# Digitale Zeugnisse im Hochschulbereich: Ein explorativer Prototyp für die TU Wien

DIPLOMARBEIT

zur Erlangung des akademischen Grades

**Diplom-Ingenieur**

im Rahmen des Studiums

**Software Engineering und Internet Computing**

eingereicht von

**Mathias Schwarzhans, BSc**
Matrikelnummer 01633059

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Ao.Univ.Prof. Mag.rer.soc.oec. Dr.rer.soc.oec. Horst Eidenberger

Wien, 19. September 2023

Mathias Schwarzhans

Horst Eidenberger

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.at

Informatics

# Digital Credentials in Higher Education: An Exploratory Prototype for TU Wien

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

**Diplom-Ingenieur**

in

**Software Engineering and Internet Computing**

by

**Mathias Schwarzhans, BSc**
Registration Number 01633059

to the Faculty of Informatics

at the TU Wien

Advisor: Ao.Univ.Prof. Mag.rer.soc.oec. Dr.rer.soc.oec. Horst Eidenberger

Vienna, 19th September, 2023

Mathias Schwarzhans

Horst Eidenberger

# Erklärung zur Verfassung der Arbeit

Mathias Schwarzhans, BSc

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 19. September 2023

Mathias Schwarzhans

# Acknowledgements

I want to thank everyone who assisted and supported me while I conducted my study and completed my thesis. First, I want to express my gratitude to my supervisor, Prof. Horst Eidenberger, for his exceptional guidance, immensely helpful feedback, and suggestions, as well as for his patience as I wrote my thesis. Moreover, I extend my appreciation to all of the experts who dedicated their time to evaluating its contents.

Furthermore, I am deeply grateful to my parents, not only for their financial support but also for their motivational and emotional encouragement over the years.

I also want to thank all of the friends who supported me during my studies. The same sense of gratitude extends to all of my classmates, with whom I tackled countless problems with both joy and determination. A special note of appreciation goes to my girlfriend for her unwavering moral and emotional support.

*Thank you!*

# Kurzfassung

Die Digitalisierung hat sich in den letzten Jahrzehnten vorteilhaft auf verschiedene Sektoren und Branchen ausgewirkt. Doch trotz der weitverbreiteten Integration digitaler Technologien verwenden Hochschuleinrichtungen bei der Ausstellung von Zeugnissen noch häufig Papier für Zeugnisse. Auch wenn digitale Zeugnisse versprechen, sicherer zu sein, die Kosten durch Automatisierung zu senken und den Datenschutz zu verbessern.

In dieser Arbeit haben wir einen Prototyp für digitale Zeugnisse für die TU Wien entwickelt, um zu demonstrieren und zu evaluieren, inwieweit digitale Zeugnisse als Ersatz für papierbasierte Zeugnisse geeignet sind. Die Implementierung basiert auf der Arbeit vom Digital Credentials Consortium (DCC), einem Zusammenschluss von Universitäten mit dem Ziel, die digitale Zeugnisinfrastruktur der Zukunft zu bauen. Wir haben ihre Referenzimplementierungen erweitert und angepasst, um fehlende Funktionen zu ergänzen, die Vertrauenswürdigkeit zu erhöhen und die Anforderungen der TU Wien zu erfüllen.

Der Prototyp selbst besteht aus unterschiedlichen Services und Bibliotheken, die zusammen das digitale Zeugnissystem bilden. Die gewählte modulare Systemarchitektur in Kombination mit dem Verifiable Credentials Data Model Standard vom W3C gewährleisten Flexibilität, Erweiterbarkeit und Interoperabilität. Zwei hinzugefügte und integrale Teile des Prototyps nutzen Blockchain-Technologie, um kritische Daten öffentlich zu speichern, wie zum Beispiel Informationen zum Rückziehstatus eines Zeugnisses oder Ausstellerkennungen glaubwürdiger Bildungsinstitutionen. Für die Interaktion mit dem Prototyp hat jeder Akteur seinen eigenen, speziell zugeschnittenen Service. Die Aussteller (z. B. Universitäten) verfügen über eine Weboberfläche für die Ausstellung und Aktualisierung von Zeugnissen. Inhaber (z. B. Studenten) haben eine Handy-App, um ihre Zeugnisse zu speichern und weiterzugeben, und Überprüfer (z. B. Arbeitgeber) haben ein Befehlszeilen-Programm, um die Gültigkeit eines digitalen Zeugnisses zu überprüfen.

Eine Gruppe von Experten evaluierte den Prototyp dieser Arbeit aus technischer und organisatorischer Sicht in Form einer Expertendiskussion. Das Ergebnis war, dass der Prototyp die Sicherheit erhöht, neue Anwendungsfälle ermöglicht und Automatisierung erlaubt, welche zu einer Reduzierung des Verwaltungsaufwands und damit der Kosten führen kann. Aufgrund der mangelnden Ausgereiftheit der derzeitigen Standards und der mangelnden Verbreitung ist es jedoch noch zu früh, um digitale Zeugnisse für den produktiven Einsatz zu verwenden und papierbasierte Zeugnisse zu ersetzen.

# Abstract

Digitalisation has advantageously impacted various sectors and industries in recent decades. However, despite the widespread integration of digital technologies, higher education institutions (HEIs) still often rely on paper-based methods for the issuance of credentials, such as diplomas and certificates. This is despite the fact that digital credentials promise to be more secure, reduce costs through automation, and improve privacy.

In this thesis, we built a digital credentialing prototype for TU Wien to demonstrate and evaluate digital credentials as a replacement for paper-based credentials. The implementation is based on work published by the Digital Credentials Consortium (DCC), a collaboration of universities that aim to build the digital credentialing infrastructure of the future. We extended and adapted their reference implementations to add missing features, improve trustability, and fulfil the requirements of TU Wien.

The prototype itself consists of various heterogeneous services and libraries that together form the digital credentialing system. The chosen modular system architecture combined with the Verifiable Credentials Data Model standard by the W3C ensures flexibility, extendibility, and interoperability. Two added and integral parts of the prototype use blockchain technology to store critical trustable data publicly, such as credential status information and trustable issuer identifiers. To interact with the prototype, each actor has its own specially tailored service. Issuers (e.g. universities) have a web interface to issue and update credentials; holders (e.g. students) have a wallet phone app to store and share their credentials; and verifiers (e.g. employers) have a command-line tool to check the validity of a digital credential.

Then, a group of experts evaluated the developed prototype in the form of an expert discussion from a technical and an organisational perspective. The results indicated that the digital credentialing prototype improves security, enables new use cases, and allows automation, which can lead to a reduction in overheads and therefore cost. However, due to the immaturity of current digital credential standards and a lack of adoption by other actors, it is too early to adopt digital credentials for production use and as replacements for paper-based credentials.

# Contents

CHAPTER 1

# Introduction

In the last few decades, many areas of the world have taken advantage of the new possibilities provided by digitalisation. Especially since the COVID-19 pandemic, the speed of digitalisation has increased [AAKWK21]. Furthermore, the education sector has seen a boost in digitalisation, as distant learning has become a part of everyday life. However, paper-based credentials are still commonly used by higher education institutions (HEIs) [WGP21], even though digital credentials have several benefits over traditional credentials and allow new use cases that would not be possible with paper-based credentials.

First, digital credentials have the ability to reliably protect the credential by using digital signatures. Digital signatures enable the possibility of automatically verifing a credential within a digital system, which removes the necessary manual and error-prone task of verifying the physical properties of a credential. Digital credentials benefit from the advancements in digital identities; for example, they can be linked to a learner's digital identity, which reduces the risk of fraud and makes it harder to create counterfeit credentials [SSRF21].

Second, digital credentials are more efficient to exchange. The process of creating and delivering new digital credentials can be fully automated, which saves time and resources compared with paper-based credentials. Digital credentials are portable and enable learners to bring their credentials anywhere with them and instantly prove their accomplishments.

Third, digital credentials give learners control over their personal information stored in their credentials, thus increasing privacy. The holder of a credential decides what information to share and with whom, without losing proof by hiding specific details, which is not possible with paper-based credentials.

This thesis takes a close look at the digitalisation of credentials with a focus on credentials issued by HEIs, such as TU Wien.

## 1.1 Problem Statement

As already alluded to, credentials issued by HEIs are mostly analogue, and this approach to credentialing has some problems. Credentials describe a set of properties of a given subject. In the area of education, these credentials can be a qualification, such as a university diploma; an assessment, such as a course certificate; an entitlement such as the right to enrol in a course; or an activity such as participation in an event [EU].

Therefore, credentials may contain highly sensitive and important information that ideally cannot be faked. The content of credentials must be trustable. Unfortunately, the credentials currently often used are frequently in the form of pieces of paper, which are prone to being faked; when skilfully crafted, these fake credentials are difficult to detect[Gil04]. Traditional credentials printed on paper often rely on physical attributes to verify their authenticity. Often, special paper, stamps, and signatures are used to harden the credential. These characteristics are lost or weakened if the paper is scanned and transformed into a digital copy [LHL15].

This digitalisation process of paper-based credentials is used heavily to exchange credentials. As it is often easier to share a digital copy of the credentials than to physically send the original document. But as mentioned before only the original document has all the characteristics used to verify the authenticity of the document and therefore faking a digital copy of a paper credential is easier than creating a faked physical document.

Another problem with paper-based credentials is their lack of integration into automated digital processes. Currently, the verification of a credential often relies on manual checks of the properties of the paper document [MvBS15]. Unfortunately, this is an error-prone task as there is no single standardised property that must be verified. Instead, issuers use various kinds of hardening properties on their paper-based credentials. This makes the verification process especially difficult if the verifier does not recognise the issuer and does not even know if it is an accredited institution [GLM08]. Furthermore, this may lead to a connection between issuers of credentials and third parties that want to verify the credentials. The verifier may contact the issuer and ask if the credential is authentic. Notably, this information exchange is problematic in terms of privacy [DCCb]. If a third party must contact the issuer to verify the credential, the issuer now knows that the holder of the credential has shared the credential with the third party. Therefore, a university may now know where their students have applied for jobs.

Another reason that credentials are difficult to integrate into automated processes is that the information written on paper or digitally stored is not in a standardised format. This makes it difficult for the verifier to compare two credentials or to determine whether they are equivalent to each other.

In sum, the following three key problems exist with current paper-based credentials:

- Verifying that a credential has not been tampered with involves manual checks and leaves the verifier with trust issues;

- Assuring that the issuer of a credential is an accredited, trustworthy source according to the verifier cannot be fully verified;
- Comparing credentials is difficult due to the diversity of descriptors and the lack of standardised, detailed information.

## 1.2 Aim of the Work

This thesis aimed to build a proof-of-concept (PoC) digital credentialing system for TU Wien's Information Systems and Services TISS. This system is based on the white paper titled *'Building the digital credential infrastructure for the future'* published by the Digital Credentials Consortium (DCC) [DCCb]. The goal of the implementation is to improve upon existing paper-based credentials, solve the verification problems, and address the trust and verification issues that verifiers currently face.

The focus of this thesis is on the aspects that are relevant for TU Wien in such a digital credentialing system, mainly the role of an issuer of HEI credentials and a verifier of credentials issued by other HEIs. By building this PoC with the use cases and requirements of TU Wien in mind, this thesis outlines the main challenges that TU Wien would face if it were to adopt a credentialing system like the system proposed by the DCC (RQ1).

Additionally, the implementation of the PoC assists in the decision-making process in various areas. It can serve as a reference for future technology choices and help to make better-informed decisions, such as whether or not to use blockchain technologies for building a digital credentialing system (RQ2).

Furthermore, switching from the current credentialing system that TU Wien uses to a new digital credentialing system may also change the workflow around grade management for TU Wien and its students. The workflow is expected to become more efficient and streamlined, as the PoC system becomes entirely digital (RQ3).

Lastly, this thesis discusses the possible advantages and drawbacks of a digital credentialing system like the one proposed by the DCC compared with the TISS currently in use. This analysis should help the decision-makers at TU Wien to develop a digital credentials strategy and to evaluate the usefulness of the proposed digital credentialing system (RQ4).

In summary, this master's thesis answers the following research questions:

**RQ1:** What are the main challenges of integrating digital micro-credential components designed by the DCC into TISS?

**RQ2:** What roles do blockchain technologies play in digital micro-credentials?

**RQ3:** How does the workflow of grade management change when the current solution is substituted with digital credentials?

**RQ4:** What are the advantages and disadvantages of the PoC implementation of credentials compared with the existing TISS implementation of credentials?

## 1.3 Methodological Approach

The methodical approach of this thesis is structured as follows:

1. **Literature Review**
   The existing scientific literature was examined for digital credentials in the field of HEIs. The results were extended by investigating developments outside of scientific research. Together, these steps led to a description of the broad current state of the art of digital credentials.

2. **Create a Proof-of-Concept**
   Once the current state has been defined, the implementation could begin with the following three steps:

   a) **Requirements Analysis**
      First, the specific requirements that the implementation must fulfil were outlined. The requirements were mainly derived from existing research and altered to fit the specific use cases of TU Wien.

   b) **Modeling of an Architecture**
      Second, the components of the system were defined and the interaction protocols were described for the different components. The architecture should enable the implementation to fulfil the aforementioned requirements.

   c) **Implementation**
      The components were implemented according to the architecture modelled previously while also considering the results of the requirements analysis.

3. **Evaluation of the Implementation**
   The resulting PoC was evaluated through an expert discussion. The experts provided their opinions about the various aspects of the PoC implementation, which enabled the research questions of this thesis to be answered.

## 1.4 Structure of the Thesis

The remainder of this thesis is structured as follows: Chapter 2 describes the relevant technologies and standards and provides a summary of the current developments in the area of digital credentials. Chapter 3 discusses, identifies and analyses the requirements for the implementation. Chapter 4 outlines the technology choices, architecture, and implementation details used to build the PoC credentialing system for TU Wien. Chapter 5 discusses and evaluates the resulting implementation and presents the results of the expert discussion. Lastly, Chapter 6 summarises the thesis and provides an outlook on the future.

CHAPTER 2

# Fundamentals

This chapter explains key terms, technologies, and frameworks to provide readers with the necessary knowledge to comprehend the upcoming chapters and to integrate the thesis into the larger context.

## 2.1 Digital Identity

This section establishes the core knowledge required to understand digital identities. The term "digital identity" is used to describe digital techniques that create a digital reference to a person or organisation [Bur20]. This reference is an identity and can also be used to specify various attributes of one. When those attributes help to identify an identity, they are called identifiers. While an identity is unique to a specific subject, a subject can have multiple identities in different contexts. For example, a person can have a passport and an identity card, both of which are the identities of that person. Furthermore, each identity has a set of identifiers. In the case of a passport, the person's name, date of birth, and other attributes are listed. This set of identifiers forms the person's identity, and the identity is linked to the subject. Moreover, the uniqueness of the identifier is limited to a specific context. The relationship between subjects, identities, and identifiers is further illustrated in Figure 2.1. [JFH+05]
The following subsections describe three categories of digital identities. Subsection 2.1.1 describes the isolated approach to digital identities; then Subsections 2.1.2 discusses federated identity techniques; and lastly, Subsection 2.1.3 describes a decentralised identity model with a focus on self-sovereign identity (SSI).

### 2.1.1 Isolated Identity

With an isolated identity, a user has an account for each service, as illustrated in Figure 2.2. This method is commonly used, often in the form of a username/password scheme.

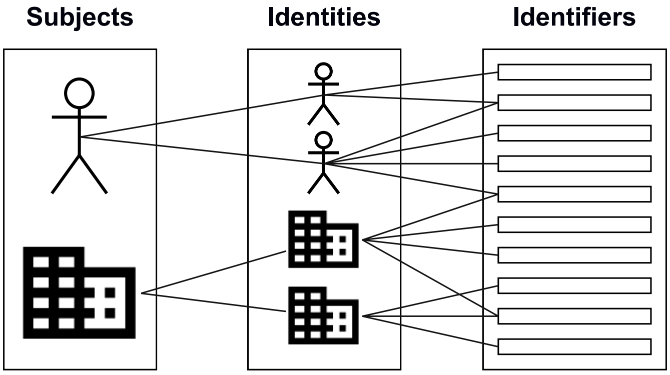


Figure 2.1: The relationship of identifiers, identity and subjects. [JP05]

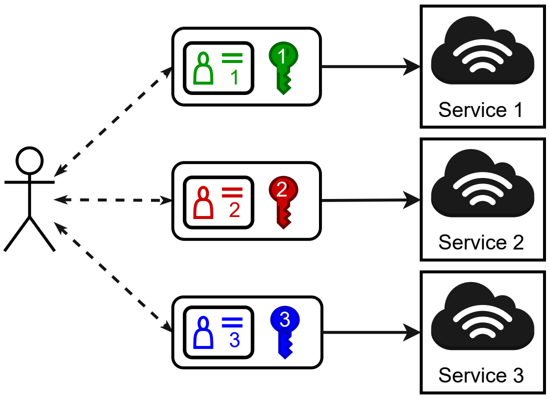


Figure 2.2: Isolated identity is a traditional approach to digital identity using different credentials for each service and each service has its own identity domain. [JP05]

The user must register for each service individually and somehow verify their identity through methods such as email ownership verification. If a service requires deeper identifying information about a user, then the user must submit this information, and the service is then responsible for verifying its correctness.

This model is frustrating for the user and the service provider. Each user must remember many different passwords, and each should be unique and difficult to guess. According to a study by Harris Poll and Google in 2019, 75% of Americans are frustrated with password management [PG19]. This leads to security problems, such as users using simple, easy-to-guess passwords; using the same password across different services; and not changing passwords regularly.

Each service provider holds identifying information relevant to their specific use cases; however, there is no seamless way for a user to transfer identifying information from one service to another [SSRF21]. This leaves them with the burden of repeatedly submitting identifying information through complex processes, which may include the disclosure of their ID cards, driving licence, or banking information.

Another problem arises from storing identity information on the service provider's side. If the service provider is attacked, then digital identities are at risk of compromise.

### 2.1.2 Federated Identity

With federated identity, users can authenticate themselves for one service and use the same identity for another. For example, a user already has a digital identity for *service 1*, which includes identifiers such as their first name, last name, and email address. The user now wants to authenticate themselves for a second service called *service 2*, and *service 2* trusts that *service 1* has already correctly verified the identity information of users. Thus, federated identity methods allow the user to authenticate to *service 2* by authenticating to *service 1* and confirming their consent to share data with *service 2*. Subsequently, the user has digital identities on both services, that are linked, and only the credentials for the identity from *service 1* are used for authentication for both services. This scheme of using one credential to log in to multiple services is also called single sign-on (SSO) and is further illustrated in Figure 2.3.

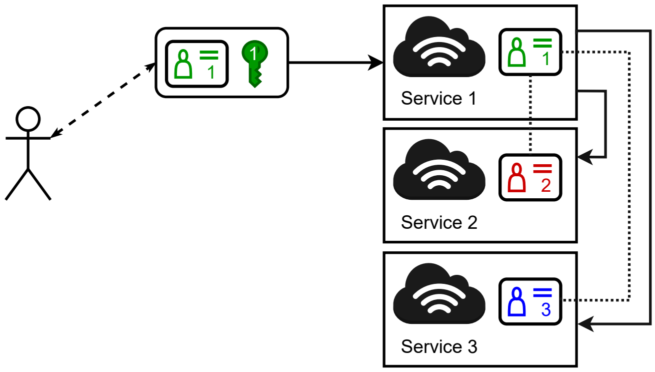


Figure 2.3: Federated identity uses a single authentication mechanism to authenticate to multiple services and allows identity data exchange between services. [JP05]

This approach allows the federated storage of identity information across different services, which can lead to greater privacy and security for the user[MKT05]. The user has more granular control over which information to share from one service to another without, for example, having to disclose a complete ID card for every service, even though they only need partial information from the ID card.

Service providers also benefit from a federated identity model, as the cost of managing identities can be offloaded to other services. There are specialised identity management services, commonly referred to as identity providers (IdPs), whose main purpose is to manage digital identities for other services.

