A Cardano Blockchain Prototype for Migrant Data Security and Cultural Heritage Preservation

A thesis

submitted in fulfilment

of the requirements for the degree

of

Master of Science (Research) in Computer Science

at

The University of Waikato

by

VIKNESWARAN RENGASAMY RAJAMANIKKAM

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

2026

Abstract

This thesis investigates the challenges faced by migrants in managing and sharing personal data during migration processes, as well as the potential privacy, security, and data sovereignty risks that may arise from poor data management practices or malicious actors. It further examines the difficulties migrants face in preserving their cultural heritage within their host countries.

Migrants are often required to disclose extensive personal and sensitive information to immigration authorities and associated organisations, which raises significant concerns regarding data privacy, data security, and data sovereignty. These issues may result in adverse outcomes, including misuse of data, loss of control over personal information, and the loss of cultural identity. To better understand these challenges, a study was conducted with twenty migrants to explore their experiences with documentation procedures, their awareness of potential privacy risks, and their perspectives on safeguarding cultural heritage information.

Based on insights from existing literature and the findings of the study, this thesis proposes a Self-Sovereign Identity (SSI) and Verifiable Credentials (VC) based system that enables paperless and secure data sharing and management in a decentralised manner among stakeholders involved in the migration process. The proposed solution also includes a mechanism that allows migrants to securely store information related to their cultural heritage using a decentralised approach and independently issue Verifiable Credentials. The system utilises the Cardano blockchain, Hyperledger Identus, and the InterPlanetary File System (IPFS) to ensure decentralisation, privacy protection, data security, data sovereignty, and data integrity. A prototype was developed to demonstrate the feasibility of the approach and was informally evaluated by a small group of migrant users to assess the usability and acceptance of the proposed system.

Acknowledgements

I would like to thank my supervisor, Professor Steve Reeves, for his guidance and support throughout my research and my time at the university.

I would also like to thank my family for the support they provided, especially my mother, sister, and late father, who always encouraged me to pursue academics, regardless of circumstances.

Contents

Chapter 1

Introduction and Background

1.1 Introduction

Migration has been a fundamental aspect of human survival and expansion since ancient times. According to studies, anatomically modern humans first appeared in Africa around 260,000–350,000 years ago and later migrated to other parts of the world [1]. Throughout history, various groups of people have migrated from one region to another at different points in time, often in search of favourable places to live or to escape danger in their current locations. The importance of migration is further emphasised by the fact that it is not restricted to humans but is also observed in many other species on the planet and can be considered an integral and universal process in the natural world. Today, migration continues for similar reasons, reflecting its lasting importance in human development.

According to the *World Report 2024* by the International Organization for Migration (IOM), a UN agency responsible for promoting humane and orderly migration, the UN currently estimates that around 281 million people live in foreign countries as migrants, which equals 3.6% of the world's population [2]. This figure is about five times higher than five decades ago, emphasising both the scale and rapid growth of international migration. In the present era, the fundamental reasons for migration have not changed significantly. Many people continue to migrate to escape threats such as wars and natural disasters, often as refugees. The UNHCR (United Nations Refugee Agency) estimates that approximately 117.3 million people worldwide were forcibly displaced due to persecution, violence, human rights violations, and

other events that threaten public order [3]. Furthermore, a substantial proportion of people migrate for work. According to estimates from the World Migration Report 2024, there were 169 million migrant workers globally in 2019.

The 2024 International Labour Organization's (ILO) report, *ILO Global Estimates of International Migrant Workers*, indicates that in 2022 there were 284.5 million international migrants worldwide, of whom 255.7 million were of working age. The number of international migrants participating in the labour force was estimated at 167.7 million, representing an increase of 3.1 million from the 2019 estimate of 164.6 million [4]. Migration thus plays a significant role in the global economy, contributing to the generation of wealth and the functioning of labour markets.

Another group of migrants, who may not be as numerous as workers but are still significant, are international students. According to the Global Migration Data Portal, there were 6.9 million international students globally in 2022 [5]. Furthermore, from 1998 to 2022, the number of international students has been steadily increasing, with only a slight decrease during the COVID period. International student migrants contribute not only to the educational and cultural environment of their host countries but also play a vital role in the exchange and distribution of knowledge and technology across borders. As Wang [6] notes, international student returnees enhance research capacity and facilitate knowledge transfer, thereby promoting academic and technological development in both their host and home countries.

1.2 Importance of migrant data security

Article 12 of the United Nations Universal Declaration of Human Rights states:

"No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." [7]

Although the UN human rights declaration does not directly speak about data security, it emphasises the importance of privacy. When we say privacy, it does not necessarily involve privacy in the physical space, but could also include data. Any harm, disadvantage, or difficulty an individual or a group may suffer due to the lack of privacy can often be experienced directly or

indirectly due to a lack of security of their private data as well. The breach of privacy occurs when personal information reaches those who are not supposed to know it.

For example, consider a student living in a dorm with thin walls who discusses a new project idea with a trusted friend, only to have a neighbour overhear and steal the idea. A similar scenario could happen if that student saves their data online in an unsecured storage space, making it vulnerable to theft.

In the information age, where data, including personal and sensitive information, is stored online and across geographical boundaries, data security plays a vital role in safeguarding the privacy of data owners. Depending on their circumstances and the nature of the data, inadequate security could also impact their physical safety, emotional well-being, and financial stability.

When it comes to groups such as migrants, a lot of their personal and sensitive data is stored by authorities, migration-related organisations, as well as third-party entities such as immigration consultants, whose services are sought after by migrants due to the complex nature of certain types of migration. Sensitive data refers to information that could be used to harm or exploit individuals. This includes personally identifiable information such as passport details, biometric data, health-related information, religious or political beliefs, ethnic or racial background, financial data, and criminal records. Storing such data is vital not only for the security of the nation hosting these individuals but also for the protection of the migrants themselves. It enables authorities to make evidence-based decisions, whether concerning a refugee fleeing a dangerous situation or a migrant labourer seeking better opportunities abroad.

Another issue migrants may face due to a lack of data security is becoming victims of scams. If entities with malicious intent get hold of an immigrant's data, they may try to exploit them. Migrants, especially in the early stages of settling in a new country, are often unaware of the rules and norms of the system, which can make them vulnerable to scams. One such example is the phone scams in New Zealand that targeted immigrants. According to the National Cyber Security Centre of New Zealand, in the last quarter of 2023, a large number of calls were made to immigrants on visas in New Zealand, specifically targeting Mandarin-speaking individuals [8]. The callers pretended to be from Immigration New Zealand, asking victims to provide personal and sensitive information and, in some cases, to make payments to resolve visa issues. This example demonstrates the risks migrants face if

their personal data, in this case their phone numbers, is leaked.

1.3 Data Storage and Ownership Rights

In the past, data in general was stored within geographical boundaries, often within the office building of the organisation that collected the data. However, as the Information Technology (IT) industry evolved and when IT corporations began offering more flexible and cheaper IT solutions, such as cloud computing, and when the cost of the Internet also dropped, organisations found it more advantageous to use such services and solutions for their data processing and storage needs rather than handling everything in-house. Nowadays, cloud providers often store data across multiple geographical locations, depending on where their servers are located. In some instances, the owner of the data has a say in which region the data should be stored; in others they do not. For example, if an individual creates a virtual machine using Google Cloud, they can specify the region for their server. However, if someone uses Google Sheets to store data, they have no control over where that data is stored.

These developments create significant complexities regarding access rights to data. For instance, the United States government passed the "Cloud Act" [9] in 2018, which mandates that American companies providing electronic communication services must grant access to user data if requested by US law enforcement agencies under certain conditions. While the Act specifies certain conditions, it effectively means that user data can be accessed by authorities. Similar laws exist in various countries and regions worldwide, indicating that personal data is not guaranteed to remain private.

In today's digital marketing landscape and age of Artificial Intelligence (AI), data has become an incredibly valuable commodity. Technology corporations often show a strong desire for data. Individuals' data can be accessed by various service providers in multiple ways. One common method involves the use of bots, which may range from simple programs that supply data to search engines to more sophisticated systems that provide information to machine learning models. Major tech companies, including Google with its Gemini platform and Microsoft with its CoPilot, require vast amounts of data to train their models and improve their AI platforms. However, the clauses related to data collection are often buried in lengthy digital agreements, and options for data sharing are typically enabled by default in the tools and

technologies provided by companies. As a result, users often give consent to share their data without properly understanding the terms, which can be a daunting task in itself. When it comes to collecting and storing migrant data, significant risks arise if that data is compromised by tyrannical governments or private corporations. For instance, if the personal data of a refugee fleeing persecution is exposed, they could become easy targets for those pursuing them. Additionally, sensitive information related to health, past criminal records, race, or religious beliefs can lead to discrimination against migrants in areas such as employment, housing, or access to other benefits.

According to a 2019 article published in Science [10], a significant racial bias was identified in an algorithm used in the US healthcare system. The algorithm, designed to allocate additional healthcare resources, consistently underestimated the health needs of Black patients compared to white patients with similar scores. In reality, Black patients were sicker than the algorithm indicated. Similarly, in 2015, it was discovered that a tool developed by Amazon for reviewing job applications discriminated against female applicants in the hiring process for software development positions [11]. These cases illustrate how reliance on algorithms that access private data can lead to biased decisions that disadvantage specific populations or groups.

Indigenous peoples are another group vulnerable to bias. The Mana Raraunga: Data Sovereignty report, published by the Royal Society Te Apārangi [12], highlights the importance of establishing strong privacy regulation standards for Indigenous communities, particularly the Māori population in Aotearoa New Zealand. The report notes that, in many Indigenous worldviews, knowledge belongs to the collective, and responsibility is shared for transmitting Indigenous ways of being, knowing, and doing through the generations. Therefore, collective rights and reciprocal obligations are fundamental to Indigenous knowledge systems and data sovereignty. Furthermore, the report notes that Indigenous and other marginalised peoples are more likely to be profiled through big data, algorithms, and predictive modelling. Similarly, migrants often encounter comparable challenges, particularly in terms of data representation, surveillance, and limited control over cultural or personal information. Both groups share concerns regarding who collects their data, how it is interpreted and used, and whether it deepens existing social inequalities. The emergence of digital platforms such as Ahau (`https://ahau.io`) demonstrates a growing commitment to community-controlled data management and cultural preservation. Although such platforms do not directly address indigenous data security concerns, they are

designed to capture, digitise, and securely store important historical and genealogical information of Māori tribes in New Zealand.

1.4 Importance of cultural heritage for migrants

Cultural heritage can be described as the ways of life or knowledge that were passed down from earlier generations. These cultural practices are preserved because they are believed to enhance the community's chances of leading a better life. When populations migrate, they often carry their native culture and knowledge to their new environments. Each community may have its unique cultural heritage, which they strive to preserve across generations.

According to Portes & Rumbaut [13], migration has an impact on cultural heritage and on defining one's own identity. For a migrant who has moved from their native place and culture to a new place, everything may seem unfamiliar and overwhelming. Over time, they may adapt to the host culture, a process that can alter their sense of self and cultural heritage. This transition can be even more challenging for the immediate descendants of the migrants who were born and raised in the new place (see pages 218–219 in Portes & Rumbaut). These second-generation migrants often wander between two different cultural worlds, one at home and another in their neighbourhoods or schools. This duality can create confusion and challenges, particularly during their formative years.

According to a study, "Impact of Migration on Identity Formation: A Study of Second-Generation Immigrants" by Washington Omole [14], access to culturally sensitive resources such as educational programmes, community organisations, and mentorship helps second-generation migrants navigate the complex identity challenges posed by migration and enhances their resilience. The study further calls for inclusive policies and initiatives that affirm the diverse cultural identities of immigrants, fostering cultural integration and well-being. It advocates for culturally responsive approaches to second-generation immigrants' identity development and stresses the need to recognise and value the diverse contributions of immigrant communities.

Another important aspect of preserving cultural heritage is the continuity of traditions and knowledge. Masi Sadaiyan and Vadivel Gopal are two Indian migrants who were hired by the University of Florida to catch pythons,

which have become a problem for the state of Florida [15]. They belong to one of India's oldest tribes, the Irula, residing in the state of Tamil Nadu. The Irula tribe is renowned for its generational knowledge and exceptional skill in snake catching [16]. They are not only experts in capturing snakes but also have expertise in extracting venom to create antivenom, which can be quite lucrative. Although the origins of the tribe and their connection to snakes are not entirely clear, they have a rich and vibrant tradition involving a deity closely associated with cobras. In India, the Irula community is often marginalised, facing discrimination, illiteracy, and low-income livelihoods primarily derived from snake catching [16]. Unfortunately, they are frequently exploited by others. Masi and Vadivel are considered among the last generations with a profound understanding of reptiles, as many in the younger generation show little interest in continuing these traditional practices for various reasons. Despite the challenges faced by the Irula community in their native lands, preserving the knowledge and skills of individuals like Masi and Vadivel, while giving them control over how their knowledge is handled, would benefit not only these migrants but also their entire tribe.

In June 2024, the online community "La Blouse Roumaine", which is dedicated to promoting the traditional Romanian blouse known as the "ie", criticised the luxury fashion brand Louis Vuitton for violating the cultural rights of Romanian communities [17]. The controversy arose after Louis Vuitton introduced to the market a blouse strikingly similar to the ie, without giving due credit or acknowledgement to its roots as a symbol of Romanian folk culture. The issue gained significant attention, even prompting Romania's Minister of Culture to intervene. Later that same month, Louis Vuitton issued an apology for failing to acknowledge the Romanian tradition and withdrew the blouse from its collection [18]. While it is unclear how Louis Vuitton first encountered this cultural symbol, the case demonstrates how easily cultural heritage can be exploited or misrepresented. Similar risks exist for migrants, whose traditions and cultural expressions may also be taken, commodified, or misused without proper recognition.

When it comes to cultural heritage, migrant communities often face two main types of threats. First, their traditions and cultural practices may gradually fade over time, as they are influenced or overshadowed by the dominant culture and traditions of the countries to which they have migrated. Second, their cultural expressions may be taken or used without permission, often without any acknowledgement of their origins.

1.5 Blockchain-based technology for migrant data security and preserving cultural heritage

A 1991 article by Stuart Haber and W. Scott Stornetta [19] outlined a method for timestamping digital documents to prevent users from backdating or forward-dating them. The paper discussed the use of cryptographic hash functions to achieve this. It may be regarded as one of the predecessors to blockchain technology, which later transformed the digital financial world and peer-to-peer applications. The following year, together with Dave Bayer, they proposed a system employing Merkle trees in their paper titled "Improving the Efficiency and Reliability of Digital Time-Stamping" [20]. Building on the concepts described in these earlier works, Satoshi Nakamoto presented the idea of the blockchain in 2008 in the paper on Bitcoin [21]. In this paper, they described an electronic cash system that was decentralised, did not require the mediation of a financial institution, and could be transferred from one person to another. They leveraged the use of Merkle trees and digital signatures, and applied proof-of-work as a consensus mechanism. Although they did not use the term "blockchain," they proposed a method of linking blocks to form a continuous chain. The technology gained widespread popularity with the launch of Bitcoin in 2009, marking its emergence as a foundational element of digital currencies. Furthermore, blockchain-based technology provides a key framework supporting decentralised applications (dApps).

A blockchain can be described as a distributed digital ledger technology used to record transactions across multiple nodes in a secure, transparent, and tamper-resistant manner. Transactions are grouped into blocks and linked to the previous block using cryptographic hashes, forming a chain-like structure. Within each block, transactions are organised using a Merkle tree, which allows efficient and secure verification of individual transactions without requiring access to the entire block. Each node participating in the network maintains a copy of the blockchain. Once data is recorded, altering it would require modifying all subsequent blocks and re-achieving consensus across the network, which is computationally not feasible in large, decentralised blockchains.

The architecture of blockchain-based technology makes it a promising

solution for gathering and maintaining data securely, in a tamper-resistant manner. Blockchains operate on peer-to-peer networks, and a copy of the data exists across all nodes, reducing the risk of a single point of failure. Cryptography is a fundamental part of blockchain technology, ensuring data confidentiality and integrity by preventing unauthorised decryption or modification. The structure of blocks ensures that altering data requires modifying all subsequent blocks, making tampering extremely difficult. Blockchains can be categorised based on access level as public or private. Public blockchains are open to all, while private blockchains are restricted to authorised participants. While public blockchains store data transparently, privacy can be enhanced through encryption or private networks, mitigating the risk of external access or misuse. Since participants can collectively control access and manage the network, blockchain can also support data sovereignty, allowing communities or individuals to retain authority over their own information. These qualities make blockchain a robust solution for preserving data with enhanced security, integrity, and participant-controlled governance. This will be explored in more detail in section 5.4.

1.6 Cardano

Cardano is a blockchain platform designed with a research-driven methodology, incorporating principles from formal verification and peer-reviewed academic research. It is run by a Swiss-based independent not-for-profit organization, the Cardano Foundation. Like many other blockchain platforms, Cardano includes a smart contract platform. A smart contract is an automated mechanism within the blockchain environment that enforces the terms of digital agreements. Its smart contract platform is designed to support complex and large-scale decentralized applications (dApps). Security is a core principle in Cardano, and it allows isolated testing of components, which contributes to the overall stability and robustness of the platform. As a fully open-source project, it is designed to support diverse financial and social applications. Cardano uses the Proof-of-Stake consensus mechanism called Ouroboros, which is the first provably secure Proof-of-Stake protocol and one of the first blockchain protocols designed using peer-reviewed research. Unlike many other blockchain platforms, which consume substantial energy, Cardano is considered highly energy-efficient due to its Proof-of-Stake consensus mechanism [22]. Furthermore, according to the Cardano Founda-

tion, Cardano is taking steps to measure and report its energy consumption and carbon footprint according to the Markets in Crypto-Assets Regulation (MiCA) guidelines, which are issued by the European Securities and Markets Authority [23]. A more detailed discussion of Cardano is provided in section 5.4.5.

1.7 Problem Statement

This research addresses two principal issues faced by migrants.

The first concerns the protection of personal and sensitive data, particularly the vulnerability of migrants to data breaches arising from various factors, including negligence or errors by authorities, threats from external entities, and structural weaknesses within immigration systems. Migrants often have limited or no control over their own data. As discussed in earlier sections of this report, when data is stored within specific geographical jurisdictions or managed by entities subject to particular governmental regulations, the migrants to whom the data belongs frequently lose any say in who can access it. Such circumstances may have serious implications for the well-being, privacy, and security of migrants.

The second issue relates to the challenges migrants face in preserving their cultural heritage while residing in host countries. These difficulties may arise from exploitation by external actors, the lack of effective mechanisms for safeguarding cultural assets, or insufficient preservation efforts. Over time, these factors can contribute to the gradual destruction of cultural identity and heritage across generations. Similar to the handling of personal and sensitive data, cultural heritage information may also fall under the jurisdiction of certain governments, thereby limiting community ownership and control.

Current systems that manage migrant data are largely centralised. Although immigration authorities and related organisations have introduced mechanisms to protect the privacy of migrants, these systems do not always provide adequate protection in all circumstances. To address these challenges, there is a need for a system that enables migrants or prospective migrants to store their personal data securely, share it safely with immigration authorities or other relevant bodies, and minimise the risk of data breaches or misuse. Such a system should allow migrants to complete immigration and documentation processes without compromising the security or ownership of their data.

Furthermore, migrants and migrant communities should have a means to preserve, share, and, if desired, monetise their cultural heritage information safely, ensuring that ownership remains with the individuals or communities concerned.

At present, due to the centralised nature of existing systems, migrants lack control over their personal data. Likewise, most data management tools used for preserving cultural heritage are also centralised. Although some decentralised migrant data management and cultural preservation systems exist, they do not address the need for a mechanism that allows migrants to securely share their personal and sensitive data with relevant authorities, or to preserve, share, and monetise their cultural heritage in a safe and reliable manner.

In summary, migrants face significant challenges in maintaining control over their personal and cultural data due to the centralised nature of current systems. This research therefore aims to explore how the Cardano blockchain and decentralized technologies can be applied to develop a secure, decentralised mechanism that empowers migrants to manage, share, and preserve their data and cultural heritage safely.

1.8 Research Aim

The aim of this research is to design and evaluate a decentralised system, using the Cardano blockchain and related decentralised technologies, that enables migrants to securely store, share, and manage personal data and cultural heritage information while maintaining ownership and privacy.

1.9 Research Objectives

To achieve the research aim, the following objectives have been identified:

- Analyse existing research and systems related to migrant data management and decentralised technologies.
- Conduct a requirements analysis to identify the data security, privacy, and cultural heritage preservation needs of migrant communities.

- Design a decentralised system architecture utilising the Cardano blockchain and related technologies, with a focus on data sovereignty, security, and usability.
- Develop and deploy a functional prototype of the proposed system on the Cardano testnet.
- Gather and analyse user feedback to provide recommendations for future improvements and system scalability.

1.10 Thesis Structure

This thesis is divided into ten chapters and an appendices section containing supporting material. **Chapter 1** discusses the background of the study, including migrant data security, cultural heritage preservation, and blockchain technology, and presents the problem statement, research aim, and research objectives. **Chapter 2** reviews relevant literature on national data infrastructures, blockchain-based identity systems, the tokenisation of property rights, and cultural heritage preservation. **Chapter 3** outlines the research methodology, including ethical considerations, participant recruitment, data collection procedures, and analytical methods. **Chapter 4** presents the results of the questionnaire, covering both open and closed ended responses, along with insights gained from conversations with participants. **Chapter 5** discusses the design of the proposed solution, examining current practices related to migrant data and documentation handling, identifying limitations within the existing system, presenting an overview of the proposed system, and introducing key concepts such as blockchain technology, decentralised identifiers, verifiable credentials, and InterPlanetary File System (IPFS). **Chapter 6** describes the implementation of the prototype system, including system components, processes, credential flows, and privacy and security considerations. **Chapter 7** evaluates the prototype in relation to the research objectives. **Chapter 8** discusses the limitations of both the research and the prototype. **Chapter 9** provides recommendations and outlines potential future work, and **Chapter 10** concludes the thesis. The appendices supply supplementary material, including development details, survey documentation, and a user guide.

Chapter 2

Literature Review

2.1 National Data Infrastructure Blueprint for Aotearoa New Zealand

The National Data Infrastructure (NDI) Blueprint for Aotearoa New Zealand [24] highlights the need for a secure, trusted, and interoperable data ecosystem. The blueprint identifies several problems in current data-sharing practices, including limited control over data infrastructure, low trust in digital systems, and frequent duplication and inconsistency of data across organisations and platforms.

The blueprint proposes a system in which individuals can establish a verified digital identity, share data in a trusted way, control access to their data, and decide how their data is processed. It emphasises that the NDI should be built on existing technologies, open standards, and well-established protocols, while delivering efficiency, usability, and trust for end users.

For individuals, the blueprint expects the NDI to provide a safe and user-friendly means to prove their identity online and manage how third parties access or process their personal information. For organisations, it offers parallel benefits and enables them to participate as service providers within the NDI ecosystem if they choose. A central concept in the blueprint is data minimisation, which allows users to disclose only the minimal information necessary to access a service, via standardised and trustworthy mechanisms.

The NDI is not centrally managed by the government or any single organisation. Instead, it is designed as a distributed ecosystem, operated by multiple independent providers who comply with the same set of open stan-

dards and rules, an architecture analogous to the Internet. The principal capabilities of the NDI include identity verification, credential issuance and validation, access management, and providing users with a personal data store that they control, rather than having digital services retain multiple copies of their data. The blueprint also describes mechanisms for secure, privacy-preserving data processing in mutually trusted environments.

The blueprint notes that individuals often lack transparency regarding whether organisations handling their data follow good practices, meet standards, or where their data is stored (either geographically or legally). To address this, the NDI introduces the concept of Trusted Custodians. These are independent service providers operating under the NDI's trust framework and responsible for handling identity and data services on behalf of users. It also highlights that users frequently must share more personal data than is strictly necessary, for instance, providing a full identity document even when only a single attribute needs to be verified.

Technically, the blueprint discusses the use of verifiable credentials and cryptographic mechanisms for identity verification. Users keep control of their private keys to assert their identity. The blueprint also adopts concepts from the World Wide Web Consortium (W3C) Verifiable Credentials model, including verifiable credentials and verifiable presentations, which allow users to selectively disclose only the information required by a verifier while providing cryptographic proof of authenticity.

Furthermore, the blueprint discusses potential implementation approaches, including blockchain based and Verifiable Data Registry (VDR) based models for managing decentralized identifiers (DIDs) and verifiable credentials (VC). However, it warns that blockchains may lead to high computational cost, reduced efficiency, and environmental impact. It further notes that the complexity of blockchain systems may prevent broad participation, and that their public nature requires careful privacy preserving design.

The blueprint acknowledges the concept of a VDR within the W3C Verifiable Credentials framework, describing how a VDR can provide integrity services in a multi-issuer, multi-verifier ecosystem (e.g., recording credentials, publishing issuer certificates, and managing revocation lists). While the blueprint considers decentralised on chain storage via blockchain to be impractical for some use cases, it suggests alternative approaches, for example, JSON Web Key (JWK) / JavaScript Object Signing and Encryption (JOSE) key lookups for fetching issuer certificates.

In contrast, the prototype developed in this research implements a VDR

on the Cardano blockchain and utilises Hyperledger Identus as the identity management framework (see Section 5.3 for details). This design enables decentralised issuance, validation, and revocation of credentials, while maintaining alignment with the NDI's principles of distributed trust, user control, and data minimisation.

Unlike the more general architectural proposals in the blueprint, the prototype described here makes specific design decisions tailored to migrant data security and cultural heritage preservation. It is implemented on Cardano, selected for its lower energy consumption and reduced operating cost compared to many other blockchain technologies, thereby minimising environmental impact.

The system protects user privacy through encryption and established best practices, ensuring sensitive data remains secure yet usable. It is in line with the principle of data minimisation, users can share only the specific information required by a service, and all interactions are cryptographically validated using digital signatures. The prototype application also uses JSON-based JWT tokens. It supports Decentralised Identifiers, identity verification, credential issuance and validation, access management, and provides a mechanism for users to securely store their data in a decentralized manner, many of the concepts recommended by the paper. While the prototype is fully functional and usable, further improvements could enhance its usability and accessibility in future versions.

In an immigration context, organisations such as the International Organization for Migration (IOM) and private companies (e.g., VFS Global) already verify documents, process data, and issue credentials. In the prototype, these parties can act as trusted third parties, an idea similar to the Trusted Custodians concept mentioned in the paper. They are responsible for validating credentials, securely storing data in a decentralised manner, and facilitating verifiable interactions between users and service providers.

2.2 Deployment of a Blockchain-Based Self-Sovereign Identity

The paper by Stokkink and Pouwelse [25] focuses on Self-Sovereign Identity (SSI), an identity model that is created, managed, and used by individuals without relying on a centralised authority. This approach places trust in

users rather than institutions and enables open enrolment, allowing anyone to participate in the system without requiring permission. The authors list a number of core SSI principles, including Existence, Control, Access, Transparency, Persistence, Portability, Interoperability, Consent, and Minimisation, and additionally introduce the property of Provability. Their proposed government-level identity system enables users to maintain control over their identity without depending on institutional validation. They argue that cryptographic mechanisms limit opportunities for fraud by requiring all claims to be provable.

In their blockchain based model, users are bound to the claims they issue, ensuring accountability if they attempt to fraud the system. The authors argue that, unlike traditional blockchain networks, their design prevents a user from being removed through a 51% attack because each user maintains their own personalised blockchain. They emphasise the need for strong signature algorithms and cryptographic keys and propose that users' digital signatures should be legally recognised by government authorities. Furthermore, they state that the global state of the network should remain readable to government institutions to support the detection of malpractice, and that legal mechanisms should be established to penalise fraudulent behaviour.

The paper also insists that a user's claims should only be considered valid if they can be proven and verified by multiple independent attestors. If an attestor provides an attestation that later proves to be incorrect, the attestor should also face penalties. To enhance privacy, the authors recommend the use of zero-knowledge proofs, allowing users to demonstrate the truth of a claim without disclosing the underlying data. They further propose a revocation mechanism in which a unique challenge is sent to the attesting party via the identity holder, ensuring that the holder's consent is part of the revocation process. Finally, the authors stress that information disclosed through claims must be limited to the specific verifier and purpose for which it is intended, strengthening the principle of data minimisation within the SSI ecosystem.

