancies and qualifications for the EU labour market in development since 2010 with v1.0 published in 2017 with several updates since then. It is intended to help clarify qualifications and find better fitting jobs by associating matching competencies. It has been integrated to be used within the Europass profile but hasn't found much adaptation beyond that.

7.2.4.7 Blockcerts

Started: 2016
Partner: n/a
Information: Website
Github Documentation

Blockcerts is an open standard for blockchain-based official records originally prototyped for, but generally not limited to educational credentials. It is an extension of OpenBadges and also aligns with W3C Verifiable Credentials. The prototypes for the system was originally developed at the MIT Media Lab together with the private company Learning machine (now Hyland Credentials). Blockcerts consists of open-source libraries, tools, and mobile apps enabling a decentralized, standards-based, recipient-centric ecosystem, enabling trustless verification through blockchain technologies.
Official Documentation: GitHub, official website

7.2.4.8 XBildung, XHochschule, XSchule (Germany)

Started: 2019
Partners: IT Planning Council Germany, German Federal Ministry of Education and Research, State of Saxony-Anhalt
Information: XBildung Website, XHochschule Website

XBildung is a standardisation project for the German education sector in the context of the OZG-implementation developing overarching data exchange standards covering a huge variety of data and documents occurring during a learner's journey in the education sector. This includes high school and university degrees, but also ex- and immatriculation certificates, BaFöG certificates and many more. Due to its scope, it is segmented into modules (XHochschule, XSchule, XBafög) covering specific areas and started with the development of the XHochschule specification. XHochschule released a first specification in Nov 2020 and has reached version 0.6 recently, while XSchule has just kicked off in April 2021.

7.2.5 Think-Tanks and Networks

7.2.5.1 Groningen Declaration Network

The Groningen Declaration Network is a unique international alliance of universities, ministries, organizations and associations from science and education, as well as digital service providers, founded in 2012. The goal of the Groningen Declaration Network is to advance Student Data Portability worldwide. This core goal is enabling citizens worldwide to consult and share their authentic educational data with whomever they want, whenever they want, wherever they are.

Its commitment to principles such as student-centeredness, security, privacy, and interoperability are laid down in the eponymous Groningen Declaration. The Groningen Declaration Network comprises more than 110 signatories from 30 countries on all continents; from existing student data repositories, universities, scientific and administrative organisations, associations of universities, students, registrars or other stakeholders in the field of digital student data to (commercial) service providers. The diversity of participants, both geographically and thematically, makes the Groningen Declaration Network unique in scope and cooperation potential.

7.2.5.2 Digital Credentials Consortium

The Digital Credentials Consortium is a coalition of 12 leading universities from North America and Europe with the mission to create a trusted, distributed and shared infrastruc-

ture for digital academic credentials. It was funded in 2018 and has since published a white paper on its infrastructure.

7.2.5.3 Netzwerk Digitale Nachweise

The Netzwerk Digitale Nachweise is a German network founded in the context of the OZG-implementation to explore approaches in the area of specifically blockchain-based digital degree certificates. The network published a Whitepaper in 2020 and several of its partners are involved in prototyping projects (e.g. German Federal Printing Office, IDunion, DigiCerts, Helix).

8 Next Steps: Validation of Requirements

After successfully eliciting requirements and recording them in the form of user stories, we will now consult stakeholders from university administrations and learners in order to determine the prioritisation of user stories and validate the completeness of our user stories. There has been considerable prior work on prioritisation techniques which has been systematically reviewed by several surveys [15] [16] [17]. Achimugu et al. concluded that the Analytical Hierarchy Process (AHP) is the most prevalent. It promises reliable prioritisation results with good resilience to errors. However it has been noted that AHP can suffer from scalability issues, as the pairwise comparisons make it time-consuming and difficult for participants when the number of requirements increase. Therefore the planned stakeholder workshops will use the MosCow method when consulting its stakeholders, this means that participants are asked to assign a priority of either must, should, could or won't to each requirement and have the opportunity to add missing user stories. While this method is not as accurate as AHP in terms of the evaluation of relative differences in priority between requirements, it is a simple and time-efficient technique and especially suitable for an audience with differing familiarity with the subject matter. To combat the issue of scalability and further encourage input from the stakeholders, we have divided the user stories into core functionality and additional functionality. The core functionality should be uncontroversial and represent the base system that a credential platform requires. The additional functionality on the other hand is dependent on domain knowledge and tailored to our selected use cases.