Federated identity solves the problem of ensuring easy data exchange between services as well as remembering multiple passwords for different services [Jen11]. However, it still faces many challenges in the field of privacy and security[Jen12]. The risk of identity-related data theft is still present, although it is reduced compared with isolated identity approaches, since the identity data are not duplicated and the number of targets for attacks is reduced. On the other hand, if the authentication with the IdP is compromised, all services that use it are at risk of being compromised. Additionally, privacy concerns exist because the IdP has knowledge of which services a user is accessing [FKS15].

### 2.1.3 Decentralised Identity

Decentralised identity, also often called SSI, goes one step further in the evolution of digital identities. The user is at the centre of administering their digital identity; no one or nothing should be able to control the identity of the user other than themselves. There is no central entity that holds identifying information. Every user manages their digital identity and shares information with others on their own, as illustrated in Figure 2.4. Everyone can make a claim about an identity and share it with others. Even the owner of the identity can make claims about themselves. These claims can be based on arbitrary information, which can include personal information, educational records, group memberships, or other facts about an identity.

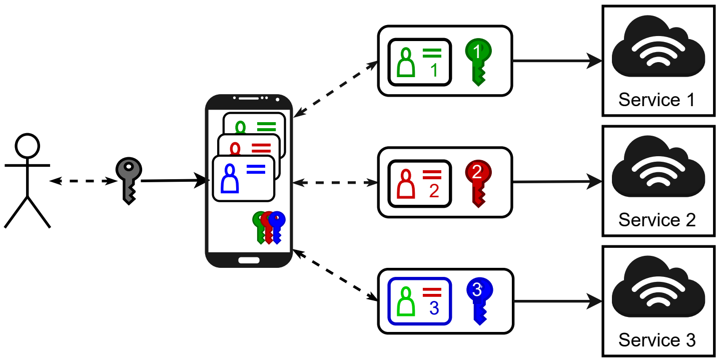


Figure 2.4: With a decentralised identity the subject owns the storage containing the digital identity information. They have control over what and whom to share their information. The storage is protected from unauthorised access and can be implemented as a mobile app. [JP05]

Even though the fundamental idea of decentralised identity is clear, no definitional consensus exists on the specific properties of SSI [TAP19]. In 2016, Christopher Allen proposed 10 principles that could be grouped into three categories as follows [All16, TRW17]:

- **Security & Privacy**
  - **Protection**: The privacy and rights of the individual are more important than the needs of the identity network and must be protected.

  - **Persistence**: An identity must be long-lived while respecting *the right to be forgotten*.
  - **Minimalisation**: When data are exchanged, only the absolute minimum required to fulfil the task should be exchanged.

- **Controllability**
  - **Existence**: An individual must have an independent existence representation of themselves.
  - **Portability**: The user can move their information and services and is not vendor-locked.
  - **Control**: The user administers their own identity and is the ultimate authority.
  - **Consent**: The user must confirm and give consent to share identity information.

- **Portability**
  - **Interoperability**: Decentralised identities should use and create open standards to make them universally usable.
  - **Transparency**: The function of systems and algorithms must be openly accessible and verifiable for anyone.
  - **Access**: The user must always be able to retrieve and see all of their identity information.

The goal of these 10 principles is to solve many of the problems associated with isolated and federated identity models, particularly privacy concerns, security issues, and dependency on large entities. SSI addresses these issues by promoting an open and interoperable ecosystem. While many standards, technologies, and implementations build upon these principles, some have been criticised for being deeply connected to blockchain technologies or for not truly providing privacy and security [Hal20]. The next subsection outlines a core standard for building an SSI ecosystem, as defined by the World Wide Web Consortium (W3C).

### Decentralised Identifiers

The W3C proposed a standard called the decentralised identifier (DID) standard [W3C22a]. Their goal is to build an open extendable standard that defines a schema for identifiers in a decentralised identity context, allowing for the resolution of globally unique identifiers to a document, which is known as a DID document. The DID standard builds upon the existing universal resource identifier (URI) specification, further strengthening the interoperability of the decentralised identity ecosystem.

A DID consists of the following three parts: the URI scheme, the DID method, and the DID method-specific identifier, which are separated by a colon, as shown in Figure

2.5. The scheme signals that the string is a URI of type DID and serves the same function as other well-known URI scheme types such as `https`, `file`, or `tel`. The DID method describes the type of DID and specifies which method specification should be used to locate the data referenced by the DID. The method-specific identifier is the actual identifier that is interpreted according to the DID method specification, and it can be interpreted differently by each DID method.

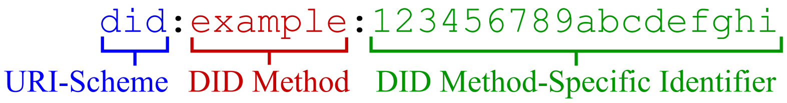

did:example:123456789abcdefghi
URI-Scheme
DID Method
DID Method-Specific Identifier

Figure 2.5: An example DID with the DID-method *example*, which gets *123456789abcdefghi* as an input. [W3C22a]

Furthermore, anyone can create their own identifier subsystem by publishing a DID method specification. This allows for a diverse ecosystem with many different methods, and multiple implementations per method by independent entities, while still maintaining interoperability between them. The method part of a DID selects which method specification should be used to process the actual identifier, which requires each method to have a unique name. To reduce the risk of method name collisions, a public method list is provided on the W3C website[1].

The purpose of DIDs is to reference to DID documents. While a DID document can be represented in different ways, the most popular representation is chosen for the purposes of this thesis, namely a document in the JSON-LD[2] format. Listing 2.1 presents an example DID document that could have resulted from the DID in Figure 2.5.

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase":
        ↪ "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

Listing 2.1: An example DID document

[1] https://www.w3.org/TR/did-spec-registries/#did-methods, last accessed on 27.01.2023

[2] https://www.w3.org/TR/json-ld/, last accessed on 17.01.2023

A DID document references a subject, assigns data to it, and allows the subject to authenticate itself and prove the connection to the DID. These authentication mechanisms may include, public keys or other cryptographic data that can be used for proofs and authentication purposes. Depending on the DID method used, the DID document can be built by simply gathering the information out of the DID itself without any other data source, while others require a data registry to look up further information. Many methods use blockchain technologies to store this information, but the data registry can be anything. The DID method specification defines which data registry is used and how to parse the data. For example, the `key` method allows cryptographic public keys to be referenced independently of any blockchain or other data registry. Conversely, the `ethr` method uses the Ethereum blockchain as a data registry, while the `web` method uses the traditional web for data retrieval.

## 2.2 Blockchain

A blockchain is a distributed ledger technology used to create secure, transparent, and distributed databases without the need for a central controlling entity. This makes blockchain technologies a popular choice for data storage for decentralised identity methods and digital credentials. Subsection 2.2.1 provides a brief introduction to the cryptographic mechanisms of blockchains and their resulting properties. Then, Subsection 2.2.2 examines the different types of blockchains, while Subsection 2.2.3 summarises their various consensus mechanisms. This is followed by a description of smart contracts, a new way of creating "intelligent contracts", in Subsection 2.2.4.

### 2.2.1 Overview

Two of the most popular blockchains are Bitcoin and Ethereum. Both are cryptocurrencies, but blockchains can be used not only to build a digital currency but also for other purposes that require a distributed ledger. Self-sovereign identity implementations often rely on a distributed ledger as their data registry, and blockchains are a popular choice [SSRF21]. Blockchains depend on many different cryptographic methods to build a distributed database, some of which have been well-known since the 1970s [SJZG19]. In 2008, Satoshi Nakamoto published a white paper titled *'Bitcoin: A Peer-to-Peer Electronic Cash System'*, in which the fundamental inner workings of Bitcoin were described, and with that, the first blockchain was proposed [Nak08].

Blockchains have a special data structure that, as the name suggests, links one block to the previous block, thus building a chain of blocks. Blocks consist of two parts, namely the block transactions and the block header. The block transactions hold a list of transactions, and a transaction holds the actual data that should be stored in the blockchain. The block header contains metadata relevant for the blockchain to function properly, such as the link to the previous block of the blockchain. The link between two blocks is represented as a hash pointer stored in the block header, as shown in Figure 2.6.

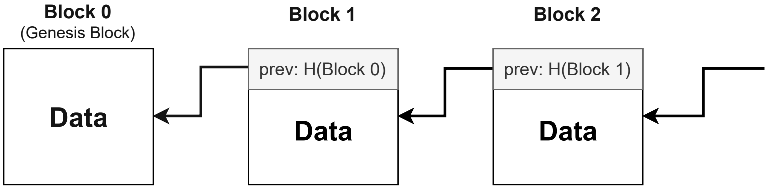


Figure 2.6: Each block has a link to the previous block containing its hash to verify the integrity

This data structure provides a blockchain with the immutability and traceability properties that are required for certain use cases. The immutability is provided by the hash added to each link between blocks, which verifies that the previous block has not been tampered with. The hash pointer to the previous block is also tamper-proof because it is part of the block itself. The traceability of data changes results from the immutability of the blockchain. It is not possible to change the content of a previous block. Instead, a new block must be appended to the chain to update the data stored in the blockchain. Therefore, each change can be traced through each update of the data on the blockchain.

With the blockchain data structure defined, the next essential part of blockchains is the decentralised protocol for exchanging the blockchain data in a peer-to-peer network. A key challenge for any distributed data storage system is how to make the data consistent across each node. Blockchains use various types of consensus mechanisms to reach a shared and agreed-upon state of the blockchain data structure. The different consensus mechanisms are further explained Subsection 2.2.3.

In summary, a blockchain is an immutable, traceable, transparent, decentralised, and secure ledger achieved through its unique data structure and consensus protocols used among a network of nodes.

### 2.2.2 Blockchain Types

There are different types of blockchains, and depending on the type, a blockchain has different properties and consensus mechanisms. Blockchains can either be private or public and permissionless or permissioned.

The distinction between private and public lies in the type of peer-to-peer network. If the network is publicly available to anyone, then the blockchain is public; otherwise, the blockchain is private as the network used is private. Furthermore, a blockchain is permissioned if there is a central entity that must actively grant participating nodes permission to join the peer-to-peer network. By contrast, if anyone can join the network without the permission of anyone, then the blockchain is permissionless.

The most well-known blockchains, Bitcoin and Ethereum, are public permissionless blockchains. Anyone can join the publicly available peer-to-peer network, receive the complete blockchain, and participate in the proposal process of appending new blocks to the blockchain. A private blockchain is only accessible to nodes within the private network. It is most likely that a private blockchain is also permissioned, as there is already an entity controlling the network. This type of blockchain can be used in, for example, supply chain management for enterprises. A public, permissioned blockchain has a central entity that decides which nodes are allowed to actively participate in the peer-to-peer network. This network is publicly available, and to participate in it, the owner of the blockchain must permit each node to actively participate.

Depending on the type of blockchain, some generally well-known properties of blockchains may no longer be valid, as it is often assumed that the blockchain is a public permissionless blockchain. However, for example, the decentralisation property is not valid for permissioned blockchains, as a central entity controls the active participants within the distributed peer-to-peer network.

### 2.2.3 Consensus Mechanisms

The consensus mechanism is a vital part of a blockchain. It ensures that the network of nodes that store the data results in a consistent and secure distributed ledger. A critical aspect is reaching an agreement among a group of distributed nodes, which may include malicious actors that do not comply with the rules set by the consensus mechanism. Nevertheless, consensus mechanisms are typically resilient to these malicious actors as long as the majority of nodes act honestly. The composition of the majority depends on the type of consensus mechanism being used.

Consensus mechanisms are an active research area that has resulted in many newly proposed consensus mechanisms. Lashkari and Musilek found 130 different consensus algorithms in their literature review in 2021 [LM21]. The discussion within this subsection is limited to Proof of Work, Proof of Stake and Proof of Authority, as only they are relevant to the implementation part of this thesis.

Proof of Work (PoW) is the consensus mechanism used by Bitcoin since its creation in 2008. The basic idea behind PoW is that nodes must add a proof of computational work to each block they add to the blockchain, which must be verifiable by everyone. Nodes are incentivised to do this computational work by receiving a reward in the form of cryptocurrency. This has resulted in different types of nodes within the network. Mining nodes are nodes that do the work to create the Proof of Work with the goal of receiving the mining reward. They get their name from the creation of blocks, which is also called mining a block. Other nodes are only there to validate the blocks created by mining nodes and use the blockchain network for reading and writing to the distributed ledger. In the case of Bitcoin, PoW is implemented by finding a nonce that, when combined with the block data and hashed, results in a hash with a certain number of leading zeros [Nak08]. The number of zeros required is called difficulty and is adjusted every 2 weeks according to the network's computational power. The goal of Bitcoin is to keep the estimated time between two blocks around 10 minutes. The rise in popularity of cryptocurrencies and Bitcoin has led to a race to create a PoW through increasing computational power, which also results in higher energy consumption [K9]. According to the Cambridge Bitcoin Electricity Consumption Index, Bitcoin had an electrical power consumption of 106 TWh in 2022, which roughly translates to $CO_2$ emmisions of 54 million metric tonnes. [fAFC]. This environmental impact was one of the reasons why Ethereum switched from PoW to PoS in 2022 [Eth].

Proof of Stake (PoS) uses locked assets to elect a node to create a new block on the blockchain. The chance to be elected as the block creator depends on the amount of assets a node has locked. The higher the stake, the higher the chance. To prevent nodes from adding an invalid, malicious block, the remaining nodes, which have locked a certain amount of assets, validate the correctness. If the block is found to be invalid, the elected node's locked assets are destroyed. A reward is given to a randomly selected node to incentivise locking assets and participating in the network. This also ensures that the node stays active so as not to miss out on the reward opportunity if it is selected. This consensus mechanism mitigates the environmental issues associated with PoW. According to the Crypto Carbon Ratings Institute, Ethereum reduced its environmental footprint by 99.91 % from 11 016 000 $tCO_2$ to 870 $tCO_2$ with the switch from PoW to PoS [CCR22].

Lastly, Proof of Authority (PoA) does not require any work or stake by the nodes. Instead, the node's reputation is the deciding factor. Thus, in a PoA blockchain, only a fixed, preset group of nodes is allowed to create new blocks and there is no reward for these nodes. Their incentive to participate is honesty and not losing their reputation. This kind of consensus mechanism is a popular choice for private blockchains that have a natural authority. For example, the European Blockchain Services Infrastructure (EBSI) blockchain uses PoA [Com21a]. Each EU Member State has a few nodes, and they decide which blocks should be appended and considered valid. This consensus mechanism also mitigates the environmental issues from the PoW consensus mechanism while also increasing the potential throughput of the blockchain, as with a PoA blockchain the number of nodes is reduced. This has the drawback of increasing centralisation, but depending on the use case, this is not a problem [MMT22].

### 2.2.4 Smart Contracts

Smart contracts are digital, intelligent contracts that run on the blockchain and are written as small programs. Depending on the blockchain, these programs may be restricted to loopless programs, such as in Bitcoin, while other blockchains, such as Ethereum, have a Turing-complete instruction set. Smart contracts are the foundation for all decentralised applications (DApps) [NBF+16].

The smart contract's code is stored on the blockchain and executed by the nodes in the blockchain network. As with any other data stored on the blockchain, the code of a smart contract cannot be changed, making smart contracts transparent and trustworthy. Every node in the blockchain network can read the code and its current data state; therefore, they can also predict the actions that will be executed by triggering a function in a smart contract. This makes the blockchain network a trustable, transparent, decentralised execution environment for small programs, which are the enablers of many blockchain use cases in supply chain management, the Internet of Things, healthcare, digital rights management, digital identity, insurance, and real estate [MPJ18].

Ethereum is a popular choice for DApps because it is the largest blockchain that supports a Turing-complete execution environment. Ethereum has developed its own bytecode definitions, which are executed in its special Ethereum virtual machine (EVM) [Woo22]. Ethereum has also developed its own higher-level programming language, named Solidity, to abstract the low-level details of the bytecode that the EVM executes. Solidity is a contract-oriented language that is syntactically a mixture of JavaScript and C [Dan17]. As a result, it provides a more rapid and familiar development experience for new developers in the new field of DApps development. As already mentioned, the EVM allows the execution of Turing-complete programs, but this creates a problem with non-terminating programs. The nodes in a blockchain network cannot execute a program that may never end and potentially stall the entire blockchain network. To mitigate this issue, Ethereum added an execution fee to every instruction defined by the EVM, and to execute the code on the blockchain, a certain amount of cryptocurrency must be paid as a fee. If the fee paid is too small to execute the required instructions of the smart contract, then the code execution is aborted and the transaction is reverted. In Ethereum, this execution fee is called *'gas'*.

## 2.3 (Micro-)Credentials

The rapidly changing labour market, driven by technological advancements and exacerbated by the COVID-19 pandemic, has resulted in drastic changes in the skills required to perform many jobs. This has led to an increasing demand for short-term learning opportunities to help individuals at any stage of their educational path to quickly up-skill or reskill [Com20a, TGT$^{+}$23]. These opportunities, which can range from massive open online courses (MOOCs) to on-the-job training, are collectively referred to as alternative credentials, or as alternative digital credentials if the certificate of completion is issued in a digital format. Digital badges and micro-credentials are some forms of alternative digital credentials. These new forms of credentials are not only issued by HEIs but also by any institution that provides any learning courses. Currently, alternative digital credentials can be implemented in several ways with a variety of standards available to represent learning achievements, assessment methods, awarding bodies, and credential holders. Some of the standards are openly available, while others use proprietary methods that are implemented by accreditation institutions and built into their products(see Subsection 2.3.2). Nevertheless, the proprietary methods often extend or build on top of the generally available open standards, which are described in Subsection 2.3.1.

### 2.3.1 Digital Credentials Standards

The most widely used open standard for digital credentials is the verifiable credentials data model specification published by the W3C [W3C22b]. The newest version at the time of writing is `v1.1`, which was released in March 2022. The goal of verifiable credentials is to build a standard way to represent credentials on the web in a secure, privacy-preserving, and machine-verifiable manner. The standard further embraces openness, extendibility, and interoperability with other standards to build a digital credentialing ecosystem. In the verifiable credentials ecosystem, the following three roles exist: the *issuer*, the *holder*, and the *verifier*. All of these roles interact with a generally trusted and *verifiable data registry* that functions as a database. A *holder* is an entity that owns a set of credentials and can create verifiable presentations of them to share with others. For example, students are role holders. An *issuer* is an entity that creates credentials and sends them to a *holder*. The credential contains a set of claims about a subject, which does not necessarily have to be the *holder* of the credential. The *issuer* role can be taken by various entities, such as universities, government bodies, or other organisations. A *verifier* is an entity that checks the validity of a verifiable presentation to assess whether the claims made about the subjects of credentials inside the presentation are correct. Employers, universities, and security personnel are examples of entities that might act as *verifiers*.

As seen in Figure 2.7, the *verifiable data registry* is a core part of the verifiable credentials ecosystem. It acts as storage for various purposes, such as cryptographic public keys of trusted issuers, a list of revoked credentials, schema definitions for verifiable credentials, and other relevant data. Government databases and distributed ledgers are examples of verifiable data registries. In a verifiable credentials ecosystem, multiple *verifiable data registries* may be involved.