The prototype application built for this thesis is based on SSI principles and, when compared to the principles outlined in Stokkink and Pouwelse, it follows most of them. The application ensures that users have an independent existence via DIDs, maintain control over their DIDs, and have access to their own data. The system and algorithms employed are widely used and open source. Furthermore, the DIDs created by users are long lived and transferable, disclosure of claims is selective, and maximum efforts have been

made to protect users' rights and privacy. In addition, the identities and VCs are provable through cryptography.

Although the paper states that users may be vulnerable to a 51% attack in traditional blockchains, the DIDs in the prototype are based on the Cardano network. It is reasonable to assume that such an attack is highly unlikely due to Cardano's design and security measures (see Section 5.4.5 for details). The paper suggests that government support for cryptographic digital signatures would be beneficial, a point that aligns with the prototype. However, its recommendation that the global state of the network must be readable by the government is not necessary for migrant data. In this context, a trusted third party appointed by the immigration authorities of the respective government is sufficient, and it is reasonable to assume they have the expertise to detect fraudulent applicants.

In the prototype built for this thesis, verification by the trusted third party is sufficient because a single VC can contain claims from multiple documents, and the trusted third party ensures that all documents are valid. For revocation, the verifier checks the trusted third party's revocation registry, therefore, no additional challenge response mechanisms are required.

2.3 Blockchain for Migrants: Promoting Self-Sovereign Identity and Financial Inclusion

The article by Francoise Vasselin [26] discusses Distributed Ledger Technology (DLT), focusing on how blockchain can help address challenges migrants face related to rights, protection, identity management, and access to financial services. It explains how blockchain supports SSI and provides the core infrastructure needed to achieve it. The article argues that combining cryptocurrencies with SSI has the potential to promote the economic inclusion of migrants. It notes that the absence of reliable and authentic documentation creates difficulties for institutions interacting with migrants and emphasises the importance of trustworthy documents for establishing confidence between migrants and authorities in their host countries. The article highlights that forced migrants, such as refugees fleeing conflict, are more likely to lack reliable documents. Because of this, it stresses the importance of blockchain based recording as an immutable and trustworthy source of information.

The article reviews several blockchain based identity initiatives, including Sovrin, IBM and Visa's digital identity system, the ID2020 Alliance, and BanQu. It emphasises that strong cryptographic algorithms make falsifying information extremely difficult, and that this level of security is essential when handling sensitive personal data and financial transactions. It also discusses how, on today's internet, individuals have limited control over their data, consent, and usage, due to the dominance of centralised, corporate infrastructures. It compares these systems with blockchain based solutions, arguing that blockchain offers enhanced security, user control, and transparency for SSI. It considers points such as failure risk, data ownership, security, transparency, and auditability, concluding that blockchain architectures provide significant advantages over centralised or cloud-based models. The article evaluates systems such as Sovrin, Civic, uPort, Jolocom, Ontology, Veres One, and Remme, noting that the Sovrin Network stands out as an open-source, decentralised identity network designed for self-sovereign identity. It argues that with Sovrin, migrants can securely and independently manage their identity data, giving them greater autonomy and control.

Furthermore, the article notes that Sovrin is built on Hyperledger Indy and operates as a public permissioned blockchain, where anyone may submit transactions, while network validation is performed by a designated group of trusted nodes. Although Sovrin was an influential early implementation of SSI principles, the Sovrin Network has since been discontinued due to low usage, insufficient investment, technical challenges (including issues related to resource allocation), and limited community engagement [27]. Its closure highlights the practical, financial, and governance difficulties involved in sustaining decentralised identity infrastructures for widespread use, even when the core concepts remain important within the broader SSI ecosystem.

The prototype application developed for this research also builds on a project based on Hyperledger technology (Identus), but it uses a public permissionless blockchain, Cardano, where validation is carried out by any participating node in the network. Although Sovrin was shut down for the reasons noted above, it is reasonable to conclude that the failure was not fundamental to blockchain technology itself, but rather related to limited adoption and ecosystem participation.

2.4 The digital tokenization of property rights. A comparative perspective

The paper by Rosa M. Garcia-Teruel and Héctor Simón-Moreno [28] examines the use of digital tokens to represent and transfer rights over real-world assets. Their work explores whether the transfer of a token on a blockchain can successfully represent the transfer of ownership or other property rights without relying on traditional intermediaries. The authors analyse the legal implications of such tokenisation within decentralised environments, highlighting the challenges posed by existing property law principles. They propose a model for tokenising the right to enjoy someone else's asset, known as a usufruct, over real estate and evaluate its compatibility across different legal jurisdictions. The paper ultimately recommends adapting private law rules to accommodate the tokenisation of property rights, while recognising the practical and legal limitations that must still be addressed.

The authors also discuss the role of smart contracts and computer code in facilitating the guarantees associated with transferring rights. They emphasise that such transactions may increasingly combine natural language agreements with automated blockchain logic. They provide conceptual examples where payments or conditions linked to the transfer of rights, such as obligations associated with land use, could be automatically monitored or enforced through smart contracts. Furthermore, the paper highlights the risk that a token may not be directly or legally connected to the underlying asset. If the legal system does not recognise the token transfer, off-chain agreements could conflict with the transfer recorded on the blockchain. The authors therefore stress the need for mechanisms that ensure adequate publicity, legal recognition, and protection of third parties when property rights are tokenised.

Although the paper focuses on property-related rights, its insights are relevant to the system developed in this thesis. The prototype application developed for this research, issues Verifiable Credentials rather than tokens to establish usage rights over cultural heritage artefacts, such as audio, text, images, video, and other forms of traditional knowledge. For such a system to operate smoothly, some degree of legal clarity and regulatory support will eventually be necessary, and the paper provides useful guidance on this point. The concern that a token might not be directly connected to its underlying asset is also applicable to cultural heritage artefacts. In the system proposed

in this thesis, this is addressed by including the file hash within the Verifiable Credential, which creates an indirect but reliable link between the credential and the specific artefact. The file hash is generated using a cryptographic hash algorithm, which produces a unique output for each file (see section 5.4.1 for details). However, the paper's discussion of an owner entering into multiple conflicting agreements is less relevant in this context, since the aim of the prototype is to grant legitimate usage rights rather than to restrict or transfer possession of the artefact. This distinction will be explored further in the future work section.

2.5 Cultural heritage preservation by using blockchain technologies

The article by Trček [29] examines how blockchain technologies can be applied to cultural heritage preservation, particularly in combination with tourism. The author proposes a multilayered architecture consisting of a ledger layer, a consensus layer and an incentives layer. A main feature of this model is the concept of users contributing their mobile phone's computational resources and, in return, receiving digital tokens. This incentive mechanism aims to create a sustainable ecosystem for supporting digital preservation activities.

The author argues that cultural heritage, both tangible and intangible, should ideally be preserved in its original form for as long as possible, and that blockchain technologies can support this goal by ensuring immutability and integrity. Blockchain cryptographic and consensus mechanisms help secure cultural heritage related metadata, promoting transparency, openness and public accessibility. The paper emphasises the significance not only of physical artefacts but also of intangible heritage, such as literature, oral traditions, poetry and mythologies. It also highlights the ubiquity of smartphones as an enabling factor, since these devices can participate in a peer-to-peer preservation network.

The paper compares its proposed approach with mainstream blockchain platforms and identifies several limitations in existing systems. These include the high energy consumption of proof of work algorithms, the heavy computational demands of conventional public key cryptography and the vulnerability of widely used cryptography algorithms to future quantum computing attacks. In order to address this, the proposed architecture makes

use of lightweight, hash-based cryptography which provides better quantum resistance and reduces computational overhead.

The use of smart contracts is also discussed, particularly with regard to their potential role in automating processes related to heritage documentation and access control. The paper briefly considers non fungible tokens (NFTs) in this context, although it stresses that the primary focus is not on tokenisation but on long term integrity and preservation. The architecture also distinguishes between the metadata stored on the blockchain and the large cultural heritage files themselves, which may range from text data to high resolution images, 4K video recordings and detailed 3D models. It suggests storing only the relevant hashes on the blockchain while keeping the heavy data in cloud storage. The paper argues that this model helps maintain verifiability while preventing excessive ledger growth. It claims that this approach enables the blockchain to grow much more slowly than traditional blockchains and contributes to system sustainability. Although the system employs a proof of work style consensus mechanism, it is deliberately simplified so that it remains computationally feasible on mobile devices. Digital tokens generated within the incentive layer are stored off chain in cloud databases so that the blockchain ledger remains lightweight.

This paper discusses several important aspects of blockchain technology that are relevant to cultural heritage preservation. Although it focuses mainly on tourism-related heritage, it emphasises the importance of cultural heritage information, including intangible data, which is highly relevant to this thesis. It reinforces the idea that blockchain can be a useful mechanism for protecting and verifying cultural-heritage-related information. Its discussion of the weaknesses of mainstream blockchain technology is also informative. Although the system proposed in this thesis uses Cardano, which employs a proof-of-stake consensus mechanism and is therefore more energy efficient than proof-of-work blockchains (see section 1.6 for details), it is important to acknowledge concerns regarding the computational demands of some cryptographic algorithms and the potential vulnerability of current public-key schemes to future quantum-computing attacks. Cardano depends on elliptic-curve cryptography (specifically Ed25519), which, like other classical public-key algorithms, would be at risk if large scale quantum computers capable of breaking such encryption were to emerge in the future. According to publicly available information, the Cardano ecosystem is actively exploring approaches to mitigate these potential risks [30]. Furthermore, cryptography and quantum computing experts suggest that there is a growing likelihood

that quantum computers capable of breaking current public-key algorithms could appear within the next 20 to 30 years. Some forecasts indicate a 10 to 30 year window, with low probability scenarios pointing to possible successful quantum attacks as early as 2034 [31]. This shows that the risk is long-term rather than immediate. Therefore, the use of the Cardano blockchain in this thesis is reasonable. Any performance limitations associated with the cryptographic algorithms in use can be considered negligible in the context of the proposed system. Given that Cardano is under active development with a strong emphasis on sustainability and long-term security, it is reasonable to expect that future updates will continue to address these considerations.

2.6 Discussion of the Literature

First, the NDI Blueprint for Aotearoa New Zealand [24] was analysed. It identifies issues such as users having limited control over their data, data duplication, and low trust in digital systems. The blueprint proposes a system in which individuals can have a verified digital identity and share their data securely, applying the principle of data minimisation. The system is designed as a distributed ecosystem operated by multiple independent providers who comply with a set of open standards. Key features include identity verification, credential issuance and validation, access management, and providing users with a personal data store that they control. The blueprint also introduces the concept of Trusted Custodians, independent service providers operating under the NDI's trust framework. It discusses VCs and Verifiable Presentations, which enable selective disclosure of data with cryptographic proof of authenticity. Furthermore, it examines VDR based models for managing DIDs and VCs. However, it notes that blockchain-based approaches may result in high computational cost, reduced efficiency, and environmental impact. The blueprint also suggests alternative approaches, such as JWK/JOSE key lookups, for fetching issuer certificates instead of storing all data on-chain.

Stokkink and Pouwelse [25] discuss SSI and identify a set of core principles as the basis for such systems. They are Existence, Control, Access, Transparency, Persistence, Portability, Interoperability, Consent, Minimisation, and Provability. The authors note that cryptography can be used to prevent fraudulent claims. They propose a personalised blockchain model with strong signature algorithms and suggest that government institutions

should have the ability to read the global state of the network to detect malpractice and enforce penalties. Furthermore, they state that a user's claim should only be considered valid if it can be independently verified by multiple attestors. To enhance privacy, the authors also propose a zero-knowledge proof mechanism, allowing users to prove the validity of a claim without disclosing the underlying data.

The next article by Francoise Vasselin [26] discusses the use of SSI and blockchain for migrants and their financial inclusion. It argues that combining cryptocurrencies with SSI has the potential to promote the economic inclusion of migrants. The article emphasises the need for reliable documentation, noting that forced migrants are particularly vulnerable to lacking such documents. It reviews several blockchain-based identity systems and highlights that strong cryptographic algorithms make falsifying information extremely difficult. Since the system handles sensitive personal data and financial transactions, high security is essential. The article considers factors such as failure risk, data ownership, security, transparency, and auditability, concluding that blockchain architectures offer significant advantages over centralised or cloud-based models.

The article by Garcia-Teruel & Simón-Moreno [28] examines the use of digital tokens within decentralised environments to represent and transfer rights over real-world assets, particularly in the context of real estate. It explores the legal implications of tokenisation, highlighting the challenges posed by differing property laws and jurisdictional constraints. The authors emphasise the practical legal limitations that must be addressed for tokens to reliably represent ownership or usage rights. The article also discusses the use of smart contracts to facilitate and enforce rights transfers automatically, combining traditional legal agreements with blockchain logic. One important concern raised is that tokens may not always be directly or legally linked to the underlying asset. This could potentially cause conflicts between off-chain legal agreements and on-chain records. The authors highlight the need for mechanisms that ensure legal recognition, publicity, and protection of third parties when assets are tokenised.

The final article by Trček [29] discusses how blockchain technology can be applied to cultural heritage preservation, particularly in combination with tourism. The article proposes a multilayered architecture, consisting of a ledger layer, a consensus layer, and an incentives layer. It describes a system in which users contribute their mobile devices' computational resources and, in return, receive digital tokens as rewards, creating a sustainable ecosys-

tem for supporting digital preservation activities. The paper emphasises the importance of preserving both tangible and intangible heritage, including literature, oral traditions, poetry, and mythologies. It compares the proposed system with existing blockchain technologies, particularly highlighting the high energy consumption of traditional proof-of-work systems. To address these challenges, it employs lightweight, hash-based cryptography that is also quantum-resistant, thereby reducing computational overhead while maintaining security. The article further discusses the potential role of smart contracts and NFTs in automating processes related to heritage documentation and access control. It proposes storing large cultural heritage files, such as text, images, video, and 3D models, in cloud storage, while only storing metadata and hashes on the blockchain to maintain verifiability without excessive ledger growth. The digital tokens generated within the system are also stored off-chain in cloud databases, ensuring that the blockchain remains lightweight and sustainable.

Although prior work has investigated SSI principles and explored blockchain-based identity and tokenisation, much of this research remains largely theoretical or generic. Studies that focus specifically on migrants, such as Vasselin [26], emphasise the importance of authentic documentation and financial inclusion. However, they do not provide detailed privacy-preserving solutions for migrant data, nor do they address the preservation of migrants' cultural heritage. Work by Garcia-Teruel & Simón-Moreno [28] on tokenisation from a legal perspective highlights the need for legal recognition and warns that digital tokens may not always be reliably linked to real world assets, yet it does not propose a privacy focused technical architecture to address these concerns.

Similarly, the NDI Blueprint [24] and the heritage preservation study by Trček [29] offer high level concepts, governance models, and energy efficient designs, but they do not provide an implementable prototype that integrates DIDs or VCs with decentralised off chain storage for migrant or cultural heritage use cases. This thesis addresses this gap by developing a working prototype using Cardano and Hyperledger Identus for DID and VC management. Furthermore, it combines this with IPFS for off chain storage, demonstrating a privacy focused, decentralised approach for sharing and storing migrant documentation and cultural heritage information.

Chapter 3

Methodology

This chapter describes the purpose of the study, how participants were selected, the data collection methods employed, and the approach used to analyse the data. Both qualitative and quantitative methods were employed to provide a thorough understanding of the research problem. In particular, this chapter explains the research design, sampling techniques, data collection methods, and the procedures followed throughout the research process. It also addresses the ethical considerations relevant to the study.

This thesis aims to develop a prototype software application based on the Cardano blockchain to securely store migrant data and cultural heritage information. The goal is to provide migrants with greater control over their personal information, better protection of their data, and a mechanism to preserve their cultural heritage. As the primary users of this software will be migrants, it is crucial to understand their perspectives and concerns regarding data sharing and cultural heritage preservation.

In order to gain this understanding, a structured questionnaire was designed to explore migrants' views on sharing personal data for immigration and immigration related purposes, as well as their opinions on cultural heritage protection. The questionnaire contains a total of 89 questions, including 33 main questions and 56 subquestions. It consisted of 83 closed-ended (multiple-choice) questions and six open-ended questions. Trust in official authorities and in the systems and procedures in place to safeguard their data, concerns about privacy and security, attitudes towards the importance of cultural heritage information and its preservation, and various factors influencing these attitudes were some of the topics addressed.

The questionnaire was developed specifically for this study and was not

directly based on any existing research tools. Instead, it was designed to collect data that would help identify the requirements and determine the design considerations for the prototype software application intended for migrants. The goal was to ensure that the future system adequately reflects migrants' needs, preferences, and concerns. The questionnaire was available in English and was distributed in both paper and online formats. A copy of the questionnaire is provided in Appendix B.3.

The questionnaire seeks to explore the following questions with migrants:

- *What data was collected from migrants?*
  During the migration process, immigration authorities in the destination country often collect a wide range of information from migrants. This data is used to assess various factors, such as the validity of the migrant's stated purpose for migration, whether the individual poses or could pose any security risk to the host country, and whether the migrant has sufficient financial resources to support themselves during their stay. Although it is possible to make assumptions about the types of data immigration authorities may require, the specific information collected can vary from person to person. In order to ensure that no critical data is missed, correctly identifying the exact details gathered by immigration authorities is essential for this research.

- *How did they feel about providing such data?*
  When immigration authorities request data from migrants, the migrants often have no choice but to comply, as refusing to provide the information may negatively impact their migration process. This is especially true for those who are forced to migrate due to circumstances such as war, natural disasters, or other crises. Although migrants may provide their data to authorities, this does not necessarily mean they are comfortable doing so. Understanding how migrants feel about the different types of data they are required to share can greatly assist in the design of the prototype software, as it addresses their concerns and helps them feel more at ease with the data-sharing process.

- *Are they aware of the risks associated with improper data collection and management?*
  Data has become a valuable commodity in the modern world. Data breaches and data theft have become a growing issue globally, affecting both government and private sectors. In recent years, large amounts

of data have been shared and sold among nefarious entities. According to the BBC, in a recent data breach at Oxford City Council (UK), two decades' worth of personal data were stolen [32]. Another BBC article states that in 2023, the DNA testing company 23andMe suffered a data breach that resulted in the theft of millions of people's personal data, including family history and health conditions [33]. This poses significant risks to data owners. Additionally, rogue employees within authorities or third parties handling immigration data (e.g., agents, contractors) may gain access to and mishandle migrant data.

This question attempts to assess two things. First, whether migrants are aware of how vulnerable their data can be. Second, whether they are aware of the potential consequences of improper data handling. Understanding this will help in designing the prototype software, particularly in determining what safety and control measures should be implemented when storing or sharing data.

- *How do they feel about preserving their cultural heritage information?*
  Cultural heritage information, at first, may not appear as critical as other types of data, such as personal or sensitive information. However, preserving cultural heritage can be valuable in many ways, not just for the migrants themselves but also for their descendants and future generations [14]. Knowledge of how much importance migrants place on the preservation of their cultural heritage will provide valuable insights. This can be used to determine the level of importance this feature should be given in the design of the prototype software.

- *Are they aware of the importance of preserving their cultural heritage information and the potential for exploitation?*
  Migrant cultural heritage information is often exploited in various ways. At times, migrants do not even realise that their cultural heritage information is being exploited, and it goes unnoticed. At other times, they are aware, but they are not sure what to do about it, as they may not know that they have rights related to the preservation of their cultural heritage. This question attempts to understand how much awareness migrants have regarding the vulnerability of their cultural heritage information to exploitation, as this will help in identifying the features that are needed in the prototype software. Furthermore, understanding this can also reveal the different ways in which cultural heritage

information is being misused.

- *Would they be interested in a solution that provides better protection and control over their data and cultural heritage information?*
  It is important to understand whether migrants would be interested in technology that provides greater protection for their personal data and helps preserve their cultural heritage. Even though many migrants may be aware of the risks involved with data breaches and the exploitation of cultural heritage information, they might not see it as an urgent issue that needs to be addressed. Migration itself can often be a difficult and stressful process, so migrants may not have the time or capacity to think about such vulnerabilities to exploitation. However, since the goal is to develop software specifically designed for migrants, it is crucial to understand their perspectives and needs.

- *Do they have any knowledge of blockchain technology?*
  Blockchain technology has been in existence for some time. However, it is not as widely recognised as some other technologies, such as Artificial Intelligence (AI) or Virtual Reality (VR), among the public. Individuals with backgrounds in IT or finance may be familiar with blockchain technology, but awareness and understanding of it among the general population are limited. Understanding the level of knowledge that migrants have about blockchain technology will help assess how much trust they might place in a system built on this technology. This insight is important for assessing the likelihood of acceptance among migrants and the effectiveness of the proposed solution.

3.1 Research Design

This study was conducted mainly through a questionnaire. In some closed-ended questions, more than one answer was permitted. Clear instructions were provided next to each question on how it should be answered. The questionnaire was designed to be completed in 30 minutes or less.

3.1.1 Ethical Consideration

The preliminary ethics committee approval request was submitted on 10 February 2025 by completing the "Preliminary Ethics Application Form"

and the "Research Consent/Participant Information Form." The Ethics Committee requested several modifications to the submitted forms, together with clarifications and copies of the questionnaire and interview questions. After these were provided, a few additional changes were suggested. Following the revisions, the application was approved on 28 April 2025. A copy of the approval is included in Appendix B.1 of this thesis.

The study collected only the full names and signatures of participants and no other personally identifiable information. The aim of the study was to collect information regarding participants' migration experiences, including the types of data collected from them by immigration or other authorities during the migration process, their feelings about providing such information, and their awareness of the potential risks associated with the data submitted to immigration authorities or agents. Furthermore, the study sought to determine whether participants were aware of risks such as data loss, data breaches, or potential threats posed by rogue authorities with malicious intent. As some migrants may have had difficult or traumatic experiences during migration, the questionnaire was carefully designed to avoid triggering painful memories or distress.

During the questionnaire sessions, some migrants asked questions or required minor clarifications regarding the questionnaire, which were addressed by the researcher. In the course of these conversations, migrants shared further experiences and expressed how they felt about the migration process, data privacy, and the preservation of their cultural heritage. Notes were taken on paper regarding the parts of these conversations relevant to the topics covered under the ethics committee's approval, excluding any personal or sensitive information.

After the interviews, in certain cases, the researcher had follow-up questions regarding answers provided in the questionnaire, and the responses were recorded on paper. Again, these notes did not include any personal or sensitive information about the participants, and all questions fell within the scope of the ethics committee approval granted for the questionnaire and interview questions.

3.1.2 Participants

This study employed a purposive sampling strategy to recruit migrants residing in New Zealand and other countries. According to the IOM, migrants are defined as [34],

"A person who moves away from his or her place of usual residence, whether within a country or across an international border, temporarily or permanently, and for a variety of reasons."

An international migrant is further defined as [34],

"Any person who is outside a State of which he or she is a citizen or national or, in the case of a stateless person, his or her State of birth or habitual residence."

This study specifically focused on international migrants, as migrants who move within a country are generally not required to provide personal or sensitive data, nor extensive paperwork for migration or visa purposes. Furthermore, when individuals move within their own country, the likelihood of losing their cultural heritage or facing risks to their cultural identity is much lower. Based on the definitions mentioned above, participants were individuals who had migrated from their country of origin for various reasons. These included work, seeking a better quality of life, family reunification, marriage, or study. The target sample size was 10 to 20 participants. This was considered sufficient to gain an understanding of the perspectives of migrants, while also ensuring feasibility within the timeframe of this thesis. Inclusion criteria required participants to be at least 18 years old, able to read English, and to have experience with immigration in the host country, such as having undergone immigration processes or handled visa-related documentation.

The survey was conducted over a four-week period, from 13 May to 9 June 2025, through campus networks at the University of Waikato and with migrants personally known to the researcher. Participants came from various countries, which helped provide a broader perspective on the research topic. Notably, one participant was both a migrant and someone who works extensively with other migrants. Participants ranged in age from 18 to 60 years and came from several regions, although most were from Sri Lanka.

Data collection involved only the names and signatures of the participants; no additional personal information was gathered. The questionnaire, approved by the University of Waikato Ethics Committee, was distributed in both paper and online formats. The paper version was administered in Hamilton, Waikato, including to students from the University of Waikato, while the online version was shared via email with participants globally.

In total, 20 participants took part in the study.

3.1.3 Limitations Related to Participants

The sample comprised mainly young and middle-aged adults. Participants were recruited either on campus premises or were personally known to the researcher. While the sample size of 20 is relatively small and not statistically significant, it was deemed sufficient to explore participants' perspectives in depth for the purposes of this qualitative study.

However, several limitations should be noted.

- A large proportion of the participants were recruited through university networks. This might limit how well the findings apply to all migrants, possibly excluding older migrants or those with lower levels of education.
- Most of the participants were from Sri Lanka. Therefore, this over-representation may mean that the results reflect views specific to that group (especially regarding cultural heritage), rather than migrants in general.
- The fact that the researcher was personally known to some participants may have influenced their answers. This could be due to reasons such as fear of judgement, reduced anonymity, and similar factors.
- Only individuals who could read English took part, which may have excluded migrants with limited English skills and affected the range of views collected.

3.2 Questionnaire Distribution

Privacy, data security, and data sovereignty were among the main considerations of this thesis. Because of this, great importance was placed on how the study was conducted and how the data was stored. As some participants' circumstances could be particularly sensitive or vulnerable, it was essential to ensure that the study was carried out as securely as possible.

Initially, it was decided that the study would be conducted exclusively through a paper-based survey. This approach was chosen because it was considered to provide a higher level of privacy. Paper-based surveys do not involve storing data online, particularly on third-party platforms. In this method, the researcher personally distributed the survey to the participant and collected it upon completion. The completed surveys were then stored securely in a locked location.

Online surveys were initially ruled out due to concerns about privacy and data protection. Although various tools such as Qualtrics, Google Forms, and Microsoft Forms were available, they were not considered suitable, as they could not fully guarantee the level of privacy and security required for this study. Efforts to identify a secure platform for conducting the study did not yield satisfactory results. As a result, a paper-based approach was regarded as the most appropriate method during the early phase of the research.

3.2.1 Decision to Include Online Questionnaire Distribution

During the questionnaire distribution phase, it was discovered that the study could reach a wider audience if an online questionnaire were made available. One reason for this was the realisation that finding participants beyond the campus premises would provide a broader range of respondents, not limited to students or staff. Furthermore, many potential participants who were nearby actually preferred an online questionnaire, as they found it more convenient.

As a result, further research was conducted to find a secure alternative method for distributing the questionnaire online. During this brief investigation, the following methods were considered:

- Emailing participants a password-protected Word file (stored in the researcher's Microsoft OneDrive) with the password included in the email. Each participant would receive a unique password to open the file, complete the questionnaire, and then upload the completed file to a unique shared OneDrive location. This approach ensured that email providers would not have access to the completed questionnaires, and Microsoft OneDrive could not access the files without the password. However, this method proved too technical for many users and was therefore not pursued.

- Sharing a custom-made HTML questionnaire file with participants via email, who would then fill out the questionnaire and click the save button. The HTML page would encrypt the data and save it as a text file. Participants would then email the text file back or upload it to a unique OneDrive location. This method was also abandoned because it presented the same usability issues as the first solution.

During this phase of the research, and following the suggestion of the researcher's supervisor, ProtonMail was considered as a potential platform for distributing the questionnaire. ProtonMail is a secure email service based in Switzerland, a country known for its strong privacy protections. Article 13 of the Swiss Constitution guarantees the right to privacy in personal spaces and telecommunications and protects against the misuse of personal data [35][36]. In addition, ProtonMail ensures that all emails are end-to-end encrypted, offering an added layer of security [37].

The proposed approach involved the researcher sending a Word document containing the questionnaire to participants via ProtonMail. Participants would then complete the questionnaire and return it via their own email (not necessarily ProtonMail) to the researcher. In this scenario, the outgoing email from the researcher would remain encrypted until it reached the participant's email provider, thereby providing at least some level of encryption and data protection during part of the transmission.

3.2.2 Use of Proton Drive and Proton Documents for Online Questionnaire Distribution

During this phase of consideration, the existence of Proton Drive and Proton Documents was discovered. Further research revealed that Proton Drive encrypts all files by default [38]. According to ProtonMail's website, all Proton products are open-source and independently audited [39], which ensures transparency in how data is handled and how secure Proton Drive and other products are. Any files shared through Proton Drive, including Proton Documents, are end-to-end encrypted, meaning that only the document owner and the intended recipient can access the contents. Files can be securely shared, with additional protection through passwords, and expiry dates can be set for each shared link to limit access within a specific timeframe. Due to these features, Proton Documents were chosen as the platform for creating the online version of the questionnaire.