A Appendix

A.1 Sources of Requirements

The requirements presented in the following sections were derived and copied (and translated) from impactful related resources as outlined below.

A.1.1 Digital Credential Consortium

The following requirements are taken from the DCC Whitepaper Building the digital credential infrastructure for the future, Chapter I Requirements.

DCC-1 The learner is at the centre of transactions related to their credentials. Both learner and issuer consent is required to issue a credential.

DCC-2 Learners must be able to use credentials flexibly, avoiding lock-in to a specific system. At the same time, the credentials issued by the system will use privacy-enhancing measures to ensure that only the learner has that freedom, while limiting other parties who may want to exploit data about the learner. This includes longer term considerations as well, such as the learner's desire for the handling of their data after they are deceased.

DCC-3 Learners can present their credentials for frictionless verification without requiring the issuer to be involved. This is particularly important during situations where the issuing institution may not be reachable, which could happen if a university has closed, or if broader political or infrastructure problems make contact infeasible.
Note: *The usability of the verification process is a primary consideration to avoid pitfalls such as social engineering exploits that occur when relying parties do not understand verification status messages or other poor visual cues. The verification process must be robust and trustworthy, but implementable in a way that supports seamless integration into a variety of tools.*

DCC-4 Sharing credentials requires the minimum necessary amount of disclosure, in particular for any personally identifying information (PII).
Note: *For example, learners need not send a transcript if all that's requested is the equivalent of a diploma, even though the transcript contains a superset of the data. Traditional credentials do not handle this well; to prove you are over the age of 21, in most jurisdictions you must show a driver's license or other government-issued ID that reveals far more information, such as your exact date of birth and address.*

DCC-5 Minimize the ability of the issuer or other parties to track activities of the learner or correlate information about them.

Note: *For example, the learner may share credentials without involving or even informing the issuer. In addition, this approach minimizes opportunities for the scraping of credential information without consent of the learner, e.g. to create a learner profile by correlating transactions that are recorded on a public blockchain.*

DCC-6 Replacements for lost credentials should be easily requested and securely received from the issuer or a trusted third-party, such as standard-compliant vendors.

DCC-7 The learner can choose where to store and manage their credentials.

DCC-8 The learner can cryptographically prove that a credential is about themself. The system enables learners to use their credentials during digital interactions with other systems that require authentication.

DCC-9 The system should minimize credential forgeability, making credentials tamper-evident in content and presentation, and offering reliable means of establishing authenticity.

DCC-10 Issuers must be able to audit their own issuance and revocation events to determine proper system behaviour and detect fraudulent activity. However, audit logs should minimise PII and only be accessible to users authorised by the issuer.

DCC-11 The visible credential and underlying data must be easily verifiable as consistent. Humans rely on a range of cues (e.g., watermarks, signatures) to make a decision about a credential's integrity, but an under-emphasised aspect of digital credentials is the integrity of how credentials may be displayed on different screens or devices ("display integrity"). Designing for easily verifiable human-readable displays is essential.

DCC-12 The system must provide a standard way to verify credentials from many different sources and support different types of credentials (and credential data standards). Content of the credential can conform to a variety of schemas and vocabularies chosen by the issuer. Some well-known examples used in academic credentialing include PESC, EQF, CTDL, CASE, CLR, ELMO, Open Badges, and Schema.org.

DCC-13 High-certainty verification of credentials is possible with minimum time and cost overhead and scales to the demands of the global higher education system. All aspects that are relied on for learner usage are required to be highly available with appropriate consideration of points of failure.

DCC-14 The system must ensure that credentials can be used by learners at a minimum throughout their lifetime.

DCC-15 The system should avoid excessive resource needs and ensure that the technical design and governance structures can evolve over time to support additional and new use-cases.

DCC-16 No part of the standards or implementing systems requires use of a proprietary solution or specific vendor, though vendors are encouraged to build standards-compliant solutions. It's especially critical that learners have control over where their data resides and are locked neither into a specific provider nor solution.

DCC-17 Issuing functionality is designed to be easy to integrate into existing university student information systems, and offer the features demanded by registrars and other university groups involved in issuing credentials, such as ease of issuance, revocation, recordkeeping, etc.

DCC-18 The open standards used in this approach may be used and adapted for a variety of governance models. Initially, issuer identity verification support will roll out in a trust-building, conservative manner that only takes responsibility for maintaining the identity of members of the initiative.