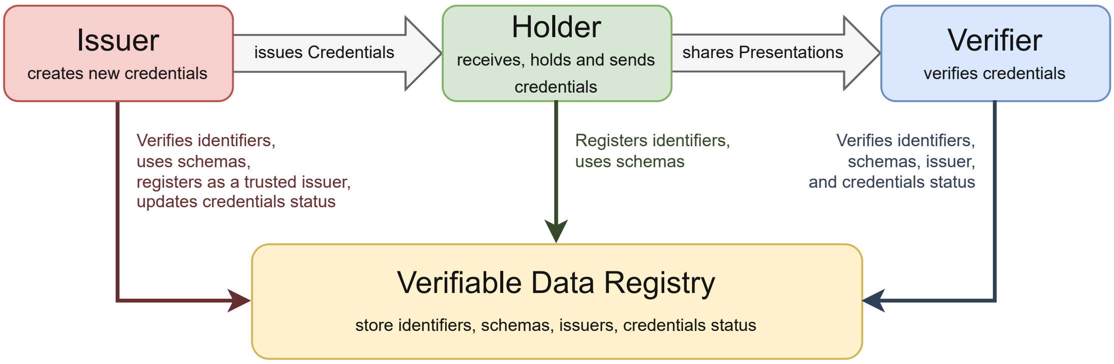

Issuer
creates new credentials
issues Credentials
Holder
receives, holds and sends credentials
shares Presentations
Verifier
verifies credentials
Verifies identifiers, uses schemas, registers as a trusted issuer, updates credentials status
Registers identifiers, uses schemas
Verifies identifiers, schemas, issuer, and credentials status
Verifiable Data Registry
store identifiers, schemas, issuers, credentials status

Figure 2.7: Verifiable Credentials Ecosystem Overview [W3C22b]

As previously mentioned a key aspect of verifiable credentials is their interoperability and extendibility. To achieve this verifiable credential data model, the DID specification from Subsection 2.1.3 is used for identifiers along with JSON-LD as a representation format. A verifiable credential has three parts, namely the credential metadata, a set of claims, and proofs. Each part is defined in a JSON-LD schema and defines which properties must or may be set. A verifiable presentation wraps verifiable credentials with the purpose of sharing them with a third party that acts as a verifier. A verifiable presentation also consists of three parts, namely the presentation metadata, a set of credentials, and proofs. This separation of verifiable credentials and verifiable presentations is intended to improve the privacy of holders. Depending on the selected type of proof of a verifiable credential, its holder might be able to selectively disclose information and create a verifiable presentation with only the information required and requested by the verifier.

The verifiable credentials standard is highly extensible while still providing interoperability. This means that each function of a verifiable credential can be implemented in various ways, and a wide set of sub-specifications exists. Open Badges v3.0 is a standard that builds on top of verifiable credentials and extends them by defining a more granular level of how claims should be structured. The main goal is to represent qualification badges as digital verifiable credentials. The Open Badge standard is already used by many accreditation platforms and universities, such as Credly, Mozilla Foundation, and Arizona State University [Glo18, Glo23].

### 2.3.2 Credentialing Platforms

Credentialing products are used by many issuers to make credentialing processes easier, not only for them but also for holders and verifiers. These products wrap the underlying credentials' implementations and provide easy-to-use user interfaces. This allows the issuer to focus more on the educational aspects and lets the credentialing products take care of implementing a secure and up-to-date credentialing system. Some products use proprietary methods that are not based on openly available specifications, and therefore, they are not interoperable with other products. The feature set of credential products is changing quickly, and new credentialing platforms emerge regularly [DDJM16]. Kiiskila et al. studied the feature set of 10 platforms and grouped them into 12 categories, which when combined resulted in 38 features [KHP22]. The 10 studied platforms were Europass[3], Credentify[4], BadgeCollect[5], Digitary[6], VerifyEd[7], DiploMe[8], Accredible[9], BCDiploma[10], LinkedIn Learning[11], and Gataca[12]. They found that apart from having user interfaces, validation and verification methods, portfolio management and the sharing of credentials on social media are currently evolving features. Furthermore, they found that adding various proof types, such as grading scheme data and standardised competence frameworks, increased the credibility of digital credentials.

[3] https://europa.eu/europass/en/ last accessed 19.02.2023

[4] https://credentify.eu/ last accessed 19.02.2023

[5] https://badgecollect.com/ last accessed 19.02.2023

[6] https://www.digitary.net/ last accessed 19.02.2023

[7] https://www.verifyed.io/ last accessed 19.02.2023

[8] https://www.diplo-me.eu/ last accessed 19.02.2023

[9] https://www.accredible.com/ last accessed 19.02.2023

[10] https://www.bcdiploma.com/en/ last accessed 19.02.2023

[11] https://www.linkedin.com/learning/ last accessed 19.02.2023

[12] https://www.gataca.io/ last accessed 19.02.2023

## 2.4 Related Work

The research field of digital credentialing is rapidly evolving, with numerous development projects underway to build digital credentialing platforms [AAU$^+$23]. This thesis focuses on digital credentialing for HEIs, such as TU Wien, and builds upon the existing work of the Digital Credentials Consortium (DCC)(see Subsection 2.4.2). Since TU Wien is located in Europe, initiatives by the European Commission (EC) are also of special interest and relevant for this thesis, and they are described in the next Subsection 2.4.1.

### 2.4.1 European Initiatives

In 2020, the EC presented the *European Skills Agenda for Sustainable Competitiveness, Social Fairness and Resilience*, with actions and goals for the following 5 years [Com20b]. The goals include having 120 million adults participate in learning events every year, which would be an increase of 32%. For adults with low qualifications, this number should increase by 67%. Furthermore, 70% of adults should have at least basic digital skills by 2025. In reaching these goals, micro-credentials and the building of a digital credentialing infrastructure play key roles. The following three subsections explain the European initiatives that are relevant for building a digital credentialing platform. Figure 2.8 provides an overview of the European initiatives and their dependencies on each other.

**Europass & European Digital Credentials Infrastructure**

Europass is an initiative by the EC for building a one-stop solution for a European digital credentials platform and providing a framework that can also be used by the private sector. The goal of Europass is to solve the problems that arise with the transition of paper credentials to a digital equivalent, such as the lack of standards, interoperability, and legal compliance.

Europass has the following four key functionalities: an interoperability mechanism, an electronic portfolio service, an information provision, and the European Digital Credentials Infrastructure (EDCI) [And19]. The interoperability mechanism connects other services and partners into the Europass ecosystem and streamlines the information exchange between the different employment and learning services to improve the end-user experience.

Another main feature of Europass is its online portfolio manager. European citizens can upload their credentials to their online portfolio and create their own online CV that contains all digitally verifiable credentials and their details. This electronic portfolio can then be sent to potential employers to display accomplishments with digital proofs for validity.

The next component of Europass, the *information provision* component, provides the information required to support European citizens in managing their lifelong learning and

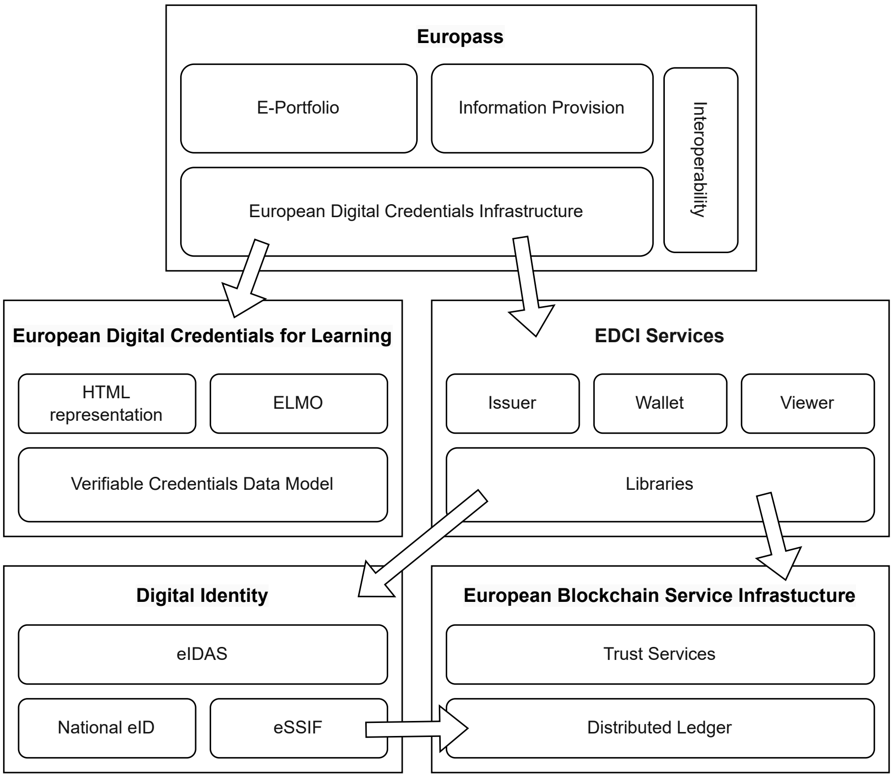


Figure 2.8: Europass on the top is the main interface for European citizens to manage their credentials. Everything underneath are the required frameworks, standards, services, and legislative measures to build the European digital credentialing ecosystem.

employment careers. This includes information on how to study or work in the different Member States of the EU or a search service for finding learning opportunities and jobs.

The last component, but also the basis for all other functionalities of Europass, is the EDCI. This infrastructure contains all of the tools and services for issuing, verifying, and exchanging European digital credentials and can be used by Member States to integrate into their own services. The EDCI is also important for the interoperability of credentials issued by different institutions through being the shared trusted infrastructure and defining a standard for modelling a digital credential, which is called the European Digital Credentials for Learning. This standard builds on top of the verifiable credentials data model by the W3C; extends it to support the XML credential format ELMO; and adds visual representation data to allow a more unique depiction of a credential. The tools and services used for the infrastructure are not specific to Europass; instead, other initiatives and projects by the EC are integrated or used by the EDCI. For example, the EBSI is used as a distributed ledger by EDCI. [Com21b]

### European Blockchain Service Infrastructure

The European Blockchain Services Infrastructure (EBSI) is the result of an initiative by 29 European countries, which joined forces to form the European Blockchain Partnership (EBP). The goal is to build a cross-country blockchain network that can be used for a variety of services, such as digital identity and digital credentials. The blockchain itself is a public, permissioned blockchain that uses Hyperledger Fabric. The operating nodes are maintained by the members of the EBP [PR20]. On top of the blockchain, EBSI builds trust services by implementing smart contracts and microservices, which expose their functionality publicly to everyone using a standardised API. The services include a trusted issuer registry for digital credentials or a DID method called *ebsi*. This method can be used to identify documents or entities on the EBSI blockchain. Many other fundamental services are exposed by EBSI, which open new trusted, cross-border information exchange use cases, such as verifiable credentials, social security, document traceability, or asylum management. Thus, EBSI has a wider scope than simply implementing a credentialing ecosystem but a more general approach to building an infrastructure that is the trusted source for transactions within the member states of the EBP.

As EBSI is a joint initiative between various countries, it has the possibility of being integrated into legal measures by those countries and making its functionalities legally binding. This is especially critical when it comes to digitally identifying citizens. The following subsection explains the current state of digital identity and its future for European citizens.

### European Digital Identity Framework

In 2014, the European Parliament and Council published a new regulation on electronic identification and trust services (eIDAS), which has been in full force since July 2016 [ge]. With this regulation, EU Member states are required to ensure the interoperability and security of their trust services with any other electronic identifications (eIDs) from other Member States. It also adds legal measures to make digitally signed documents that are compliant with the eIDAS Regulation legally binding and equally valid as those with a paper-based signature. In 2021, the EC proposed a new framework for the European digital identity, which builds on the eIDAS Regulation; therefore, it is often called eIDAS 2.0. This continuation of the regulation adds the requirement to provide a European Digital Identity Wallet to every citizen of every EU Member State. This wallet encompasses the national eID already in place along with newly added features, such as storing verifiable credentials, as standardised by the W3C.

Thus, European digital identities follow the same principles as SSI. To implement a European SSI, a part of EBSI built the European self-sovereign identity framework (eSSIF), which builds a digital identity system following SSI principles on the EBSI blockchain [SAA]. To integrate national eIDs into the EBSI blockchain, an eIDAS bridge was added that translates national identities into identities on the blockchain and vice versa [Com22b]. This eIDAS bridge is a crucial addition for all services provided by

EBSI, as this enables the identification of European citizens for digital services.

### 2.4.2 Digital Credentials Consortium

The Digital Credentials Consortium (DCC) is a collaboration of 12 leading universities in North America and Europe, such as the Massachusetts Institute of Technology, Harvard University, and TU Munich. With their expertise in digital credentials, their mission is *'to create a trusted, distributed, and shared infrastructure that becomes the standard for issuing, storing, displaying, and verifying digital academic credentials'*[DCC20]. They see three main benefits to digital credentials over paper-based credentials, namely increased efficiency for exchanging and evaluating credentials, stronger security mechanisms for preventing fraud, and greater control for learners over their credentials [DCC20].

The DCC published a white paper in February 2020 that contained their conceptual intentions and goals to build a digital credentialing infrastructure [DCC20]. This infrastructure aims to modernise the concept of credentialing for HEIs and demonstrate how a credentialing system can be designed today. The DCC has identified three groups that participate in such a credentialing infrastructure, which are comparable to the roles of verifiable credentials data model specification from Subsection 2.3.1. The holder role is held by learners, the verifier role is held by relying parties, and the issuer role is held by the issuer group. The DCC believes that each group can benefit from the use of a digital credentialing infrastructure.

In their white paper, the DCC also described their commitment to preserving privacy, building trust, and using open standards with wide interoperability. These are also guidelines for the requirements analysis and implementation aspects of the credentialing infrastructure. Moreover, the DCC lists several actions to be taken to fulfil each of their goals. These include measures for minimising disclosed data to preserve privacy or integrating it into the existing infrastructure to enable interoperability. A more detailed discussion of these actions can be found in Chapter 3.

To build a global digital credential infrastructure, the DCC must also consider legislation, such as the General Data Protection Regulation (GDPR). The DCC's privacy intentions match many privacy aspects of the GDPR, and therefore, the infrastructure further follows the privacy-by-design principle while also evaluating compliance with the said regulation. These aspects also have an influence on the choice of technology used to build the digital credentialing infrastructure. Blockchain technologies must be evaluated and checked to determine whether they are the appropriate choice for a distributed ledger and fulfil the privacy requirements by the DCC and GDPR. For example, the GDPR includes the *right to be forgotten*, which states that personal data must be removed if requested. By default, many blockchains are immutable and therefore unable to remove data.

Furthermore, the DCC must consider advancements of other initiatives in the field of digital credentialing to fulfil its goal of interoperability. Therefore, the DCC actively participates in other initiatives, such as the W3C Verifiable Credentials for Education Task

Force, to drive digital credentialing standards forward and build on existing standards whenever possible.

The focus of the DCC is on proposing changes to existing standards, proposing completely new standards that are openly available to anyone, and building the foundation for a digital credentials infrastructure. They are also building a reference implementation of these standards to enable the easier adoption of digital credentials. These implementations and standards focus on the "envelope" of the digital credential, which means that they contribute digital credential signatures, exchange protocols, and formats but not on the content of the credential itself. They compare themselves to a post office, which is only responsible for transmitting an envelope but does not care about its content. The contents of digital credentials are standardised by other efforts, such as the European Qualifications Framework (EQF)[13] and IMS Global's Comprehensive Learner Record (CLR)[14] [DCC20]. As previously mentioned, the DCC provides reference implementations for a variety of components. Many of them are libraries that abstract lower-level technical details, such as handling cryptographic functions, into higher-level methods that can be used to integrate into other tools. For each library created by the DCC, they also create an example service that demonstrates the functionalities of the underlying libraries and how to integrate them into other tools. To further ease the integration of digital credentials into existing systems, the DCC also plans to provide so-called Student Information Systems Adapters, which act as a middleware between the existing credentialing infrastructure and their new digital credentials infrastructure. This allows issuers that use a commonly used student information system, such as CAMPUSonline, to easily integrate the digital credentials infrastructure into their existing infrastructure by simply installing the adapter provided by the DCC.

In March 2022, the DCC released the first version of their wallet app on the Google Play Store and the Apple App Store [DCC22b]. This app can be used by learners to receive, send, and manage their credentials. In July 2022, 4 months after the release, they published the "Final Report", which documents the wallet app's challenges and provides insights into the development process. To make the wallet interoperable with other wallets, they first had to write a wallet app specification. This specification was released in May 2021 and included all of the technical details of the wallet app, such as the wallet building on top of both the Verifiable Credentials Data Model and the Learning and Employment Record (LER)[15]. It also extends the Universal Wallet 2020[16] specification.

To more effectively evaluate the wallet app, the DCC piloted it with three institutions, namely the Georgia Institute of Technology, College Unbound, and San José City College.

[13] https://europa.eu/europass/en/europass-tools/european-qualifications-framework last accessed 04.03.2022

[14] http://www.imsglobal.org/activity/comprehensive-learner-record last accessed 04.03.2022

[15] https://www.t3networkhub.org/resources/public-specification-for-learning-and-employment-record-ler-wrapper-and-wallet last accessed 05.03.2023

[16] https://w3c-ccg.github.io/universal-wallet-interop-spec/ last accessed 05.03.2023

These institutions were selected carefully to obtain a broad field of institutions and find issues with corner cases as early as possible. The wallet app's development team supported the institutions in setting up the credentialing infrastructure. The report states that each step of the setup process was straightforward, but it took some time to get everything set up as it was quite a complex setup and had to be integrated into the existing infrastructure. The entire process took approximately a month for each deployment site. Overall, the report states that while the development of the wallet and its specification was a straightforward process, the main challenge was the lack of production-ready tools for issuing digital credentials that institutions could use to issue digital credentials that learners would receive and manage within their wallets. Furthermore, the DCC recognised that deployment sites will likely require technical assistance to integrate the digital credentialing infrastructure into the existing issuing infrastructure, and that institutions must make certain decisions before they can adopt digital credentials. These decisions include whether to use batch issuance or single issuance at a time, whether blockchain-based technologies should be used, and what the lifecycle management of credentials looks like.

Until now, the focus has been on universities and their students, but there is a third actor within the digital credentialing ecosystem, namely the relying party or verifier. In September 2022, the DCC published a report titled *'Credentials to Employment: The Last Mile'* [Cam22]. The authors evaluated the digital credentials infrastructure from an employer's perspective and interviewed leading experts and decision-makers from different sectors and regions, who shared their insights. The interviews revealed a gap between the digital credentials currently issued and the information required by employers. To close this gap, the report proposed actions for each actor in the digital credentialing infrastructure. The interviews also revealed that all actors have compatible goals, but that cross-field communication does not exist; therefore, the current digital credentials solutions of universities do not represent the requirements of employers. Moreover, the study found that the current digital credentialing system does not have enough benefits for employers to overcome the cost of implementing digital credentials in their hiring process. To improve the situation, digital credentials should contain more information while still being highly interoperable to be useful for skill matching in hiring processes. Furthermore, the interviews demonstrated that the current situation can be compared to a chicken-and-egg problem. Issuers wait for employers to use digital credentials while employers do not integrate digital credentialing infrastructure into their workflow because not enough institutions are issuing digital credentials. Therefore, both sides have problems with a lack of support for using digital credentials in their current infrastructure services.

With the foundational understanding of digital identity, blockchain technologies, digital credentials, and relevant related research, we leverage this knowledge and delve into the next chapter: requirements analysis.

CHAPTER 3

# Requirements Analysis

The goal of this chapter is to establish requirements for a digital credentialing infrastructure, such as the prototype developed within this thesis. Existing literature that has evaluated the requirements of a digital credentialing system is used, forming the basis for the requirements analysis presented in this chapter. Section 3.1 describes the use cases of the different actors and analyses them, which results in requirements and features. Then, Sections 3.2 and 3.3 explore other relevant cross-cutting aspects that should be considered when developing and designing digital credentialing services.

## 3.1 Functional Requirements

To ensure that the prototype developed in this thesis meets its target objectives, specific requirements are necessary. They are derived from the use cases and the needs of entities in a digital credentialing system. The use cases and needs are gathered from various sources, including the whitepaper by the DCC, the verifiable credentials use cases published by the W3C, and EBSI's verifiable credentials use cases [DCC20, W3C19, Com22a]. They are then adapted to fit TU Wien.
In a digital credential system, the three roles are issuers (Subsection 3.1.1), holders (Subsection 3.1.2) and verifiers (Subsection 3.1.3). Each of these roles has its own goals and use cases for such a system. An overview of the use cases is provided in Figure 3.1.