A separate questionnaire document was generated for each participant, assigned a unique name using a GUID (Globally Unique Identifier), which is a randomly generated string used to ensure each document has a unique and unguessable identifier. Each document was password-protected with a strong password, and a two-week expiry date was set for the sharing link. The link and password were emailed to the participants. A sample email is attached in Appendix B.2.

This method ensured that email providers could not access the encrypted documents. Even if the link were detected, accessing the end-to-end encrypted document without the password would be extremely difficult. This approach provided a reasonable level of security for distributing the questionnaire. The Participant Information Sheet and instructions were included in the email, and the Participant Consent Form was embedded within the questionnaire.

In the questionnaire itself, the participants were again given the following instructions.

> *This questionnaire is conducted as a partial requirement for the Master of Science (Research) in Computer Science. The goal of this research project is to build a decentralised application to securely store migrant data and cultural heritage-related information.*
>
> *If you take part in the study, you have the right to:*
>
> - *Refuse to answer any question and withdraw from the study within two weeks of your participation.*
> - *Ask any further questions about the study that occur to you during your participation.*
> - *Receive a summary of the study's findings once the study is concluded.*
>
> *If you have any questions or concerns about the project, either now or in the future, please feel free to contact us using the contact information provided in the Participant Information Sheet.*

3.3 Data Collection and Storage of Data

The data collected using paper questionnaires were digitised into PDFs, and the original paper questionnaires are stored in a locked location. The online questionnaires were also exported into PDFs. The completed digital questionnaires were encrypted with a strong password and stored on the researcher's computer, with a backup kept in the University's OneDrive account assigned to the researcher. Since the files were protected with strong passwords and secure encryption, it is reasonable to assume that they will remain safe and inaccessible to unauthorised individuals. The data storage obligations under the ethics application were strictly followed.

3.3.1 Data Transfer

The data captured via paper questionnaires as well as through Proton Documents was manually transferred into a CSV file using Microsoft Excel. This method was chosen instead of automating the process for two main reasons:

- First, the digitised paper questionnaires were scanned as PDFs, and the Proton Documents were printed as PDFs using the web browser. Although Proton Documents offered an option to export to PDF, this functionality disrupted the document's formatting. Therefore, the documents were printed as PDFs instead. While text in most PDF files can usually be selected or copied, the PDF files generated from Proton Documents did not allow text selection or copying, so the documents had to be processed with OCR (Optical Character Recognition) to read the content. Furthermore, the scanned paper questionnaires would also have required OCR processing. Using OCR would involve third-party software, and depending on the tool, data might be sent to external servers. Even if open-source OCR software were used, security concerns would remain, as the original documents contain participants' full names and other sensitive information.

- Second, OCR processing can introduce inaccuracies, potentially resulting in significant additional effort for data cleansing and verification.

Due to these concerns, the data was carefully transferred to CSV manually, despite the process being time-consuming. In the CSV file, participants'

names were not recorded; instead, each participant was assigned a unique number to ensure anonymity.

3.4 Data Analysis

Data analysis is an important part of any study. This is where the researcher examines the collected data in greater depth to identify patterns and underlying rationale. This section briefly describes the data analysis procedures applied in this thesis. Chapter 4 will discuss the results of the analysis and the findings in detail.

3.4.1 Data Cleansing

In the questionnaire, none of the questions were mandatory. Participants were instructed to answer only the questions they felt comfortable with and could skip any questions or subquestions they wished. Therefore, some questions and subquestions have missing responses, which were marked as "N/A" in the results CSV file.

Furthermore, for a few closed-ended questions, some participants provided their answers in the "Other" field even when similar options were available in the multiple-choice list. The data cleansing process addressed these scenarios. The CSV file was cleaned and prepared for further processing. Additionally, during the manual transfer of data into the CSV file, there were minor errors, such as extra spaces or inconsistent formatting. The data cleansing process corrected these issues as well.

3.4.2 Tools and Libraries Used

- *Microsoft Excel* is a popular tool originally developed for accounting, but it is widely used in fields where data analysis, calculation, or processing is required. In this study, *Microsoft Excel* was used for updating and cleansing the data, as well as for some processing tasks.
- *Python* is a programming language particularly used in data processing and analysis. Its extensive ecosystem of libraries for data manipulation and visualisation makes it popular among the scientific community. In this research, *Python version 3.13.3* was used for data cleaning, data analysis, and visualising data in the form of graphs.

- *Pandas* is a Python library used for data manipulation and analysis. It provides data structures such as DataFrames, which make it easy to clean, transform, and explore datasets efficiently. *Pandas version 2.2.3* was used in this thesis for loading, cleaning, and preprocessing data, as well as for performing statistical analysis.

- *Matplotlib* is a widely used Python library for creating visualisations. It helps users to produce high-quality graphs and plots to represent data insights visually. In this thesis, *Matplotlib version 3.10.3* was used to generate charts and graphs for data visualisation and presentation of results.

- *VS Code (Visual Studio Code)* is an open-source text editor and integrated development environment (IDE) that supports many programming languages, including Python. It was chosen for this thesis because it is a popular IDE for Python development and simplifies the coding, compiling, and debugging process.

In summary, the surveys were successfully conducted with 20 participants, all of whom were migrants originating from a range of countries worldwide. The study was carried out in strict accordance with the university's ethical guidelines, and all data were securely stored both physically and electronically. While the sample size may not be statistically significant and does entail certain limitations, it was nonetheless considered adequate given the time constraints and overall objectives of the research.

Chapter 4

Results

4.1 Overview

The results section discusses the methods used to analyse the data collected from the survey. The analysis involved both quantitative and qualitative techniques to provide a comprehensive understanding of participants' opinions. Quantitative data gathered via closed-ended questions were summarised using descriptive statistics. Qualitative responses from open-ended questions were carefully analysed to identify recurring patterns and themes. The analysis was conducted using Excel and Python, ensuring data accuracy and confidentiality throughout the process.

4.2 Analysis of Closed-Ended Questions

This section presents the analysis of the closed-ended questions. To visualise participants' responses, bar charts, stacked bar charts, and pie charts have been used where appropriate. Some questions deemed less significant for the analysis have been omitted from this section. For clarity and ease of interpretation, certain questions have been grouped, and some answer labels have been rephrased; however, the original context and meaning have been preserved.

4.2.1 Age Group Distribution

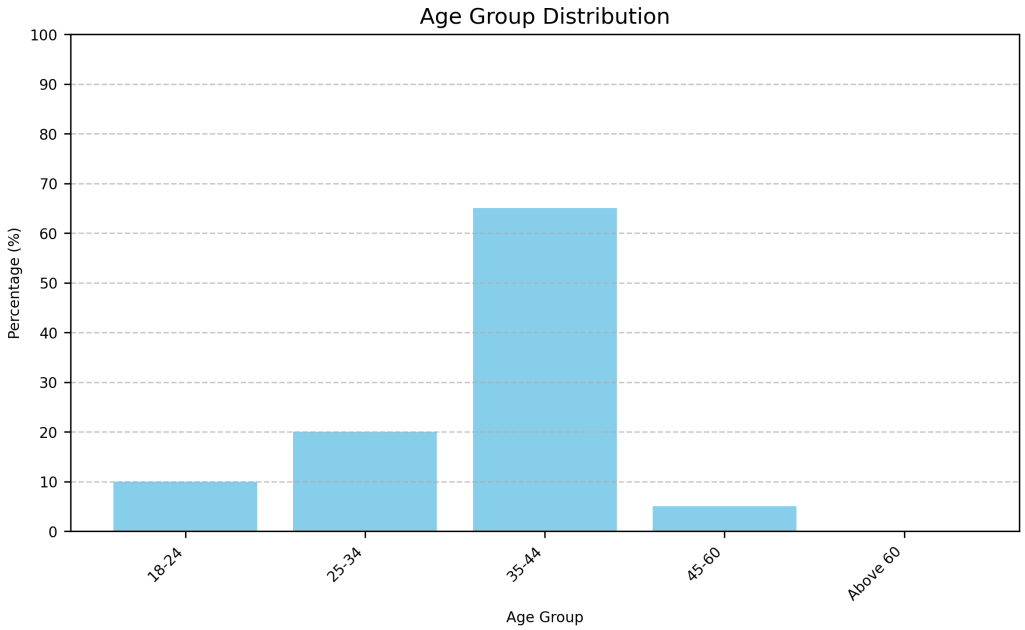


Figure 4.1: Age group distribution

The age group distribution was analysed to identify any trends related to participants' ages. Understanding how age correlates with specific preferences or opinions is essential for interpreting the results and drawing meaningful conclusions. Among the participants, the majority were middle-aged adults. There were no participants above 60 years of age. This could be because participants were mainly recruited on campus or were individuals known to the researcher, who are in a similar age group.

4.2.2 Country of Origin

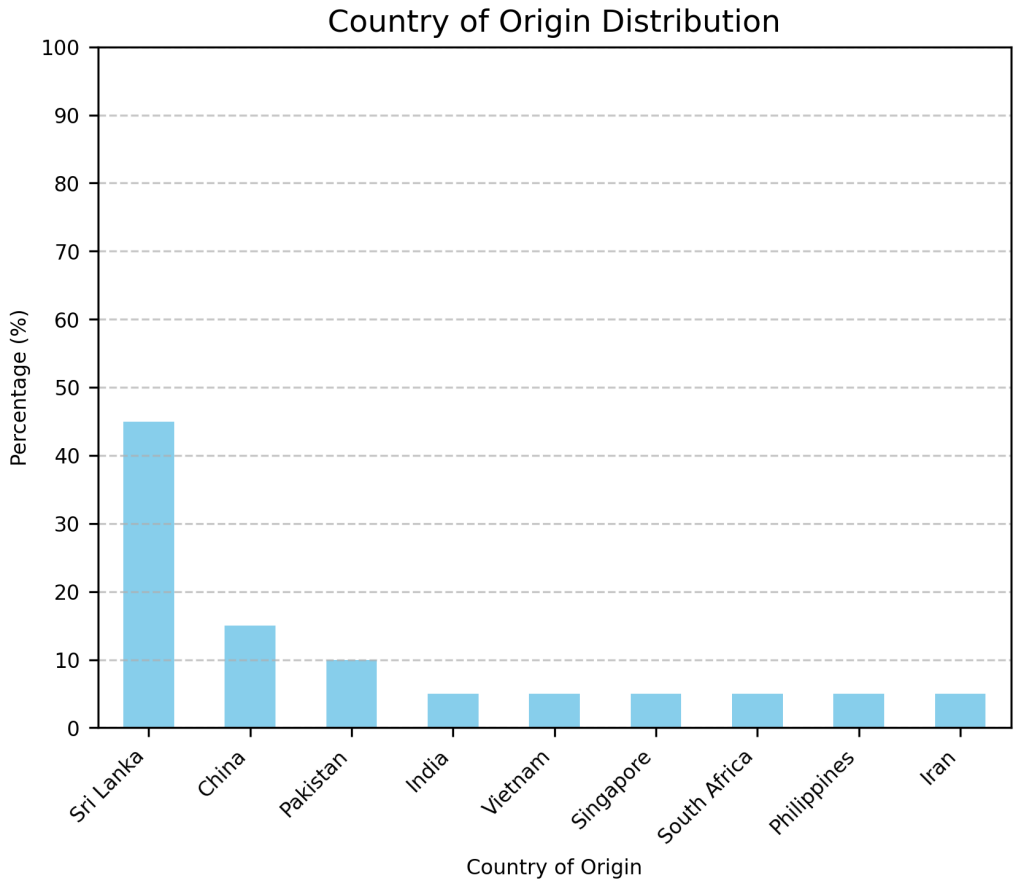


Figure 4.2: Country of origin distribution

The participants came from nine different countries. Including participants from diverse countries allows for a broader understanding of the types of information collected. Sri Lankans made up the largest group at 45%, which may introduce some bias. Fifteen per cent of participants were from China, and ten per cent were from Pakistan, while each of the other countries represented less than ten per cent of the participants.

Except for participants from Vietnam and a large portion of those from Sri Lanka, most others were located either on campus or in Hamilton city, having migrated to New Zealand. This group also included a small number of

Sri Lankan participants. The data collected by immigration authorities could vary depending on participants' countries of origin. Since participants from eight different countries had migrated to New Zealand, it may be possible to capture all or most types of data collected from migrants, regardless of their country of origin.

However, one issue is that all participants were from Asia, except for one individual from Africa. It would be interesting to analyse whether the findings would differ if the sample included migrants from Western countries.

4.2.3 Reasons for Migration

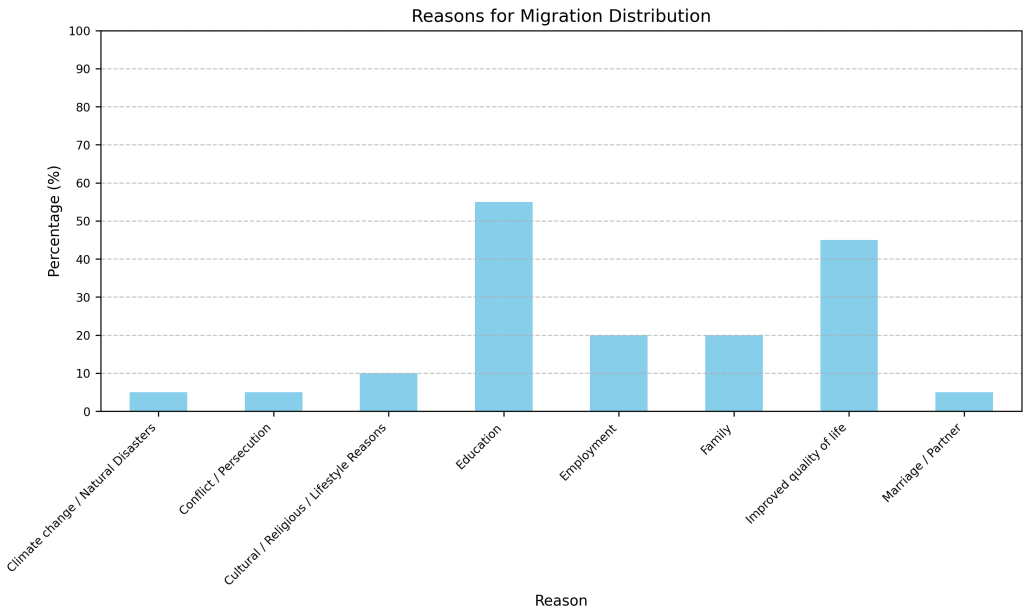


Figure 4.3: Reasons for migration

Participants could select multiple reasons for their migration. Education was chosen by 55% of participants, which may reflect the fact that many were recruited from campus premises. Nearly 50% of respondents mentioned seeking an improved quality of life as their reason for migrating. Employment and family were each selected by 20% of participants. Additionally, marriage or joining a partner was chosen by 5% of participants. Crisis-related reasons

for migration, such as climate change or natural disasters, war, or persecution, were each selected by 5% of participants. These results indicate that most participants migrated for reasons related to improving quality of life, education, employment, or family connections.

4.2.4 Personal Data

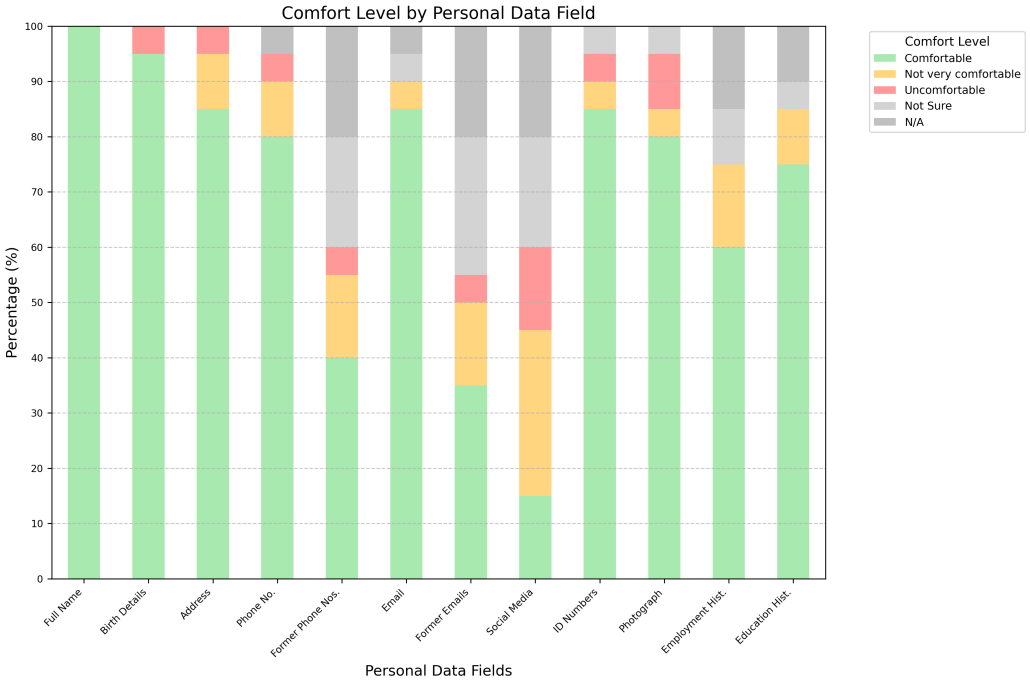


Figure 4.4: Feeling about personal data

All participants were comfortable sharing their full name. This is likely because names are routinely used for identification in almost all contexts and are considered a basic detail that any immigration authority would require.

Most participants (approximately 95%) were comfortable sharing their date and place of birth. However, a small percentage (around 15%) expressed concerns about sharing details such as their phone number or address, while the majority were still comfortable providing this information. This may be because participants trust immigration authorities to some extent and recognise that such basic details are necessary for verification purposes.

Approximately 20% of participants were either not very comfortable or uncomfortable sharing their former phone numbers or former email addresses, and about 20–25% were unsure about sharing this type of information. Around 20% marked "Not Applicable," which could indicate either that the question was not relevant in their context or that they chose not to answer it. The lower number of participants who felt comfortable sharing this information may be because many people no longer have access to their former email accounts or phone numbers and may have even forgotten them. In some cases, unused mobile numbers or free email addresses are recycled, which can create confusion if immigration authorities attempt to use outdated contact details for verification or other purposes.

Only around 15% of participants were comfortable sharing their social media profiles, while approximately 45% were either not very comfortable or uncomfortable, and about 20% were unsure. This is understandable, as people often share personal and family-related content, including photos and videos, on social media, as well as posts that reflect their social or political views. Participants may feel uneasy about immigration staff accessing this information or requiring social media account details. Another 20% mentioned it was not applicable to them, which could indicate that they either do not use social media or were not asked to provide this information in their context.

Participants were generally comfortable sharing their ID, passport, or licence numbers and photographs, although around 10–15% reported feeling not very comfortable or uncomfortable with sharing this data.

Approximately 60–75% of participants were comfortable sharing their employment history and educational history, while about 10–15% were not very comfortable providing this information.

4.2.5 Sensitive Data

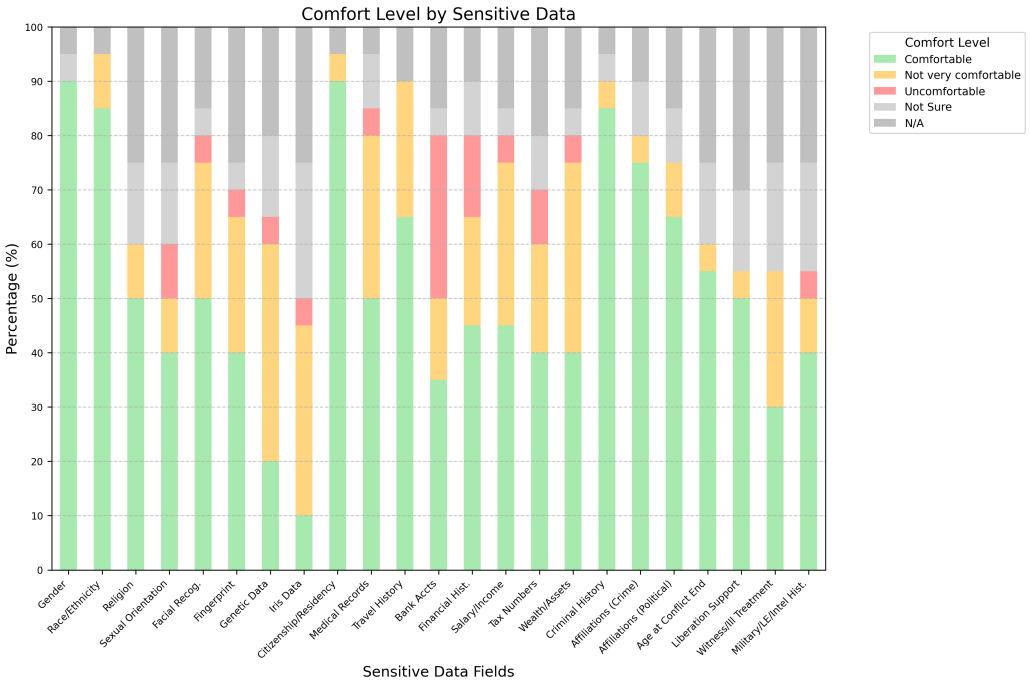


Figure 4.5: Feeling about sharing sensitive data

When asked about providing gender information, almost all participants reported feeling comfortable. A small percentage (5%) were unsure. This may be because many people consider gender a basic piece of personal information that authorities might need for identification and verification purposes.

About 85% of participants were comfortable sharing their race or ethnicity information. Around 10% did not feel very comfortable, and 5% indicated that it was not applicable to them. This could mean either that they were not required to provide this information or that they chose not to answer.

Questions about religious beliefs or sexual orientation saw more varied responses. Approximately 40–50% of participants were comfortable sharing this information, while 20–35% indicated they were either not very comfortable or uncomfortable. Around 15% or fewer were unsure, and about 25% mentioned it was not applicable. This could mean they were not required to provide this information, or they preferred not to answer the question.

For biometric data such as facial recognition, fingerprints, genetic information, or iris scans, the majority of participants reported feeling not very comfortable. A small number of participants expressed clear discomfort, while only a few reported feeling comfortable sharing such data. Around 15–25% mentioned it was not applicable to them, possibly because they were not required to provide this information or chose not to answer. People may perceive biometric data as highly personal and closely tied to their bodies, leading to less comfort in sharing it.

When it came to sharing data related to citizenship or residency status, around 90% of participants felt comfortable. This may be because people understand that immigration authorities must establish an individual's nationality or legal status before allowing them to enter or stay in a host nation.

Regarding data related to criminal history or affiliations with political groups or governments with criminal behaviour, more than 65% of participants indicated they were comfortable sharing this information. A small proportion (5–10%) reported feeling uncomfortable. The majority of participants were students or individuals with stable jobs who were not from crisis backgrounds. This may be one reason they felt relatively comfortable sharing information about criminal history or political affiliations.

In the case of sensitive data such as medical history, financial status, or personal wealth, a larger portion of participants (25–45%) reported feeling not very comfortable or uncomfortable. Around 5–10% were unsure. People may understandably feel uncomfortable sharing medical history because they consider it very private. Discomfort in sharing financial or wealth-related data may stem from concerns about personal risk or security.

About 40–55% of participants felt comfortable sharing information about their age when conflicts ended in their home country, any support they gave to liberation organisations, or their history in military or intelligence organisations. Around 10% were unsure. Approximately 25–30% mentioned it was not applicable to them, possibly because such data was not required from them or they chose not to answer these questions.

When asked whether they had been a witness to or participated in the ill-treatment of people, only 30% of participants felt comfortable answering. About 25% were not very comfortable, 20% were unsure, and 25% indicated it was not applicable to them. This could be because they were not asked this question or chose not to respond.

4.2.6 Marriage or Relationship Data

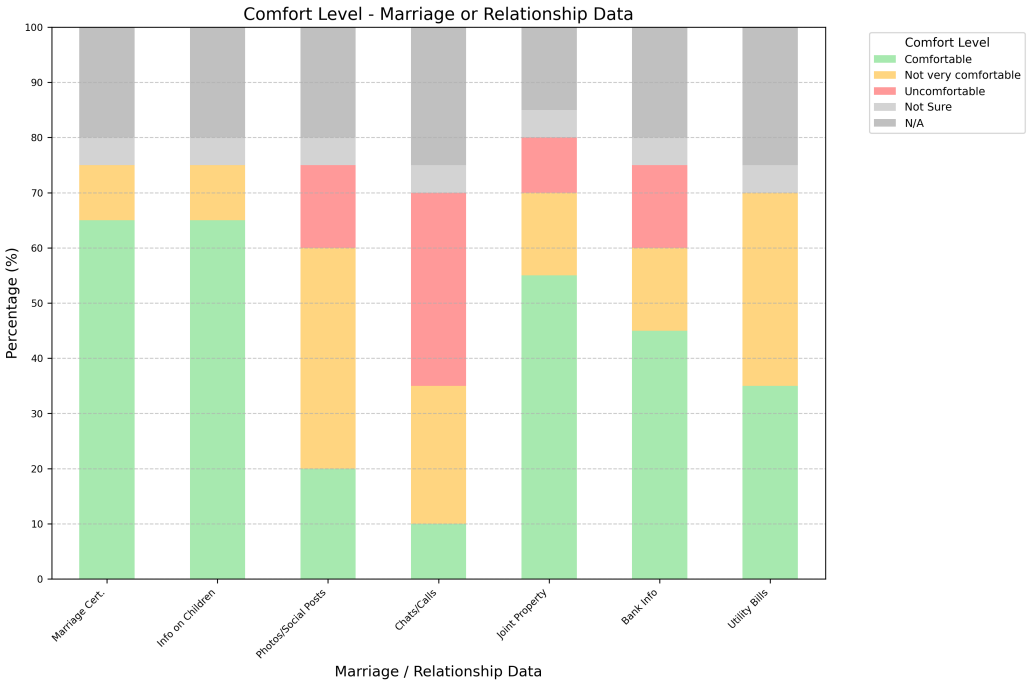


Figure 4.6: Feeling about sharing marriage or relationship data

About 65% of participants were comfortable sharing data such as a marriage certificate or information about children they have with their partner. Around 10% were not very comfortable sharing this information, and about 5% were unsure.

Approximately 60% of participants were either not very comfortable or uncomfortable sharing photos or social media posts related to their relationship, as well as chat or call logs. This is understandable, as many people prefer to keep private the conversations they have with family or loved ones, or photos of personal moments. Only about 10–20% felt comfortable sharing such information. Around 20–25% indicated that this question was not applicable to them, which could mean either that immigration authorities did not ask them for this information or that they chose not to answer.

Around 45–55% of participants were comfortable sharing data related to joint properties or financial information, while 25–30% were either not very

comfortable or uncomfortable doing so. This discomfort may stem from the fact that such information is linked to finances and revealing it could raise security or privacy concerns.

When asked specifically about sharing jointly held utility bills, 35% felt comfortable, while another 35% were not very comfortable. Again, the hesitation may be due to the financial nature of this information and concerns about security or privacy.

4.2.7 Concerns and Opinions Related to Access and Storage

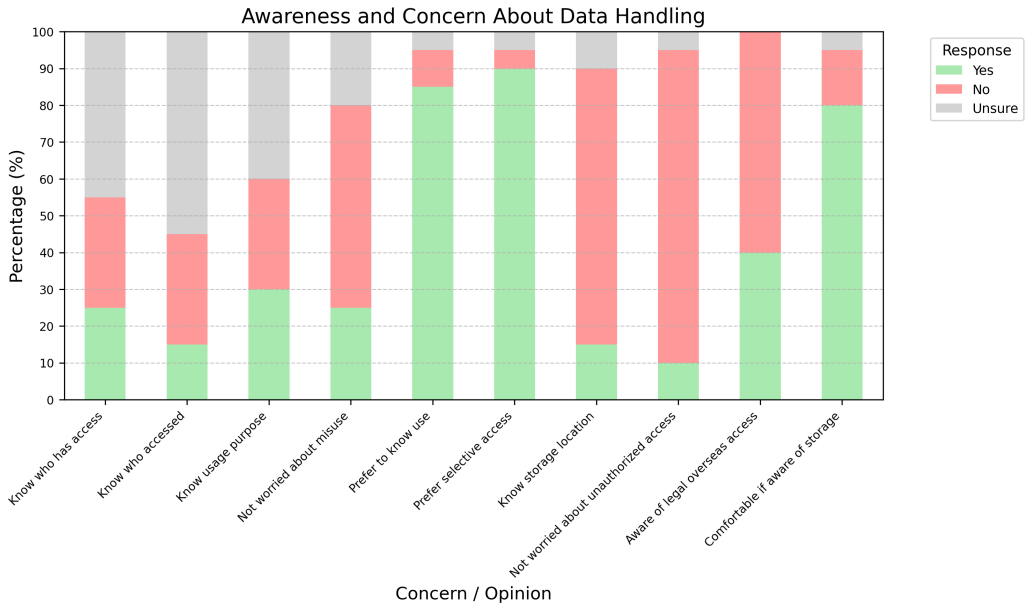


Figure 4.7: Awareness and concern about data handling

Around 30% of the participants were not aware of who has access to their data or the purposes for which it is used. About 15–25% said they knew, while 40–55% were unsure.