DCC-19 In addition to adhering to accessibility guidelines and standards (such as the W3C Web Content Accessibility Guidelines), we will seek partnerships to ensure that we are promoting accessibility best practices. Credentials and systems based on this standard should Support Diverse Use-Cases and Technology Best-Practices This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License 12 is broadly accessible, including to those using assistive technologies.

DCC-20 Our approach will ensure usability in different languages, jurisdictions, and conventions.

A.1.2 EDSSI

The European Digital Student Service Infrastructure is intended to bring together various services and standards to create a common infrastructure for Higher Education Institutions. This should allow data about students to be exchanged securely and reliably between Higher Education Institutions and providers of solutions for students.

EDSSI-1 eIDAS serves as a standard for student authentication and identification.

EDSSI-2 The national eID ist the student's used identity or the legitimation or an identity used by the student.

EDSSI-3 The student receives an ESI (European Student Identifier).

A.1.3 Blockchain for Education

Gräther et al. have published their system design for the minimal viable product [3]. They have conducted several workshops and meetings with educational institutions and their use case specific partners in personnel certification authorities. The elicited requirements

were used to derive the features of their first product.

B4E-1 The import of data from legacy systems needs to be supported.

B4E-2 The issuer can browse and search the generated certificates.

B4E-3 The issuer can issue certificates by signing and storing them into a blockchain.

B4E-4 The ongoing validity and authenticity of the certificates has to be ensured. This includes the possibility for the issuer to revoke them.

B4E-5 Learners can create an application portfolio by importing new and existing certificates.

B4E-6 Learners can manage and share their certificates.

B4E-7 The learner is informed about the actions performed on his data such as reading or verifying.

A.1.4 QualiChain

The Horizon 2020 project *QualiChain* has produced an extensive stakeholder requirements elicitation and use case elaboration [2].

QFR-1 QualiChain must allow the creation of users with different profiles.

QFR-2 QualiChain must provide a Web Interface.

QFR-3 QualiChain must allow the creation of degrees and certifications by the Universities.

QFR-4 QualiChain must provide notifications to users.

QFR-5 QualiChain must notify users on their consent to share information regarding their CVs.

QFR-6 QualiChain must be able to create and allow users to attribute smart badges.

QFR-7 QualiChain must provide personalised suggestions for extra-curricular activities, courses they should attend, extra skills that would fit well with their profile, jobs.

QFR-8 QualiChain must alert users with job seeker profiles that new vacancies are available.

QFR-9 QualiChain must provide users with recruiter profiles the list of candidates that match their job offers

QFR-10 QualiChain must provide users with recruiter profile the possibility to define and search competencies/skills when creating job offers.

QFR-11 QualiChain must provide the certification of diplomas, CVs and recommendation letters.

QFR-12 QualiChain should provide users with possible career paths.

QFR-13 QualiChain should advise users with student profiles on courses to attend.

QFR-14 QualiChain should support users with professor profiles when updating courses.

QFR-15 QualiChain should provide users with professor profiles a structured way to assess students evaluations.

QFR-16 QualiChain should provide users with University role analytics and decision support tools to update their curriculums.

QFR-17 QualiChain should provide users with recruiter roles the possibility to create new job offers with employer, specialisation, qualifications, methods, criteria, etc.

QFR-18 QualiChain should provide an automatic CV re-organisation service to their users with candidate profiles.

QFR-19 QualiChain should provide a CV evaluation service.

QFR-20 When a user with a candidate profile has a new verified qualification in QualiChain, this should automatically appear on their CV.

QFR-21 QualiChain should provide a CV shared repository.

QFR-22 QualiChain should screen CVs and provide to Recruiters only the candidates that meet the minimum requirements for that job.

QFR-23 QualiChain should provide to Recruiters access to a career projection service.

QFR-24 QualiChain should provide to Recruiters access to the Multi-Criteria Decision Support Functionality (MCDSS)

A.1.5 Dimitrijević et al.

Dimitrijević et al. identified functional requirements related to different steps of a typical interaction with a bading platform [4]. Subsequently they reviewed six current badging systems compliant with the Open Badges Infrastructure standard. While they focused on the context of Open Badges, the described requirements are still generalisable and relevant to any credential/badge issuance system.

Dimitrijevic-1 Make badges available for issuance which includes the creation of a visual representation of the badge and its different types.