### 3.1.1 Issuers

The main use case for issuers (e.g. HEI) in a digital credentialing system is to create digital credentials and offer them to holders (e.g. students). To issue the credential to the correct person, the issuer requires a method for verifying the identity of the receiver of the credential. Furthermore, HEIs demand the ability to invalidate all of their issued credentials at any time. This is required to fix credentials that contain mistakes,

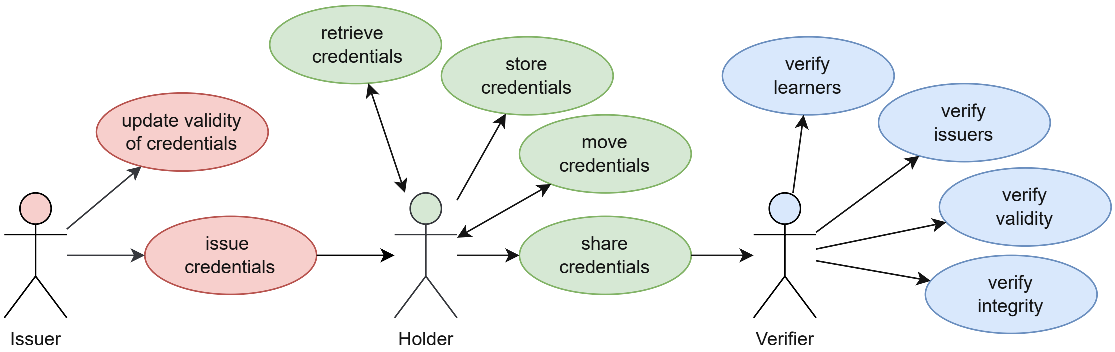


Figure 3.1: Digital credentialing system use cases overview [W3C19]

are outdated, or have changed. By issuing a new credential as a replacement for an invalidated credential, the issuer has a way to update credentials and fix mistakes.

The resulting requirements are as follows:
**RQD1:** The issuer must be able to create new credentials.
**RQD2:** The issuer must be able to notify a holder about newly available credentials.
**RQD3:** The issuer must be able to identify and authenticate a holder.
**RQD4:** The issuer must be able to send credentials to holders.
**RQD5:** The issuer must be able to update the validity of their issued credentials.

### 3.1.2 Holders

Holders, such as students, are at the centre of a credentialing system and are the deciding factor in every credential exchange. Holders need to be able to receive and request credentials from issuers and store them for later use. Stored credentials should also be shareable with verifiers by the holder of the credential. The holder should be able to decide which credentials are stored or shared with other entities, such as if students want to store all of their course credentials and degrees, to later show them to other parties to display their skill set.

The resulting requirements are as follows:
**RQD6:** The holder must be able to receive and request credentials from issuers.
**RQD7:** The holder must be able to choose which digital identity is used to identify themselves to the issuer.
**RQD8:** The holder must be able to store and display credentials.
**RQD9:** The holder must be able to move identities and credentials between different storages.
**RQD10:** The holder must be able to share credentials with verifiers.

### 3.1.3 Verifiers

A verifier uses digital credentials to obtain contained information about a subject, which is most often the holder who shared the digital credential. An example would be, an employer who wants to obtain verifiable information about the skills of a job applicant to find the best person for a specific job. It is crucial for the verifier that the information within the digital credential is correct, trustworthy, valid, and up-to-date. To verify these properties, the verifier demands reliable information about the issuer, credential subject, and credential status, which states whether the credential has been invalidated, as well as the integrity of the credential.

The resulting requirements are as follows:
**RQD11:** The verifier must be able to receive credentials from the holders.
**RQD12:** The verifier must be able to extract the information contained within the credentials.
**RQD13:** The verifier must be able to identify the subject and the holder of a credential.
**RQD14:** The verifier must be able to identify the issuer of a credential.
**RQD15:** The verifier must be able to validate the trustworthiness of issuers.
**RQD16:** The verifier must be able to validate the status of a credential.
**RQD17:** The verifier must be able to validate the integrity of a credential.

## 3.2 Security and Privacy

A digital credential system exchanges large amounts of information about individuals. Therefore, privacy and security are critical aspects; in particular, the privacy rights and expectations of holders must be taken into account. Privacy and security aspects are not only a design and moral choice but also a requirement of legislation, such as the GDPR in Europe or the Health Insurance Portability and Accountability Act (HIPAA) in the United States [W3C22b]. The following subsections describe the necessary privacy and security requirements of a digital credentialing system.

### 3.2.1 Privacy

As already mentioned, in a digital credentialing system, personally identifiable information (PII) is exchanged regularly; hence, privacy has a high priority and must be considered from the beginning when designing such a system. We define the following three main privacy aspects: holder centricity, data minimisation, and traceability prevention.

#### Holder Centricity

The data that should be protected is personal information, which is most often about the holder of the credential. Therefore, the holder should be the central entity of the credentialing system and the deciding factor in every data exchange. It is essential for holders that their data is only exchanged with their explicit consent and that every detail of the data is known by them. This includes the holder's ability to decline a credential exchange or be the initiator of the credential exchange. Furthermore, the holder must be able to store the credentials offline on a device under their control. This gives the holder more control over their data.

The resulting requirements are as follows:
**RQD18:** The holder must confirm every credential exchange.
**RQD19:** The holder must be able to store credentials on their own controlled device.

### Data Minimisation

The principle of data minimisation, a key aspect of many privacy frameworks, stipulates that every information exchange should only include the absolute minimum amount of data necessary to fulfil a task. This has many benefits in terms of privacy preservation and security. The less information that is exchanged, the less information is at risk of being compromised by malicious actors. Data minimisation has several consequences for a digital credential infrastructure. The credentials issued should either only contain the information required by possible verifiers or provide the holder with the possibility to select the information disclosed to the verifier. This selective disclosure can, for example, be achieved with zero-knowledge proofs (ZKPs). If the issuer does not allow selective disclosure methods, then they must issue multiple credentials with varying detail grades to the holder. Thus, the holder can decide which of the received credentials should be used to present them to the verifier.

Data minimisation is not only relevant for the credentials themselves but also for every service in a digital credentialing infrastructure. Every service should only store, receive, and send data that is necessary. Furthermore, the complete architecture of such a system should be built in a way that allows minimal data disclosure overall.

The resulting requirements are as follows:
**RQD20:** Each component must only receive, transmit, and store the minimum amount of personal identifying information that is necessary to achieve the desired goal.

### Traceability Prevention

Preventing traceability in a digital credentialing infrastructure is a significant challenge. Everything uses identifiers to link to something, but one still wants to prevent the traceability of identifiers and credentials as much as possible. Credentials contain identifiers of issuers and holders combined with potentially highly sensitive information claims about a subject, most often about the holders themselves. The goal is to design an architecture that prevents traceability by only making it possible to gather information about something if it is explicitly and intentionally sent. To achieve this goal, every aspect of the digital credentialing infrastructure must carefully consider this privacy goal. For example, to verify a credential, the issuer should not be involved in the verification process. This is to prevent the issuer from gaining information about where the issued credentials are sent.

The resulting requirements are as follows:
**RQD21:** The verification of a credential must maintain confidentiality and not disclose any information to other entities.
**RQD22:** The revocation of a credential must maintain confidentiality.

### 3.2.2 Security

Ensuring security in a digital credentialing infrastructure is key to establishing trust and confidence. This subsection explores various security requirements associated with digital credentialing, including measures for preventing malicious activities, such as establishing tamper-proofness and authorisation mechanisms, as well as reactive measures for detecting malicious actions by monitoring the system.

#### Integrity

An essential trust mechanism of digital credentials is the trust in their correctness and integrity. If digital credentials could be easily manipulated, then there would be no trust in them, and the complete infrastructure would become useless. Therefore, credentials must use secure cryptographic methods for signatures and integrity stamps. Creating secure cryptographic methods requires substantial knowledge and experience [W3C22b]. Consequently, only methods considered secure by experts should be used within a digital credentialing infrastructure. With technological progress and the evolution of attacks, cryptographic methods that were originally considered secure can become vulnerable to attacks over time and should be replaced by other cryptographic methods. This requires active monitoring, as discussed in the next subsections.

Furthermore, in a distributed setting, links to other data should also include an integrity mechanism. Often, it is the case that the linked data are outside of the trusted context and could unexpectedly be altered. Thus, adding integrity check values is key for every outside link in a credential.

The resulting requirements are as follows:
**RQD23:** Every communication channel must use integrity mechanisms.

#### Authentication

Every access to data, independent of the digital credentialing service, should use some kind of authentication process. Holders must authenticate to get into their wallets to display or receive credentials. Issuers must authenticate themselves to the credential- issuing service to create new credentials. It is crucial that all of these authentication processes are linked to the digital identities of the digital credentials. Moreover, it is desirable that authentication mechanisms use multi-factor authentication, which may include passwords or biometrics, to authenticate a user. For machine-to-machine communication, every data exchange should be encrypted to prevent man-in-the-middle attacks.

The resulting requirements are as follows:
**RQD24:** Every communication channel must be encrypted.
**RQD25:** Every communication channel must use signatures.

### Auditing

For the maintainer of a digital credentialing infrastructure, it is vital to monitor the system to quickly detect potential malicious activity. For the issuing service in particular, there should be functions in place to audit potential fraudulent behaviour. These auditing and monitoring functions should follow privacy-preserving principles to store as little information and restrict access as much as possible. The rapid detection of malicious activity can limit the damage done and countermeasures can be taken.

The resulting requirements are as follows:
**RQD26:** Every exchange of high-value data must be logged.

## 3.3 Interoperability

The prototype of this thesis has the important goal of achieving interoperability with existing standards and services published by the DCC, which also emphasises interoperability. This is accomplished by publishing specifications that are openly available to everyone, providing reference implementations, and designing everything such that it has broad use-case applicability while still being extensible. The open specifications enable anyone to build their own implementations while still being interoperable with other implementations out of the box, provided that everything is implemented according to specification.

Furthermore, the extendibility of the specification allows implementers to create and extend the existing feature set to fulfil special use cases that are not relevant to everyone. This customisability should not affect interoperability with other systems concerning the shared base functionalities. For example, the verifier should be able to verify a credential that contains extended features that are not included in the base specification without having to implement the custom extension.

The core of digital credentials by the DCC is the Verifiable Credentials Data Model specification published by the W3C, which uses JSON-LD as a data format combined with the DID standard to achieve the desired interoperability and extendibility. This combination of open standards and specifications enables a highly flexible, extendable ecosystem for digital credentials while still ensuring excellent interoperability in the potentially large and diverse digital credentialing infrastructure. Therefore, the standards published by the W3C must be used by the prototype developed within this thesis to provide interoperability with other existing systems.

In addition to the data model of digital credentials, there are also specifications for standardising the communication protocol to exchange digital credentials. At the time of designing and starting the development of the prototype of this thesis in May 2022, most of these standards were only drafts. The DCC uses the Verifiable Credentials API specification, which is still a draft as of March 2023 [DCCa, W3C23]. Two other prominent standards, OpenID for Verifiable Credential Issuance (OID4VCI)[1] and OpenID for Verifiable Presentations (OID4VP)[2] which will be used by EBSI are also still not finalised as of March 2023. Therefore, these drafts can be considered for the prototype of this thesis; however, customisation along the way may be required because of a lack of finalised open specifications.

The resulting requirements are as follows:
**RQD27:** The credentials must be formatted according to the W3C Verifiable Credentials Data Model specification.
**RQD28:** Existing standards must be used whenever possible.

Having established the functional and non-functional requirements for the digital credentialing prototype, the focus now shifts to the implementation details in Chapter 4. The chapter outlines the reasoning for technology selections and architectural decisions. This is followed by a detailed description and discussion of the implementation, where the alignment between the chosen design and the identified requirements of this chapter is emphasised to create a functional and effective digital credentialing system.

[1] https://openid.bitbucket.io/connect/openid-4-verifiable-credential-issuance-1_0.html last accessed 30.04.2022

[2] https://openid.bitbucket.io/connect/openid-4-verifiable-presentations-1_0.html last accessed 30.04.2022

# CHAPTER 4

# Implementation

This chapter focuses on the implementation details of the prototype, beginning with an in-depth discussion of the selected technologies in Section 4.1. This is followed by the architectural decisions in Section 4.2, which details the considerations made in designing the overall structure and interactions of the prototype system. The list of requirements resulting from the previous requirement analysis in Chapter 3 guides the design and implementation decisions of this chapter. The design and implementation details of individual components of the digital credentialing system are explained in Section 4.3.

Overall, this chapter provides an in-depth insights into the technical implementation of the digital credentialing system prototype and provides reasoning for the decisions made during the development process.

## 4.1 Selection of Technologies

The selection of appropriate technologies for a given task is crucial for the implementation and design processes. The technology choice has a high influence on the final outcome of the prototype, and therefore, the choice of a specific technology should be made carefully while considering the requirements. For the prototype of this thesis, the requirements listed in Chapter 3 provide a rough outline of which technologies should be selected. A critical aspect of the resulting prototype is its interoperability with existing standards and systems.

First, we must define which technology choices need to be made. Based on the requirements and aim of this thesis, it is clear that the goal is to build a digital credentialing prototype for TU Wien, based on the implementations, specifications, and principles of the digital credentialing system by the DCC. This means that the resulting prototype will consist of various services that together form a digital credentialing infrastructure.

To build this infrastructure, three main categories of technological decisions must be made.

The first category of technology decisions involves defining a protocol and technology for the communication between distributed services, which each service is able to integrate. For the prototype of this thesis, the HTTP[1] protocol is used to exchange data, as it is already used by the existing implementation of services by the DCC and is the de facto standard for communication between services on the web. Another advantage of using HTTP is its popularity, which makes it easy to implement with almost any programming language and framework. This is important, as we do not want to limit our selection of programming languages or frameworks for each service just because of the communication standard chosen. The use of HTTP enables the prototype to achieve strong interoperability and security with the extension of HTTPS[2], which encrypts the communication channel.

With the communication protocol defined(i.e. HTTP or HTTPS), depending on the required protection of the communication channel, the next step is to define the infrastructure technologies that will be used to build and run the credentialing prototype. Containerisation has emerged as a popular choice for the packaging and deployment of services. This is because it abstracts the runtime environment and bundles the service into a package that can be easily ported between different systems without any prerequisites other than the container runtime environment itself. Therefore, the infrastructure used for this thesis takes advantage of containerisation, specifically through the use of Docker[3], the most widely used container technology, which is easy to use and integrate [PBSJ19]. Another benefit of containerisation is that the prototype can be executed in a uniform process, even if individual services use different technologies and have different dependencies. Each service is packaged into a Docker image that contains all the necessary dependencies and runtime environments.

As mentioned earlier, the prototype consists of various different services packaged as Docker images that communicate with each other over HTTP. This necessitates some kind of orchestration tool for managing individual services. The required features for the prototype's orchestration include a configuration method for each service, networking features to discover other services and manage communication between them, and the ability to execute the services themselves. Many tools meet these requirements, but for the purpose of this prototype, Docker Compose[4] is selected as it comes bundled with the Docker installation, which makes the initial setup very easy. Docker Compose only requires one simple configuration file that declares everything from the service configuration to the network configuration. This makes Docker Compose our preferred choice over other orchestration tools, such as Kubernetes, which often require a more complicated setup.

[1] https://www.rfc-editor.org/rfc/rfc9110.html last accessed 16.04.2023

[2] https://www.rfc-editor.org/rfc/rfc2818 last accessed 16.04.2023

[3] https://www.docker.com/ last accessed 16.04.2023

[4] https://docs.docker.com/compose/ last accessed 16.04.2023

With the infrastructure communication technologies fixed, the last selection of open technology pertains to the choice of technologies used within each service of the prototype system. Different types of services are planned, each with different requirements. This makes a common technology choice for all services pointless, and it makes much more sense to have different technology selections for each service that consider individual requirements. Nevertheless, it is already clear from the previous chapters that some services will create, manage, or verify digital credentials, which should be formatted according to the Verifiable Credentials Data Model specification by the W3C, as stated in requirement RQD27. Even though this specification does not directly enforce a specific serialisation, it is clear from the specification and the reference implementation by the DCC that JSON-LD is the preferred serialisation method[W3C22b]. As the name already suggests JavaScript Object Notation for Linked Data (JSON-LD), the JSON-LD format is closely related to JavaScript, which naturally gives JavaScript-based technologies an advantage over other technologies. Therefore, JavaScript-based technologies are our preferred choice when it comes to services that must parse digital credentials.

Another key standard that must be considered when implementing verifiable credentials is the DID standard, as it links distributed information together. As explained in Subsection 2.1.3, the DID standard is an umbrella specification for many subspecifications. Therefore, for each DID method, a method-specific implementation is required. To provide maximum interoperability, the choice of technology should consider the availability of libraries that implement these DID methods, making the integration of multiple DID methods very easy with minimal effort. The DCC's digital credentialing implementation uses two DID methods, namely `did:key` and `did:web`. The most popular libraries on GitHub for both methods are implemented in a JavaScript-based language [Baz23, Fou23]. This further supports the selection of JavaScript-based technologies for services that parse credentials.

However, the prototype not only contains services that parse credentials but also those that may need to interact with some type of blockchain or require a user interface. For example, RQD8 states that the holder needs some method of displaying and storing credentials. Combined with RQD19, it is clear that an application executed outside of the core credentialing system is required and instead runs on a holder-controlled device. In this case, the device is a smartphone running a mobile app. This choice was made because smartphones are the most portable device that holders may own, and a study by Eurostat demonstrated that most people in Europe use their smartphones to interact with the Internet [Eur16]. The mobile app of this prototype runs on as many smartphones as possible, and therefore, it must support both of the main smartphone operating systems, namely Android and iOS, which cover 99% of all smartphones in Europe [Szc18]. The credentialing system built by the DCC uses the React Native[5] framework to build the mobile app, which supports building mobile apps for both major mobile operating systems from just one shared codebase. Another benefit of React Native is that it is JavaScript-based, which means that libraries built for the credential handling

[5] https://reactnative.dev/ last accessed 16.04.2023

services might be reusable for the mobile app. Other mobile app frameworks also support multiple mobile operating systems and support JavaScript libraries, such as Flutter; however, to reuse as much of the implementation by the DCC as possible, the mobile app of this thesis also uses React Native for the mobile app built for the holder.

The next core functionality is the integration of blockchain technologies into the credentialing prototype. At the time of writing, the current implementations by the DCC do not contain any blockchain integrations. Therefore, the selection of blockchain technologies is not guided or limited by an existing implementation, as was the case for the previously selected technologies. As mentioned in Subsection 2.2.4, applications on a blockchain are often implemented in Solidity, a programming language that allows smart contracts to be written for blockchains that support the EVM. For the development and demonstration of the prototype, it is crucial to have a testing blockchain environment that does not require any real money to be paid. Moreover, the blockchains used should use a sustainable and environmentally friendly consensus mechanism for ethical reasons. More information can be found in Subsection 2.2.3. Ethereum is the most popular blockchain that fulfils all of the requirements of having a Turing-complete execution environment for application code, easily accessible test networks, an environmentally friendly consensus mechanism, a robust ecosystem, and an active community. At first, the test networks Rinkeby and Ropsten were used to implement the prototype, both of which were deprecated in Q3 of 2022, leading to the switch to the Goerli test network [Fou22]. This demonstrates the importance of configurability and deployment processes for the blockchain services in the prototype.

The smart contracts themselves should be written in Solidity and developed within the Hardhat[6] development environment, which makes building, integrating, and deploying Solidity smart contracts easier. For the development of the prototype, the most critical feature of Hardhat is the automated generation of JavaScript-based classes and methods that allow easy integration of Solidity smart contracts into JavaScript-based services. This ties in with the selection of JavaScript-based technologies for the credentialing services as now the blockchain interactions are possible directly within the JavaScript context.

Thus far, all of the discussed areas can be built using a JavaScript-based technology stack – with one exception. The prototype of this thesis should integrate with the existing TISS infrastructure of TU Wien, and TISS is implemented in Java. Therefore, all parts that are, in the case of a production deployment, directly integrated into TISS must be implemented using Java.

In summary, the prototype of this thesis uses a JavaScript-based technology stack whenever possible, with the only exception being parts that would be directly integrated into TISS in the case of a production deployment. HTTP or HTTPS is used to implement communication between services, independent of the technology they are built with. To

[6] https://hardhat.org/ last accessed 16.04.2023

configure and run the prototype in a flexible and portable manner, Docker Compose is used to orchestrate the services, which are packaged as Docker images.