Between 55% and 75% of participants were worried about misuse of their data or unauthorised access. Only 10–25% reported not being worried.

More than 85% of participants preferred to know how their data is used and wanted control over who can access it. Around 75% did not know where

their data was stored or were unaware that overseas governments might have legal access to data stored in certain jurisdictions. However, 80% said they would feel comfortable if they knew where their data was stored.

4.2.8 Access to Internet and Opinion on Data Storage Mechanism

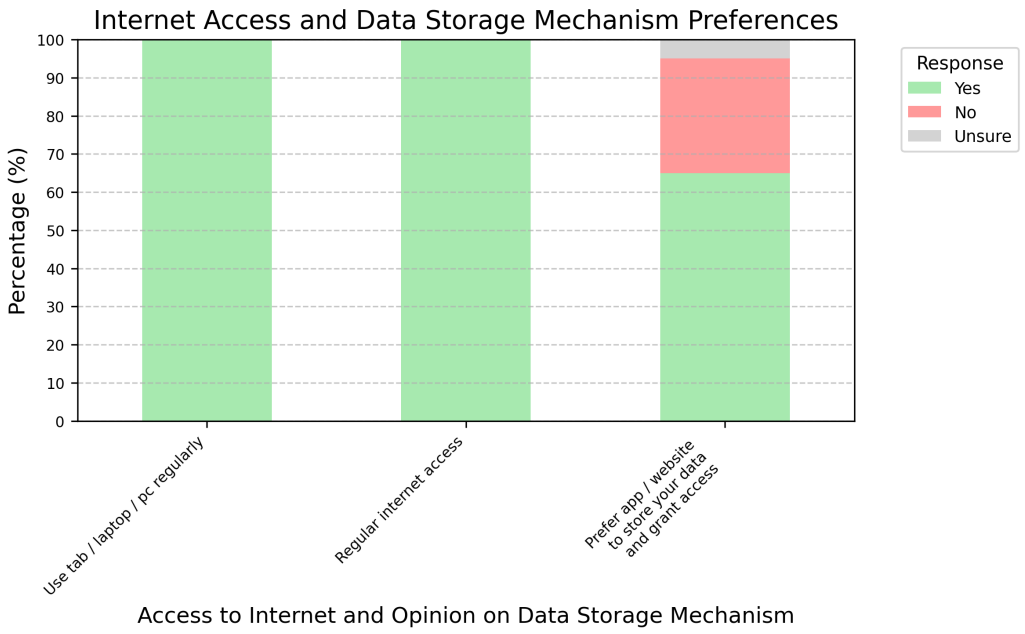


Figure 4.8: Access to the internet and opinion on data storage mechanism

All participants responded that they have a device with regular internet access for browsing. When asked whether they preferred a website or an app that would store their data and allow them to control access permissions, 65% answered yes, 30% said no, and 5% were unsure. The participants who answered no or were unsure might have concerns about trusting online data storage, possibly due to growing fears over data breaches and privacy issues.

4.2.9 Blockchain Knowledge and Trust in Blockchains

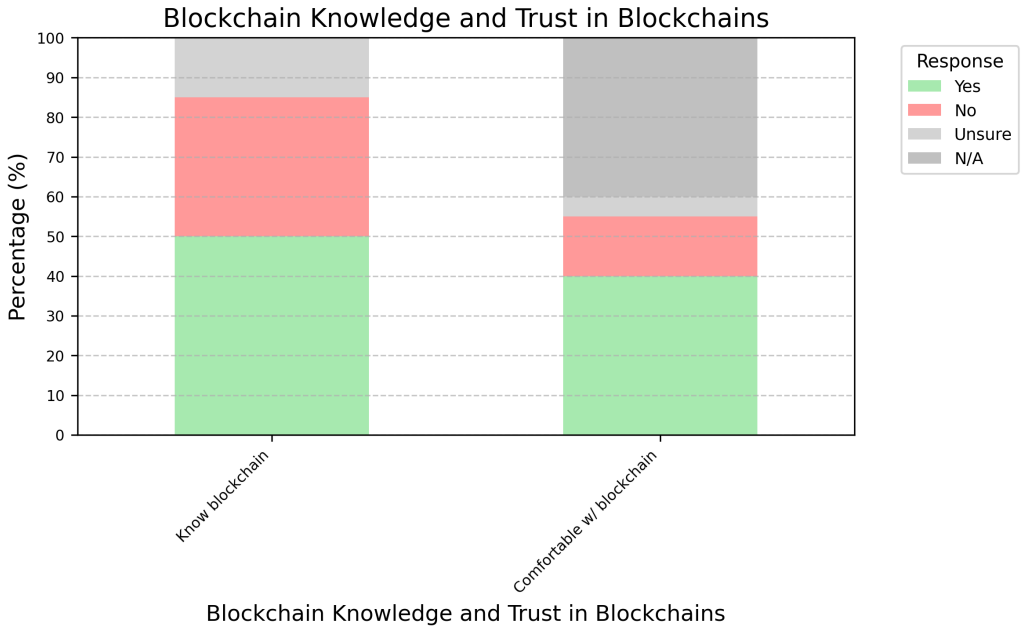


Figure 4.9: Blockchain knowledge and trust in blockchains

When asked about their knowledge of blockchain, 50% of participants reported having some familiarity with the technology, 35% indicated that they did not know about it, and 15% were unsure. Although distributed ledger technologies (DLTs), such as blockchain are well known among IT and finance professionals, primarily in relation to cryptocurrencies or through negative media coverage, it remains relatively unfamiliar to the general public, despite having existed for some time. This may explain why a substantial portion of participants are not familiar with it.

When asked if they would feel comfortable using a solution designed to help protect their personal data and cultural heritage information, 40% said they would welcome it, 15% said no, and 5% were unsure. Notably, 40% of responses were marked as not applicable, which could indicate that these participants chose not to answer the question. This suggests that a solution based on blockchains might require some introduction or explanation in order to be trusted by the general public.

4.2.10 Having No Control over Personal and Cultural Heritage Data

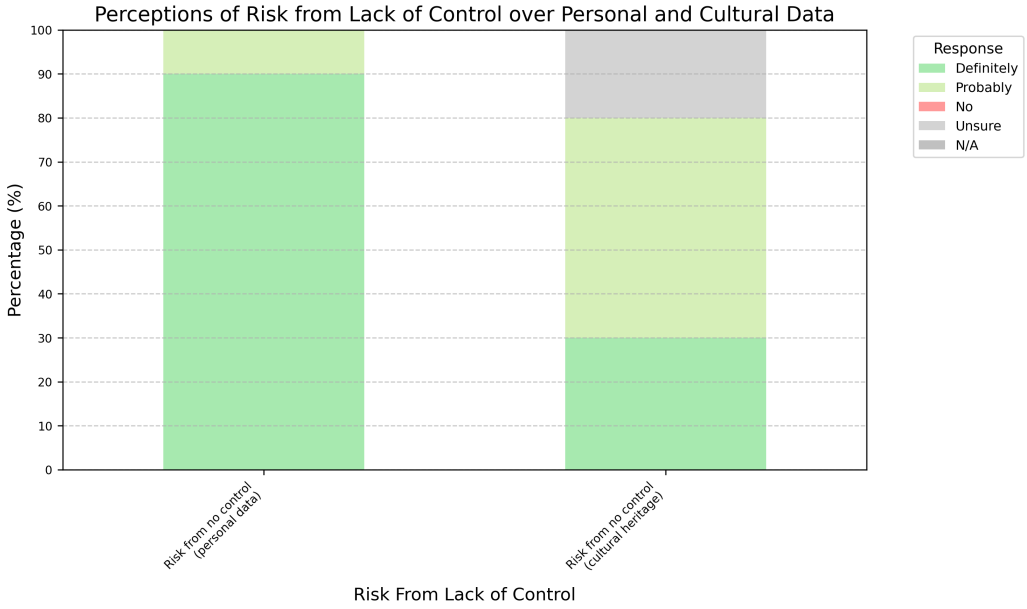


Figure 4.10: Having no control over personal and cultural heritage data

When asked about the risks of having no control over personal data, almost 90% of participants answered "Definitely" and 10% said "Probably." This result is understandable, as people often have a general awareness that personal information can be misused, even if they may not fully understand exactly which types of information can be exploited or to what extent.

However, when asked the same question regarding cultural heritage data, only 30% responded "Definitely," while 50% said "Probably," and 20% were unsure. The relatively lower sense of importance may come from the perception that cultural heritage information is mostly public and less personal, and participants might not realise how it could impact them or future generations.

Despite these differences, participants clearly recognised that having control over their data, whether personal or related to cultural heritage, is very important.

4.2.11 Importance of Preserving Cultural Heritage Information

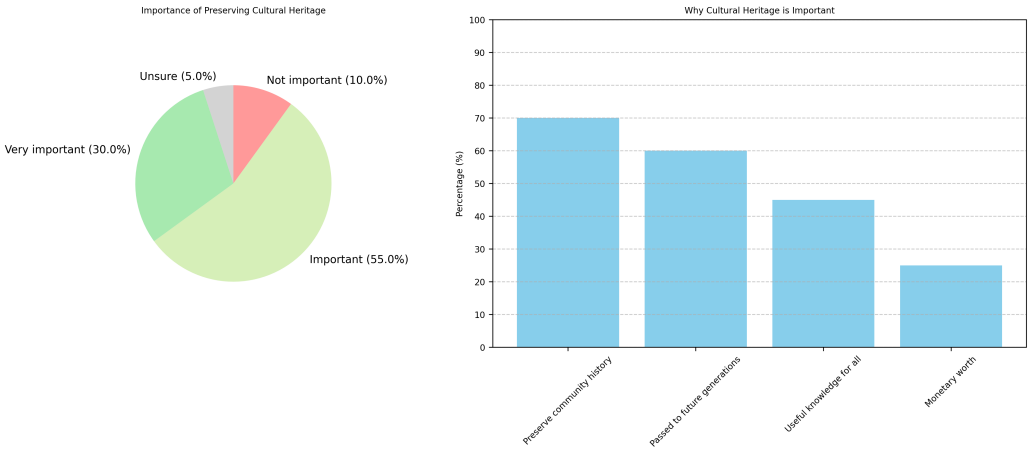


Figure 4.11: Importance of preserving cultural heritage information

Participants were asked whether they believe preserving cultural heritage information is important. The pie chart summarises their responses. Among the participants, 30% indicated that preserving cultural heritage is "very important" to them, while 55% stated it is "important". Conversely, 10% said it is "not important", and 5% were "unsure". These results suggest that the majority of migrants consider the preservation of their cultural heritage information to be important.

Participants were then asked why they believe preserving cultural heritage information is important. This was a close-ended, multiple-response question. The most frequently selected reason (70% of responses) was to preserve the community's history. Furthermore, 50% indicated that they wished to pass down traditional knowledge to future generations. About 45% believed that cultural heritage contains unique or important knowledge that could be useful for everyone, while 25% mentioned its potential monetary value. These findings indicate that while some participants see monetary worth in preserving cultural heritage information, the majority value it primarily for historical preservation and intergenerational knowledge transfer.

4.2.12 Types of Knowledge Intended to Preserve

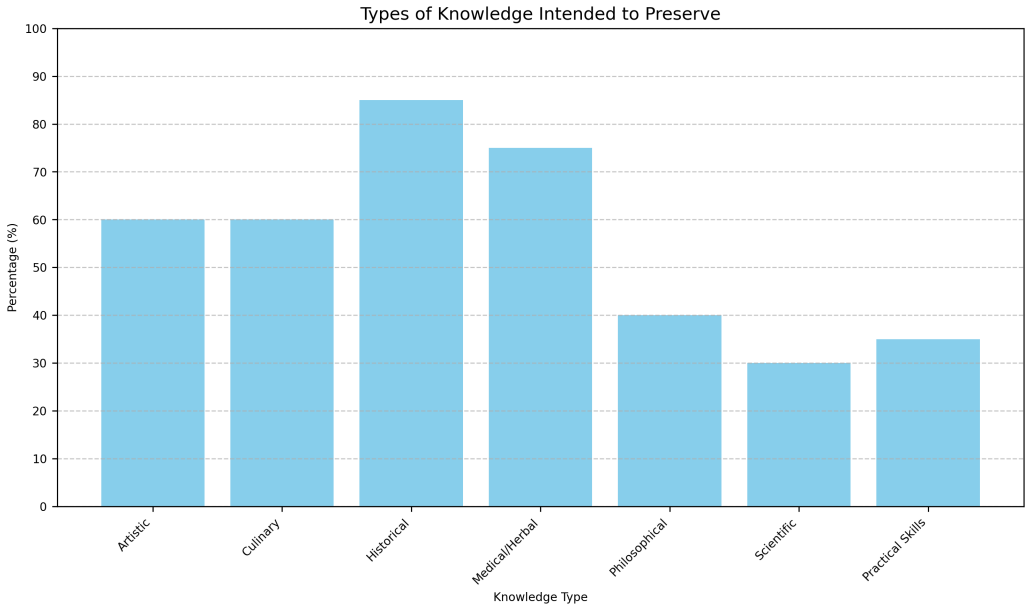


Figure 4.12: Types of knowledge intended to preserve

Participants were asked which types of cultural or traditional knowledge they intend to preserve. This was a close-ended, multiple-response question. A significant proportion of participants indicated that historical and medical or herbal knowledge from their cultures should be preserved. Furthermore, 60% of participants believed that artistic and culinary knowledge were important to preserve. Between 35% and 40% showed interest in preserving philosophical knowledge and practical skills such as woodwork or masonry. Approximately 30% of participants indicated that scientific knowledge should be preserved.

A considerable importance was placed on preserving historical knowledge. This may reflect the concern that when migrants move from their country of origin to a host country, there is a high risk of their cultural history being lost over time, particularly among future generations. This could explain why 85% of participants considered historical knowledge important to preserve.

The importance given to medical or herbal knowledge may be attributed to the fact that traditional medicines are still widely used, especially within

Asian communities. Similarly, culinary skills remain part of daily life and contribute to maintaining cultural identity, which explains their perceived importance. Traditional arts may also help individuals identify with their cultural heritage and maintain a connection to their country of origin.

In contrast, scientific knowledge was regarded as less important, possibly because science and technology evolve rapidly, rendering older knowledge potentially obsolete. Practical skills may also be considered less essential in the context of migration, as such skills may not be required or relevant in the host country.

4.2.13 Vulnerabilities to Exploitation of Cultural Heritage Information and the Importance of Preservation

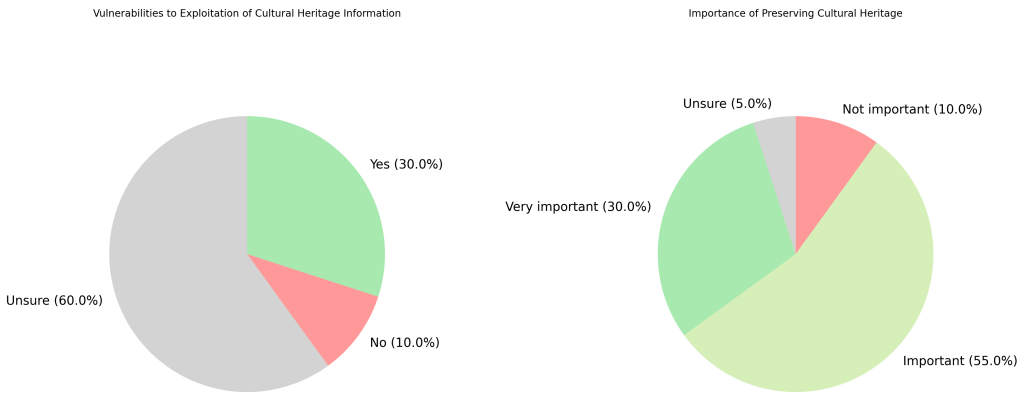


Figure 4.13: Vulnerabilities to exploitation of cultural heritage information and the importance of preservation

The pie chart on the left depicts participants' responses to the question of whether they believe their cultural heritage information is misused or exploited by others. The majority (60%) reported that they were unsure, while approximately 30% said yes and 10% said no.

In contrast, when participants were asked whether they preferred to digitise cultural heritage information and store it securely, with access managed

either by themselves or their community (as shown in the pie chart on the right), around 85% expressed support for this approach. About 10% considered it was unimportant, 5% were unsure.

Although a large proportion of participants were uncertain about whether their cultural heritage information is being exploited, the findings indicate that most still consider it important to digitise and preserve this information. These results suggest that, despite concerns or uncertainties about misuse, there is a strong preference for secure, digital methods of storing cultural heritage information.

4.2.14 Preferred Digital Formats for Preserving Cultural Heritage Information

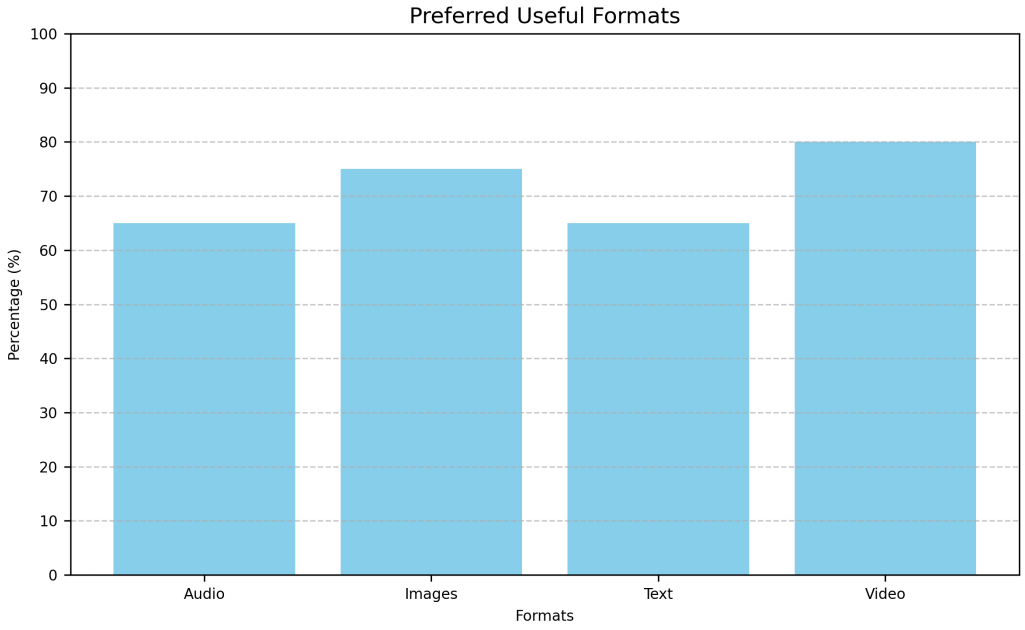


Figure 4.14: Preferred digital formats for preserving cultural heritage information

Participants were asked which digital formats they consider most suitable for preserving cultural heritage information. This was a close-ended question allowing multiple responses. The four options provided were video, images,

audio, and text. All formats received substantial support, with at least 65% of participants selecting each. Video emerged as the most preferred format, with 80% of participants choosing it, followed by images, which were selected by 75% of participants.

4.3 Analysis of Open-Ended Questions

This section presents the analysis of the open-ended questions included in the questionnaire. It should be noted that some open-ended questions, especially those posed as sub-questions, were left unanswered by participants. The analysis in this section focuses only on the responses provided to open-ended questions that are relevant to the objectives of this thesis.

4.3.1 Personal Information – Any Other Details Collected

As part of a sub-question related to personal data collected by immigration authorities, participants were asked whether any additional personal information had been requested that was not covered in the questionnaire. One participant indicated that they were asked to provide a copy of their old passport with visa stamps, as well as an attested copy of all pages of their current passport.

4.3.2 Desired Features in a Personal Data Management System

In response to the open-ended question, "What features would you like in a system designed to protect and manage your personal data?", 12 out of 20 participants provided answers. Several responses shared similar points. Based on their input, the following key features were identified:

- *Consent-Based Access* – Most participants expressed a strong preference for the ability to approve or deny access requests to their personal data.
- *Secure Access Control* – Participants emphasised the need for secure access, ideally through password protection or similar authentication methods.

- *Data Control and Flexibility* – Many participants indicated that they would like the ability to add or remove personal or sensitive data and update existing data as needed.
- *Update Notifications* – One participant suggested that when their data is updated, they should have the option to send individualised notifications (based on their preferences) to any organisations currently using that data.
- *Access Notifications* – Another participant recommended a notification feature, preferably via email, whenever someone accesses their data.
- *Automatic Data Disposal* – One participant proposed a feature that would allow their data to be automatically destroyed after it has been used.
- *Ease of Use* – One participant mentioned that the application should be user-friendly.

The above responses indicate that participants place high value on security, control, and transparency when it comes to managing their personal and sensitive data.

4.3.3 Ideas on Data Privacy and Having Control of Their Own Data

For the question, "Do you have anything you would like to share about data privacy, having control over your own data, or any other topics related to the questions above?", six out of 20 participants provided responses.

Most participants emphasised that it is important to safeguard data privacy and maintain control over one's own data. They expressed concerns that, without such control, individuals are vulnerable to risks and exploitation, particularly in light of frequent data breaches.

One participant noted that they were aware their data was being shared more widely than they would prefer, yet they felt they had little control over this process. Despite this awareness, they often found themselves required to share personal data in order to access essential applications.

Another participant mentioned that while studying migrant populations is a good way to examine data privacy issues, privacy concerns affect everyone. They emphasised that a system designed to safeguard privacy would benefit all individuals, not just migrants.

Furthermore, one participant highlighted the need to communicate how data is stored and managed in simpler language. They noted that many older individuals may become confused by technical terminology, which can hinder their understanding of their rights and lead to miscommunication.

4.3.4 Countries or regions the participant would prefer or not prefer to store their data

Around 25% of the participants mentioned that they had no such preference. Another 20% left it unanswered or indicated that it was not applicable to them.

Among the participants who responded, many said they would be comfortable if their data were stored in countries with strong data protection laws in place, such as the General Data Protection Regulation (GDPR). One participant mentioned that they would not be comfortable if their data were stored anywhere outside New Zealand, where they currently live. Other participants indicated that they were not comfortable having their data stored in certain countries. Countries such as China, India, Israel, and the US were mentioned by more than one participant.

4.3.5 How Cultural Heritage Information Is Being Exploited

Participants were asked the question, "Do you think your cultural heritage information is misused or exploited by anyone? If yes, how?" Out of the 20 participants, six responded to the open-ended question.

Manipulation of history and cultural misinterpretation emerged as common concerns among participants. One participant specifically believed that Hollywood and the film industry are at the forefront of such misrepresentation and exploitation.

Several participants stated that their cultural information is being exploited by large industries, such as the medical and fashion sectors, which use their cultural knowledge without permission or authorisation.

Another participant mentioned that certain types of knowledge, traditionally intended for use only within their culture or specific cultural groups, are becoming universalised. They expressed concern that such widespread use can harm both their own culture and those who adopt the knowledge without permission, especially when it is used for profit.

4.3.6 Opinions on Digitally Preserving Cultural Heritage Information

When asked, "Do you have any opinions you would like to share about digitally preserving cultural heritage information?", four participants responded out of the 20.

The participants expressed the general belief that cultural heritage information is important to preserve, particularly historical information. They highlighted that having such information digitised makes it easier to share with others and promotes learning. They also emphasised that valuable knowledge should be protected from damage or loss.

One participant noted that it is crucial for communities to share their own stories in their own words. They emphasised that community members know their culture best and should decide how it is shared. While some cultural knowledge can be made public, other parts might be private or sacred and should remain within the community. They added that digital tools can help younger generations learn about their culture, language, and traditions in new ways, helping them stay connected to their identity.

Another participant observed that cultural heritage can sometimes be harmful, particularly when individuals unfamiliar with the culture do not fully understand it. They expressed concern that cultural information is often treated as a commodity rather than with the seriousness it deserves. They suggested that there should be mechanisms to restrict access to certain cultural knowledge. Specifically, they proposed that if even one member of a cultural group designates certain information as private, it should not be made public, regardless of how many others consider it public. This restriction should hold as long as there is some evidence or justification within the culture for keeping that information private or specific to the group.

One participant also stressed the importance of safe digital access to cultural information and ensuring its protection. They pointed out that in past conflicts, physical cultural resources such as libraries and museums have

been destroyed, and that digital storage can help safeguard this information for the future.

4.4 Analysis of Brief Conversations That Occurred During the Surveys with the Participants

During the survey, it was occasionally necessary for the researcher to clarify certain questions and answers, as well as respond to queries from participants, often prompted by their curiosity to learn more. During these moments, short conversations took place regarding the protection of privacy and the preservation of cultural heritage information. Some of the information shared by participants was useful for the study. Key points from these conversations are summarised in this section. The information shared during these conversations and included in this study was strictly within the scope of the questionnaire and interviews approved by the university's ethics committee.

4.4.1 Participant 4

During the survey process, one participant shared more detailed views in a brief conversation. They expressed that they were generally comfortable with sharing personal data, including contact information, education, and employment history with immigration authorities, mentioning their trust in the host government as the reason. The participant further stated they were comfortable disclosing sensitive data, including their religion and sexual orientation, as well as biometric data like fingerprints, facial recognition, and genetic information. Although they were not entirely comfortable with sharing iris data, they indicated they would still comply if required. Interestingly, their views were influenced by a dystopian film, which made them reflect on potential risks despite their willingness to share. The participant emphasised that while they were open to sharing a broad range of personal data, they believed the immigration or government should practise caution and reconsider the long-term implications, as "things can go wrong." They suggested that the data should be destroyed once it has fulfilled its purpose. The participant mentioned that they were not comfortable with sharing political opinions, private chat history, or family-related information, indicating clear

limits in their perception of acceptable data sharing.

4.4.2 Participant 8

Another participant mentioned that they were comfortable with sharing biometric information with migration authorities, specifically referencing their migration to the UK. They mentioned they had confidence because they believe the UK follows the GDPR and similarly strict privacy laws in other jurisdictions. On the contrary, they were uncomfortable sharing such sensitive information with countries or authorities lacking robust privacy protections.

They further stated that the immigration authorities clearly communicated the purpose of data collection and the duration of data storage, which contributed to their willingness to share information. They preferred to provide data only through formal and secure platforms and trusted that the authorities handling their data were well-trained in privacy laws, reducing concerns about misuse. Furthermore, they believed that even if someone intended to misuse the data, the information shared would not be sufficient to cause harm. Regarding unauthorised access, the participant was not concerned due to their belief in strong security measures protecting their data. Although open to using mobile applications or websites for data storage with controlled access, they preferred to provide data manually on a need-to-know basis rather than continuously storing it online.

The participant also noted that sharing personal data is often mandatory for migration, leaving little choice but to comply. When asked whether losing control over their cultural heritage information could be a disadvantage to them or their community, the participant initially responded "No" but later changed their answer to "Probably" after some explanation by the researcher.

When asked about blockchain technology, the participant mentioned that they did not trust cryptocurrencies. However, after a brief explanation of blockchain technology was given, the participant showed interest in it. Their background in finance likely contributed to their familiarity with and understanding of privacy and data protection issues.

4.4.3 Participant 17

Due to scams reported in certain countries, they were concerned and did not want their data to be stored there, giving India and Thailand as examples. However, more than where the data was stored, they cared about who

had access to it. They were uncomfortable sharing financial, banking, and property-related information but felt they had no choice.