Dimitrijevic-2 Facilitate badge discovery by offering search, review, comparison and selection of a badge opportunity through the badging platform.

Dimitrijevic-3 Allow a learner to apply for a badge.

Dimitrijevic-4 Issue a badge to a learner.

Dimitrijevic-5 Management of and reflection over collected badges. This includes not only collecting badges earned within the platform but also elsewhere. The user should be able to freely organise and visualise the badges.

Dimitrijevic-6 Display and share badges.

A.1.6 Caldarelli et al.

Caldarelli et al. have recognised a number of desired characteristics of an academic blockchain application as well as features that address the central trust issue in such a system (oracle problem) [5]. They conducted a systematic literature review by querying three databases (Scopus, Web of Science and Ebsco HOST Business Source Premier)

Caldarelli-1 **Longevity** It ensures the continued security and immutability of academic records.

Caldarelli-2 **Store diploma and personal skills** Academic records should include students' specific skills, other than just a general certificate.

Caldarelli-3 **User-friendly interface** The blockchain application interface should not require any specific competence on the technology to be accessible.

Caldarelli-4 **Social and economic sustainability** Although functioning and useful, a blockchain application will hardly be implemented if characterised by high economic and social costs.

Caldarelli-5 **Public over permissioned** Data should be publicly auditable in order to be trusted.

Caldarelli-6 **Identifiable Oracles** Oracles need to be known in order to be trusted. Institutional oracles are less efficient.

Caldarelli-7 **Transparent Feedback system** Oracles should be open to public feedback. On the other hand, anonymous feedback is unfavorable

Caldarelli-8 **Incentive mechanism** Oracles should receive compensation for their work. Or a fine if they fail to operate in the desired way.

A.1.7 Keck et al.

Keck et al. formulated challenges in eduation credential management which we take into account [6].

Keck-1 Prevent fraud and facilitate verification.

Keck-2 Verify the issuer of a statement.
Note: *Especially for informal statements such as recommendation letters it is currently hard to verify the issuer.*

Keck-3 Facilitate an easy handling of credentials.

Keck-4 Facilitate long term secure storage of credentials.

Keck-5 Facilitate the transition between anaolgue and digital systems and support existing credentials.

Keck-6 Support both analogue and digital workflows and if necessary create digital or analogue twins.

Keck-7 Ensure data protection, data minimisation and prevent private data leakage.

Keck-8 Ensure the user's control over their data.

A.1.8 Ehrlich et al.

The following requirements are stated by Ehrlich at al.

Ehrlich-1 Datenschutzkonformität, d. h. nur notwendige Daten werden übertragen

Ehrlich-2 Portabilität von Identitätsmerkmalen zwischen ID-Diensten, um Lock-In Effekte zu vermeiden

Ehrlich-3 Hohe Benutzbarkeit (Usability), ohne die Sicherheit zu beschränken.

Ehrlich-4 Breite Anwendbarkeit, d.h. Identitätsdaten sollten in vielen Situationen einsetzbar sein.

Ehrlich-5 Verfügungsmacht über eigene ID-Daten, um ungewünschte Verwertung durch Dritte zu verhindern

Ehrlich-6 Einfacher Zugang für alle berechtigten Nutzer ohne zusätzliche Registrierung

Ehrlich-7 Eindeutige Identifikation von Nutzern für rechtssichere Transaktionen

Ehrlich-8 Geringer Aufwand für ID-Prüfung und Verwaltung personenbezogener Daten

Ehrlich-9 Geringe Kosten bei Einbindung und Verwendung eines ID-Dienstes

A.1.9 Carey and Stefaniak

Carey and Stefaniak conducted interviews in the context of higher education institutions and their digital badge initiatives [7]. While their work mainly focused on user motivation and user perceptions of digital badge programs they still tackled the research question on which design considerations should be considered during the development of such a system.

Carey-1 Evidence and evaluation criteria should be associated with skills-based badges. These should be available through metadata of the badge.

Carey-2 Transferability needs to be ensured so that badges can be shared with other platforms.

Carey-3 Scalability needs to be taken into account.

A.1.10 Ozga et al.

The following requirement was derived from Ozga et al. [8]

Ozga-1 Before an inspection event, key metrics such as student performance and success rates need to be available to be inspected. They are compared to national standards and metrics of other similar institutions.
Note: *Inspection processes shouldn't solely rely on (big) data but can be integrated in a larger*

context of inspection tools.