## 4.2 Architecture

The architecture of the digital credentialing prototype of this thesis is influenced by various factors, such as existing implementations and standards, as analysed in Subsection 2.4.2, and the desired goals of TU Wien. Naturally, there are three main actors in a digital credentialing system, namely the issuer, who creates new credentials and updates their validity; the holder of the credentials, which in most cases is the subject of the credential but may be a different entity; and the verifier, who checks the validity of credentials owned by the holder. Each of them has their own requirements for the digital credentialing system. The architecture of the prototype is designed around the requirements evaluated in Chapter 3, and the designed architecture considers every technical and feature requirement.

Moreover, it is possible to implement most services within the credentialing system using a similar technology stack, as discovered in the previous Section 4.1. This enables an architecture that can reuse components of other services without the burden of reimplementing similar functionalities multiple times.
The design process starts with the evaluation of the different actors within the system and their expressed feature requests and interaction methods with the system. The issuer in the case of this thesis is TU Wien, and more precisely lecturers at TU Wien who, for example, want to issue certificates to the participants of their lectures. This is currently done within TISS, which provides a web interface for issuing new credentials. This thesis evaluates the feasibility of integrating a digital credentialing system like the one proposed by the DCC into the existing TISS infrastructure (RQ1). For this purpose, this thesis simulates TISS's ability to stay independent and separate from the existing TISS infrastructure while still emulating a similar experience for the issuers. To achieve this similarity, the simulated TISS (hereinafter the *'TISS Dummy'*) should use the same interaction methods and technologies as the real TISS.

The next actor is the holder, who receives credentials from the issuer and later shares them with verifiers. As mentioned in Section 4.1, the holder will interact with the digital credentialing system via a mobile app called a wallet. The wallet app stores all of the credentials owned by the holder and handles the interactions with the other actors within the system. The implementation of the wallet is based on the Learner Credential Wallet (LCW) implemented by the DCC and adapted to work with the extensions and adaptations made within this prototype. To receive a credential from the issuer, the wallet uses a REST interface of the TISS Dummy. After the credentials are retrieved from the issuer, the wallet stores them on the mobile device owned by the holder. Stored credentials can then be shared with verifiers by exporting the credential as a credential presentation file. This file can be exchanged in different ways, which are not specified, as this should be the decision of the holder and verifier. This exchange can, for example, take place via email, an online form, or social media.

After the verifier receives the credential presentation file from the holder, the verifier uses the file to verify the claims made within the credential. This verification consists of multiple checks, two of which require data access from outside. The first one is the verification of the trustworthiness of the issuer of the presented credential (RQD15), while the second is the verification of the status of the credential (RQD16). Every other verification check can be performed locally without retrieving data from outside. For the purpose of this thesis, the verifier is implemented as a simple command-line interface (CLI) tool that demonstrates the verification functionality and serves as a reference implementation for other services that may want to integrate credential verification. In a production environment, the functions of the CLI tool would be integrated into a larger application, such as a human resources management system (HRMS), for example, to verify the credentials of job applicants.

All of the services mentioned up to this point are user-facing applications used by the different actors in the digital credentialing system. Each of these services depends on other services and libraries under the hood to fulfil the requirements of the actors using the services. Figure 4.1 illustrates the different services, libraries, and components that are relevant to this thesis and together form the digital credentialing prototype.

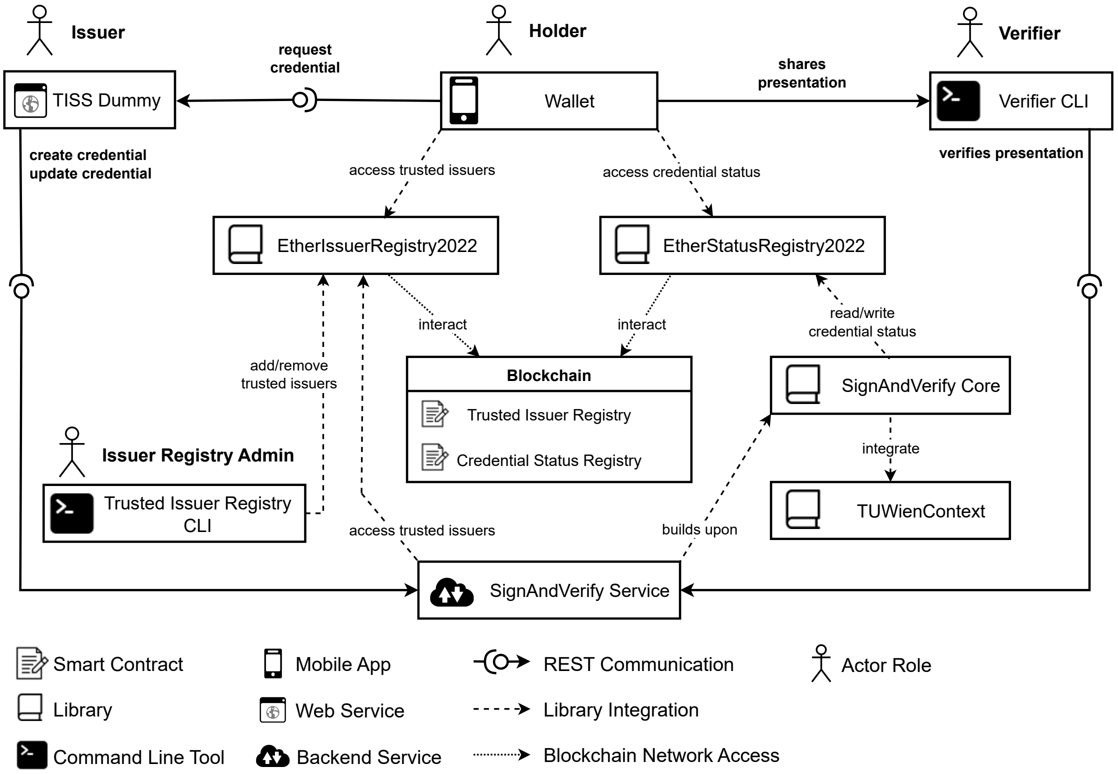


Figure 4.1: Overview of the prototype architecture

The SignAndVerify service is a key component as it implements all the required methods and functions to create, update, and verify digital credentials. Even though this service combines the required features of the issuer and the verifier, each actor should have their own instance of this service. This architectural decision was made by the reference implementation of the DCC. An advantage of this decision is that issuers can, out of the box, also verify credentials, which is a welcome feature for TU Wien, as it might also want to verify the credentials of other universities in the future. Furthermore, merging features of both issuers and verifiers reduces the infrastructure complexity and eases the development process.

The core contributions of this prototype are the blockchain-based services for maintaining a trusted issuer registry and updating the credential status after issuance. For the trusted issuer registry, a new actor is required, namely the issuer registry admin, who is responsible for maintaining a list of trusted issuers. The list is publicly available to everyone, but only the admin can change its content. It is the administrator's task to verify the credibility of the issuers on their list and demonstrate their own trustworthiness to other entities. The trusted issuer registry admin may be a legal entity or an accreditation institution that is generally considered trusted. Verifiers can then select a trusted issuer list, which is maintained by an issuer registry admin they trust. If verifiers do not want to trust other entities, they can create their own trusted issuer list and act as an issuer registry admin of their own list. This flexible, distributed, and secure design of the verification process of issuers is a core component in the trust model of the prototype's architecture.

This continues with the design decisions of the credential status registry, which is responsible for updating the validity of already issued credentials. Issuers might want to invalidate a credential after they have already sent it to the holder (RQD5). For this purpose, the credential status registry is created, which holds information about the current status of a credential publicly. Possible statuses are suspended, revoked, or valid. The difference between revocation and suspension is that revocation cannot be undone, whereas suspension is only a temporary invalidation of the credential and can be reversed. Generally, we consider the issuer to be the controller of the status of the credential, but the design of the credential status registry of this thesis allows everyone to express their opinion regarding the credential status; and then, the verifier decides who they consider a trustworthy credential status maintainer. By default, this is the issuer of the verified credential, but verifiers can change that behaviour and use the credential status expressed by another entity other than the issuer.

Both registries are key components for building trust in the complete digital credentialing system, as both can influence the validity of every credential issued. Therefore, the flexible, distributed, and secure design should support trust in the complete digital credentialing infrastructure.

## 4.3 Services

This section explains the technical details of key components of the digital credentialing prototype. Each component is discussed individually, and for each one, descriptions of its responsibilities within the credentialing system and the requirements to be met are provided. This is followed by a description of the features and implementation of the component, including screenshots of the result, and a discussion of potential limitations.

### 4.3.1 TISS Dummy

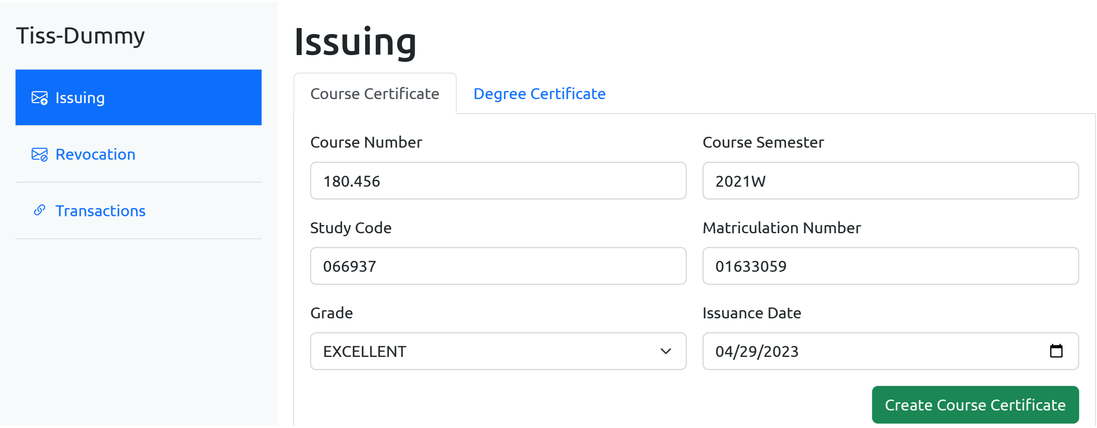
The TISS Dummy is the interface for the issuer to interact with the digital credentialing prototype and serves as a reference implementation for other potential services that may want to integrate a digital credential issuance capability. The features of the TISS Dummy are derived from the requirements of the issuer described in Subsection 3.1.1. The TISS Dummy has two main functions, namely creating new digital credentials and updating their status after issuance. The credential creation form can be found under the *Issuing* menu point of the TISS Dummy user interface, as depicted in Figure 4.2a. This page is subdivided into two tabs, each of which is a separate credential creation form that contains all of the required field inputs for a specific type of credential. The TISS Dummy currently supports *course certificates* and *degree certificates*.

After a new certificate is created, it is stored in a database tied to the TISS Dummy, and the subject of the credential can be informed that a new certificate has been issued. The TISS Dummy has not implemented a notification of the subject but instead displays a QR code directly within the TISS Dummy web interface. The QR code is required to retrieve the credential using the holder's wallet app. An example QR code can be seen in Figure 4.3b. In a production deployment of an issuing service, this QR code should be sent to the holder of the certificate by email, or another mechanism should be provided to the holder to access the QR code.

When the holder scans the QR code, the wallet app of the holder connects to the TISS Dummy using a REST interface and receives a newly created credential if the holder has successfully authenticated themselves to the TISS Dummy. The creation of the actual verifiable credential according to the Verifiable Credentials Data Model is achieved using the SignAndVerify service, which is explained in more detail in the next subsection 4.3.2. The authentication is implemented using a secret stored within the QR code; therefore, anyone with access to the QR code can retrieve the credential. If desired, this authentication could be hardened by adding additional authentication mechanisms, such as requiring a login to the TISS Dummy before the credential is received. As mentioned in Section 3.3, OID4VCI is a standard in development that defines what this interaction between the wallet app and the TISS Dummy could look like. Unfortunately, this standard is not finished, and therefore, authentication is currently based on a secret token integrated into the QR code.

A certificate created with the TISS Dummy can be received multiple times by the holder. Each received credential is unique and can be individually invalidated. The *Revocations* page of the TISS Dummy contains a list of all issued credentials, as seen in Figure 4.4c. For each credential, the issuer has the possibility to revoke, suspend, or unsuspend the credential. These actions ultimately create a blockchain transaction that updates the credential status in the credential status registry. As blockchain transactions require some time until they are considered final and may fail for various reasons, a third menu item was added called *Transactions*, which displays a list of all credential status transactions triggered by the TISS Dummy, as seen in Figure 4.5d. This should give the issuer better feedback on the progress of the credential-updating process and indicate whether the updating has failed, along with the reason for the failure.

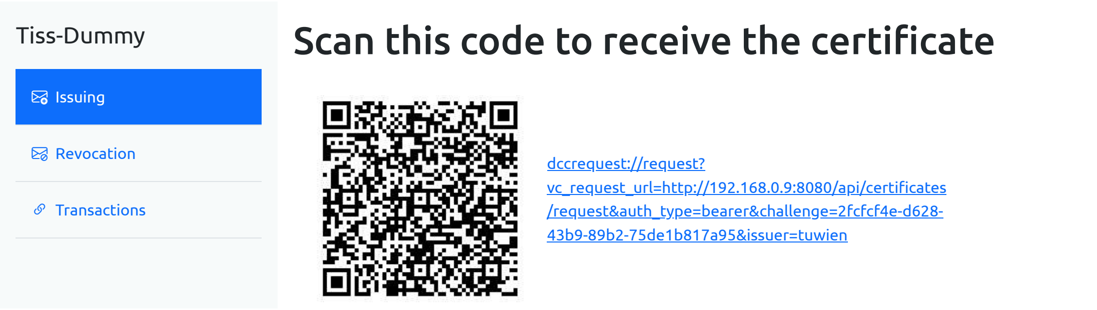
Overall the TISS Dummy is the web interface for the SignAndVerify Service, which is discussed in the next subsection.



Issuing

Course Number: 180.456
Course Semester: 2021W
Study Code: 066937
Matriculation Number: 01633059
Grade: EXCELLENT
Issuance Date: 04/29/2023

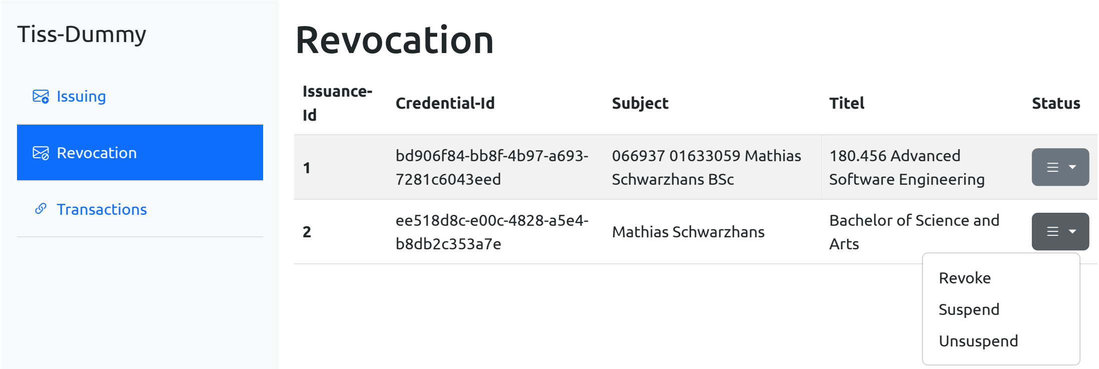
(a) The "Issuing" tab, where it is possible to create new certificates. Each type of certificate is represented as a tab.



Scan this code to receive the certificate

dccrequest://request?vc_request_url=http://192.168.0.9:8080/api/certificates/request&auth_type=bearer&challenge=2fcfcf4e-d628-43b9-89b2-75de1b817a95&issuer=tuwien

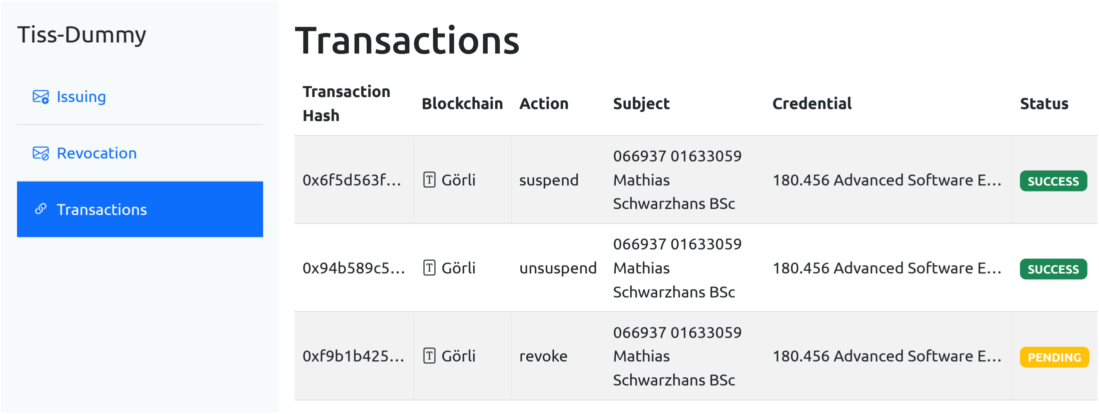
(b) The QR code sent to the holder, contains all the information to retrieve the newly created certificate. The URI next to the QR code is the content of the QR code.



## Revocation

| Issuance-Id | Credential-Id | Subject | Titel | Status |
|---|---|---|---|---|
| 1 | bd906f84-bb8f-4b97-a693-7281c6043eed | 066937 01633059 Mathias Schwarzhans BSc | 180.456 Advanced Software Engineering | ≡ ▾ |
| 2 | ee518d8c-e00c-4828-a5e4-b8db2c353a7e | Mathias Schwarzhans | Bachelor of Science and Arts | ≡ ▾ |

(c) The "Revocation" tab contains a list of all issued credentials and allows updating the credential status.



## Transactions

| Transaction Hash | Blockchain | Action | Subject | Credential | Status |
|---|---|---|---|---|---|
| 0x6f5d563f... | Görli | suspend | 066937 01633059 Mathias Schwarzhans BSc | 180.456 Advanced Software E... | SUCCESS |
| 0x94b589c5... | Görli | unsuspend | 066937 01633059 Mathias Schwarzhans BSc | 180.456 Advanced Software E... | SUCCESS |
| 0xf9b1b425... | Görli | revoke | 066937 01633059 Mathias Schwarzhans BSc | 180.456 Advanced Software E... | PENDING |

(d) The "Transactions" tab contains a list of all credential status blockchain transactions and their current status.

Figure 4.5: The different user interfaces of the TISS Dummy

### 4.3.2 SignAndVerify Service

The SignAndVerify service is a core part of the digital credentialing prototype. It provides a REST interface for performing all issuing, holding, and verification tasks that an issuer, holder, or verifier might need to do. The service's implementation is based on the reference implementation[7] by the DCC, and the REST interface exposed is inspired by the Verifiable Credential API[8] specification. This specification is still in progress as of May 2023, and therefore, the REST interface exposed by the SignAndVerify service of this prototype might deviate from the current specification. Table 4.1 presents the four most important interfaces for the issuer and verifier.

[7] https://github.com/digitalcredentials/sign-and-verify last accessed 01.05.2023
[8] https://github.com/w3c-ccg/vc-api last accessed 01.05.2023

| Role | Endpoint | Description |
|---|---|---|
| Issuer | `POST /request/credentialwithdata` | Creates and signs a new credential based on the data in the body. |
| Issuer | `POST /status/credential` | Updates the status of a credential |
| Verifier | `POST /verify/credentials` | Verifies the passed credential |
| Verifier | `POST /verify/presentations` | Verifies the passed presentation |

Table 4.1: SignAndVerify REST endpoints

The issuer uses the SignAndVerify service for two functions, namely creating new credentials and updating their status. To create a new credential, the SignAndVerify service receives the following two core data objects: the certificate data that should be embedded into the credential and the holder's verifiable presentation, which verifies their identity and contains the secret challenge required to receive the credential. After the holder has been verified, the credential is built, signed by the issuer, and returned by the REST interface.