When it comes to a system, their preference was for one that notifies them when their data is accessed, provides a reason, and asks for permission, allowing them to grant or deny access. They preferred that access be granted on a case-by-case basis, as they were concerned it could be misused by those handling it. They wanted a system where data is stored in a personal data vault.

After being informed about blockchain features, they were comfortable with the idea of storing their data on the blockchain. Regarding cultural heritage information, they were fine with it being used for personal or non-commercial purposes but opposed its use for commercial gain.

4.4.4 Participant 18

This participant had a strong understanding of privacy due to their line of work. They mentioned that if a platform were secure, they wouldn't mind providing sensitive biometric details. They cared less about where data is stored and more about encryption and privacy protocols, feeling more comfortable with regions where laws such as the GDPR are in place.

They expressed concern about identity theft and were particularly cautious about sharing details of family members, citing frequent data breaches in New Zealand. They were unsure which third parties might receive their data, either from immigration authorities or agents handling documents, and worried it could be sold to unauthorised parties. The participant preferred a feature that would notify them if their data was accessed.

They shared a negative experience where an immigration consultant processing their immigration documents accessed their family's bank accounts without consent. They preferred a system allowing them to authorise a third-party company, ideally involving a human representative and protected by Non-Disclosure Agreements (NDAs), to manage their credentials.

Initially, they were not concerned about others accessing their cultural heritage data. However, after learning how communities and cultures have been exploited for profit, they expressed interest in preserving cultural heritage data and having control over its access.

After learning how blockchain works, they showed interest in using it to store personal and cultural heritage information.

4.4.5 Participant 19

The participant was a community worker who was themselves a migrant and had been working extensively with migrants and migrant-related organisations. They were not comfortable sharing most of their personal and sensitive data but mentioned that they had no choice but to do so during the migration process. The same applied to family-related data. The participant was aware that data stored in the cloud can be accessed by third parties (e.g., governments) without the knowledge or consent of the individuals to whom the personal data belongs.

According to the participant, refugees often do not have documents such as passports, birth certificates, or licences with them, and these are frequently reissued during the resettlement process. Additionally, refugees are often unlikely to use their previous contact details. The participant mentioned that for migrants, especially refugees who have had traumatic experiences, going from one government or settlement-related organisation to another and repeatedly retelling their stories is very difficult.

The participant also stated that resettlement organisations had been discussing the idea of storing all migrant data in a centralised location, accessible by various organisations. According to the participant, it is likely that the data gathered from migrants is not used by just one organisation but can be accessed by multiple organisations.

Initially, the participant did not understand why there is a risk to migrant cultural heritage information; however, after explanation, they understood. They also shared personal experiences that highlighted the value of preserving cultural heritage information.

They were not aware of blockchain technology or how it worked and were initially sceptical about it. They asked questions such as how it functions, where the data would be stored, and whether it could be exploited by others or even by the developer. After the features of blockchain technology were explained, along with how it operates and how the research-based prototype would be built, they became more comfortable with the idea. They were particularly concerned about all participants in the blockchain network storing a copy of the data. However, once it was clarified that, although participants may hold the data, they cannot access it due to measures like encryption, their concerns were eased.

4.5 Summary of Results

The findings from both the survey and interviews reveal important insights into participants' demographics, motivations for migration, attitudes towards personal data sharing, and perspectives on cultural heritage preservation.

Most participants were middle-aged, likely due to the recruitment process, which relied heavily on campus networks and personal contacts. Almost half of the participants originated from Sri Lanka, with the rest representing a further eight countries, contributing to a degree of cultural diversity within the sample. Education and the pursuit of a better quality of life emerged as the primary motivations for migration, while employment, family, and crisis-related factors played smaller roles.

The consistent pattern across the survey and interviews was the participants' discomfort with sharing personal and sensitive data. Although many acknowledged that sharing data was unavoidable for the migration process, they expressed a preference for minimal data collection, destruction of data after use, and transparency mechanisms such as permission requests or notifications when information was accessed. Several participants mentioned that they would have greater trust if compliance with privacy regulations such as GDPR were in place, while others expressed concerns about identity theft.

A minority of participants stated that they would even consider delegating the supervision of their data to a trusted third party. The comfort levels varied depending on the type of data in question. Basic identifiers such as names, dates of birth, gender, and citizenship details were generally not considered problematic by the participants; however, information relating to social media, biometric data, financial status, and medical history caused greater hesitation. Participants were generally more willing to share educational and employment histories, which may reflect the student and professional background of much of the sample. Regardless of these hesitations, most participants emphasised the importance of retaining control over their data and expressed significant concern about misuse or unauthorised access.

Only half of the participants were familiar with blockchain technology, of whom most had only heard of it and did not have much knowledge. While initially they were uncertain, when the technology and its advantages were explained, the participants were more open to the idea. Participants recognised

its potential value for protecting personal and cultural heritage-related data. Cultural heritage was widely recognised as important to preserve, especially when the risks of exploitation and loss across generations were explained. Historical knowledge, intergenerational transmission, and the safeguarding of artistic and culinary traditions were prioritised, while scientific and practical knowledge was seen as less critical. Participants also expressed concern that migration increases the risk of cultural destruction, reinforcing their support for secure, community-managed systems for the digitisation and preservation of heritage.

The overall results indicate mainly two concerns among participants. First, the need to strengthen protections around personal data and the parallel desire to preserve cultural heritage. Both the survey and interview findings point towards the potential for secure, transparent, and community-centred digital solutions, including blockchain-based systems, to address these concerns effectively.

Chapter 5

Design

5.1 Overview

This chapter discusses in detail how the immigration process currently works, how the proposed solution or prototype software operates, and its technical and usability aspects. Furthermore, it explains how the prototype software can help migrants securely store and share cultural heritage information.

5.2 Present Process

If someone wishes to migrate to another country, they are usually expected to submit documents to the immigration authorities of the host country. Based on these documents, the authorities will determine whether to allow the individual to migrate. Typically, a visa is granted to a migrant who is successful in the migration process. The documents required by the immigration authorities may vary depending on factors such as the migrant's country of citizenship, character, financial status, background, and purpose of the visit. However, in general, the immigration process usually follows the steps outlined below.

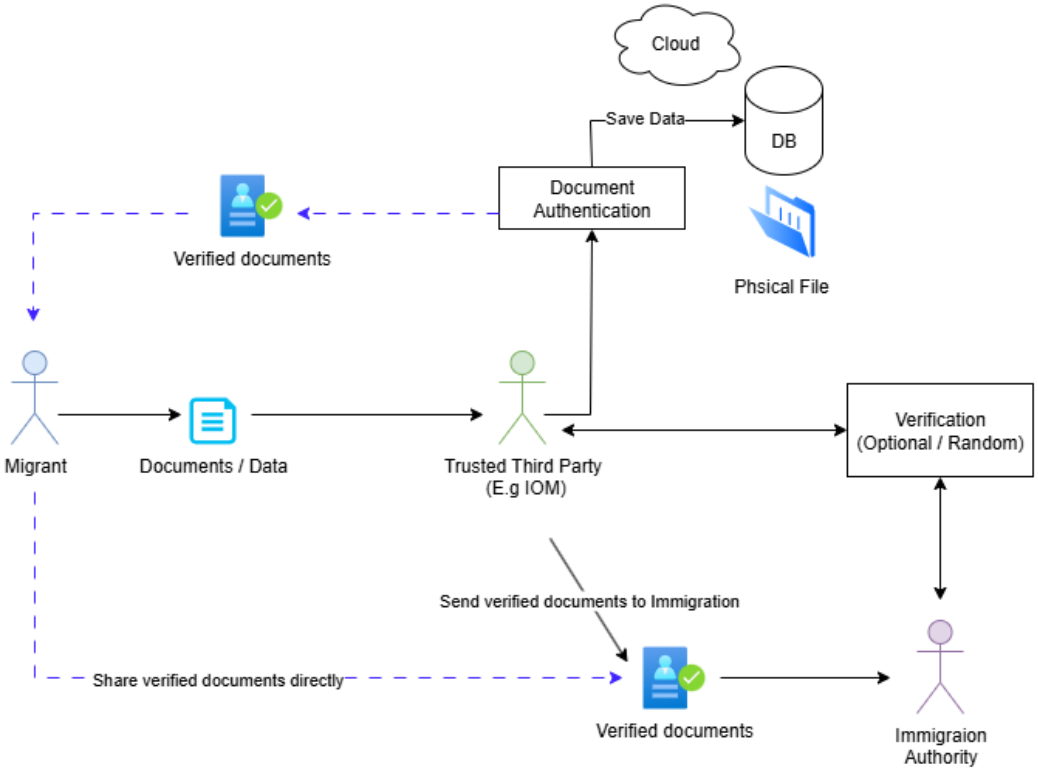


Figure 5.1: Present process

Initially, as shown in Figure 5.1, an individual seeking to migrate to a foreign country submits their documents to a third-party authority recognized by the immigration authority. Organisations such as the International Organization for Migration (IOM) and private service providers like VFS Global [40], which manage visa, passport, and consular applications on behalf of governments, are involved in the handling and verification of documents that often contain personal and sensitive information. This process involves verifying the validity of the documents or confirming their details with the issuing authority. Once the documents are handed over to a trusted third party, they are stored in the third party's systems while the verification process is conducted. These systems could include a private database, cloud storage, or physical files. After verification, depending on the procedures of the immigration authority, the trusted third party may either forward the authenticated documents directly to the immigration authorities, as indicated by the black lines, or return them to the migrant, who then submits them

to the authorities. This alternative process is depicted in the figure using dashed purple lines. In cases where the immigration authority has concerns regarding the authenticity of the documents, it may seek verification from the trusted third party.

In some cases, there is no third party involved. The migrant submits their documents directly to the immigration authorities, who carry out the verification process. However, nowadays, most immigration authorities prefer to rely on a trusted third party for verification rather than conducting it themselves. This is due to factors such as reduced workload and more thorough verification by entities with greater expertise in the process.

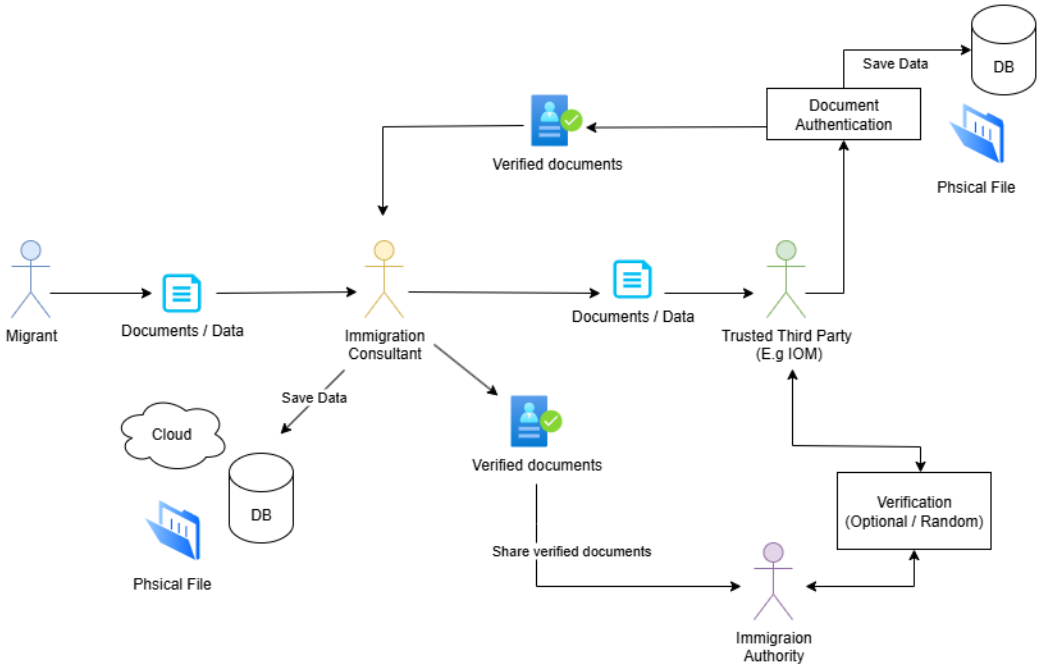


Figure 5.2: Present process with immigration consultant

Figure 5.2 depicts an alternative of this process, where an additional consultant may become involved. This could be an immigration consultant approached by the person planning to migrate, often students, workers, or individuals wishing to join their family abroad, in order to navigate the often complex migration procedures that require extensive verification. In this scenario, the immigration consultant acts on behalf of the migrant and has

access to a copy of their documents. In cases where immigration processes are simple and straightforward, the need for this intermediary can be eliminated.

5.2.1 The Issues in the Present Process and How to Improve It

There are a number of issues in the present process. One main issue is that data passes through too many parties, especially in cases where more than one entity is involved in the verification process (excluding the immigration authorities). When documents or data pass through multiple entities, it becomes difficult to track who has access to which information and which privacy or data protection guidelines are being followed. While it can be assumed that trusted third parties recognised by immigration authorities comply with the necessary data protection and privacy requirements, the same cannot always be said for immigration consultants. Immigration consultants are not necessarily required to be recognised or regulated by the immigration authorities. During the study, some participants also expressed concern about their data being handled by too many parties. In particular, one participant mentioned a negative experience with an immigration consultant in which their family's private data was at risk of misuse (see Chapter 4, Results). Therefore, eliminating unnecessary intermediaries in the process could help enhance the privacy and data security of migrants.

Another issue is that when data passes through too many entities, each is likely to retain a copy. Having multiple copies of the same data increases the risk for the data owner. The more copies there are, the greater the likelihood of a data breach or unauthorised access. Furthermore, when several copies of sensitive information are stored across different systems, it becomes very difficult to ensure consistency, monitor access, and enforce data protection policies. This not only raises privacy concerns but also weakens accountability, as it becomes unclear which entity is responsible in the event of data misuse or a security incident. As mentioned earlier, eliminating unnecessary intermediaries in the process could also help to minimise this risk.

Furthermore, data may be stored in one or multiple locations, depending on the IT systems used by the entity handling it. Data may be stored in physical files, within local databases, or, very often, in cloud-based systems. Depending on the geographical location of the stored data, as well as the data host provider's national laws, foreign entities could potentially

gain legal access to it. This situation places the data owner at significant risk, as data stored in cloud infrastructures may fall under the jurisdiction of multiple countries simultaneously. For example, data hosted on servers located abroad or managed by international providers could be subject to foreign surveillance or disclosure requests under that country's legislation. Such scenarios raise serious concerns about data sovereignty and the protection of migrants' sensitive personal information, especially in the case of vulnerable groups such as refugees. It is worth noting that, in the study, many participants mentioned that they would be comfortable if their data were stored in countries or regions where strict data privacy laws, such as the GDPR, are followed. Some participants also indicated that they were not comfortable with their data being stored in certain countries (see Chapter 4, Results). Taking these considerations into account, storing the data securely using strong encryption and following security best practices, including those outlined in regulations such as GDPR wherever feasible, and implementing a decentralised storage strategy could help mitigate this issue by reducing reliance on centralised service providers who are bound to countries or laws.

Sometimes, data collected from migrants may include information that is not strictly required by the immigration authorities, forcing the migrant to disclose personal details that are irrelevant to the migration process. For example, immigration authorities often need to verify that the person has sufficient funds to support themselves in the host country, which may require evidence of maintaining a certain amount of savings over a specified period. Currently, the only way to prove this is by sharing bank statements, which reveal all income and expenses, including private information. Similarly, verifying the date and place of birth may require sharing a birth certificate, which in some countries also contains sensitive information about the migrant's parents or grandparents. This over-collection of data infringes on privacy and is unnecessary for the migration process. The same sentiment was shared by many of the study participants. They preferred sharing only the data that was necessary (see Chapter 4, Results). Such issues could be mitigated by implementing a mechanism that allows verification of only the required details, giving migrants the option to share just the specific information needed rather than entire documents.

Presently, there is no mechanism for the data owner to know if or when their data is being accessed. This lack of transparency can create uncertainty and concern for potential migrants, who have no way of knowing how many times their information has been viewed or by whom. Although the data is

initially provided for a specific immigration purpose, once submitted it may continue to exist in the system and could potentially be accessed by others even after the migrant's immediate needs have been fulfilled. This raises significant privacy and accountability concerns, as the migrant loses control over how their sensitive information is handled. Some participants in the study indicated that they would prefer a feature notifying them whenever their data is accessed (see Chapter 4, Results). Implementing such a mechanism could provide greater transparency, build trust in the system, and help ensure that data is used only for its intended purpose.

The current process involves significant delays when verifying documents or credentials. For certain countries and visa types, immigration authorities or their appointed agents often need to contact every institution a migrant has attended or each organization they have worked for to ensure that the certificates or letters issued are genuine. Adopting digital credentials that can be verified for authenticity using digital signatures could significantly reduce these delays. This approach could not only facilitate migration but also benefit the general public who require document verification. Furthermore, when institutions or organizations are contacted by immigration authorities or their appointed agents, it informs those organizations that the individual is planning to migrate, potentially compromising the migrant's privacy. Using digital credentials with digital signatures would maintain verification integrity without compromising privacy.

5.3 High-Level Overview of the Proposed Solution

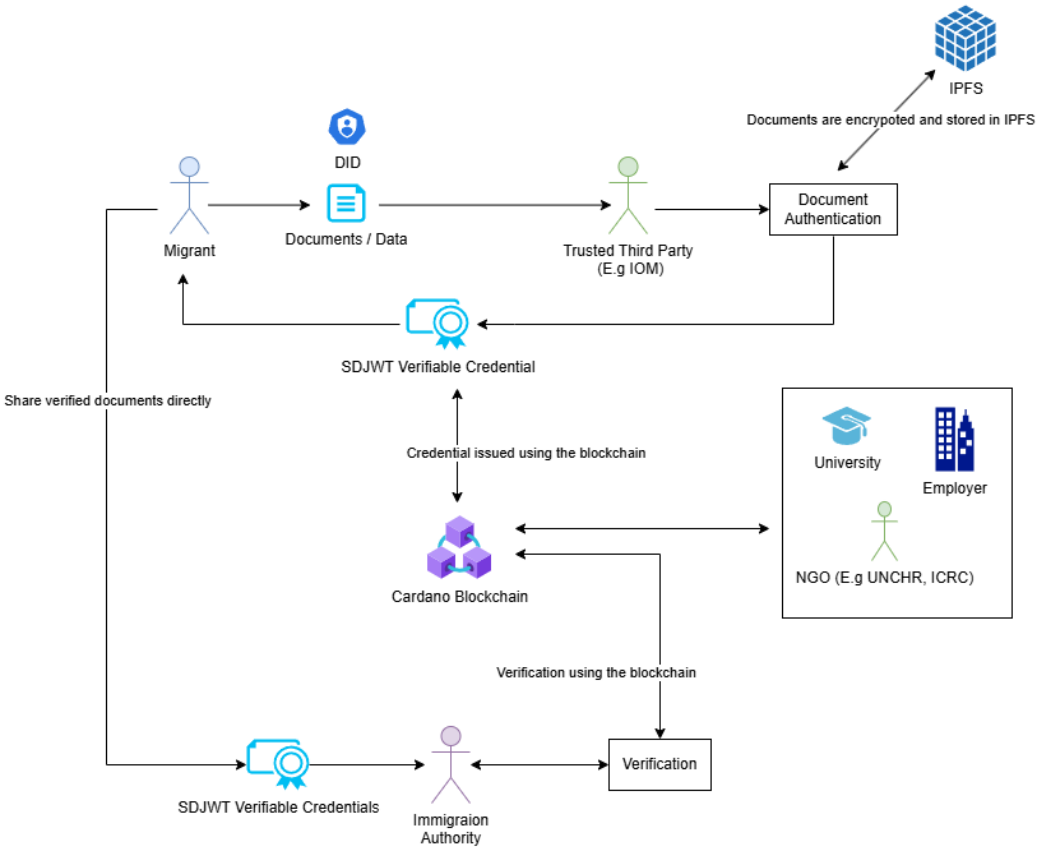


Figure 5.3: Proposed solution high level overview

The goal of the proposed system is to provide a mechanism through which the issues present in the current process can be eliminated or significantly minimized, while ensuring that immigration authorities are able to verify a migrant's data without compromising the quality of verification. In the proposed system, there will be three primary stakeholders: the potential migrant, the trusted third party, and the immigration authority. A fourth stakeholder, the immigration consultant, may also exist in the system and act on behalf of the potential migrant. The involvement of an immigration

consultant is often required due to the complex nature of certain immigration rules and the challenges associated with attesting and submitting documents to immigration authorities. In the proposed system, since document-handling requirements are reduced, the need for immigration consultants may be lower, except in cases where their expertise is required to interpret complex immigration regulations for potential migrants.

The proposed solution, depicted in Figure 5.3, will include a web application accessible to all stakeholders. This application is built on the Cardano blockchain and adopts the principles of Self-Sovereign Identity (SSI). According to Frontiers in Blockchain [41], "Self-Sovereign Identity (SSI) is an identity management model where individuals maintain control and custody of their identification attributes." In this model, individuals can generate their own verifiable credentials (VCs) or obtain them from trusted issuers, which can then be presented to verifiers. The paper further explains that the trust relationship between issuers and verifiers is established through registered cryptographic proofs.

Each migrant will have their own instance of the application. To run the prototype, a Preprod Cardano Testnet wallet is required. The application can be hosted individually for personal use or shared with family members or friends, provided that the user consents to storing credentials and decentralized identity (DID) information in the wallet. Each individual can create and publish a DID for themselves and subsequently share their DID, along with scanned PDF versions of their documents, via the trusted third party's application portal. These documents will be temporarily stored on the trusted third party's server. Once the documents are successfully verified, they will be moved to the InterPlanetary File System (IPFS), a decentralized storage space. If the document authentication process fails or, for any other reason, a verifiable credential (VC) cannot be issued, the documents will be deleted from the server.

The trusted third party is then responsible for performing the necessary document authentication. They may issue a verifiable credential (VC) to the individual whose documents were authenticated. The individual can then share this credential through the immigration portal. It is worth noting that they do not have to share the whole credential, but rather only the claims they wish to share (e.g. they can share only the current bank balance from their bank statement instead of all of the transactions in the statement). The immigration authority can verify the authenticity of the credential using digital signatures and, if needed, cross-check with the trusted third party. All

interactions occur via secure web portals.

Furthermore, using the same concept, the credential issuance process can also be applied by entities such as universities, employers, and NGOs to issue digital documents or credentials. In immigration scenarios, migrants often need to provide education certificates, employment records, or, in the case of refugees, documentation from organizations such as the United Nations High Commissioner for Refugees (UNHCR) or the International Committee of the Red Cross (ICRC). The same application could be used by these entities to issue digital credentials, which can later be verified by the relevant immigration authorities.

5.4 How does blockchain technology work?

Although blockchain was introduced in the Introduction chapter, it is useful to briefly recall its practical applications. Blockchains are commonly used with cryptocurrencies, with Bitcoin being a notable example, while platforms such as Ethereum and Cardano provide blockchain infrastructures that support cryptocurrencies and decentralized applications. In the introduction of this report, blockchain was described as a "distributed digital ledger technology used to record transactions across multiple nodes in a secure, transparent, and tamper-resistant manner."

To understand how blockchain operates, it is necessary to consider three important IT concepts: hash functions, encryption and digital signatures. These concepts form the foundation of blockchain security, ensuring the authenticity of transactions and the integrity of the ledger.

5.4.1 Hash Functions

Hashing is the process of applying a mathematical function, known as a hash function or hashing algorithm, to data in order to generate a much shorter fixed-length output that uniquely represents the original data. The resulting value, called the hash or hashed value, typically consists of alphanumeric characters. An important characteristic of hashing is that applying the same algorithm to the same data will always produce the same hash. According to the National Institute of Standards and Technology [42], even a very minor change in the input data results in a completely different hash. The probability of two distinct data inputs generating the same hash using the same

algorithm, known as a collision, is extremely low and generally considered negligible. Another important feature of hashing is that it is computationally infeasible to reconstruct the original data from its hashed value, even if the hashing algorithm is publicly known. Hashing algorithms are widely used in software engineering, particularly in areas related to security, data integrity, and database management. Common hashing algorithms include SHA-256, SHA-1, MD5, and SHA-3.

5.4.2 Encryption

Encryption is the process of protecting data by applying mathematical functions known as encryption algorithms. When data is encrypted, an algorithm is applied to the data together with an encryption key or a password. The encryption algorithm then generates a new, unreadable form of the data, known as ciphertext, based on the key provided. To recover the original data, the same encryption algorithm must be applied using the same key; otherwise, decryption will not be possible. A simple analogy is that of a padlock. A lock can only be opened with the same key that was used to secure it. Similarly, in encryption, the correct key must be used to retrieve the original data [43].

There are two main categories of encryption algorithms: symmetric and asymmetric. The description above refers to symmetric encryption, in which the same key is used for both encryption and decryption. Symmetric encryption is commonly used in processes such as user authentication, file protection, and secure data transmission. Examples of symmetric encryption algorithms include Advanced Encryption Standard-128 (AES-128) and AES-256.

Asymmetric encryption algorithms, however, operate using two distinct keys. A private key and a public key. The private key must be kept secret, while the public key can be shared openly. If data is encrypted using a private key, anyone with the corresponding public key can decrypt it to verify the origin of the data. On the other hand, if data is encrypted using a public key, only the holder of the private key can decrypt it and access the original content. Asymmetric encryption is commonly used in applications such as digital signatures and public key infrastructures (PKI). Examples of asymmetric encryption algorithms include Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), and Digital Signature Algorithm (DSA) [44].

To illustrate this process more simply, an analogy can be made with a newspaper subscription. Consider a newspaper that is distributed to all of its subscribers. Everyone who subscribes receives a copy of the newspaper. Suppose the newspaper includes a crossword puzzle and provides an address for readers to send their completed entries. When subscribers send their completed puzzles to that address, only the newspaper organisation can receive and open them. Likewise, in asymmetric encryption, anyone in possession of the public key can encrypt data that can only be decrypted by the corresponding private key held by the key owner. On the other hand, data encrypted with the private key can be decrypted or verified by anyone using the public key.

5.4.3 Digital Signatures

According to the National Institute of Standards and Technology (2023)[45], "A digital signature is an electronic analogue of a written signature that can be used to provide assurance that the claimed signatory signed the information." It further states that digital signatures are designed to be resistant to forgery. A digital signature is used to verify the authenticity of a message and to confirm that it originated from the intended sender.

In simple terms, the process works as follows: the sender first generates a hash of the message and signs this hash using their private key. The hash is signed instead of the entire message, as this minimizes the computational and transmission cost. The message and the signed hash are transmitted electronically to the receiver. Upon receipt, the receiver computes a hash of the received message using the same hash function and decrypts the signed hash using the sender's public key. If the resulting hash matches the one computed by the receiver, it confirms that the message was indeed sent by the legitimate sender and that the data has not been tampered with during transmission.

5.4.4 A Brief Overview of the Bitcoin Network

First, the Bitcoin network is studied to explain how blockchain operates. The network consists of nodes running the Bitcoin software, which are responsible for creating new transactions and validating existing ones.

In order to initiate a transaction, a wallet is required on the blockchain. For example, if person A sends 1 bitcoin to person B, the transaction is

broadcast to the entire network. The nodes then verify the transaction by checking conditions such as whether the sender has sufficient balance and whether the sender's digital signature is valid. Once verified, the transaction is added to a local pool of unconfirmed transactions, known as the memory pool or mempool. This is where transactions wait until they are added in a new block.

Special nodes called miners select transactions from their local mempool to include in a candidate block, which is a temporary block where transactions remain until they are successfully added to the blockchain. Miners then compete to solve a computationally intensive puzzle known as Proof-of-Work (PoW). The purpose of this puzzle is to ensure that adding a new block requires significant computational effort, making it costly and discouraging malicious entities from easily altering the blockchain. This process also enables the network to achieve consensus in a decentralised environment. Consensus is the process by which nodes agree on which block to add to the blockchain. They determine this based on the longest valid chain, in other words, the one in which the greatest amount of computational effort has been invested. The first miner to solve the PoW puzzle broadcasts the block to the network, and other nodes validate the solution. After validation, the block is added to the blockchain, and all nodes update their copies of the ledger, ensuring that every participant agrees on the current state of the blockchain. This is how consensus is achieved.