A.1.11 International Council for Open and Distance Education

The International Council for Open and Distance Education has conducted a state of the art analysis and formulated recommendations for online and open learning education systems [9].

ICDE-1 Assist institutions in designing a personalised quality management system.
Note: *Although some quality systems provide eligibility checks or self-evaluation tools, it should still be made easier for institutions to select or customize an appropriate quality management system.*

ICDE-2 Address quality issues around credentialisation through qualifications frameworks.
Note: *The system should use qualification frameworks to facilitate certifying the aquired learning and enable the recognition of that learning for the purpose of education and employment.*

ICDE-3 Support quality assurance audits and benchmarking exercises.

A.1.12 Ben Williamson

Ben Williamson has described the latest developments and trends of education governance in the context of digitalisation in the European Educational Research Journal [10].

Williamson-1 Support a distributed range of commercial, international and non-governmental actors working in a network to realise educational governance.

Williamson-2 Enable the usage of digital instruments for governing such as eduational data analysis.

A.1.13 Christopher Allen

Allen-1 **Existence**. Users must have an independent existence.
Note: *Any self-sovereign identity is ultimately based on the ineffable "I" that's at the heart of identity. It can never exist wholly in digital form. This must be the kernel of self that is upheld and supported. A self-sovereign identity simply makes public and accessible some limited aspects of the "I" that already exists.*

Allen-2 **Control**. Users must control their identities.
Note: *Subject to well-understood and secure algorithms that ensure the continued validity of an identity and its claims, the user is the ultimate authority on their identity. They should always be able to refer to it, update it, or even hide it. They must be able to choose celebrity or privacy as they prefer. This doesn't mean that a user controls all of the claims on their identity: other users may make*

claims about a user, but they should not be central to the identity itself.

Allen-3 Access. Users must have access to their own data.
Note: *A user must always be able to easily retrieve all the claims and other data within their identity. There must be no hidden data and no gatekeepers. This does not mean that a user can necessarily modify all the claims associated with their identity, but it does mean they should be aware of them. It also does not mean that users have equal access to others' data, only to their own.*

Allen-4 Transparency. Systems and algorithms must be transparent.
Note: *The systems used to administer and operate a network of identities must be open, both in how they function and in how they are managed and updated. The algorithms should be free, open-source, well-known, and as independent as possible of any particular architecture; anyone should be able to examine how they work.*

Allen-5 Persistence. Identities must be long-lived.
Note: *Preferably, identities should last forever, or at least for as long as the user wishes. Though private keys might need to be rotated and data might need to be changed, the identity remains. In the fast-moving world of the Internet, this goal may not be entirely reasonable, so at the least identities should last until they've been outdated by newer identity systems. This must not contradict a "right to be forgotten"; a user should be able to dispose of an identity if he wishes and claims should be modified or removed as appropriate over time. To do this requires a firm separation between an identity and its claims: they can't be tied forever.*

Allen-6 Portability. Information and services about identity must be transportable.
Note: *Identities must not be held by a singular third-party entity, even if it's a trusted entity that is expected to work in the best interest of the user. The problem is that entities can disappear — and on the Internet, most eventually do. Regimes may change, users may move to different jurisdictions. Transportable identities ensure that the user remains in control of their identity no matter what, and can also improve an identity's persistence over time.*

Allen-7 Interoperability. Identities should be as widely usable as possible.
Note: *Identities are of little value if they only work in limited niches. The goal of a 21st-century digital identity system is to make identity information widely available, crossing international boundaries to create global identities, without losing user control. Thanks to persistence and autonomy these widely available identities can then become continually available.*

Allen-8 Consent. Users must agree to the use of their identity.
Note: *Any identity system is built around sharing that identity and its claims, and an interoperable system increases the amount of sharing that occurs. However, sharing of data must only occur with the consent of the user. Though other users such as an employer, a credit bureau, or a friend might present claims, the user must still offer consent for them to become valid. Note that this consent might not be interactive, but it must still be deliberate and well-understood.*

Allen-9 Minimalization. Disclosure of claims must be minimized.
Note: *When data is disclosed, that disclosure should involve the minimum amount of data necessary to accomplish the task at hand. For example, if only a minimum age is called for, then the exact age*

should not be disclosed, and if only an age is requested, then the more precise date of birth should not be disclosed. This principle can be supported with selective disclosure, range proofs, and other zero-knowledge techniques, but non-correlatibility is still a very hard (perhaps impossible) task; the best we can do is to use minimisation to support privacy as best as possible.