To update the status of a credential, the credential update endpoint requires a complete, verifiable credential and the desired action to be executed. The SignAndVerify service then uses the credential status registry to set the status accordingly and return the blockchain transaction data. The SignAndVerify service does not wait until the transaction has finished; instead, it is the caller's task to track the status of the transaction.

Both endpoints for the issuer are secured by signature verification and a digest integration check. The signature is implemented using a shared secret between the client and server, in this case, between the TISS Dummy and the SignAndVerify service. The signature is built using the HMAC-SHA512 algorithm and signs the digest combined with the timestamp of the request. The digest is the SHA512 hash value of the body of the request. These two security measures ensure secure data exchange between the TISS-Dummy and the SignAndVerify service (RQD23,RQD25).

Furthermore, the endpoints of the SignAndVerify service should not be publicly available. The REST interfaces of the service are intended to be used by a single entity that is tightly coupled to the service. For example, the TISS Dummy has an instance of the SignAndVerify service that is only used by the TISS Dummy and nothing else. The Docker network is configured so that only the coupled service can communicate with the SignAndVerify service.

The other main actor who uses the SignAndVerify service is the verifier. There are two endpoints intended to be used by a verification service, both with a similar goal of verifying information. One endpoint is for verifying verifiable credentials, while the other is for verifiable presentations.

As mentioned in Subsection 2.3.1 a verifiable presentation is a wrapper of a list of verifiable credentials with added benefits, such as demonstrating ownership of credentials within the list. To verify a presentation, the SignAndVerify service must check the presentation's signature, followed by verifying the individual credentials within the presentation. To verify a verifiable credential, the following aspects must be checked:

- **Credential Schema**: The credential must be formatted correctly and contain all of the required fields as defined by the JSON-LD schema for the credential.
- **Signature**: The credential must be properly signed by the issuer and must not be tampered with.
- **Trusted Issuer**: The credential must be signed by a trusted issuer as listed in the trusted issuer registry.
- **Credential Status**: The issuer must not have revoked or suspended the credential.
- **Expiration**: The credential must not have passed its expiration date.

The verification of the credential schema, signature, integrity, and expiration is handled directly within the SignAndVerify service and does not require any information gathering from other services. By contrast, the verification of the issuer and credential status requires data stored in a verifiable datastore – in this case a blockchain. The integration and implementation of the trusted issuer registry and credential status registry are explained in Subsections 4.3.4 and 4.3.5, respectively.

### 4.3.3 Wallet

The wallet app has been built specifically to meet the holder's functional and technical requirements. This thesis's wallet app is an adapted version of the LCW app by the DCC, the core functionalities of which remain unchanged. However, certain changes have been made to support the newly added features of the credentialing system prototype proposed in this thesis. One is the addition of a newly created credential schema that includes more information than the regular schema, such as the grade, lecturers, study code, and matriculation number. Another change is the integration of the credential status registry and trusted issuer registry into the wallet's integrated verification view.

All changes made to the LCW have been carefully implemented without dropping support for other credential schemas. Thus, the wallet app presented in this thesis is interoperable with all credentials supported by the original LCW app, including credentials with the additions made in the digital credentialing prototype of this thesis. Unfortunately, the LCW does not support the credentials issued by the prototype, as it has no implementation for the proposed credential status registry standard.

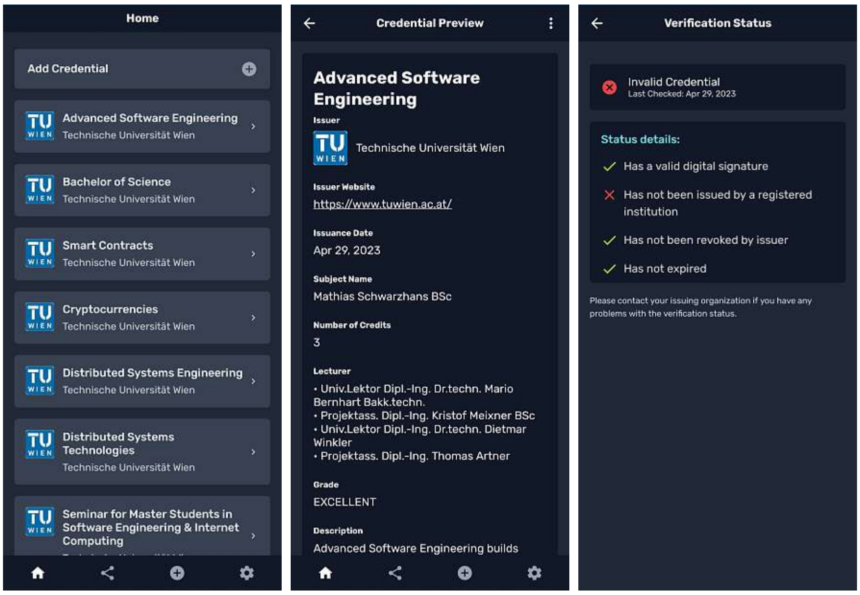
The key feature of the wallet app is its capability to store the holder's credentials in a secure and privacy-preserving manner (RQD8). All credentials are stored directly on the holder's device and secured through encryption (RQD19). To access the stored credentials, the holder must enter a password, which is used as the encryption key. After the authentication, the holder gains access to all four function categories of the wallet app, which are described as follows:

- **Home**: This displays a list of all stored credentials and is used as an entry point for inspecting individual credentials in more detail.
- **Share**: This displays a selectable list of all stored credentials and is used to share credentials with others.
- **Add Credential**: This allows the holder to add new credentials by scanning a QR code provided by the issuer.
- **Settings**: This contains all of the management functions for the wallet app itself, such as exporting and importing identities and credentials.

The *Home* category is the starting point after one unlocks the wallet app and contains all functions that the holder requested through RQD8. Figure 4.6 illustrates how the holder can access the credential details and its verification details. The verification process includes the same checks as the verification service for the verifier and uses the same libraries under the hood to access the trusted issuer registry and credential status registry but it is integrated into the wallet app. The wallet directly connects to a blockchain node to access the required data.

To add new credentials to the wallet, the holder must scan the QR code provided by the issuer. The holder can use any QR code reader installed on their device or the wallet's built-in QR code reader. Once the QR code has been scanned, the wallet connects to the issuing service hosted by the issuer, authenticates the holder, and retrieves the credential linked to the QR code (RQD6). Before adding the credential to the wallet's storage, the holder is presented with a list of credentials that were retrieved from the issuing services and given the option to accept or decline each one. Only after being accepted is the credential stored in the wallet (RQD18). This process of adding a credential to the wallet is illustrated in Figure 4.7.

Another key feature of the wallet app is the ability to share credentials with others (RQD10). The holder can select credentials from the list of all stored credentials and export them as a verifiable presentation in the form of a JSON-LD file, which can be sent to another entity. Figure 4.9 depicts the sharing functions and demonstrates that the holder can choose the method to be used to exchange the presentation file with the other entity.



Home

Add Credential

Advanced Software Engineering
Technische Universität Wien

Bachelor of Science
Technische Universität Wien

Smart Contracts
Technische Universität Wien

Cryptocurrencies
Technische Universität Wien

Distributed Systems Engineering
Technische Universität Wien

Distributed Systems Technologies
Technische Universität Wien

Seminar for Master Students in Software Engineering & Internet Computing

Credential Preview

Advanced Software Engineering

Issuer
Technische Universität Wien

Issuer Website
https://www.tuwien.ac.at/

Issuance Date
Apr 29, 2023

Subject Name
Mathias Schwarzhans BSc

Number of Credits
3

Lecturer
- Univ.Lektor Dipl.-Ing. Dr.techn. Mario Bernhart Bakk.techn.
- Projektass. Dipl.-Ing. Kristof Meixner BSc
- Univ.Lektor Dipl.-Ing. Dr.techn. Dietmar Winkler
- Projektass. Dipl.-Ing. Thomas Artner

Grade
EXCELLENT

Description
Advanced Software Engineering builds

Verification Status

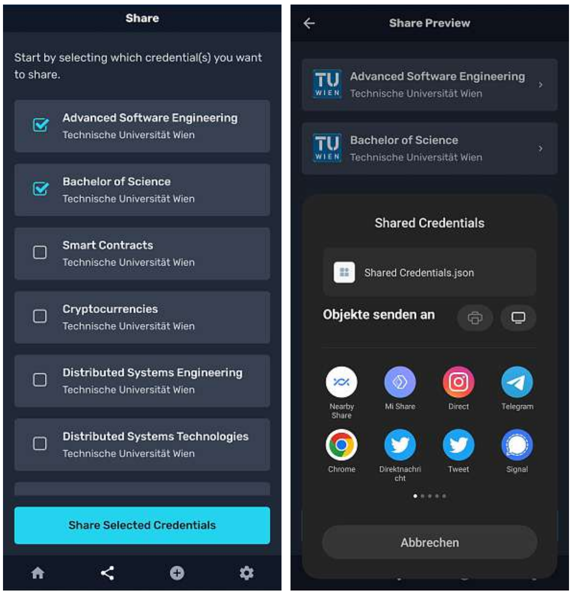
Invalid Credential
Last Checked: Apr 29, 2023

Status details:
✓ Has a valid digital signature
✗ Has not been issued by a registered institution
✓ Has not been revoked by issuer
✓ Has not expired

Please contact your issuing organization if you have any problems with the verification status.

(a) List view (b) Details view (c) Verification view

Figure 4.6: The *Home* category lists all the stored credentials and allows inspection of individual credentials and their verification details.



Share

Start by selecting which credential(s) you want to share.

☑ Advanced Software Engineering
Technische Universität Wien

☑ Bachelor of Science
Technische Universität Wien

□ Smart Contracts
Technische Universität Wien

□ Cryptocurrencies
Technische Universität Wien

□ Distributed Systems Engineering
Technische Universität Wien

□ Distributed Systems Technologies
Technische Universität Wien

Share Selected Credentials

Share Preview

Advanced Software Engineering
Technische Universität Wien

Bachelor of Science
Technische Universität Wien

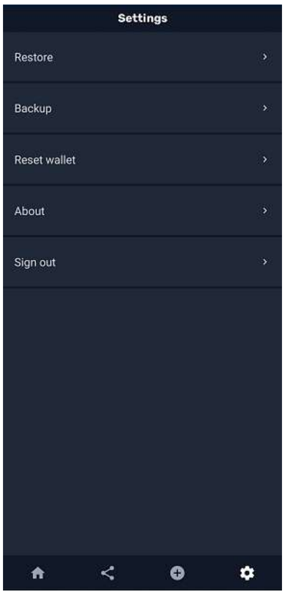
Shared Credentials

Shared Credentials.json

Objekte senden an

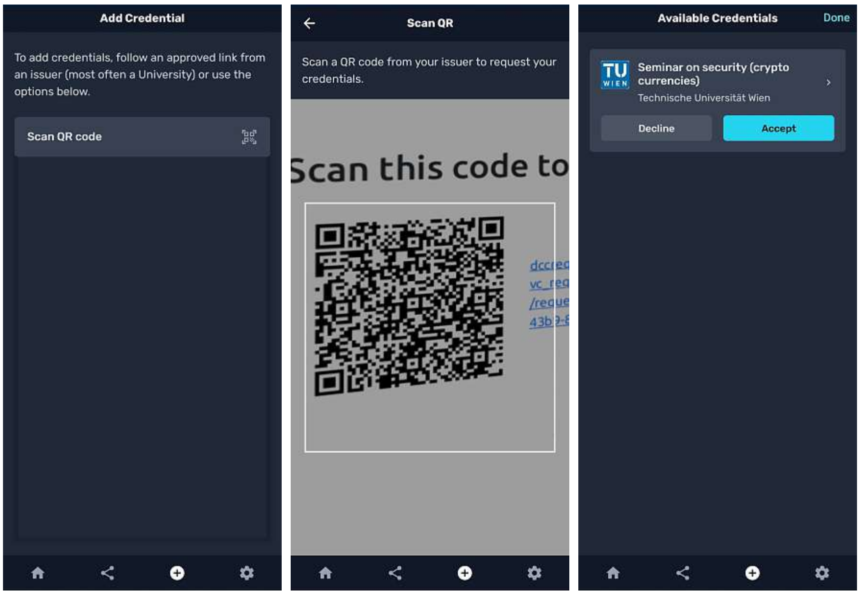
(a) Credential selection list (b) Share method selection

Figure 4.9: The *Share* category presents a list of all credentials, which can be marked to share with others.



Settings

Figure 4.11: The *Settings* category provides access to all the management functions of the wallet.



To add credentials, follow an approved link from an issuer (most often a University) or use the options below.

Scan a QR code from your issuer to request your credentials.

(a) Add Credential view (b) Integrated QR code reader (c) Credential preview

Figure 4.7: The *Add Credential* allows the user to add new credentials by scanning a QR code.

Lastly, the *Settings* page of the wallet app provides the holder access to the management functions of the wallet, such as exporting and importing all of the wallet's data, as illustrated in Figure 4.11. The export and import feature is a result of the RQD9 requirement, which aims to prevent vendor lock-in.

### 4.3.4 Trusted Issuer Registry

The trusted issuer registry is a key component in the trust framework of the digital credentialing prototype presented in this thesis. As expressed in RQD15, the verifier needs a method to validate the trustworthiness of the issuer of a credential. A popular method for establishing trust in an entity is through trust registries. In this case, the trust registry is a list of trustworthy issuers managed by a generally trusted entity, such as a government body. The verifier can trust an issuer if the issuer is on a trusted issuer registry managed by an entity that the verifier already trusts. The administrator of the registry only adds issuers to the list that she or he trusts.

This trust framework is highly flexible and perfectly suits the use case of this thesis. The verifier can decide whom to trust by managing a list of trusted issuers, or they can even manage their own trusted issuer registry if they prefer. The digital credentials implementation by EBSI also follows a similar model, with additional trust delegation and more restrictive properties. However, the key concept remains the same, namely that only the trusted issuer registry is adapted to support nested registries. This means that the registry can link to another registry as long as the links do not create a loop. Additionally, the registry defines what kind of credentials an issuer is authorised to issue [Com23].

For the purpose of this thesis, the trusted issuer registry is a simple list of issuers, and for each issuer, the following four properties are stored: the identifier, name, location, and URL. The reference implementations by the DCC use a JSON file in a public GitHub repository[9] as a trusted issuer registry. This solution is only temporary and serves as a minimal viable product while developing the credentialing system. In its whitepaper, the DCC describes plans to use blockchain technology in later stages of the development process for the trusted issuer registry and the credential status registry [DCC20].

The trusted issuer registry presented in this thesis uses blockchain technologies and is an evolution of the initial trusted issuer registry established by the DCC. The blockchain-based solution has the same functionalities and can be used as a drop-in replacement for the initial solution by the DCC.

The core of the blockchain-based trusted issuer registry is a smart contract, which functions as a publicly distributed list of issuers that can be read by anyone and modified by admins of the smart contract. When working with smart contracts, it is essential to optimise the code to reduce the gas cost required to interact with the contract. For this reason, the list of trusted issuers is implemented using two data structures within the smart contract, namely an array containing all identifiers of the trusted issuers and a mapping that maps the identifier to the corresponding issuer details. The specific data structure mix is presented in Listing 4.1 and has been chosen because Solidity mappings are much more gas-efficient than arrays; yet, mappings are not iterable. This means that only using mappings is not possible, as it would not allow one to retrieve all trusted issuers of the registry and would only support checking whether a specific issuer is in the registry. On the other hand, using only an array of all issuer-related information would result in a higher gas cost compared with the mixed approach chosen within this thesis.

```
struct IssuerData {
   uint256 index; // index within the issuerDid Array
   string name;
   string location;
   string url;
}
mapping(string => IssuerData) private trustedIssuers;
string[] issuerDids;
```

Listing 4.1: The core data structure of the trusted issuer registry smart contract written using Solidity.

[9] https://github.com/digitalcredentials/issuer-registry/blob/main/registry.json last accessed 07.05.2023

As previously mentioned, the solution presented in this thesis is a drop-in replacement for the existing trusted issuer registry by the DCC. To achieve this, the smart contract implementation is abstracted by building a TypeScript library called the EtherIssuerRegistry2022. This library makes the integration of the trusted issuer registry smart contract much easier by abstracting all of the smart contract details. A user of the library only needs to define a configuration for the blockchain node and the address of the smart contract to access the trusted issuer registry information. Furthermore, the library also contains abstractions for administrative actions of the smart contract, which makes the integration of administrative methods of the trusted issuer registry into other tools easier, such as the EthrIssuerRegistryCLI. This CLI tool serves as a reference for the integration of the administrative function of the trusted issuer registry and allows the complete registry to be managed through the CLI. Moreover, the EtherIssuerRegistry2022 library is used by the SignAndVerify service and wallet app to verify the issuer's trustworthiness, as illustrated in Figure 4.1.

### 4.3.5 Credential Status Registry

The credential status registry is another key component of the digital credentialing prototype of this thesis. Its purpose is to provide the issuer with a mechanism for permanently or temporarily invalidating already issued credentials. This is a requirement expressed by the issuers in RQD5 and allows them to fix potential errors made in the already issued credentials. While this is a critical feature for issuers, the DCC's digital credentialing system does not, as of writing in May 2023 have a finished reference implementation for this functionality [DCCa].

Since July 2022, a development branch has been implementing this status-updating mechanism, but the implementation is not finished [DCC22a]. This implementation of the credential status mechanism by the DCC is based on the Verifiable Credential Status List v2021[10] specification. This method of credential status validation adds a new endpoint to the issuing service that responds with the current status of a credential. However, this introduces privacy concerns because it might provide the issuer with information on who is validating the credential, which RQD21 explicitly states should not be the case. To mitigate this concern, the credential status list v2021 aggregates multiple statuses of credentials status into one block. This blurs the indication of which credential the verifier seeks to validate since she or he asks for a complete block of multiple credential statuses, and now the issuer does not know which of these credentials the verifier is interested in. Unfortunately, this solution has other limitations and problems, which are explained within the specification.

The credential status method proposed in this thesis was designed and implemented before the credential status list was developed by the DCC, and it uses a different approach to implement this functionality. The method employed in this thesis uses a smart contract on a blockchain to store the status information of a credential. This naturally solves the

[10] https://w3c.github.io/vc-status-list-2021/ last accessed 12.05.2023

problem of information gathering by the issuer when a credential status is accessed. This is because the blockchain consists of a distributed set of nodes, each of which holds a copy of the credential status data. However, this approach has a different problem to solve, namely that all of the data on the blockchain are publicly available to everyone, and PII within the credential should not be published publicly to preserve the credential holder's privacy, as required by RQD22. The solution proposed for the credential status registry is that it should only hold a hash value of the credential and its corresponding status. This hash value must be designed carefully to preserve the holder's privacy while also resulting in the same hash for the same credential.

This EthrStatusRegistry2022 standard developed within this thesis uses the RDF Dataset Canonicalization[11] to normalise every verifiable credential to a binary format, which then gets hashed by the SHA256[12] hash function. The hashing algorithm allows the creation of a unique deterministic identifier for a credential, as long as the input of the hashing algorithm is the same for the same credential. This is where the normalisation of the credential plays a crucial role. It guarantees that a credential with equal contents but different representations leads to the same binary output, which is then processed as an input for the hash function. Without this normalisation, the credential holder could simply change the credential representation, such as through switching the order of the JSON-LD properties, to circumvent possible revocation actions by the issuer. The normalisation, also called the canonicalisation of the credential, prevents this and always provides the same output for the same credential in various representations.