To solve the PoW puzzle, the miner must find a nonce. When this nonce is combined with the block's data and passed through a cryptographic hash function, it produces a hash that meets the network's difficulty target. The network difficulty target is a value that is regularly adjusted to ensure that block creation is neither too easy nor too difficult, maintaining a consistent block generation rate. The first miner to solve the puzzle broadcasts their block to the network, where other nodes verify its validity before attaching it to the blockchain.

Each node checks the validity of all transactions contained in the block, as well as the correctness of the PoW. If the block is considered valid, it is attached to the existing blockchain, forming a sequential chain of blocks. This distributed ledger is continuously updated throughout all nodes, ensuring transparency, consistency, and security throughout the network.

Next, the miner who successfully adds a block is rewarded with newly minted bitcoins and the transaction fees associated with the transactions included in the block. This incentive mechanism encourages miners to maintain

network security and validate transactions honestly. By linking blocks via cryptographic hashes, Bitcoin ensures that altering the content of any previous block would require redoing the PoW for all subsequent blocks, thereby updating the blockchain in a secure and tamper resistant manner.

In this way, the Bitcoin blockchain achieves decentralised consensus, immutability, and security, providing a reliable platform for peer-to-peer digital transactions without the need for a centralized authority. [21]. Figure 5.4 illustrates the operation of the Bitcoin network.

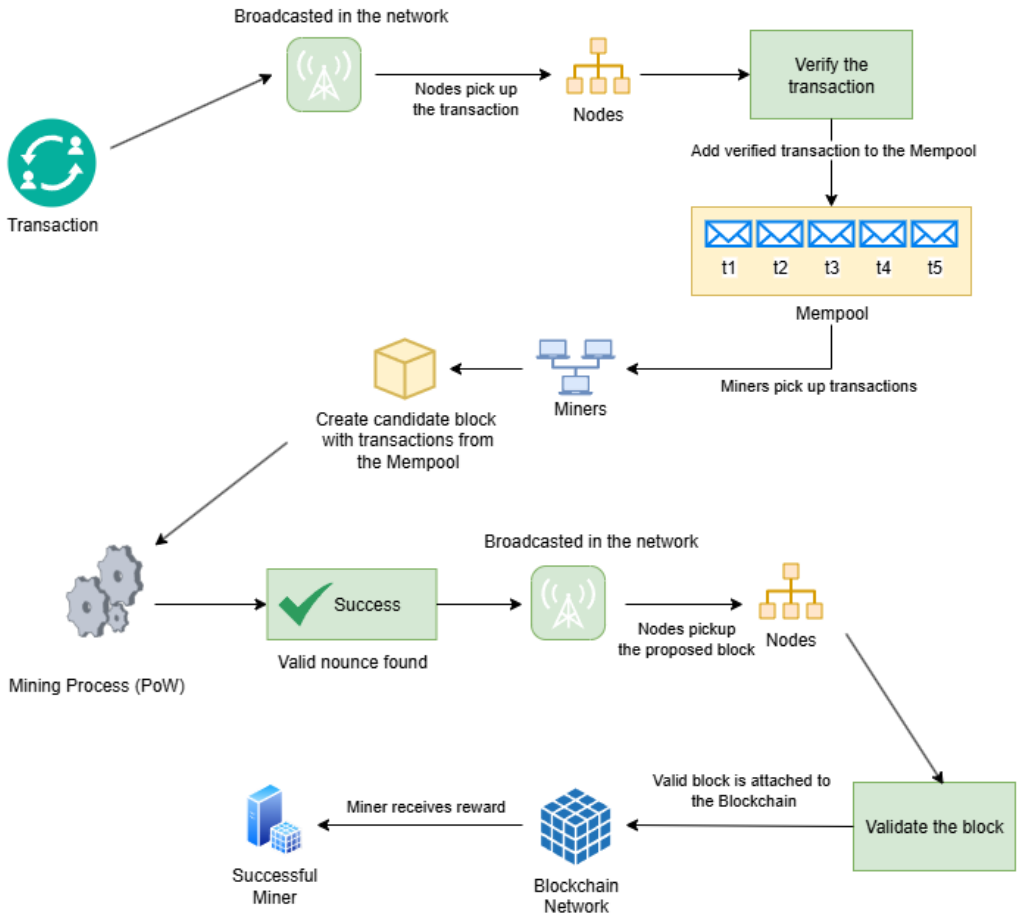


Figure 5.4: Bitcoin Network

In order to explain how blockchain operates in a simplified manner, the following analogy can be used.

Consider a goods train at a loading station. Several workers are responsible for loading goods into individual compartments and attaching them to the train.

When the goods are ready to be loaded, the workers are notified. Each worker receives a set of goods and checks the accompanying documentation to ensure that everything is valid. However, their task does not end there. Each worker must also solve a puzzle, in this case, correctly arranging the goods within the compartment so that they fit perfectly.

Once a worker completes this task, they announce it to the others. The other workers then inspect the compartment and verify that the job has been completed correctly. When the majority agree that the loading is accurate, the compartment is attached to the train. After successful verification, the worker responsible receives an allowance or reward for their effort.

In this analogy, the train represents the blockchain, each compartment represents a block, and the goods represent transactions. The process of arranging the goods represents to solving the Proof-of-Work puzzle, while the workers represent miners who verify and add new blocks to the blockchain.

5.4.5 A Brief Overview of the Cardano Network

Cardano is another blockchain technology that differs from Bitcoin, which was explained earlier. In Cardano too a wallet is required to perform transactions. The cryptocurrency of Cardano is called ADA, and one ADA is equal to 1,000,000 smaller units called Lovelaces. For example, if Person A sends 1 ADA to Person B, similar to Bitcoin, the transaction is broadcast across the Cardano network to the nodes.

When Cardano nodes receive the transaction, they validate it in a manner similar to Bitcoin nodes. Validation includes ensuring that the sender has sufficient funds and that all transaction parameters are satisfied. After this, the transaction is added to the node's local mempool [46].

Unlike Bitcoin, Cardano achieves consensus using a protocol called Ouroboros. According to Cardano documentation, the network divides time into epochs. Each epoch consists of a number of slots, each lasting one second in theory, with blocks produced approximately every twenty seconds in practice [47]. At present, a Cardano epoch lasts for five days, which is equivalent to 432,000 slots. For each slot, a number of nodes can be randomly selected as slot leaders using a Verifiable Random Function (VRF) [48]. Sometimes there may be zero selections due to the probabilistic nature of the selection process.

This is governed by the network's active slot coefficient, which controls the probability that a slot is active, ensuring probabilistic leader selection and fair distribution of block production among stake pools. On average, one slot leader is expected to be selected every 20 seconds, resulting in approximately 21,600 selections per epoch. If multiple slot leaders are randomly selected for the same slot and each produces a block, the block with the longest chain is added to the blockchain, while the other candidate blocks are discarded [49]. However, if no slot leader is selected for a particular slot, no block is produced during that time, and the blockchain simply moves on to the next slot without adding a new block [50] [51].

The Cardano network supports multiple stake pools, which are reliable nodes that manage the stake of their owners as well as that of others, called delegators. Stake pools help maintain the ledger, process transactions, and produce new blocks using the combined stake of their owners and delegators. When a stake pool is selected as a slot leader, the corresponding stake pool operator produces the block [52].

The more stake a pool controls, the greater its probability of being chosen as a slot leader. Slot leaders are responsible for creating new blocks and adding them to the blockchain. To prevent monopolisation and maintain fairness, Cardano implements an incentive mechanism that discourages delegators from joining pools that already control a disproportionately large share of the network's total stake.

The slot leader selects transactions from its mempool and validates them in a manner similar to Bitcoin nodes. Once validated, the slot leader creates a new block and attaches it to the blockchain. Unlike in Bitcoin, recent blocks in Cardano are considered transient. Only the chain that precedes the prespecified number of transient blocks is considered settled. This mechanism is referred to as the settlement delay. It allows honest nodes to stay in sync, even if a slot leader goes offline or a temporary fork occurs. After the slot leader attaches the new block, it is broadcast to the network, and the nodes validate it again. This is how consensus is achieved in Cardano. Figure 5.5 illustrates the operation of the Cardano network.

Smart contracts are another feature of the Cardano blockchain network. Although the prototype application will not utilise smart contracts, it is useful to understand them. Cardano defines smart contracts as "digital agreements defined in code that automate and enforce the terms of a contract without the need for intermediaries, enabling secure and transparent transactions on a blockchain." It further states: "By leveraging predetermined

conditions defined within the smart contract code, the state of a contract can only be updated in a way that follows the rules defined in that contract." [53]

Although the term smart contracts might give the impression that something "smart" is happening behind the scenes, the process is actually not that complex. Even Vitalik Buterin, the co-founder of Ethereum, the platform that popularised smart contracts, has stated that he regrets adopting the term "smart contracts" and believes they should have been called something more boring and technical, perhaps "persistent scripts" [54].

In reality, on Cardano, smart contracts are simple programs, often referred to as validator scripts. These scripts contain custom logic defined by the user and are automatically executed by Cardano nodes to validate transactions whenever an attempt is made to move funds from the script's address. Smart contracts cannot be altered once deployed and are tamper-proof. Furthermore, Cardano is not the only blockchain platform to offer smart contracts; other platforms, such as Ethereum, also support them [55].

Understanding the Extended Unspent Transaction Output (EUTXO) model is useful, as it forms the basis of Cardano's implementation of smart contracts. Cardano adopts EUTXO, an extension of Bitcoin's Unspent Transaction Output (UTXO) accounting model. In this model, the blockchain records unspent outputs from previous transactions, each of which can be used as input for new transactions. A simple analogy is using cash: when someone uses a twenty-dollar bill to pay for an item costing ten dollars, they receive change in the form of two five-dollar bills. The original bill is no longer available, but the two five-dollar bills can be used in subsequent transactions [56].

Cardano extends the UTXO concept by allowing each UTXO to carry not only value (such as ADA) but also additional data, providing support for smart contracts. Each output can be associated with a validator script that defines the conditions under which it can be spent. This extension enables more complex logic and programmability while maintaining the deterministic and tamper-proof properties of the underlying blockchain [56].

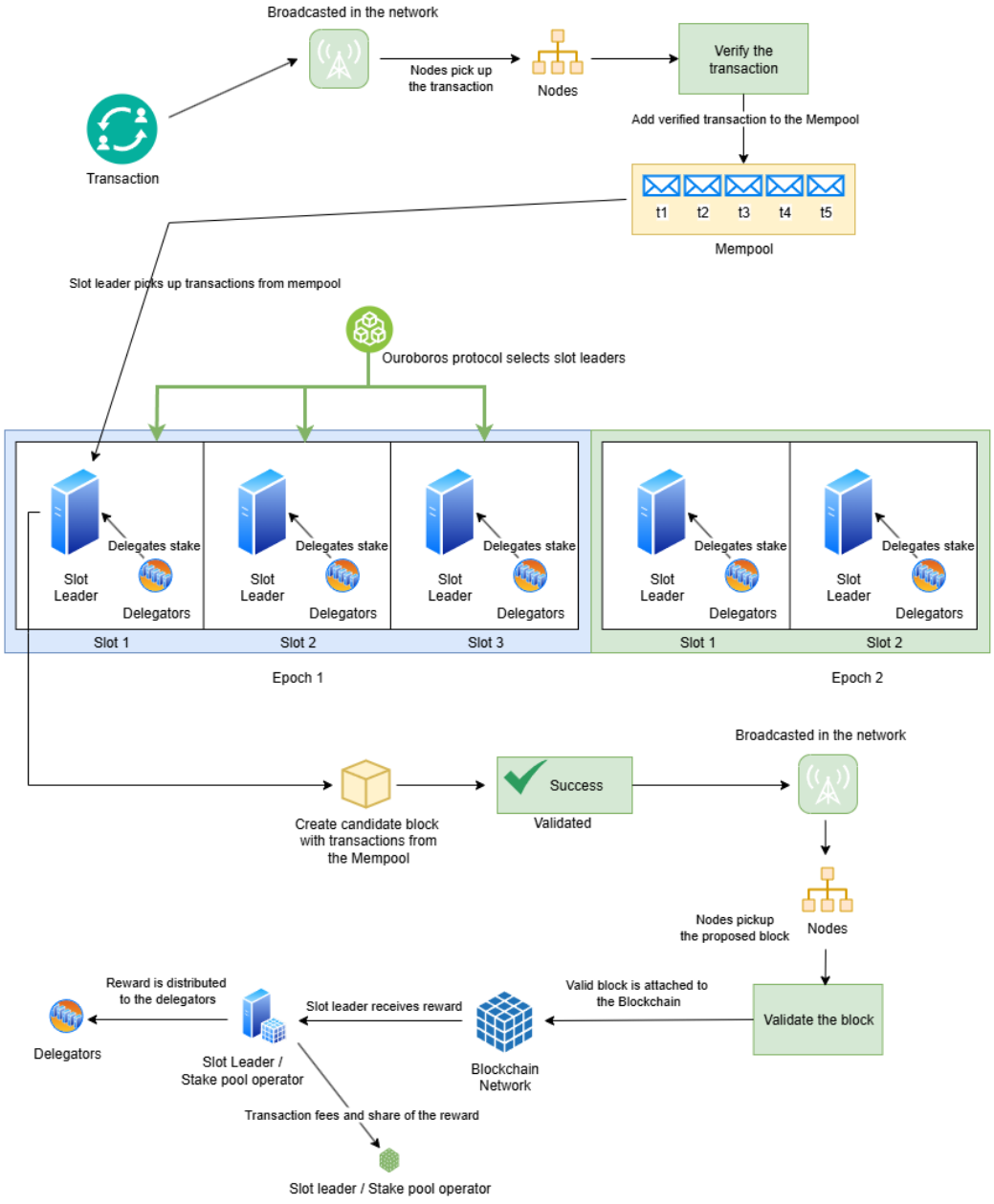


Figure 5.5: Cardano Network

Let's take the loading station analogy from the previous section to explain how Cardano works. Consider another loading station run by a different

company. Here, the process differs slightly. One key difference is that there is no puzzle to solve, as arranging the goods in the compartments is done automatically by robots. However, workers are only allowed to check documentation and load goods if they have a good reputation. The higher a worker's reputation, the more likely management is to assign them the task. Workers can also receive recommendations from their fellow workers, which increase their reputation. Another difference is that for each workday, management divides the day into shifts. At the beginning of the day, workers are assigned to shifts based on their reputation, and in each shift, one worker is allowed to load goods.

Once a job is completed successfully, the worker announces it to the others. The other workers then inspect and verify that the task has been correctly completed. After successful verification, the worker receives a reward, a portion of which is distributed to the fellow workers who recommended them, in proportion to their reputation compared to the total reputation. However, if verification fails, the worker loses reputation, which is costly and requires significant effort to rebuild. This incentivizes workers to perform the task honestly.

Similarly to the earlier analogy, the train represents the blockchain, each compartment represents a block, and the goods represent transactions. The staking of reputation represents the Proof-of-Stake (PoS) mechanism, while the workers represent validators who verify and add new blocks to the blockchain. Workdays represent epochs, and shifts within each workday represent slots. The worker assigned to load goods during a shift represents the slot leader.

5.5 Decentralised Identifiers (DID) and Verifiable Credentials (VC)

Traditionally, data and identity-related information, has been managed through centralised systems. Decentralised identity technologies offer an alternative approach by removing the need for a single controlling authority. In earlier sections, the challenges associated with centralised identity management were discussed, particularly in relation to migrant data security and cultural heritage management. Decentralised identity systems can help bridge these gaps and mitigate the vulnerabilities in centralised identity management approaches. This section discusses the decentralised identity technologies and

protocols employed in the proposed solution.

The World Wide Web Consortium (W3C) is an international organisation responsible for developing standards related to the web. It has more than 350 member organisations that contribute to the creation and maintenance of these standards. The W3C plays an important role in ensuring that organisations and developers adopt consistent, interoperable web technologies. Its standards are implemented by browsers, search engines, and other software systems that form the backbone of the modern web. The W3C is widely regarded as one of the most important bodies in the standardisation of web technologies. Its members include major public and private organisations such as Mozilla, Microsoft, and Google, among many others [57] [58].

In addition to its work on core web standards such as HTML, CSS, and JavaScript, the W3C also heads the development of emerging standards for decentralised identity and verifiable credentials (VCs). These standards especially the Decentralised Identifiers (DID) Core and Verifiable Credentials Data Model specifications, provide the base for secure, user-controlled digital identity frameworks. W3C, by defining open and interoperable protocols, supports the creation of decentralised identity ecosystems that promote privacy, transparency, and trust across different platforms and organisations.

5.5.1 Decentralized Identifiers (DIDs)

Decentralised Identifiers (DIDs) are digital identity instruments that do not rely on any centralised system or authority for verification. Each DID is associated with a DID Document, which describes the cryptographic material, verification methods, and service endpoints associated with the DID. A DID can represent any subject or entity, including a person, organisation, or thing, as determined by the controller (owner) of the DID. The DID Document can be resolved using a DID Method, which defines how the DID and its document are stored and accessed from a Verifiable Data Registry (VDR).

According to the W3C specification, a DID Method is a schema that defines operations such as the creation, resolution, updating, and deactivation of a DID. A VDR is a system that supports the creation, verification, updating, and/or deactivation of DIDs and DID Documents. The W3C further states that a VDR can also be used to manage other cryptographically verifiable data structures, such as Verifiable Credentials (VCs). DID resolution is the process of retrieving a DID Document using the DID as input, allowing the associated cryptographic and service information to be accessed and

verified. To perform DID resolution, a DID Resolver can be used. A DID Resolver is a software or hardware component that takes a DID as input and returns the corresponding DID Document as output [59].

Other parties may assist in providing or verifying information related to a DID. However, the design ensures that the controller can prove ownership without requiring permission from others, enabling secure and trusted interactions. DID Documents contain information such as public keys, verification methods, and service endpoints, which allow the controller to authenticate, sign, and communicate securely. By being globally unique, decentralised, and interoperable, DIDs support self-sovereign identity principles, allowing users to fully own and control their digital identities across multiple systems and platforms.

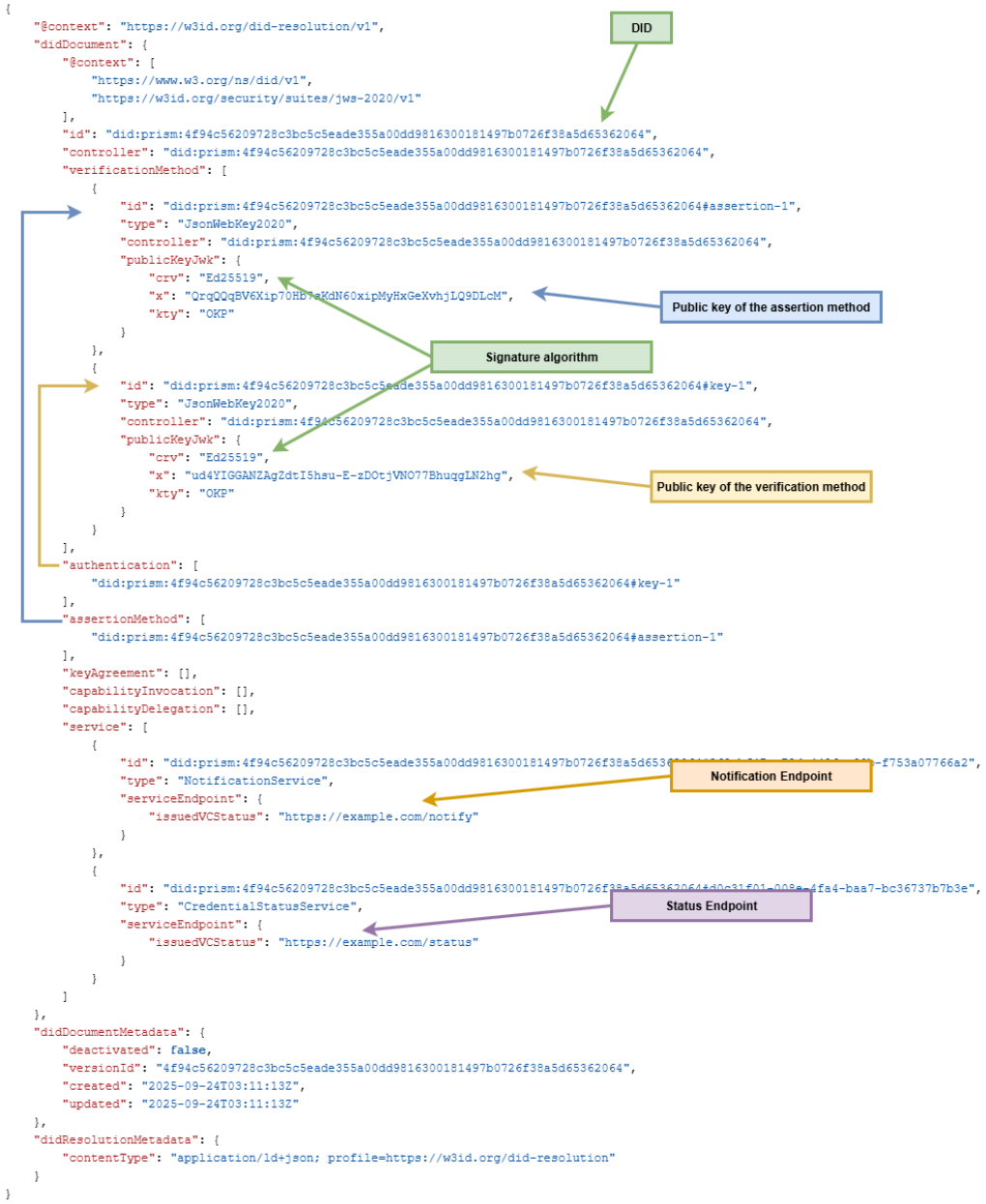


Figure 5.6: Sample DID document

A sample Decentralized Identifier (DID) Document is shown in Figure 5.6. This DID Document was generated through a PRISM node, which will be

explained later in this chapter. The DID generated by the prototype application will follow a similar structure. Some important elements relevant to this report are highlighted in the figure.

Each DID Document contains a **DID identifier (id)**, which is a unique string that distinguishes it from other DIDs. In this example, the DID is:

```
did:prism:4f94c56209728c3bc5c5eade355a00dd9816300181497b0
726f38a5d65362064
```

Here, "did" represents the URI scheme identifier, "prism" specifies the DID method, and the final alphanumeric string denotes the unique identifier assigned according to that method. The DID identifier is used to resolve DIDs, that is, to fetch DID documents.

Verification Method defines how a proof can be independently verified. In this DID document, a cryptographic public key is used as a verification method according to digital signatures. It allows verification that the signer used the corresponding private key to create a signature. Earlier sections of this report explain how digital signatures and public-private key pairs function. In this DID document, the public key is provided in field "x". This key can be used to verify any proof signed by the owner of the DID [60].

There are two verification methods in this document. The authentication method is used to authenticate ownership of the DID by its owner. The public key associated with this method has the ID

```
did:prism:4f94c56209728c3bc5c5eade355a00dd9816300181497b0
726f38a5d65362064\#key-1
```

In this example, the corresponding public key is ud4YIGGANZAgZdtI5hsu-E-zDOtjVNO77BhuqgLN2hg. If the owner of this DID needs to prove ownership, they can sign a nonce, which can then be verified using the corresponding public key. A nonce is a random, one-time value that ensures each authentication request is unique, thereby preventing replay attacks. By signing a nonce, the owner demonstrates control over the private key associated with the public key in the DID document.

The next verification method is the assertion method, which is used to make a claim about a subject. This functions in a similar manner to the authentication method.

Verification methods must specify the signature algorithm so that the verifier knows how to validate the signature. In this document, the signature algorithm is indicated using the "crv" field. In this case, the Ed25519 digital signature algorithm is used [59].

The DID document defines two services: *NotificationService* and *StatusService*. Each service specifies two URLs that can be used to access or consume the respective service endpoints. These endpoints can represent any type of service, depending on the implementation and the requirements of the system.

5.5.2 Verifiable Credentials (VC)

According to the W3C, a verifiable credential (VC) is a credential, a set of claims made by an issuer about a subject, that can be cryptographically verified for authenticity and integrity. The subject may be an individual, an organisation, or any other entity. A verifiable credential is designed to be tamper-evident, meaning that any modification of its contents can be detected, and its authorship can be verified through cryptographic means. Verifiable credentials can be used to create verifiable presentations, which are cryptographically verifiable collections of one or more credentials, enabling the selective disclosure of information by the holder [61].

The verifiable credentials data model ensures that credentials are resistant to tampering and falsification through the use of cryptographic proofs and decentralised identifiers (DIDs). Three primary roles are defined within this model:

Issuer: The entity that issues the credential.

Holder: The entity to whom the credential is issued.

Verifier: The entity that requests and validates the credential to establish its authenticity.

Verifiable credentials can be represented in various formats depending on the issuer and the system. Common formats include JWT, SD-JWT, and AnonCreds.

5.5.3 JSON Web Token (JWT)

The Internet Engineering Task Force (IETF), an organisation responsible for developing internet standards, created the JSON Web Token (JWT) specification. A JWT is a compact, URL-safe method for securely transmitting claims between parties over the internet. JWTs use the JavaScript Object Notation (JSON) format to represent data. The claims in a JWT are encoded as a JSON object and included either as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web Encryption

(JWE) structure. This design allows the claims to be digitally signed and/or encrypted, ensuring authenticity, integrity, and, if desired, confidentiality of the data [62] [63].

A JWT consists of three parts that are separated by dots (.), The Header, Payload and the Signature.

The Header has two parts. One describes the type of the token (E.g JWT, SD-JWT) and the next describes the signature algorithm. In the below example the type of the token is JWT and the signature algorithm is Edwards-curve Digital Signature Algorithm (EdDSA).

{ “typ”: “JWT”, “alg”: “EdDSA” }

The Payload contains the claims. Claims are information about an entity and additional data. The below is an example of a claim.

{ “name”: “Ada Lovelace”, “nationality”: “British” }

The signature is generated by first encoding the header and payload separately using Base64URL encoding, then concatenating them with a dot (.) separator. The resulting string is then signed using the algorithm specified in the header, on this instance EdDSA. Finally, the signature is attached as the third component of the JWT after being encoded with Base64URL [64]. This process can be represented as:

$$\text{signature} = \text{EdDSA}\Big(\text{base64UrlEncode(header)}+\texttt{"."}+\text{base64UrlEncode(payload)}\Big)$$

So the JWT would be,

$$\begin{aligned}\text{JWT} = {} & \text{base64UrlEncode(header)} \ . \\ & \text{base64UrlEncode(payload)} \ . \\ & \text{EdDSA}\Big(\text{base64UrlEncode(header)} + \texttt{"."} + \text{base64UrlEncode(payload)}\Big)\end{aligned}$$

To verify a JWT, the verifier performs the same Base64URL encoding and combining of the header and payload, then uses the public key corresponding to the signing algorithm (for example, an Ed25519 public key when using

EdDSA) to verify the signature. If the computed signature matches the signature included in the token, and not been tampered with, the JWT is considered valid. This ensures that the data has not been modified and that it was issued by a trusted party.

5.5.4 Selective Disclosure for JWTs (SD-JWT)

SD-JWT is a specialised form of JWT that enhances user privacy by allowing selective disclosure of claims. For example, a standard JWT might include claims about a user's name, date of birth, and salary. If a verifier only needs to know the name and date of birth, a standard JWT would require the user to disclose all claims, including sensitive information such as salary. However, an SD-JWT allows the user to reveal only the necessary claims, such as name and date of birth, while keeping other claims, such as salary, hidden. The verifier can then confirm the authenticity and integrity of the disclosed claims using the cryptographically signed SD-JWT, without learning anything about the undisclosed claims.

The SD-JWT has two main parts. The first part follows the same structure as a standard JWT. It consists of a header, payload, and signature, separated by dots (.). The header specifies the signing algorithm used by the issuer. However, unlike a standard JWT, the payload of an SD-JWT includes an additional field called _sd, which is an array containing hashes of the claims as its elements. The _sd_alg field specifies the hashing algorithm used (e.g. sha-256).The signature is generated in the same way as a standard JWT and provides cryptographic integrity and authenticity.

The second part of the SD-JWT consists of the disclosures, which are separated from the core JWT by the tilde (~) symbol. Each disclosure is a small array containing three elements, which are a random salt, the claim name, and the claim value. The salt ensures that the resulting hash value is actually random, even if two claims have identical values, their hashes will differ. This property prevents correlation or guessing of claims based on their hash values in the _sd array.