Allen-10 Protection. The rights of users must be protected.
Note: *When there is a conflict between the needs of the identity network and the rights of individual users, then the network should err on the side of preserving the freedoms and rights of the individuals over the needs of the network. To ensure this, identity authentication must occur through independent algorithms that are censorship-resistant and force-resilient and that are run in a decentralised manner.*

A.1.14 Satybaldy et al.

Satybaldy et al. have recognised Self-Sovereign Identity systems as the next evolution in identity management and have developed an evaluation framework to evaluate, describe and compare SSI systems [13]. In the process they aimed to answer the questions of what the characteristics of an ideal Self-Sovereign Identity system could be. The majority of the work is based on Allen's 10 principles of SSI as well as Cameron's Laws of Identity [15], extending it by the principle of usability.

Satybaldy-1 User control and consent The user must control their identities and personal data can only shared with consent.

Satybaldy-2 Privacy and protection The user's rights must be protected and the desired privacy level of the user supported. The principle of data minimisation should also be observed.

Satybaldy-3 No trust in central authority The system should not rely on a single third-party entity.

Satybaldy-4 Portability and persistance The longevity of the identities as well as the tranportability of it needs to be ensured. This includes the ability to recover keys and credentials in the case of loss or theft. The inverse of this, the deletion of data, also needs to be supported by the system.

Satybaldy-5 Transparency The system should be designed and operated in a transparent manner. The functionality, operation as well as used algorithms should be free, well-known and architecture independent.

Satybaldy-6 Interoperability The funtionality of the system accross different national boundaries and systems should be supported.

Satybaldy-7 Scalability To keep up with increasing user demands, the system should be highly scalable.

Satybaldy-8 Usability The user experience must be consistent with the needs and expectations of the user. This includes the experience across different platforms and services involved in the system.

A.1.15 Andreas Abgraham

The Austrian government together with the TU Graz identified the potential of self-sovereign identities in 2017 in [12]. The whitepaper is already proposing a blockchain based solution which is reflected in the explicit mentioning of the blockchain within their requirements.

EGIZ-1 Each user must have full control over [their]own identity data.
Note: *This includes not only what identity data are being stored but also who has access to these data. The user should be able to add or import identity attributes as well as delete or revoke them at their leisure. Also, all access of identity data of a user should be logged for later verification.*

EGIZ-2 All identity data have to be stored and processed in a highly secure manner. Additionally, the user's privacy has to be preserved.
Note: *For instance, unlinkability between the user wallet and their identity data increases the user's privacy.*

EGIZ-3 [...]The user should be able to use their identity data wherever they want.
Note: *For instance, a SSI system can be used as identity provider when the user tries to access an online service.*

EGIZ-4 No trust in a central authority is required.
Note: *The underlying blockchain technology solves the required trust related to a central authority.*

EGIZ-5 Ensure data integrity.
Note: *The integrity of identity data can be ensured by utilizing the blockchain. This is one of the main advantages of using the blockchain technology.*

EGIZ-6 Transparency of the identity data is maintained.
Note: *The blockchain technology provides data transparency of all data stored in the blockchain. All changes to the data in the blockchain are fully transparent so that no one can alter of delete data without someone else noticing it.*

A.1.16 openHPI

We were able to derive the following requirements from the expert interview with Thomas Staubitz, Administrator and architect of the openHPI platform.

openHPI-1 The solution shall be scalable.
Note: *There are 100.000 accounts.*

openHPI-2 The solution shall support the three types of credentials:

- (Proctored) Credential
- Record of Achievement
- Confirmation of Participation

openHPI-3 The solution shall allow login via:

- Local database
- HPI Identity Provider (openIDConnect)
- Shibboleth Identity Provider (e.g. from the openHPI instance in the eGovernment-Project)
- Various SSO solutions (e.g. KI-Campus, SAP, WHO)

openHPI-4 The system shall support pseudonymous learners.
Note: *Anonymous learners would be nice to have but the current system is pseudonymous, which suffices.*

openHPI-5 If a learner requires a proctored credential the system shall support the identification and authentication of a learner.
Note: *Currently, only the printing of a learners image to the certificate is supported. The binding of a certificate to the identity of the learner would therefore add value to the current system.*

openHPI-6 Credentials shall be an additional option to document learners achievements.
Note: *Currently, pdf files with verify-link and openBadges are supported.*
The current system provides mostly low risk certificates without ECTS. Thus, enhanced security and unforgeability can support further use cases in regards to higher risk certificates e.g. ECTS courses.

openHPI-7 The test coverage for the production system needs to be 100%.