As mentioned earlier, the credential status registry of this thesis is implemented using a smart contract and uses nested mappings to store the credential status information, as illustrated in Listing 4.2. The outer mapping structure maps the credential's hash, created using the aforementioned methods, to the inner mapping that maps Ethereum account addresses to the potential block number of revocation. If a credential is not revoked by the specified Ethereum account, then 0 is returned.

```
contract StatusRegistry {

    mapping(bytes32 => mapping(address => uint)) private revocations;
    mapping(bytes32 => mapping(address => uint)) private suspensions;

    function revoke(bytes32 digest) public {
        require (revocations[digest][msg.sender] == 0, 'Must not be
            ↪ already revoked');
        revocations[digest][msg.sender] = block.number;
    }
    ...
}
```

Listing 4.2: A snippet of the credential status registry

[11] https://w3c.github.io/rdf-canon/spec/ last accessed 12.05.2023
[12] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf last accessed 12.05.2023

The nested mapping data structure allows for a more flexible and distributed approach to the credential status functions, as anyone can express their own opinion on a credential's status. In most cases, the verifier will check the credential status set by the issuer of the credential, but it would be possible for the verifier to consider statuses set by other entities if desired.

To abstract the implementation details of the credential status registry and ease integration efforts, we also provide a library called EthrStatusRegistry2022. It handles all of the required parsing, normalisation, hashing, and communication with the blockchain node to access a credential's status information. This library is used by all services of the digital credentialing prototype of this thesis that read from or write to the credential status registry.

```
{
   "@context": [...],
   "type": [...],
   "issuer": {...},
   "credentialSubject": {...},
   "credentialStatus": {
      "id": "did:ethr:goerli:
         ↪ 0x28f83eFb018F560e2960CC3df3Fa7B3D7c29eC1a
         ↪ ?i=0x33e94A68B847B6AaF3aF48dAA41F50a27adEE92a",
      "type": "EthrStatusRegistry2022"
   },
   "issuanceDate": "...",
   "proof": {...}
}
```

Listing 4.3: An example of a credential status integration into a verifiable credential using the EthrStatusRegistry2022 standard proposed within this thesis.

In addition, the verifiable credentials data model specification specifies how the different credential status methods should be integrated into the credential itself. Listing 4.3 presents an example integration of the EthrStatusRegistry2022 method of this thesis. Under the `credentialStatus` property, all of the information required to access the credential's status is held, and the sub-property `type` defines which standard is used for the credential status. In the case of the EthrStatusRegistry2022, the only other sub-property is the `id`, which is a DID that points to the credential status registry smart contract, and the Ethereum address defined with the `i` query parameter, which the issuer will use to potentially update the credential's status.

With the implementation of the digital credential completed, the next step is to evaluate the resulting digital credentialing prototype for TU Wien. The next chapter explains how the evaluation is conducted and presents the results from organisational and technical perspectives.

CHAPTER 5

# Evaluation

This chapter presents the evaluation of the prototype digital credential system developed in this thesis and its results, which answer the research questions presented in Section 1.2. First, Section 5.1 provides an explanation of the evaluation methodology and procedure used to evaluate the credentialing prototype. The evaluation results are then presented from two perspectives, namely organisational and technical. Section 5.2 outlines the organisational challenges and considerations expressed by the experts in the evaluation discussion, and then Section 5.3 focuses on the technical evaluation results, providing insights from a technical standpoint. Lastly, Section 5.4 contextualises the results from the technical and organisational discussion to the research questions.

## 5.1 Expert Discussion Setting

To evaluate the credentialing prototype built in this thesis, an expert discussion was chosen as the evaluation method. This discussion aimed to find answers to the research questions from an organisational point of view by the decision-makers at TU Wien as well as to evaluate the technical aspects of the prototype by discussing it with experts of the TU Wien's Campus Software Development Department. The aim was to provide an overall, in-depth look from different perspectives as well as acquire the information required to decide how TU Wien could use and integrate digital credentialing.

The expert discussion was conducted with two experts from the Campus Software Department, which is responsible for the development of the current credentialing system TISS. One expert from the dean's office of business informatics, who was able to provide insights from the decision-maker's perspective, while the others were the supervisor and the author of this master's thesis, who contributed their expertise in digital credentialing in general.

The expert discussion was structured in the following three main parts:

1. **Introduction Presentation (10min)**: The first part was a presentation, which served as a short introduction to the field of digital credentials. It explained the current state of credentials, their problems, and the motivation and aim of this thesis. This was aimed at providing the experts with a rough overview of the thesis and of digital verifiable credentials in general.

2. **Practical Demonstration (15min)**: The second part was a practical demonstration of the credentialing prototype. It presented the feature set offered by clicking through the individual service's UI while explaining the technical processes occurring in the background in a simplified, non-technical manner. This part aimed to practically present the results of the aforementioned theoretical goals and to delve into the thesis's digital credentialing prototype implementation in greater depth.

3. **Open Discussion (65min)**: The third and main part of the evaluation was the actual expert discussion. In this part, the language was switched from English to German as it was easier for the experts to express themselves in German. The discussion was unstructured; only a few bullet points served as a rough guide for the discussion topics.

The discussion was held remotely over Zoom and recorded by the author to enable an effective evaluation of the results of the open discussion. The following section explains the results from an organisational point of view.

## 5.2 Organisational Discussion

From the start, the experts recognised the importance of digital credentialing for TU Wien. Especially in the role of a verifier of credentials, the benefits that digital credentials can bring to TU Wien are clear. TU Wien must often accredit course credentials from other HEIs and faces the problems that current paper credentials often have. One of them is the difficulty of comparing two credentials issued by two different HEIs. It is crucial to determine which skills the students have already acquired by receiving this credential from another HEI, to find the equivalent course offerings at TU Wien, and accredit the credentials accordingly. Currently, this credential comparison and search for equivalent offers by TU Wien are mostly conducted by comparing the titles of the credentials.

The digital credentialing solution of this thesis includes the objectives and teaching contents of a specific course in the digital credential. This added information aims to provide the verifier with as much information about the skills acquired by the holder through receiving this credential. One expert stated that this is one of the most important pieces of information and that it should be included in all credentials. This additional information could be added to any credential independent of the credential medium used, but the same expert also expressed the huge potential he sees in automating accreditation processes, which is only applicable if the credential is represented in a digital machine-readable format. Furthermore, the automation requires a set of well-defined and standardised fields within the credential that can be used to implement the automated accreditation process.

All experts agreed that this standardisation is a key asset of digital credentialing and also one of the most difficult aspects when building a digital credentialing ecosystem. One expert especially outlined the importance of the well-definedness of the standard. Not only should the syntax of the credentials be defined but also the semantics are critical. As this standard should ideally be used globally, and the number of different education systems as well as regional interests and requirements are enormous. Getting everyone involved to agree on a single set of well-defined digital credential properties is very difficult, as an expert in the field of interoperability and standardisation of global systems expressed.

Noteworthily, the integration of a qualification classification framework, such as the European Skills, Competences, Qualifications, and Occupations (ESCO) framework, into digital credentials was a controversial topic. The potential benefits are that the learning outcomes and skills acquired are defined in a standardised schema, which comes with other benefits such as translatability. One expert criticised how such a qualification classification framework can not be sufficiently detailed to depict the skills acquired by, for example, successfully completing a course at TU Wien. One example given by this expert was that the learning outcomes listed on certificates issued by HTLs are quite similar to those of many bachelor courses at TU Wien. For context, an Höhere Technische Lehranstalt (HTL) is a secondary school with a technical focus specific to Austria. The potential consequence could be that graduates of an HTL already have a nearly finished bachelor's degree at TU Wien if accreditation is automated and the automation is based on the skills defined by the qualification framework. This expert also stated that in practice, graduates of HTLs often struggle to complete courses that educate them in the skills they already have according to their HTL certificates. Another expert disagreed and stated that he did not learn many new things at TU Wien after graduating from an HTL. It was also noted that a simple list of acquired skills does not express the skill level and that students who barely pass the course have the same learning outcomes as someone with an excellent grade.

Either way, it was clear from the discussion that the automation of processes is where the disagreement originates. The inclusion of as much information as possible, ideally in a standardised and well-defined schema, was agreed upon by every expert. Only when it came to automating the accreditation processes, did the experts have different opinions; however, it was clear that such automation must be designed carefully and consider all possible consequences.

Another area where digital credentials improve on paper-based credentials is verifiability and security. Digital credentials are cryptographically signed, which makes them more secure against manipulation. The experts agreed that current paper-based credentials are easy to fake and counterfeit. In particular, credentials issued in a location far away are very difficult to verify, as the person verifying the credential might not even understand the language or signatures written on it. Moreover, the verification of paper credentials might also involve contacting the alleged issuer and asking for verification of whether the credential was issued by them. With the digital credentials prototype of this thesis, these problems are addressed. The complete verification process is more secure, less error-prone, and more automated. One expert mentioned the possible resistance to digitising the credentials and verification process from the current TU Wien study department. He expected the haptics of a paper credential to give the credential a feeling of being more real than a digital credential, which might be displayed only as a QR code on a phone.

Furthermore, the verification of credentials in practice might be handled differently than expected by the design of the digital credentialing system, which might lead to new attack methods to submit invalid credentials. For example, if someone wants to verify that the person in front of them has some credentials, such as a bachelor's degree credential, and the person takes out their phone, opens the alleged bachelor's degree credential in the wallet app, and shows it to the verifier. The verifier might just look at the phone's screen, check that all of the required data are on there and accept the properties of the credential. However, this way, the critical verification step on the verifier's behalf would be skipped. The verifier cannot trust the integrated verification checks of the holder's wallet. The verifier must request the digital credential from the person, verify the contents with their verification software, and never trust the data displayed on a foreign device.

This highlights the fact that replacing paper credentials with digital credentials also requires changes to the processes and workflows using credentials. By digitising the credential, new use cases open up and allow a more effective integration into other digital workflows. TU Wien is already planning to digitise the internal workflows for credential accreditation. Digital accreditation workflows are especially prominent in the backlog of the TU Wiens Software Department. An expert working on these topics mentioned the potential helpfulness of this thesis when it comes to designing internal workflows and allowing them to more effectively plan for the potential change to digital credentials in the future. Another expert added that it is clear that, sooner or later HEIs will be required by law to issue some form of digital credentials and that TU Wien must be prepared as well as able to recognise when digital credentials are mature enough to integrate them into TISS.

Moreover, a decision maker at TU Wien was sure that digital credentials will only be implemented by universities when they are forced to by law, as is often the case with public administrative administration, and he advises active participation in pilot programs. This will allow TU Wien to possibly influence digital credential standards at an early stage of development and obtain better insights into the current development. Complementary to this, another expert noted that he thinks that Austrian universities should work together to build a digital credentialing system, and he suggested that perhaps such a digital credential issuing service could also be hosted centrally for all Austrian HEIs. However, as stated by another expert the implementation effort is expected to be minimal; therefore, a centralised solution might not be advantageous.

Overall, the experts viewed digital credentials as strategically important for TU Wien and saw many benefits over paper credentials, even though the standardisation process with so many entities is cumbersome.

## 5.3 Technical Discussion

The first discussion point from a technical perspective was the required efforts and challenges that TU Wien would face if a digital credentialing system – such as the prototype of this thesis – was to be integrated into the existing TISS infrastructure. An expert from the campus development team believed that the integration effort is comparable to the integration of the *Grüner Pass* verification during the COVID-19 pandemic. The main functionalities that TISS would have to include are credential data transformation and transmission to a credential issuing library and the integration of a credential verification user interface. Depending on the requirement details, especially for the integrated verifier, the efforts required could vary. This assumes that libraries are available and mature enough to abstract all digital credentials implementation details and expose a well-defined application interface.

In practice, digital credentialing standards are currently evolving rapidly, and new versions with drastic changes appear regularly. This leads to a very short life cycle for credential libraries as they become quickly deprecated and require substantial changes to stay compatible with the newest credential standards. Furthermore, the digital credentials data model by the W3C focuses on openness and extendibility, which increases the number of possible implementations of specific credential parts. This variety of specifications and standards makes developing digital credentialing libraries difficult and, as one expert noted, interoperability is critical for the success of digital credentialing in general. This is not only important for the software parts that TU Wien would use but also for the credential wallet used by its students. People do not want to install a specific app for each use case. This is where the wallet app of this thesis falls short; it only supports credentials from the issuing service developed in this thesis.

One expert wanted to know if it would be possible to issue digital credentials from the past. Technically, nothing prevents the issuance of new digital versions of old paper credentials issued years ago. Legally, credentials issued by TU Wien must be stored for 80 years and include information about the title of the assessment, assigned ECTS points, grading, name of the examiner, date of the assessment, name, and matriculation number of the student, according to the Austrian university law § 53[1]. Furthermore, issuing digital versions of old credentials supports the goal and vision of life-long learning expressed by the EC [Com20b]. The experts agreed that this could be an interesting use case and would have to be reconsidered when TU Wien starts issuing digital credentials.

This digital credentialing re-issuance process and other credential handling processes, such as accreditation, can be automated if everything required is digital, which includes

[1] https://www.ris.bka.gv.at/eli/bgbl/i/2002/120/P53/NOR40232338 last accessed 27.07.2023

the credential itself. Automation is a key aspect of digital credentials in general. It allows the credentials to be automatically issued and validated, which according to the experts is a significant benefit over paper credentials. They were also sure that even though digital credentials allow for many new use cases, the automated handling of credentials introduces new risks, such as new attack vectors for fraud. For example, one expert feared that credential mills might get approved by automated accreditation processes, while currently the issuer of a credential gets checked manually by the study department. To prevent approving credentials of untrusted issuers, the verification system must be configured carefully. For the implementation of this thesis, it is crucial to use a trusted issuer registry that is maintained by an entity that TU Wien fully trusts and endorses.

Establishing trust in digital credentials is crucial for their success and widespread use. A critical aspect of this trust is the ability to reliably verify a digital credential and to be sure that it is genuine and fulfils the trust requirements (Subsection 3.1.3). To achieve these requirements, the digital credentialing prototype uses various methods, which are detailed as follows:

First, a digital credential should be immutable and any modifications made to it should lead to its invalidation. This is achieved by the digital signature of the issuer. The experts agreed that this method is secure and a great improvement over paper-based credentials.

Second, the credential should prove that it was issued by a trusted entity. The digital credentialing system provides a method for asserting whether a specific entity has issued a credential. Whether this issuer can be trusted depends on the verifier's definition of trust. One expert stated that technical implementations can only solve the problem of who has signed the credential but will never be able to build trust that the issuer is also a real and trusted entity. The trusted issuer registry proposed in this thesis is a digital replacement for the already existing analogue list of all trusted HEIs that the study department of TU Wien currently uses to verify whether an issuer is trusted. The digital implementation of this thesis has the advantage that it allows the outsourcing of the maintenance of this list if desired. For example, TU Wien could decide that it trusts the EC to manage its trusted issuer registry.

Third, the digital credentials issued by the prototype of this thesis can be invalidated after they have been issued. The credential status can be updated on the fly by the issuer or other entities to, for example, fix a mistake in the credential or revoke a credential that was signed by a signing key that was compromised. One expert believed that this feature cloud be useful for lecturers to temporarily suspend credentials.

Next, with the technical and organisational discussion finished, Section 5.4 puts the results into the context of the research questions.

## 5.4 Results vs. Research Questions

The results of the organisational and technical expert discussion evaluation have outlined three main challenges that TU Wien would face by integrating a digital credentialing system, such as the system designed by the DCC into the current TISS infrastructure(RQ1).

1. **Infrastructure**: The digital credentialing service is packaged as a separate service that runs alongside the original TISS. This means that the TISS infrastructure must be adapted to execute this newly introduced digital credentialing service and be configured securely so that only services that should be able to access it can do so. Furthermore, this introduces additional maintenance costs to keep all services up and running continuously.

2. **Data Transformation**: Even though the digital credentialing service handles all of the credential creation and verification functionalities, TISS must communicate with the service over a predefined interface. This requires a translation layer between TISS and the digital credentialing service. Within this layer, the credentialing data stored in TISS are mapped to the data model required by the digital credentialing service.

3. **User Interface**: The addition of digital credentials to TISS requires new user interface elements that will allow end users to interact with the newly added functionalities. These include interface options for administrative personnel as well as students. For example, lecturers need a way to update a credential's status, and students need a way to request a digital credential.

Moreover, the evaluation results indicated that blockchain technologies are a popular choice for trust-contributing parts of a digital credentialing solution. Blockchains provide an immutable, transparent, traceable, and decentralised data storage method that can be used for many different purposes within a credentialing system. These properties can be provided by blockchains and can be important for building trust in the system. For example, a credentialing system that uses a blockchain to store the current status of a credential, such as the credentialing prototype of this thesis, will always be able to verify a credential's status even if the issuer no longer exists. Other implementations, such as the Verifiable Credentials Status List v2021[2] by the W3C, which do not use blockchain technologies and instead request the issuer of the credential for its current state are not capable of retrieving the status of a credential when the issuer is not responding. Depending on the requirements and desired behaviour, this might not be a problem.

In general, blockchain technologies can provide properties that other implementations can often not provide; however, these properties are not always required. Implementations without blockchains might still be capable of fulfilling all requirements, while not being reliant on a blockchain for its functionality. On the other hand, when traceability,

[2] https://www.w3.org/TR/vc-status-list/ last accessed 01.08.2023

transparency, and especially decentralisation are crucial aspects, blockchains are a good solution for storing credentialing metadata, and these properties are critical when it comes to building trust in sensitive parts of a digital credentialing system (RQ2).

Moreover, the evaluation discussion highlighted that the digital credentialing solution of this thesis is just another representation method of the currently issued analogue paper credentials and digital PDF credentials. Thus, it faces the same challenges that the current credentialing solution faces but provides digital solutions to them. These solutions are tightly integrated into the digital credentialing system to automate many processes that are currently manual, which reduces overhead and streamlines the handling of credentials. This means that substituting the current credentialing system with the digital credentialing system created in this thesis will not directly lead to drastic changes to workflows (RQ3). It makes credentials completely digital and machine-readable, which allows many automation processes, but the automation can be implemented independently of the introduction of digital credentials. Digital credentialing is only the enabler of many new use cases through the digitalisation of currently analogue documents. However, we advise adapting the workflows to fully benefit from digital credentials by considering the new possibilities that digital credentials bring.

Furthermore, the digital credentialing prototype of this thesis has various advantages and disadvantages over the credentials currently issued by TU Wien (RQ4). First, by digitising credentials, new use cases can be implemented that would not be possible with paper-based credentials. For example, the digital credentials issued by the prototype can be invalidated after issuance by the issuer or any other accredited entity. Furthermore, digital credentials are machine-readable, which allows their automated verification as well as the improved automation of credentialing processes in general. These automations can reduce the administrative overhead that paper credentials have. Moreover, digital credentials are more tamper-resistant than paper credentials, which reduces the risk of fraud. Additionally, they improve the privacy of credential holders by considering privacy throughout the design process. For example, unlike a paper credential, the verification of a digital credential does not involve the issuer.

On the other hand, digital credentials will introduce more technical complexity to TISS. The software components and services used require careful maintenance to keep everything up and running. Furthermore, the digital credentialing software handles sensitive PII, which must be protected, and security updates are very critical. Additionally, TU Wien must maintain cryptographic keys that are used to sign the credentials. These keys must also be secured safely, as a compromised key could be used to issue fake credentials, which would require the invalidation of all credentials issued with that key. It must be noted that the TISS infrastructure already manages critical data, such as PII or cryptographic keys used for signatures. The digital credentialing prototype would only extend these reliabilities to the prototype's software components.

Another disadvantage of the digital credentialing solution of this thesis compared with the currently issued credentials is the very low adoption rate within the field. Currently, only a few pilot universities worldwide issue digital credentials using the verifiable credentials standard by the W3C. Most issuing and verifying institutions do not already have the digital infrastructure to issue or validate these credentials; therefore, these credentials are useless to their holders. A report titled *’The Last Mile’* by Camilleri et al., published by the DCC, also revealed a set of problems that hinder the adoption of digital credentials [Cam22]. Most notable verifying institutions, mainly employers, depended on their HRMS to accept digital credentials and these systems have not integrated digital credentials because of the small number of issuers issuing them. Thus, digital credentials will take time to gain widespread acceptance and recognition.

Next, in the final chapter, a summary and outlook are provided of digital credentialing in general and more specifically of the prototype.