When the user (the holder) chooses to share a particular claim, the verifier recomputes the hash using the given salt, the claim name, the claim value, and the specified hash algorithm. The verifier then checks whether the resulting hash matches one of the hashes in the _sd array. If it matches, the claim is verified as authentic and known to have been issued by the original issuer [65].

Below is a sample of the _sd section from an SD-JWT payload:


```
{
 "_sd":  [
   "0LOWl2NMhfmYYI6JCcEoqqTIMDxKH6GIyL8n0EyzPKE",
   "PiB6hj3nDDG5Brrj4-Vl0caRTlUNfjiitpp7a7ohCoI"
 ],
 "_sd_alg":  "sha-256",
 "iss":
"did:prism:706c481ad34b17a38a88eaff56671b5c88fcfeace6ade797540e552df875
eae9",
 "iat":  1759183892,
 "exp":  1761775892
}
```


Below is a sample of a disclosure. The first element represents the random salt value, followed by the claim name and then its corresponding value.

$\text{Disclosure}_1 = [\texttt{"G2EHqjIG651DFHWGBweGYA"}, \texttt{"passportNumber"}, \texttt{"123"}]$
$\text{Disclosure}_2 = [\texttt{"ELUDhgVLnCfka\_yy8KVNiA"}, \texttt{"passportAgeAbove18"}, \texttt{"true"}]$

So the SD-JWT would be,

$$\texttt{\_sd} = \{\text{sha256(claim1)},\ \text{sha256(claim2)},\ \ldots\}$$
$$\text{payload} = \texttt{\_sd} + \{\texttt{"iss"} : \text{issuer\_DID},\ \texttt{"iat"} : \text{issued\_at},\ \texttt{"exp"} : \text{expiry}\}$$

$$\begin{aligned}\text{SD-JWT} = {} & \text{base64UrlEncode(header)} \ . \\ & \text{base64UrlEncode(payload)} \ . \\ & \text{EdDSA}\Big(\text{base64UrlEncode(header)} + \texttt{"."} + \\ & \text{base64UrlEncode(payload)}\Big) \ \sim \\ & \text{disclosure}_1 \ \sim \ \text{disclosure}_2 \ \sim \ \ldots\end{aligned}$$

An analogy can be used to explain the difference between a JWT and an SD-JWT. Imagine a group of people approaching a hotel receptionist to request five rooms. The hotel has twenty rooms in total, and all the room

keys are kept together in one bundle. In the case of a JWT, it would be as if the receptionist handed over the entire bundle of twenty keys to the guests. In contrast, with an SD-JWT, the receptionist would provide only the five specific keys corresponding to the rooms that were requested.

5.6 The InterPlanetary File System (IPFS)

The InterPlanetary File System (IPFS) is a decentralised technology. According to the official IPFS website [66], it is "A set of open protocols for addressing, routing, and transferring data on the web, built on the ideas of content addressing and peer-to-peer networking". IPFS itself is not a storage provider; rather, it is a protocol that enables data to be stored and shared in a decentralised manner.

Similar to blockchains the participants of the IPFS network are called nodes and they form a backbone to the IPFS network. Each Node has a unique identity referred to as the peer identity (Peer Id) [67]. The IPFS documentation defines a node as "An instance of an implementation of IPFS that you run on your local computer (directly or via a browser) to store files and connect to the IPFS network." In other words, an IPFS node is an application that runs on a computer and can communicate with the IPFS network to perform file transfers.

In order to understand IPFS, it is useful first to have an understanding on how Uniform Resource Locators (URLs) work. According to Mozilla, a URL is the address of a unique resource on the Internet. When a URL is entered into a browser, the browser first checks the URL with a Domain Name System (DNS) server. A DNS server maintains an index of domain names and their corresponding IP addresses. Using this information, the browser contacts the server hosting the requested resource and retrieves the content [68].

```
www.example.com/images/test.jpg
```

For example, in the URL above, example.com is the domain name. When this URL is entered in a browser, the browser first looks up the domain using a DNS server and then connects to the web server hosting the content. Based on the rest of the URL, images/test.jpg, the web server and any relevant applications running on it fetch the appropriate content, in this case, a JPG image [69].

When a file is added to IPFS via a node, it is first divided into smaller chunks, each of which is hashed using a cryptographic hash function (e.g., SHA-256). IPFS then organises these chunks into a data structure known as a Merkle Directed Acyclic Graph (Merkle DAG) [70]. In this structure, each chunk of the file is identified by its hash and represented as a data node. IPFS then creates parent nodes that reference the hashes of their child nodes, forming a hierarchical, linked structure. The root node of this structure represents the entire file and contains links to all the file chunks, either directly or through intermediate nodes. The hash of the root node is known as the Content Identifier (CID), which serves as a unique and permanent identifier for the file within the IPFS network. One important feature of IPFS is that the CID is content-dependent. If the same file is added to the network via two different IPFS nodes, they will generate the same CID. Even a slight modification to the file will result in a completely different CID. The image in Figure 5.7 shows the process by which a file is added to the IPFS network.

Once a CID is created, the IPFS node announces to the network that it hosts the CID. This process is referred to as providing, where the node makes the network aware that it can serve that content [71].

In order to locate a file and identity which nodes store its chunks, IPFS uses a distributed hash table (DHT). It implements a DHT algorithm known as Kademlia, which organises peers based on their IDs [72]. When an IPFS node requests a CID, it queries peers whose IDs are closest to the CID. If a node possesses the requested CID, it delivers the content to the requesting node. If not, it can provide references to peers whose IDs are closer to the target. This process continues iteratively until the requesting node reaches the peer storing the content. This system is fully decentralised, with no central authority controlling the network. Figure 5.8 illustrates how a file is requested from the IPFS network.

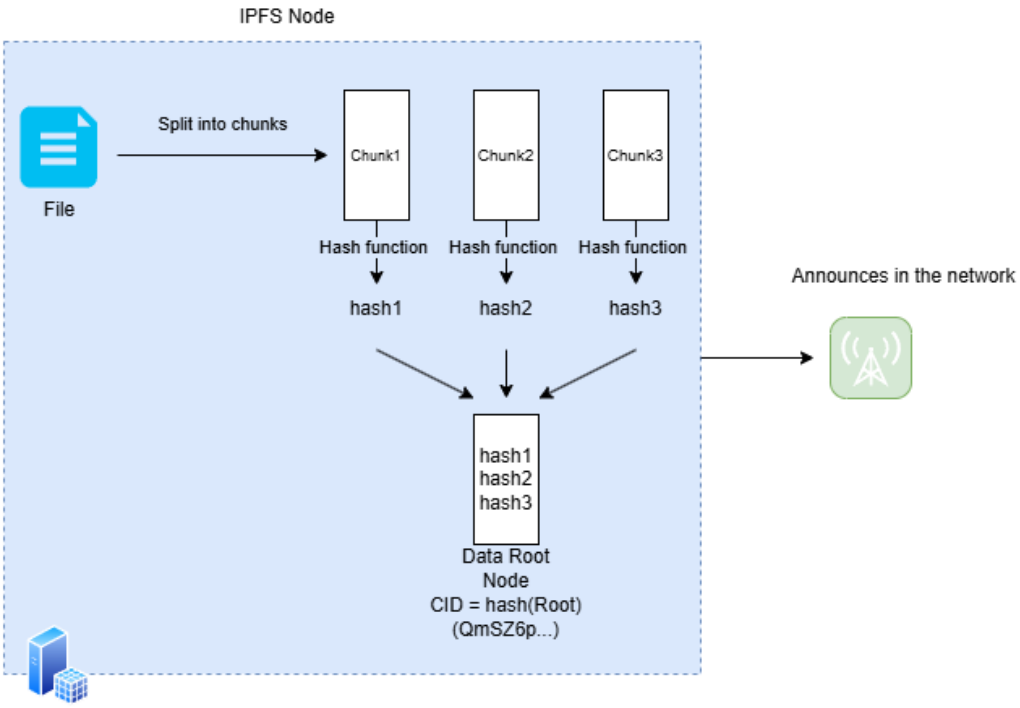


Figure 5.7: Adding a file to the IPFS Network

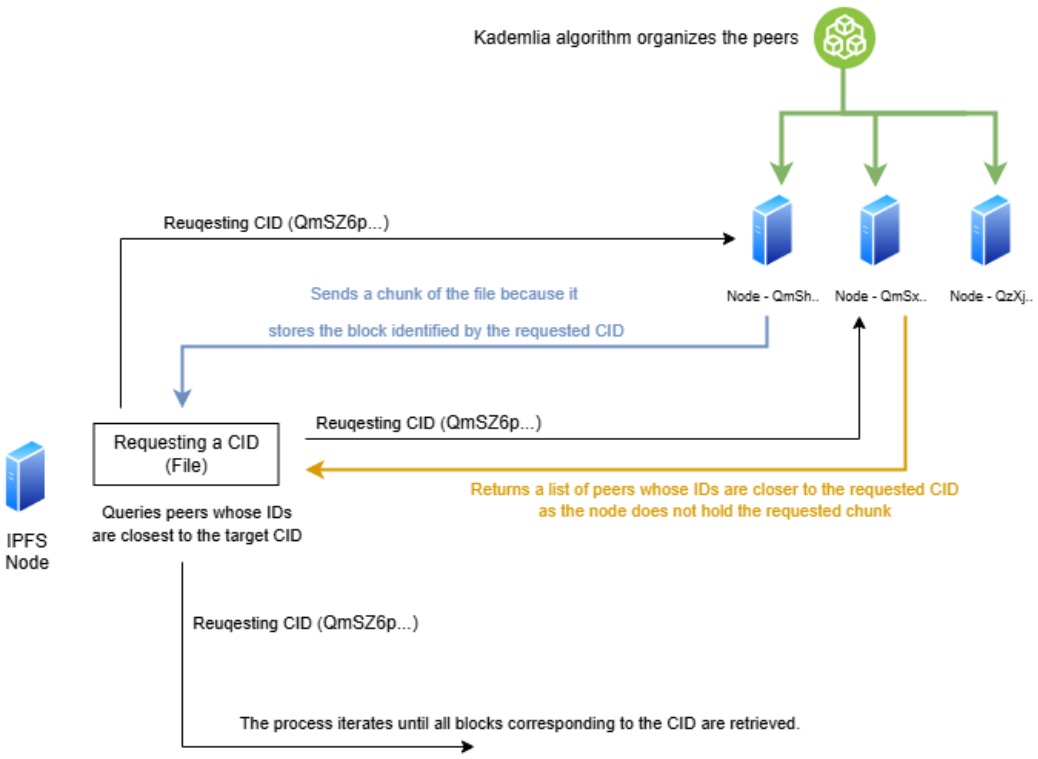


Figure 5.8: Requesting a file from the IPFS Network

Chapter 6

Implementation

6.1 Overview

The previous chapters discussed the background of the study, the migrant data privacy domain, and the issues present in the current process. They also reviewed related work in this area, analysing its relevance to the project. The Design chapter outlined the technologies selected for the prototype and justified their suitability. This chapter presents the implementation of the prototype in detail. It explains how the proposed technologies were integrated and how the overall system was built to address the issues identified in earlier chapters.

6.2 System Overview

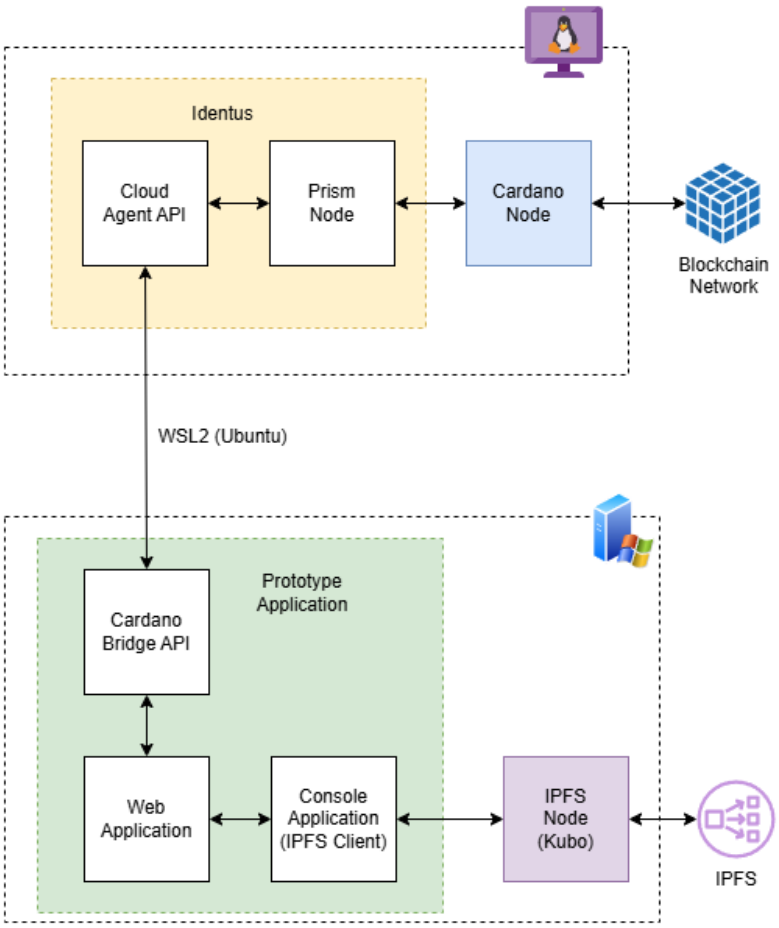


Figure 6.1: System Overview

The diagram in Figure 6.1 provides a high-level overview of the proposed solution. The prototype application is shown within the green boundary and consists of three main components:

Cardano Bridge API: This API connects to the Identus Cloud Agent API within the Identus system. It facilitates the transmission and retrieval of data from the Identus Cloud Agent and, indirectly, from the Cardano blockchain.

Web Application: The web application serves as the primary user interface through which users directly interact with the system. It also functions as the control centre, coordinating the operations of the other components within the prototype software.

Console Application: The console application is responsible for handling file-processing tasks. It communicates with the InterPlanetary File System (IPFS) node to send and retrieve files from the IPFS network.

The Identus environment is shown within the yellow boundary. It consists of two main parts: the Prism Node, which connects to the Cardano network via the Cardano Node (shown in blue), and the Identus Cloud Agent, which provides a set of APIs for communication with the Prism Node.

The Cardano Node, represented in blue, is responsible for establishing and maintaining the connection with the Cardano blockchain network.

6.3 Cardano Node, Hyperledger Identus, IPFS

The following sections of this chapter provide a detailed discussion of each external component of the application.

6.3.1 Cardano

The Cardano node is the software responsible for communicating with the Cardano blockchain and serves as a top-level component within the Cardano network. It is an open-source application maintained by Intersect, a member-based organisation within the Cardano ecosystem that ensures its continuity and future development [46] [73].

The Cardano node can be acquired either by downloading and compiling the source code from its official GitHub repository: `https://github.com/IntersectMBO/cardano-node` , or by using the pre-built Docker images provided there. Docker is a containerisation technology that enables applications to run within isolated and reproducible environments. This is achieved by packaging an application together with all its dependencies and configuration files into a portable unit known as a Docker image [74].

In the prototype application, a Docker image of the Cardano node was used. Initially, the plan was to download the latest Cardano source code and compile it locally. However, this approach was changed due to issues encountered during the setup of the Haskell environment and attempts to

compile the Cardano source code, as detailed in Appendix A of this report. Therefore, it was decided to use Hyperledger Identus, for which the Docker image of the Cardano node was considered sufficient.

The Cardano node setup and the Atala PRISM node setup were based on examples provided by Ley Lawrence [75] (see section A.1.6 for details) . The initial Docker setup script was taken from this example; however, it was modified to meet the specific requirements of the prototype, particularly due to incompatibilities and certain outdated Docker image versions. The Docker script, *docker-compose-cardano.yml*, is provided in the prototype application's code repository (see Section C for details).

The key components of the *docker-compose-cardano.yml* script are discussed in detail below.

Cardano node: The prototype uses the official Cardano node Docker image (version 10.5.1), configured to run in the preprod network, which is a testing environment that allows developers to experiment with applications before deploying them to the main Cardano network. The node operates within a Docker network named "Cardano" to enable communication with other Cardano-related containers. Persistent storage is configured through mounted volumes, with the environment variable $NODE_DB mapped to /data/db for storing the node's blockchain data, and the Docker-managed volume node_ipc mapped to /ipc for inter-process communication. The container is configured to restart automatically on failure to improve reliability. In summary, this configuration ensures that the Cardano node operates reliably and provides a stable environment for development and testing.

PostgreSQL Database (DB Sync): This service provides a PostgreSQL 14.10 database that supports the Cardano DB Sync module. The database stores blockchain data extracted from the Cardano node, allowing queries of transactions, blocks, and other information without directly communicating with the blockchain. The container uses the lightweight Alpine-based PostgreSQL image and is configured to run within the "Cardano" Docker network. Persistent storage is provided via the postgres-db-sync volume, ensuring that all database data is retained across container restarts.

Cardano Wallet: This service runs the official Cardano Foundation wallet image (version 2025.3.31). The wallet component connects to the Cardano node through the shared node-ipc volume. It provides a REST API that allows functionalities such as creating and managing wallets and querying wallet and transaction related blockchain data. The container is configured to operate within the "Cardano" Docker network, allowing communication

with other Cardano services. Persistent storage is managed via the wallet-db volume, while configuration files for different networks are mounted from the local ./configs/cardano directory. The API is exposed on port 8090 (mapped to port 7090 on the host). A wallet UI client application could be connected to interact with the wallet, however, for the purposes of the prototype, this was not necessary and was therefore omitted.

Cardano DB Sync: The cardano-db-sync service runs the official Cardano DB Sync image (version 13.5.0.2) and serves as the intermediary between the Cardano node and a PostgreSQL database. Its purpose is to extract blockchain data from the node and store it in the SQL database, allowing efficient querying of blocks, transactions, and other ledger information. The service is configured to run within the "Cardano" Docker network and depends on both the Cardano node and the PostgreSQL database (postgres-db-sync) being healthy before starting. Persistent storage is provided via the db-sync-data volume, while the shared node-ipc volume allows communication with the Cardano node through IPC sockets. This configuration ensures that DB Sync maintains an updated representation of the blockchain for use by wallet services or other applications.

The image in Figure 6.2 illustrates how the components described above interact and how they connect with the PRISM node [75].

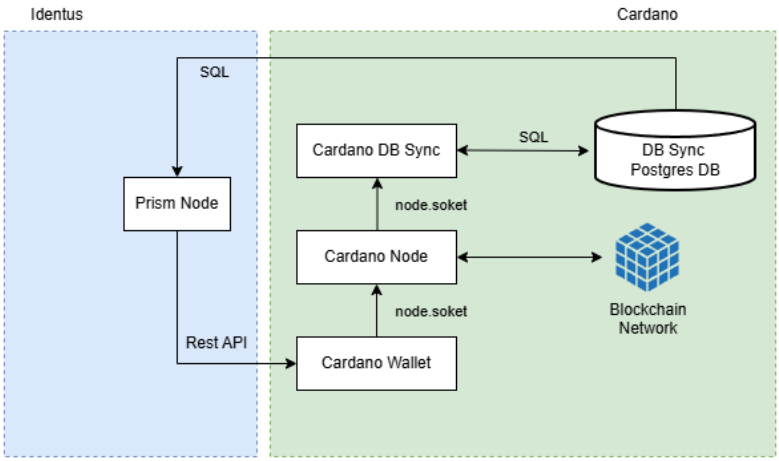


Figure 6.2: Interaction of Cardano components within the Docker environment

6.3.2 Prism (Hyperledger Identus)

The PRISM node, based on Hyperledger Identus, facilitates communication with the Cardano node. It acts as a bridge between the Cardano node and the user application. Similarly to the Cardano setup, the components of the PRISM node are installed via a Docker script named *docker-compose-prism.yml*. As with docker-*compose-cardano.yml*, this script was modified to meet the specific requirements of the prototype software and to resolve compatibility issues.

The key components of the *docker-compose-prism.yml* script are discussed in detail below.

PostgreSQL Database for PRISM: The postgres-prism service runs a PostgreSQL 13 container that provides persistent database storage for the PRISM node components. It is configured to create databases pollux, connect, agent, and node_db. These databases are initialized via two scripts, *init-script.sh* and *max_conns.sql*. Persistent storage is provided through the postgres-db-prism volume, ensuring that all database data is retained across container restarts.

pgAdmin: This service runs the pgAdmin 4 container, providing a web-based interface for managing the PostgreSQL databases used by the PRISM node. Persistent storage for pgAdmin settings and data is provided via the pgadmin volume. This configuration allows users to access the databases conveniently through a web interface.

PRISM Node: The prism-node service runs the official PRISM node container, acting as an intermediary between the Cardano blockchain and user applications. The prototype uses version 2.6.1. Although the example used version 2.2.1, experimentation revealed that the latest version provided better compatibility with the Identus Cloud Agent and ensured smoother operation of the application. The node connects to the PostgreSQL database provided by the postgres-prism container, using the node_db database. The service is configured with various environment variables to specify network settings, wallet API endpoints, transaction parameters, and ledger connections.

PRISM Agent: The prism-agent service runs the Hyperledger Identus Cloud Agent container (version 2.0.1-SNAPSHOT). This acts as a middleware component that interacts with the PRISM node and multiple PRISM related databases. It connects to the PostgreSQL databases pollux, connect, and agent hosted by the postgres-prism container. The agent is configured

with environment variables that specify service endpoints, wallet settings, Vault secrets management. It also relies on the prism-node and vault-server services for connectivity and secret management. The prototype application doesn't use a vault server, however when being used in a production environment, a vault server such as Hashicorp Vault can be used.

Swagger UI: The swagger-ui service runs the official Swagger UI container (version 5.1.0). Swagger provides a web-based interface for exploring and testing the PRISM Agent API. This allows to interact with the API endpoints directly through the browser, facilitating testing and verification of the agent's functionality.

API Gateway (APISIX): The apisix service runs the Apache APISIX container (version 2.15.0-alpine). This functions as the API gateway for the PRISM Agent and related other services.

The Figure 6.3 depicts how the components described above interact and how they connect with the Cardano node as well as the prototype application.

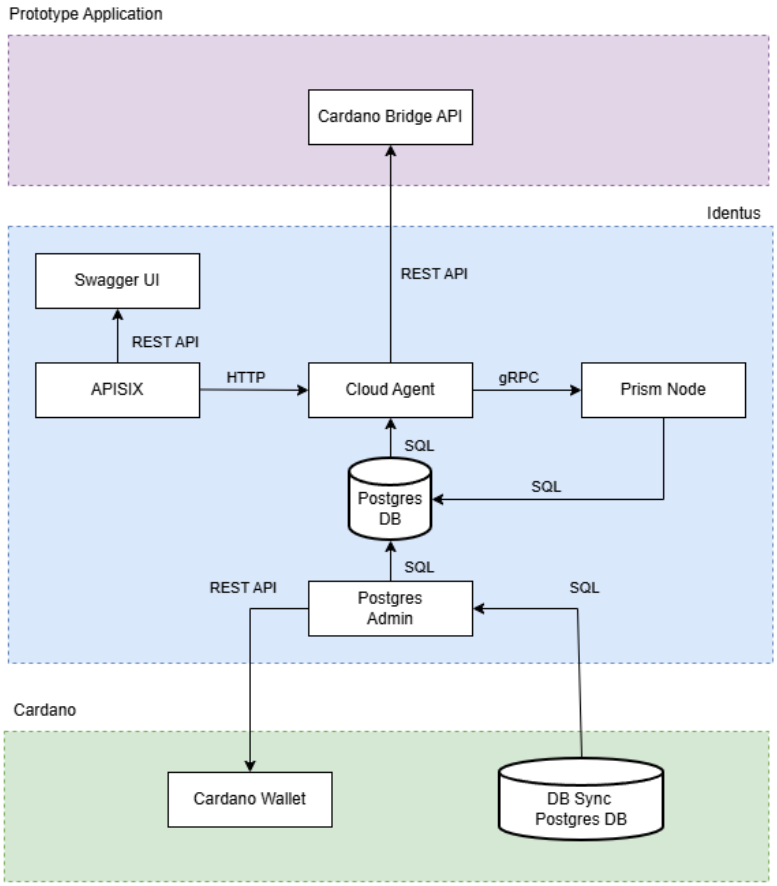


Figure 6.3: Interaction of Identus components within the Docker environment

6.3.3 Notes on the Identus Cloud Agent

During the experimentation phase, it was observed that the Identus Cloud Agent version 1.28.0 used in the example had several issues that made development difficult. One of the main challenges was the lack of online documentation for this version. The available documentation referenced methods and functionalities that either did not exist or produced errors when used, making it impractical to work with this version. Attempts to use Docker images of later versions also encountered unresolved issues.

According to the documentation, the Identus Cloud Agent supports a multi-tenant setup, allowing multiple users to interact with the system by

creating separate wallets. Initial experiments involved creating two users, an issuer and a holder and then issuing a verifiable credential (VC). However, this configuration did not produce the expected results, as the system did not function correctly when both users were on the same node.

Another issue with version 1.28 arose during experiments with AnonCreds, an alternative form of verifiable credential supported by Hyperledger Identus. AnonCreds were not used in the prototype due to their complexity and because JWT and SD-JWT were preferred for their scalability, particularly for potential mobile implementations. However, AnonCreds were explored during the initial development phase. During this process, creating a credential definition for the VC schema required a JSON file. The generated JSON, however, was not recognized by the credential definition API, even though the schema table contained the necessary fields and data. Although manually bypassing this issue allowed the process to succeed, this approach was avoided as it did not follow best practices.

Due to these limitations, the source code of the Identus Cloud Agent was downloaded, and a Docker image was built from the latest version. The lack of reliable online documentation for earlier versions meant that only the latest version was adequately supported. Even the latest documentation is sometimes incomplete or confusing, as it is spread across three sources:

1. Swagger API documentation
2. The Identus tutorial
3. Agent API documentation

The documentation provides generic instructions for multiple authentication and credential flows, including JWT, SD-JWT, AnonCreds. The parameters for issuing and verifying credentials differ depending on the flow, but the documentation does not clearly indicate which parameters should be used in each case. Therefore, it was necessary to experiment extensively and review the source code to determine the correct parameters.

During this process, several issues were identified:

- Schema and credential definitions for AnonCreds were not in the correct format. This issue was resolved by modifying the JSON files and hosting them in a new location.
- In the multi-tenant setup, attempts to issue invitations to users sometimes failed with errors such as “record already exists.”

- The Identus Cloud Agent did not support publishing Ed25519 keys, which are required for SD-JWT functionality.

The issues encountered were investigated using online resources and GitHub repositories, however, no solutions were found. To overcome these challenges, the Identus Cloud Agent was compiled from the latest source code, ensuring that known bugs were resolved and that the prototype could take advantage of the most recent features and improvements.

6.3.4 Kubo (IPFS)

Kubo is an open-source implementation of the InterPlanetary File System (IPFS) protocol, used to add and retrieve data from the IPFS network. It is compatible with all major operating systems, including Windows, macOS, and Linux. Kubo provides both a Command-Line Interface (CLI) and an HTTP API, which enable users and applications to upload, download, and manage files on the IPFS network.

In this project, the prototype application uses Kubo to perform essential operations such as adding files to and retrieving files from the IPFS network. The Windows version of Kubo is employed, as the prototype application currently runs in a Windows environment. It is important to note that all files, including documents and artefacts, are encrypted using the Advanced Encryption Standard (AES-256) algorithm with a strong, randomly generated key by the prototype application before being handled by Kubo and added to the network.

IPFS offers a number of advantages over traditional centralised file storage systems. Due to its decentralised nature, it is resilient to single points of failure. File downloads can be faster because files are retrieved from multiple sources simultaneously. Since navigation in IPFS is based on content hashing, unlike traditional systems that rely on URLs and are therefore vulnerable to broken links, this issue is largely avoided. For the same reason, IPFS is also resistant to tampering, as each file is identified by a cryptographic hash that verifies its integrity [76].

However, the main reason for using the IPFS network in the prototype is its decentralised architecture. Since IPFS operates without any central servers, no single entity, government, or jurisdiction can control the stored data. The data owner, in this case the migrant, retains data sovereignty. Furthermore, IPFS is an open-source and community-maintained project,

which enhances transparency and long-term sustainability [76].