A.1.17 DAAD

DAAD-1 As a digital artifact, a verifiable claim, such as a digital Transcript of Records, must be portable and must be able to be sent to the recipient – the person, organization, or object (such as a vessel) about which a statement is made as part of the verifiable claim – for further transmission.

DAAD-2 The verifiable claim may only be transmitted by the person, organization, or object about which a statement is made as part of the verifiable claim.

DAAD-3 The processing and storage of a verifiable claim by third parties requires dedicated consent of the person, organization, or object about which a statement is made as part of the verifiable claim. The issuer does not require consent for this purpose. In the

case of the object, consent is given by a person or organization whose property the object is.

Note: *This requirement contradicts DiBiHo 2 in section 7.5, as this is a use case specific requirement. The system should be able to meet different requirements in regard to different use cases.*

DAAD-4 The transmission of a verifiable credential from the issuer to the person, organization or object about which a statement is made as part of the verifiable claim shall be carried out in such a way that the transmission is documented and secure for both the issuer and the recipient.

DAAD-5 Verifiable claims must contain all necessary (and standards-based) information for each particular verifiable claim in plain text and in a structured, readable (and standards-based) form. This information must be readable with a standard text viewer, the verifiable claim must allow for machine processing.

DAAD-6 The person, organization or object about which a statement is made as part of a verifiable claim must be readable in the plain text of the verifiable claim in such a way that verification is possible without the use of digital tools (e.g. through available identification documents). The issuer of the verifiable claim and the persons entrusted with it must also be legible in the plain text of the verifiable claim. Further additions in the form of, for example, digital, structured information or concepts such as self-sovereign identities are possible, but may not be mandatory for the issuance of a verifiable claim.
Note: *This is specified in Bürgerliches Gesetzbuch §126b "Textform."*

DAAD-7 The verifiable claim must contain a description of the standards used to generate the verifiable claim (including the signature and hash values) and how the verifiable claim can be verified.

DAAD-8 The verifiable claim may contain other elements such as images or be integrated in other file formats such as a PDF. In this case, the corresponding document must at least meet the respective standards existing for the respective document format and must be accurately readable without requiring manual tasks.
Note: *This requirement focuses on the automatic processing of verifiable claims. This can be understood as an extension of DAAD-5 with a focus on automatic processing of verifiable claims.*

DAAD-9 The issuer of a verifiable claim must be authorized to issue the respective type of verifiable claim at the moment of issuance. This also applies to the persons involved in the process of issuance on behalf of the issuer.

DAAD-10 This authorization must be traceable for third parties through secure certificate chains (or similar technologies) that are time, location, and technology agnostic. Ideally, authorization should be provided by a higher-level government authority.

DAAD-11 The issuer of a verifiable claim may operate the solution for the signature and verification of a verifiable claim autonomously or within the boundaries of its organization.

DAAD-12 The issuer of a verifiable claim shall provide at least one service for the validation and withdrawal of the verifiable claim. If at any time the issuer is no longer able to operate these services, the issuer will arrange for a suitable third party to operate these.

DAAD-13 Both the actual generation of a verifiable claim and the services for validation and withdrawal of the verifiable claim shall be free of charge for the recipient at all times.

DAAD-14 The solution must be scalable.
Note: *DAAD issues around 15.000 individual scholarships per year.*

DAAD-15 The solution must be easily and quickly connectable to existing back-end systems, such as an SAP system. The use of OPEN API or similar standards is a prerequisite for this.

DAAD-16 Verifiable claims must be integrated into the back-end systems in such a way that the respective regulations for document archiving can be implemented and that verifiable claims can be retrieved within the framework of the administrative software (e.g. campus management system) used.

DAAD-17 The solution must be able to depict various national, EU-wide and international technologies and standards concerning the issuance, transport, storage, verification and withdrawal of verifiable claims in the future.

DAAD-18 The solution should be able to simultaneously depict multiple standards and technologies that affect the issuance, transport, storage, verification and withdrawal of verifiable claims. The interoperability thus achieved is the basic prerequisite for the global use of verifiable claims.

A.1.18 TUM CEO

TUMCEO-1 Credentials (representing degrees) must be securely associated with a natural person.