# CHAPTER 6

# Conclusion

## 6.1 Summary

The main objective of this thesis was to build a digital credentialing prototype based on the implementations published by the DCC to demonstrate and evaluate its potential use cases for HEIs such as TU Wien. The digital credentialing prototype was required to have stronger security, easier exchangeability, and better privacy compared with the paper-based credentialing solutions that are currently commonly used.

First, we started by examining the current state of digital credentialing solutions and related research areas, such as digital identity and blockchain technologies. The current state of the art, related research, and an introduction to the fundamental concepts required to understand this thesis were described in Chapter 2.

In Chapter 3, with the literature review's results and desired goals in mind, we continued by defining the functional and non-functional requirements of the digital credentialing prototype. The functional requirements defined the features desired by the different actors (i.e., issuer, holder, verifier), while the non-functional requirements described the security, privacy, and interoperability goals set by this thesis.

These requirements demonstrated the lack of functionalities of the implementations by the DCC, which served as the foundation for the digital credentialing prototype of this thesis. Therefore, we introduced two new services into the digital credentialing system, namely the trusted issuer registry and the credential status registry. In Chapter 4, we documented the reasoning for the selected technologies and architectural design as well as explained and illustrated the inner workings of each service that together formed the digital credentialing prototype of this thesis.

After the implementation, we evaluated the prototype with an expert discussion, which was presented in Chapter 5. The results were split into two main categories. One category examined the prototype from a technical point of view and discussed the technical challenges of the prototype, while the other category examined the prototype from an organisational point of view. The evaluation revealed that the prototype of this thesis has great potential in use cases for HEIs such as TU Wien, but lacks maturity due to various factors. Digital credentials can, for example, improve tamper resistance and privacy and enable the automation of currently labour-intensive tasks. However, they are held back by the lack of mature well-defined standards and reference implementations, along with the limited adoption by entities engaging in the credentialing ecosystem.

## 6.2 Future Work

The prototype of this thesis demonstrated some of the potential improvements that digital credentials have over paper-based credentials; however, further improvements are possible. Our implementation focused on demonstrating the possibilities of digital credentialing and was heavily influenced by the underlying implementation published by the DCC. To improve the digital credentialing prototype, further research into the following three areas is required:

**Enhancing Digital Identity**: We used a simple and non-legally binding form of digital identity for the digital credentials issued by the prototype. To switch to a national electronic identification framework, further research into the implementation efforts, benefits, and risks is required.

**Integrating Zero-Knowledge Proofs**: Another area for improvement is privacy. If ZKPs are integrated into digital credentials, holders should be able to selectively disclose partial data of a digital credential without compromising verifiability, and also to create proofs for specific properties of a digital credential [CGSB20]. It would be interesting to see whether and how ZKPs can be integrated into a digital credentialing solution such as the prototype of this thesis.

**Broadening Perspectives**: The prototype of this thesis was built from an HEI perspective. Therefore, the expert evaluation mainly discussed verifiers from the perspective of HEIs as a verifier, which does not represent other verifiers such as employers. Therefore, we advise further research into digital credentialing implementations from the perspective of other actors within the credentialing field to satisfy the requirements of all actors and improve the adoption of digital credentials in general.

In closing, the goal of advancing digital credentialing remains an evolving and collaborative effort. The exploration of these domains will shape the future of credentialing systems in search of increased efficiency and privacy in the digital age.

# List of Figures

# List of Listings

# Acronyms

**CLI** command-line interface. 38, 49

**CLR** Comprehensive Learner Record. 22

**DApp** decentralised application. 14, 15

**DCC** Digital Credentials Consortium. xi, 3, 18, 21–23, 25, 30, 31, 33–37, 39, 42, 44, 48, 49, 59, 61, 63, 64

**DID** decentralised identifier. 9–11, 20, 30, 35, 51, 65, 67

**EBP** European Blockchain Partnership. 20

**EBSI** European Blockchain Services Infrastructure. 14, 19–21, 25, 31, 47

**EC** European Commission. 18–20, 57, 58

**EDCI** European Digital Credentials Infrastructure. 18, 19

**eID** electronic identification. 20

**eIDAS** electronic identification and trust services. 20

**EQF** European Qualifications Framework. 22

**ESCO** European Skills, Competences, Qualifications, and Occupations. 55

**eSSIF** European self-sovereign identity framework. 20

**EVM** Ethereum virtual machine. 15, 36

**GDPR** General Data Protection Regulation. 21, 27

**HEI** higher education institution. xi, 1–4, 15, 18, 21, 25, 54, 56, 58, 63, 64

**HIPAA** Health Insurance Portability and Accountability Act. 27

**HRMS** human resources management system. 38, 61

**HTL** Höhere Technische Lehranstalt. 55

**HTTP** Hypertext Transfer Protocol. 34, 36

**HTTPS** Hypertext Transfer Protocol Secure. 34, 36

**IdP** identity provider. 7, 8

**JSON-LD** JavaScript Object Notation for Linked Data. 10, 30, 35, 44, 45, 50

**LCW** Learner Credential Wallet. 37, 44

**LER** Learning and Employment Record. 22

**MOOC** massive open online course. 15

**OID4VCI** OpenID for Verifiable Credential Issuance. 31, 40

**OID4VP** OpenID for Verifiable Presentations. 31

**PII** personally identifiable information. 27, 50, 60

**PoA** Proof of Authority. 13, 14

**PoC** proof-of-concept. 3, 4

**PoS** Proof of Stake. 13, 14

**PoW** Proof of Work. 13, 14

**SSI** self-sovereign identity. 5, 8, 9, 11, 20

**SSO** single sign-on. 7

**TISS** TU Wien Informations-Systeme & Services. 3, 4, 36, 37, 53, 56, 57, 59, 60

**URI** universal resource identifier. 9, 10, 41

**W3C** World Wide Web Consortium. ix, xi, 9, 10, 15, 19–21, 25, 30, 31, 35, 57, 59, 61

**ZKP** zero-knowledge proof. 28, 64

# Bibliography

[AAKWK21] Joseph Amankwah-Amoah, Zaheer Khan, Geoffrey Wood, and Gary Knight. COVID-19 and digitalization: The great acceleration. *Journal of Business Research*, 136:602–611, November 2021. URL: https://www.sciencedirect.com/science/article/pii/S0148296321005725, doi:10.1016/j.jbusres.2021.08.011.

[AAU+23] Hada A. Alsobhi, Rayed A. Alakhtar, Ayesha Ubaid, Omar K. Hussain, and Farookh Khadeer Hussain. Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review. *Knowledge-Based Systems*, 265:110238, April 2023. URL: https://www.sciencedirect.com/science/article/pii/S095070512201334X, doi:10.1016/j.knosys.2022.110238.

[All16] Christopher Allen. The Path to Self-Sovereign Identity, April 2016. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html.

[And19] Jeremie Anderlin. New Europass, February 2019. URL: https://ec.europa.eu/futurium/en/europass/new-europass.

[Baz23] Digital Bazaar. did:key method resolver, April 2023. URL: https://github.com/digitalbazaar/did-method-key.

[Bur20] Oscar Burgos. SSI eIDAS Legal Report, April 2020. URL: https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-legal-report.

[Cam22] Anthony F Camilleri. Digital Credentials Consortium Credentials to Employment: The Last Mile. September 2022. URL: https://digitalcredentials.mit.edu/docs/Credentials-to-Employment-The-Last-Mile.pdf.

[CCR22] CCRI. The Merge - Implications on the Electricity Consumption and Carbon Footprint of the Ethereum Network, September 2022. URL: https://carbon-ratings.com/eth-report-2022.

[CGSB20] Melissa Chase, Esha Ghosh, Srinath Setty, and Daniel Buchner. Zero-knowledge credentials with deferred revocation checks. February 2020. URL: https://github.com/decentralized-identity/snark-credentials/blob/master/whitepaper.pdf.

[Com20a] European Commission. A European Approach to Micro-credentials. Final Report. Output of the Micro-credentials Higher Education Consultation Group, December 2020.

[Com20b] European Commission. European Skills Agenda for sustainable competitiveness, social fairness and resilience, 2020. URL: https://ec.europa.eu/social/BlobServlet?docId=22827&langId=en.

[Com21a] European Commission. EBSI Architecture, explained, October 2021. URL: https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/447687044/%28210610%29%28EBSI_Architecture_Explained%29%28v1.02%29.pdf.

[Com21b] European Commission. Europass Digital Credentials Infrastructure (EDCI), 2021. URL: https://ec.europa.eu/futurium/en/system/files/ged/edci_presentation.pdf.

[Com22a] European Commission. EBSI Verifiable Credentials explained chapter 2: Verifiable Credentials in action, June 2022. URL: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/EBSI+Verifiable+Credentials.

[Com22b] European Commission. SSI eIDAS Bridge, February 2022. URL: https://joinup.ec.europa.eu/collection/ssi-eidas-bridge.

[Com23] European Commission. Issuers trust model - Accreditation of Issuers, 2023. URL: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Issuers+trust+model+-+Accreditation+of+Issuers.

[Dan17] Chris Dannen. Solidity Programming. In Chris Dannen, editor, *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*, pages 69–88. Apress, Berkeley, CA, 2017. doi:10.1007/978-1-4842-2535-6_4.

[DCCa] Digital Credentials Consortium DCC. Digital Credentials Consortium GitHub Repositories. URL: https://github.com/digitalcredentials.

[DCCb] Digital Credentials Consortium DCC. Digital Credentials Consortium Website. URL: https://digitalcredentials.mit.edu/.

[DCC20] Digital Credentials Consortium DCC. Digital Credentials Consortium Whitepaper, February 2020. URL: https://digitalcredentials.mit.edu/docs/white-paper-building-digital-credential-infrastructure-future.pdf.

[DCC22a] Digital Credentials Consortium DCC. Digital Credentials Consortium - Credential status management - GitHub Issue, July 2022. URL: https://github.com/digitalcredentials/sign-and-verify/pull/55.

[DCC22b] Digital Credentials Consortium DCC. Digital Credentials Consortium Final Report, March 2022. URL: https://digitalcredentials.mit.edu/docs/Open%20Source%20Student%20Wallet%20Final%20Report%20-%20Public%20Web%20Version.pdf.

[DDJM16] Sonja Dimitrijević, Vladan Devedzić, Jelena Jovanović, and Nikola Milikić. Badging Platforms: A Scenario-Based Comparison of Features and Uses. In Dirk Ifenthaler, Nicole Bellin-Mularski, and Dana-Kristin Mah, editors, *Foundation of Digital Badges and Micro-Credentials: Demonstrating and Recognizing Knowledge and Competencies*, pages 141–161. Springer International Publishing, Cham, 2016. doi:10.1007/978-3-319-15425-1_8.

[Eth] Ethereum. Development Documentation: Proof-of-stake (PoS). URL: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[EU] European Union EU. European Digital Credentials for Learning. URL: https://europa.eu/europass/en/europass-tools/digital-credentials.

[Eur16] Eurostat. Almost 8 out of 10 internet users in the EU surfed via a smartphone, December 2016. URL: https://ec.europa.eu/eurostat/documents/2995521/7771139/9-20122016-BP-EN.pdf.

[fAFC] Cambridge Centre for Alternative Finance CCAF. Cambridge Bitcoin Electricity Consumption Index (CBECI). URL: https://ccaf.io/cbeci/index.

[FKS15] Daniel Fett, Ralf Küsters, and Guido Schmitz. SPRESSO: A Secure, Privacy-Respecting Single Sign-On System for the Web. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, pages 1358–1369, New York, NY, USA, 2015. Association for Computing Machinery. doi:10.1145/2810103.2813726.

[Fou22] Ethereum Foundation. Ropsten, Rinkeby & Kiln Deprecation Announcement, June 2022. URL: https://blog.ethereum.org/2022/06/21/testnet-deprecation.

[Fou23] Decentralized Identity Foundation. did:web method resolver, February 2023. URL: https://github.com/decentralized-identity/web-did-resolver.

[ge] go.eIDAS e.V. eIDAS. URL: https://www.eid.as.

[Gil04] Audrey Gillan. A few clicks of the mouse, and you become a doctor. *The Guardian*, July 2004. URL: https://www.theguardian.com/uk/2004/jul/05/elearning.politics.

[GLM08] Gilles Grolleau, Lakhal, and Naoufel Mzoughi. An Introduction to the Economics of Fake Degrees. *Journal of Economic Issues*, 42:673–693, September 2008. doi:10.1080/00213624.2008.11507173.

[Glo18] IMS Global. Open Badges Specification v2.0, April 2018. URL: https://www.imsglobal.org/sites/default/files/Badges/OBv2p0Final/index.html.

[Glo23] IMS Global. Open Badges Specification v3.0, February 2023. URL: https://www.imsglobal.org/spec/ob/v3p0/.

[Hal20] Harry Halpin. Vision: A Critique of Immunity Passports and W3C Decentralized Identifiers. In Thyla van der Merwe, Chris Mitchell, and Maryam Mehrnezhad, editors, *Security Standardisation Research*, Lecture Notes in Computer Science, pages 148–168, Cham, 2020. Springer International Publishing. doi:10.1007/978-3-030-64357-7_7.

[Jen11] Jostein Jensen. Benefits of Federated Identity Management - A Survey from an Integrated Operations Viewpoint. In A. Min Tjoa, Gerald Quirchmayr, Ilsun You, and Lida Xu, editors, *Availability, Reliability and Security for Business, Enterprise and Health Information Systems*, Lecture Notes in Computer Science, pages 1–12, Berlin, Heidelberg, 2011. Springer. doi:10.1007/978-3-642-23300-5_1.

[Jen12] Jostein Jensen. Federated Identity Management Challenges. In *2012 Seventh International Conference on Availability, Reliability and Security*, pages 230–235, August 2012. doi:10.1109/ARES.2012.68.

[JFH$^{+}$05] Audun Jøsang, John Fabre, Brian Hay, James Dalziel, and Simon Pope. Trust requirements in identity management. *AusGrid 2005, AISW 2005*, 44:99–108, 2005. URL: http://www.scopus.com/inward/record.url?scp=54849408511&partnerID=8YFLogxK.

[JP05] A. Jøsang and Simon Pope. User Centric Identity Management. 2005. URL: https://api.semanticscholar.org/CorpusID:30347622.

[KHP22] Padmasheela Kiiskila, Ahmed Hanafy, and Henri Pirkkalainen. *Features of Micro-credential Platforms in Higher Education*. January 2022. Pages: 91. doi:10.5220/0011030600003182.

[K9] Sinan Küfeoğlu and Mahmut Özkuran. Bitcoin mining: A global review of energy and power demand. *Energy Research & Social Science*, 58:101273, December 2019. doi:10.1016/j.erss.2019.101273.

[LHL15] Chak Man Li, Pili Hu, and Wing Cheong Lau. AuthPaper: Protecting paper-based documents and credentials using Authenticated 2D barcodes. In *2015 IEEE International Conference on Communications (ICC)*, pages 7400–7406, June 2015. ISSN: 1938-1883. doi:10.1109/ICC.2015.7249509.

[LM21] Bahareh Lashkari and Petr Musilek. A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access*, 9:43620–43652, 2021. Conference Name: IEEE Access. doi:10.1109/ACCESS.2021.3065880.

[MKT05] Paul Madsen, Yuzo Koga, and Kenji Takahashi. Federated identity management for protecting users from ID theft. In *Proceedings of the 2005 workshop on Digital identity management*, DIM '05, pages 77–83, New York, NY, USA, November 2005. Association for Computing Machinery. doi:10.1145/1102486.1102500.

[MMT22] Manuel Adelin Manolache, Sergiu Manolache, and Nicolae Tapus. Decision Making using the Blockchain Proof of Authority Consensus. *Procedia Computer Science*, 199:580–588, January 2022. URL: https://www.sciencedirect.com/science/article/pii/S1877050922000710, doi:10.1016/j.procs.2022.01.071.

[MPJ18] Bhabendu Kumar Mohanta, Soumyashree S Panda, and Debasish Jena. An Overview of Smart Contract and Use Cases in Blockchain Technology. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–4, July 2018. doi:10.1109/ICCCNT.2018.8494045.

[MvBS15] Barbora Micenková, Joost van Beusekom, and Faisal Shafait. Stamp Verification for Automated Document Authentication. In Utpal Garain and Faisal Shafait, editors, *Computational Forensics*, Lecture Notes in Computer Science, pages 117–129, Cham, 2015. Springer International Publishing. doi:10.1007/978-3-319-20125-2_11.

[Nak08] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. January 2008. URL: `https://bitcoin.org/bitcoin.pdf`.

[NBF$^+$16] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, USA, 2016.

[PBSJ19] Claus Pahl, Antonio Brogi, Jacopo Soldani, and Pooyan Jamshidi. Cloud Container Technologies: A State-of-the-Art Review. *IEEE Transactions on Cloud Computing*, 7(3):677–692, July 2019. Conference Name: IEEE Transactions on Cloud Computing. `doi:10.1109/TCC.2017.2702586`.

[PG19] Haris Poll and Google. The United States of P@ssw0rd$, October 2019. URL: `https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf`.

[PR20] Altmann Peter and Erik Rissanen. *Self-Sovereign Digital Identity on the European Blockchain Services Infrastructure*. September 2020. `doi:10.13140/RG.2.2.30892.49281`.

[SAA] Steffen Schwalm, Daria Albrecht, and Ignacio Alamillo. eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI. `doi:https://doi.org/10.18420/OID2022_05`.

[SJZG19] Alan T. Sherman, Farid Javani, Haibin Zhang, and Enis Golaszewski. On the Origins and Variations of Blockchain Technologies. *IEEE Security & Privacy*, 17(1):72–77, January 2019. Conference Name: IEEE Security & Privacy. `doi:10.1109/MSEC.2019.2893730`.

[SSRF21] Johannes Sedlmeir, Reilly Smethurst, Alexander Rieger, and Gilbert Fridgen. Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*, 63(5):603–613, October 2021. `doi:10.1007/s12599-021-00722-y`.

[Szc18] Marcin Szczepański. European app economy, May 2018. URL: `https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2018)621894`.

[TAP19] Kalman C. Toth and Alan Anderson-Priddy. Self-Sovereign Digital Identity: A Paradigm Shift for Identity. *IEEE Security & Privacy*, 17(3):17–27, May 2019. Conference Name: IEEE Security & Privacy. `doi:10.1109/MSEC.2018.2888782`.

[TGT$^+$23] Giedre Tamoliune, Rasa Greenspon, Margarita Tereseviciene, Airina Volungeviciene, Elena Trepule, and Estela Dauksiene. Exploring the potential of micro-credentials: A systematic literature review. *Frontiers in Education*, 7, 2023. URL: `https://www.frontiersin.org/articles/10.3389/feduc.2022.1006811`.

[TRW17] Andrew Tobin, Drummond Reed, and Phillip Windley. Inevitable Rise of Self-Sovereign Identity. Technical report, Sovrin Foundation, March 2017. URL: `https://sovrin.org/library/inevitable-rise-of-self-sovereign-identity/`.

[W3C19] W3C. Verifiable Credentials Use Cases, September 2019. URL: `https://www.w3.org/TR/vc-use-cases/`.

[W3C22a] W3C. Decentralized Identifiers (DIDs) v1.0, July 2022. URL: `https://www.w3.org/TR/did-core/`.

[W3C22b] W3C. Verifiable Credentials Data Model v1.1, March 2022. URL: `https://www.w3.org/TR/vc-data-model/`.

[W3C23] W3C. Verifiable Credentials API v0.3, March 2023. URL: `https://w3c-ccg.github.io/vc-api/`.

[WGP21] Elena Wolz, Matthias Gottlieb, and Hans Pongratz. Digital Credentials in Higher Education Institutions: A Literature Review. In Frederik Ahlemann, Reinhard Schütte, and Stefan Stieglitz, editors, *Innovation Through Information Systems*, pages 125–140, Cham, 2021. Springer International Publishing. `doi:10.1007/978-3-030-86800-0_9`.

[Woo22] Dr Gavin Wood. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. October 2022. URL: `https://gavwood.com/paper.pdf`.