TUMCEO-2 One digital degree must consist of five individual credentials representing their current day paper counterparts:

- Diploma
- Certificate
- Transcript of Records
- Diploma Supplement
- Grading Table

TUMCEO-3 The system must be scalable in terms of issuance, revocation, and credential size.
Note: *TUM issues about 10.000 degrees every year and roughly 10% are revoked, usually due to minor errors. Especially this significant revocation percentage could have a major impact on system design. Current degree documents encompass about 20 pages of DINA4 paper and depending on chosen credential format, data size might also become relevant.*

TUMCEO-4 The system must allow employees from multiple offices to sign credentials while having each signature attributable to exactly one natural person.
Note: *TUM degree documents currently feature 5 signatures from 3 different persons as well as one university seal.*

TUMCEO-5 The system must allow the university to fulfill its legal obligation to archive issued documents for a set time.
Note: *This might compete with some aspects of self-sovereignty.*

TUMCEO-6 Credentials must be verifiable by third parties without manual input by the issuer.
Note: *Other universities as well as companies regularly inquire about the authenticity of documents they are presented with, requiring manual verification from university employees.*

TUMCEO-7 The system must support reissuance of degree credentials in case of loss.

Note: *Alumni regularly require new documents after lossing them (e.g., in a house fire). Having to address reissuance might be avoidable by ensuring that credentials can never be truly lost.*

References

[1] Digital Credentials Consortium. *Building the digitalcredential infrastructurefor the future*. URL: https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf. Zugriff am: 18. June 2021.

[2] C Agostinho, R Melo, I Keck, C Kontzinos, V Karakolis, et al. *D2. 2–qualichain stakeholders' requirements and use cases*. Tech. rep. Tech. Rep., 2019.[Online]. Available: https://alfresco. epu. ntua. gr/share ...

[3] Wolfgang Gräther, Sabine Kolvenbach, Rudolf Ruland, Julian Schütte, Christof Torres, and Florian Wendland. „Blockchain for education: lifelong learning passport". In: *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET). 2018.

[4] Sonja Dimitrijević, Vladan Devedzić, Jelena Jovanović, and Nikola Milikić. „Badging platforms: A scenario-based comparison of features and uses". In: *Foundation of Digital Badges and Micro-Credentials*. Springer, 2016, pp. 141–161.

[5] Giulio Caldarelli and Joshua Ellul. „Trusted Academic Transcripts on the Blockchain: A Systematic Literature Review". In: *Applied Sciences* 11.4 (2021), p. 1842.

[6] Ingo R Keck, Maria-Esther Vidal, and Lambert Heller. „Digital Transformation of Education Credential Processes and Life Cycles–A Structured Overview on Main Challenges and Research Questions". In: *Mobile, Hybrid, and On-line Learning (eLmL 2020)* (2020), p. 62.

[7] Kimberly L Carey and Jill E Stefaniak. „An exploration of the utility of digital badging in higher education settings". In: *Educational Technology Research and Development* 66.5 (2018), pp. 1211–1229.

[8] Jenny Ozga. „Trust in numbers? Digital education governance and the inspection process". In: *European Educational Research Journal* 15.1 (2016), pp. 69–81.

[9] Ebba Ossiannilsson, Keith Williams, Anthony F Camilleri, and Mark Brown. *Quality models in online and open education around the globe. State of the art and recommendations*. Oslo: International Council for Open and Distance Education, 2015.

[10] Ben Williamson. *Digital education governance: An introduction*. 2016.

[11] Christopher Allen. *The Path to Self-Sovereign Identity*. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

[12] *Whitepaper – Self-Sovereign Identity*. Oct. 2017. URL: https://technology.a-sit.at/en/whitepaper-self-sovereign-identity/.

[13] Abylay Satybaldy, Mariusz Nowostawski, and Jørgen Ellingsen. „Self-Sovereign Identity Systems Evaluation framework". In: (2020).

[14] Tobias Ehrlich, Daniel Richter, Michael Meisel, and Jürgen Anke. „Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten“. In: *HMD Praxis der Wirtschaftsinformatik* 58.2 (Feb. 2021), pp. 247–270. DOI: 10.1365/s40702-021-00711-5. URL: https://doi.org/10.1365/s40702-021-00711-5.

[15] Kim Cameron. „The laws of identity“. In: *Microsoft Corp* 12 (2005), pp. 8–11.

List of Tables

List of Figures