6.4 Prototype Application

The primary objective of the prototype application is to provide a secure mechanism through which migrants can share their documents with immigration authorities without compromising their privacy. Furthermore, the prototype enables the safe storage and controlled sharing of cultural heritage information, thereby preventing potential exploitation. This aligns with the findings of the study, in which a majority of participants indicated that preserving cultural heritage information across various domains was important (see Chapter 4, Results). The system aims to achieve these objectives by offering a suite of software tools that can be used by the various stakeholders involved in the migration process.

The proposed solution has been developed using technologies from the .NET 8 ecosystem. This choice was made since .NET is an open-source and mature technology that has been successfully used in numerous production grade applications. Furthermore, the researcher's prior experience with the platform allows more time to be focused on system design and experimentation rather than learning a new framework.

In addition, .NET 8 provides cross platform support, high performance, and robust security features, making it ideal for scalable web and distributed applications. Its compatibility with RESTful APIs, modular architecture, and the .NET 8 long term support release further ensure the reliability and maintainability of the proposed system [77] [78] [79].

In the context of migration, three main parties are typically involved: the migrant, trusted third parties responsible for verifying documents, and the immigration authority. Within the proposed solution, each of these parties hosts an instance of the prototype application on their respective systems. Figure 5.2 provides an overview of the prototype software's functionality.

For Migrants:

- The prototype enables migrants to create a Decentralised Identifier (DID) and publish it on the Cardano pre-production test network. They can also specify a notification URL, which is used to automatically send alerts whenever their Verifiable Credentials (VCs) are accessed.

- It allows migrants to issue VCs for their cultural heritage content and share these securely with others. The related content (such as videos, images, text, or sound files) is hosted on the InterPlanetary File System (IPFS) network in an encrypted and secure manner.
- The prototype provides a digital wallet for storing VCs and creating presentations from them, giving migrants the option to share only the specific information they wish to disclose to another party.

For Trusted Third Parties:

- The prototype allows trusted third parties (e.g., the International Organization for Migration (IOM) or VFS Global) to create their own Decentralised Identifiers (DIDs) and publish them on the Cardano preproduction test network. They can also specify a status URL, which is utilised to check and monitor the status of issued credentials.
- It enables these entities to receive documents from migrants and store them securely in a decentralised manner.
- The prototype provides mechanisms for verifying documents and processing VC requests submitted by migrants, including the ability to approve or reject credential requests.
- It supports credential revocation, allowing the invalidation of previously issued VCs when necessary.
- It facilitates the retrieval and re-evaluation of stored documents at a later stage.

For Immigration Authorities and Related Entities:

- The prototype allows immigration authorities or related organisations (e.g., refugee agencies) to verify the validity of credentials by cryptographically validating both the content and its source of issuance.

6.4.1 SD-JWT vs JWT

Sections 5.5.3 and 5.5.4 explain how JWT and SD-JWT function. In the prototype application, when issuing a VC for migrants based on their immigration related documents, an SD-JWT is used. This enables migrants to

selectively share specific claims with relevant authorities or entities, disclosing only the information required for verification. Such selective disclosure supports privacy preservation, which is one of the primary goals of the prototype application.

However, when issuing a VC for an artefact, a standard JWT is used. This is because artefact VCs are issued by the artefact owner to ensure that their property is used in accordance with defined terms and conditions. Using an SD-JWT in this context could lead to potential misuse. For example, if a VC is issued for an artefact with a specified validity period, a holder could omit or withhold the "duration" claim when presenting the credential, preventing other parties from verifying whether the artefact usage is still valid. To avoid such misuse and ensure the full disclosure of all relevant claims, the prototype uses JWTs for artefact VCs.

6.4.2 CardanoBridgeAPI

The API module serves as an intermediate layer between the user-facing application (web application) and the Hyperledger Identus decentralised identity system. It is responsible for handling all communication and data exchange between these components. The module has been implemented using .NET 8 Core Web API, adopting a RESTful architecture to ensure interoperability, scalability, and ease of integration.

The rationales for implementing a separate Web API layer include:

- **Improved flexibility:** The communication logic is separated from the front-end application to enable greater flexibility. This allows future user interfaces, such as mobile applications or third-party integrations, to interact seamlessly with the Identus infrastructure through the same API endpoints.

- **Enhanced modularity and maintainability:** This modular design enhances maintainability and supports the independent development, testing, and deployment of the core identity-management logic.

- **Increased security:** Isolating the front-end from direct interaction with blockchain-related operations introduces an additional layer of security, reducing the likelihood of blockchain-related operations being targeted or exploited.

The API follows a two-layer architecture, consisting of a controller layer and a service layer. The controller layer is responsible for handling incoming HTTP requests and routing them to the appropriate service methods. The service layer contains the business logic required to process these requests and communicate with the Hyperledger Identus system. The API application contains three controllers:

DID Controller: Handles operations related to the creation, publication, and resolution of Decentralised Identifiers (DIDs).

Issuance Controller: Manages operations associated with Verifiable Credential (VC) issuance, such as generating schemas, sending and accepting invitations for VC offers, and processing VC acceptances.

Key Controller: Signs nonces.

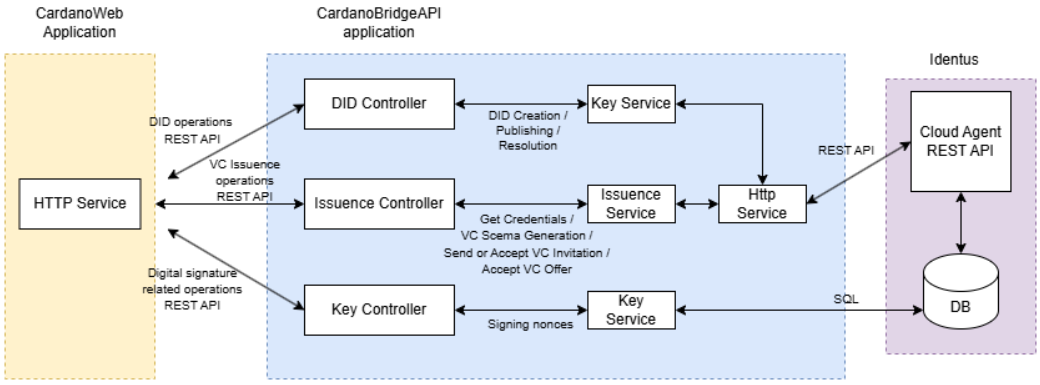


Figure 6.4: CardanoBridge API Architecture

Figure 6.4 illustrates the architecture of the CardanoBridge API application. All operations related to Hyperledger Identus are communicated from the user-facing web application to the CardanoBridge application, which then invokes the appropriate Identus Cloud Agent APIs. The corresponding endpoints subsequently call the relevant service components to perform the required operations. These service components implement the necessary business logic. The DID and Issuance services then communicate with the relevant Identus Cloud Agent APIs, while the KeyService connects directly to the Identus Cloud Agent's database.

The DID Controller has the following endpoints, as shown in Table 6.1.

Endpoint Name	Type	Description
Create	POST	Creates a DID based on the given JSON template.
Publish	POST	Publishes a DID based on the given long-form DID.
ResolveDid	GET	Fetches a DID document based on the provided DID.

Table 6.1: Endpoints of the DID Controller

The Issuance Controller has the following endpoints, as shown in Table 6.2.

Endpoint Name	Type	Description
GenerateSchema	POST	Generates a JWT or SD-JWT schema based on the provided JSON template.
GetCredential	GET	Retrieves a Verifiable Credential (VC) based on the credential record ID.
Invitation	POST	Creates a VC offer invitation based on the JSON template.
AcceptInvitation	POST	Accepts a VC offer invitation based on the JWT.
AcceptOffer	POST	Accepts a VC offer based on the record ID and assigns it to the specified DID.

Table 6.2: Endpoints of the Issuance Controller

The Key Controller has the following endpoints, as shown in Table 6.3.

Endpoint Name	Type	Description
SignNonce	POST	Signs a given nonce using the specified DID's private key.

Table 6.3: Endpoints of the Key Controller

The CardanoBridge API application does not store any data. Its sole function is to communicate with Hyperledger Identus. It accesses the private key from the Agent database in the Identus Cloud Agent system solely to

sign nonces and return the signed values to the CardanoWeb application via the SignNonce endpoint.

Table 6.4 lists the CardanoBridge API application's controllers and endpoints, along with the corresponding Identus Cloud Agent endpoints with which they communicate [80].

Controller	**Endpoint**	**Cloud Agent Endpoint**
DID Controller	[POST] Create	[POST] /did-registrar/dids
DID Controller	[POST] Publish	[POST] /did-registrar/dids/{did}/publications
DID Controller	[GET] ResolveDid	[GET] /dids/{did}
Issuance Controller	[GET] GetCredential	[GET] /issue-credentials/records/{recordId}
Issuance Controller	[POST] GenerateSchema	[POST] /schema-registry/schemas
Issuance Controller	[POST] Invitation	[POST] /issue-credentials/credential-offers/invitation
Issuance Controller	[POST] AcceptInvitation	[POST] /issue-credentials/credential-offers/accept-invitation
Issuance Controller	[POST] AcceptOffer	[POST] /issue-credentials/records/{recordId}/accept-offer

Table 6.4: CardanoBridge API endpoints and corresponding Identus Cloud Agent endpoints

6.4.3 IPFS Client

The IPFS Client is a console application responsible for file handling operations related to the InterPlanetary File System (IPFS). It receives commands from the CardanoWeb application and, based on these commands, performs operations such as adding or retrieving files from the IPFS network. The client is implemented as a .NET 8 console application.

The rationales for implementing a separate application for file operations include:

- **Reducing load on the CardanoWeb application:** Handling large files directly within the web application, whether for adding to or retrieving from the IPFS network, could negatively impact responsiveness and overall performance.
- **Managing potentially long running operations:** File operations, particularly for large files or in low-bandwidth environments, can be time consuming. Running these operations in a separate process ensures that the web application remains responsive and avoids blocking user interactions.
- **Improved reliability:** IPFS operations may fail due to network issues. A separate application can implement retries and error-handling

mechanisms more effectively without affecting the web application.

- **Scalability:** As the number of files and processing demands increase, having a dedicated application allows the system to handle higher workloads more efficiently.
- **Modularity and maintainability:** This design improves modularity, making the system easier to maintain and test. It also allows for future extensions, such as parallelised or asynchronous file processing.

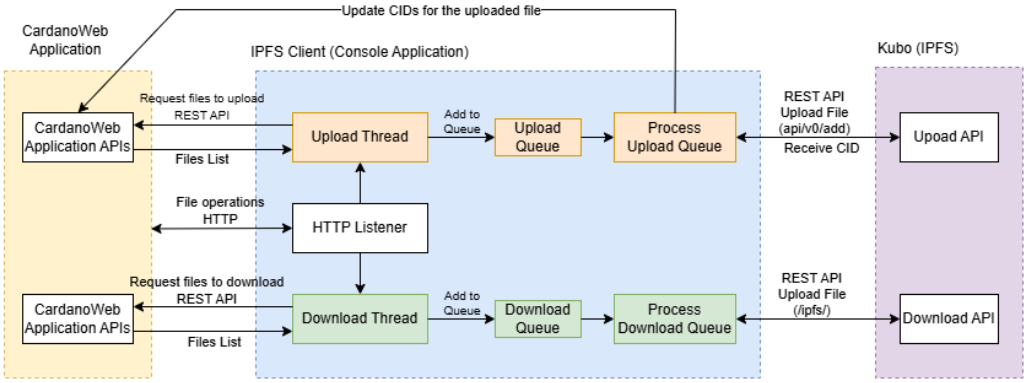


Figure 6.5: IPFS Client Architecture

Figure 6.5 illustrates the architecture of the IPFS Client application. The application listens for HTTP requests via localhost on port 7575 (configurable). When the CardanoWeb application requires a file to be uploaded or downloaded, it triggers the IPFS Client via an HTTP call. Upon receiving a request, the IPFS Client starts two separate threads: one for handling uploads and another for handling downloads.

Upload Thread: The upload thread calls the /api/filejob/FilesToUpload API in the CardanoWeb application. If any files require uploading, the API returns a list of files. The upload thread adds these files to a queue and communicates with Kubo via the /api/v0/add API running on localhost port 7575 (configurable). Kubo then uploads the files to the IPFS network and returns a CID. The IPFS Client's upload thread then calls the /api/document/cid API in the CardanoWeb application to update the files with their corresponding CIDs.

Download Thread: The download thread calls the /api/filejob/FilesToDownload API in the CardanoWeb application. If any files need downloading, the API returns a list of files. The download thread adds these files to a queue and communicates with Kubo via the /ipfs/ API running on localhost port 8282 (configurable). Kubo then downloads the files from the IPFS network to the specified path, making them available for access by the CardanoWeb application.

6.4.4 CardanoWeb Web Application

The CardanoWeb application is the user-facing component of the system. All stakeholders, including migrants, immigration authorities, and trusted third parties, interact with the application through this interface. The application is built using ASP.NET Core Razor Pages on the .NET 8 framework, which is open-source. ASP.NET Core Razor Pages is a web technology that employs a simplified Model-View-Controller (MVC) architecture, making it more page-focused and easier to develop page-centric web applications [81].

The application is structured into three layers: the UI layer, the service layer, and the data layer. Users interact with the UI layer, which is implemented as a Razor Pages website. The business logic resides in the service layer, while the data layer handles communication with the database. The application uses a PostgreSQL database and the Entity Framework Core (EF Core) Object-Relational Mapper (ORM) to facilitate database access and operations.

The diagram Figure 6.6 illustrates the design of the application. The service layer is further organised based on the main functionalities of the application. The application utilizes the ASP.NET Core Identity framework for authentication and authorization. Identity is an open-source .NET 8 framework from Microsoft that simplifies the development of authentication and authorization mechanisms for .NET-based applications [82].

In the diagram, green lines and arrows indicate communication between the user interface (web pages) and the service layer via the appropriate services. Blue lines and arrows represent communication between the service layer and the CardanoBridge API. All services that interact with Cardano blockchain functionality go through the HTTP Service, which communicates with the CardanoBridge API's REST endpoints. Purple lines and arrows represent service connections to the data layer, which in turn communicates with the PostgreSQL database.

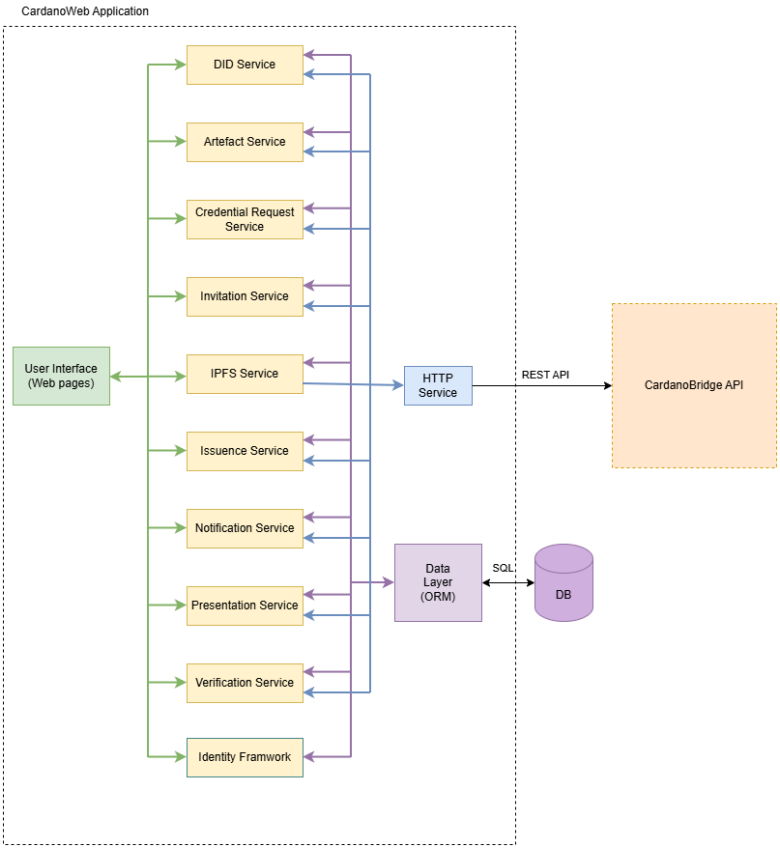


Figure 6.6: CardanoWeb Web Application

6.5 Authentication and Authorization process

The prototype application is intended to be used by three parties: the migrant (VC holder), the trusted third party (VC issuer), and the immigration authorities (verifier). The application includes a configuration setting called Mode, which can be adjusted in the *appsettings.json* file.

At present, there are two available modes: *Issuer* and *User*. The application should be set to *Issuer* mode when it is hosted or used by the trusted third party (issuer). It should be set to *User* mode when used by the migrant or holder. The immigration authority (verifier) may also use the *User* mode, as the verification functionality is available within this mode. The verification option is accessible to all users.

As this is a prototype application, and there is currently no strict requirement for a distinct set of features for the immigration authority (verifier), a separate *Verifier* mode has not been implemented, as this also falls outside the scope of this thesis. Furthermore, individuals or organisations wishing to host cultural heritage content should also use the *User* mode. The mode configuration determines the features that are available within the application.

The prototype application currently defines two roles: *Admin* and *Holder*. Any user or entity hosting the application is assumed to have the *Admin* role. For instance, if a migrant hosts the application for their own use, they will be operating under the *Admin* role. Anyone who requires credentials to be issued by them can create an account, which will take the *Holder* role.When the immigration authorities host the application, they will also operate under the *Admin* role.

At present, since this is a prototype, there is only one administrator (*Admin* role) within the system. However, support for multiple administrators is implemented at the application level, although a user interface for this feature has not yet been developed.

When a migrant creates an account within the immigration authority's application in order to verify their credentials, their account will also assume the *Holder* role.

Figure 6.7 illustrates how roles and modes behave.

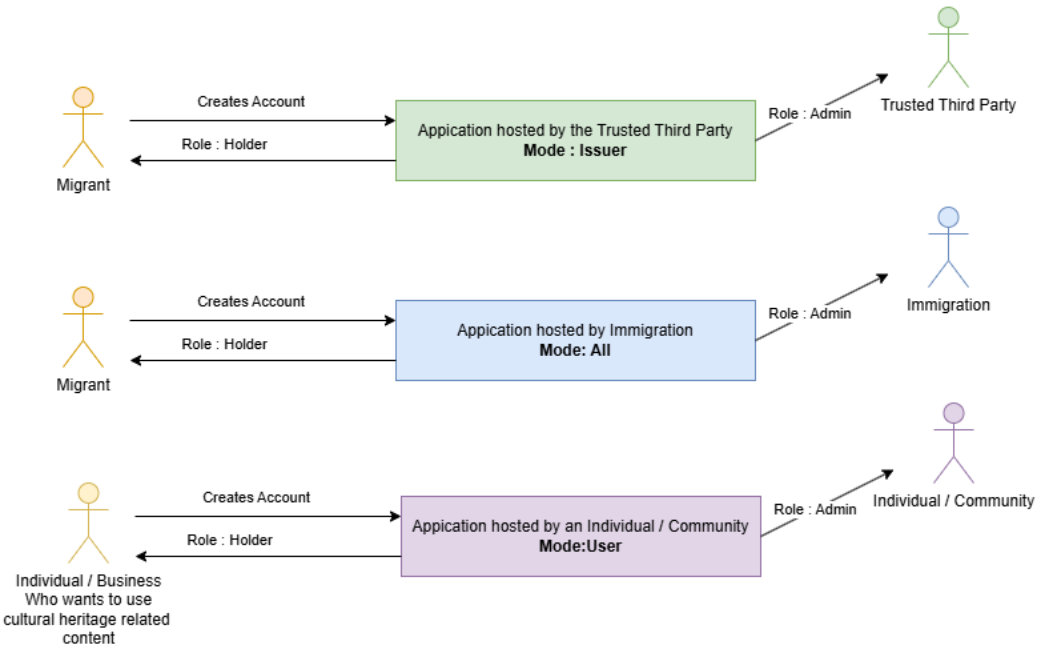


Figure 6.7: User Roles

6.6 Application Functionality and Communication Diagrams

This section describes the key operations of the application using a series of diagrams.

To illustrate how the prototype application functions and how communication occurs among its major components, the following sequence diagrams are presented. Figure 6.8 shows the different arrows used in the diagrams and their corresponding meanings.

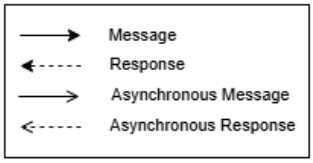


Figure 6.8: Arrows used and their meanings

6.7 DID Creation, Publishing and Resolution

Decentralised Identifiers (DIDs) are an important component of the prototype application. They serve as a fundamental element of Verifiable Credentials (VCs), providing a secure and decentralised means of representing identities. In the prototype application's workflow, a DID is required for migrants, trusted third parties, and any authority that issues a VC. However, it is not mandatory for immigration authorities. This workflow takes place within the DID creator's (or DID owner's) application.

In the All DIDs page, all DIDs are listed along with their details, such as their publication status. The user can either select an existing DID to view its details or create a new one. If a DID has not been published, the user has the option to publish it from the details page.

When creating a new DID, the user must provide a unique name, which serves as a label. This is useful because a user may have multiple DIDs for different purposes. Optionally, the user can add a description, as well as notification and status endpoints, depending on the intended use of the DID. Figure 6.9 illustrates this process.

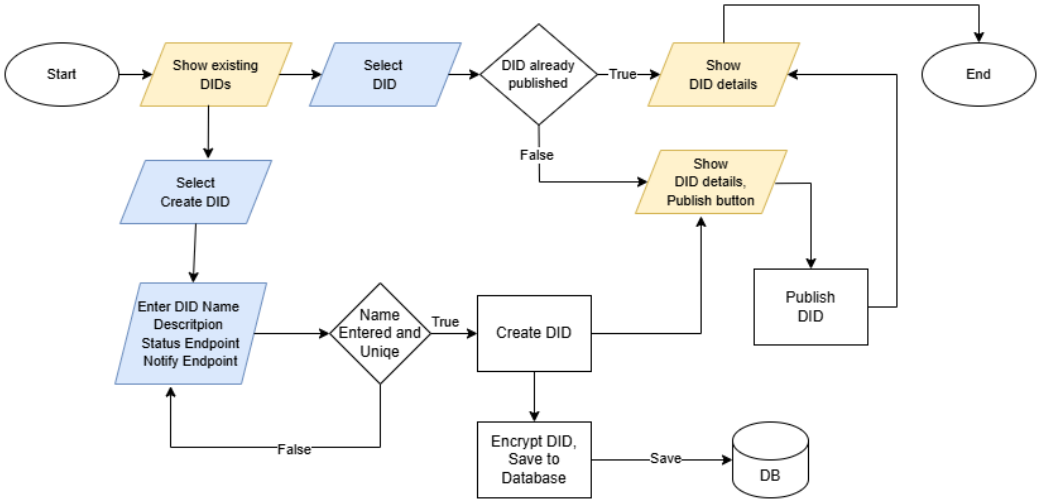


Figure 6.9: Flowchart of DID creation and publishing.

During DID creation, publication and resolution, several components of the system work together to accomplish the operation. Their interactions are shown in the sequence diagram in Figure 6.10. When a user initiates a DID

creation request, the CardanoWeb Application generates a JSON template and sends it via the CardanoBridge API's REST endpoint. The API then forwards the request to the Identus Cloud Agent through its corresponding REST API. The Identus Cloud Agent creates the DID and returns it to the CardanoBridge API, which subsequently shares it with the CardanoWeb Application.

After creation, the DID details are encrypted using AES-256 (see Section 6.21 for details), stored in the local database, and displayed to the user. If the user decides to publish the DID, the same routing flow is followed. The CardanoWeb Application communicates with the CardanoBridge API, which interacts with the Identus Cloud Agent to publish the DID. Once published, the DID becomes resolvable on the network after a delay of approximately 15 minutes to one hour, depending on block confirmation times.

The sequence diagrams also show the types of data exchanged between components and the APIs involved. Further details on the CardanoBridge API and its mapping to the Identus Cloud Agent APIs are provided in the CardanoBridge API section.

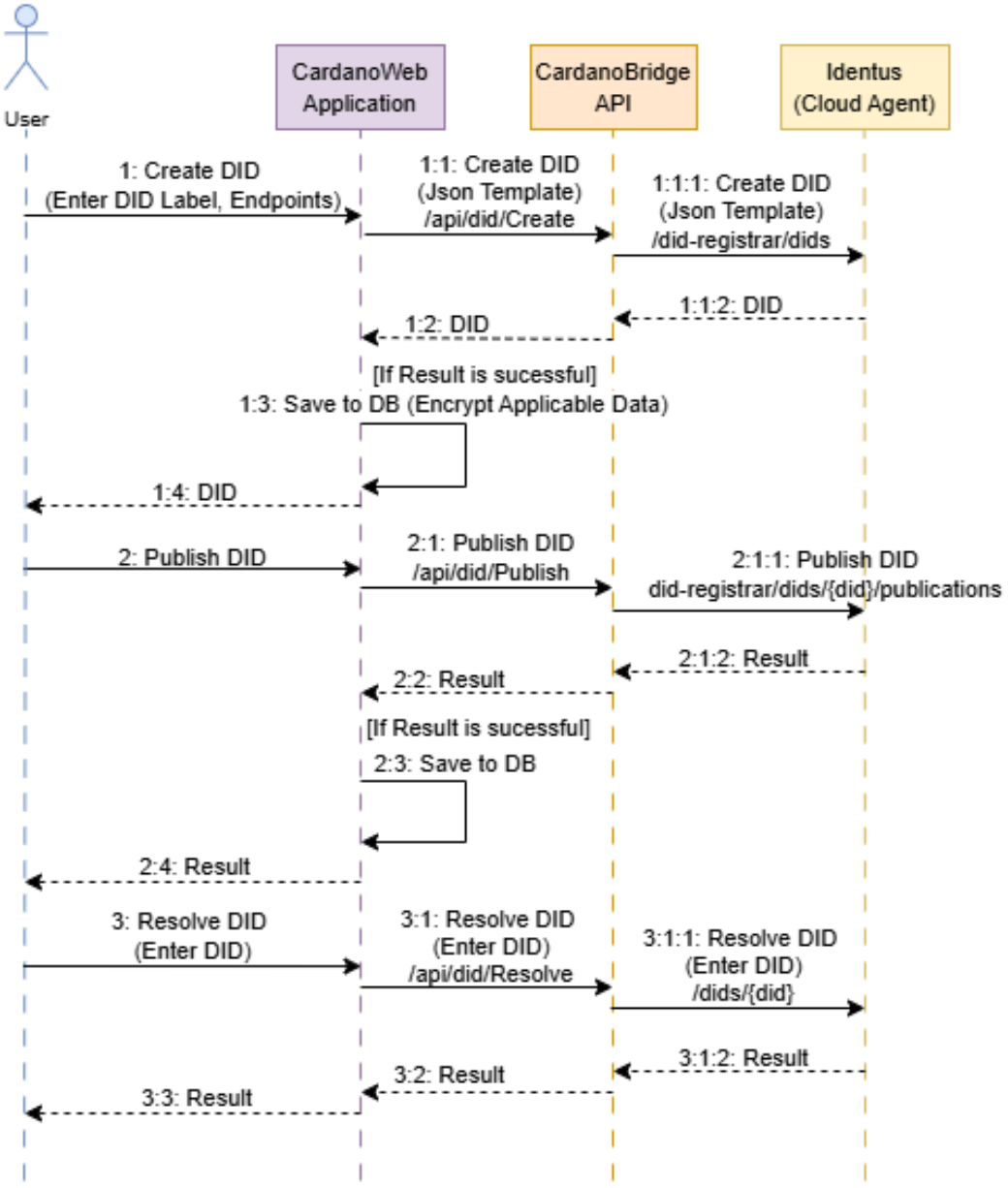


Figure 6.10: Sequence diagram of DID creation and publishing.

A sample JSON template used during DID creation is shown below.

```
  {
"documentTemplate": {
```

```
    "publicKeys": [
      {
        "id": "key-1",
        "purpose": "authentication",
        "curve": "Ed25519"
      },
      {
        "id": "assertion-1",
        "purpose": "assertionMethod",
        "curve": "Ed25519"
      }
    ],
    "services": [
    {
      "id": "9993d0ae-1cae-434e-93d6-286e64e82e0c",
      "type": "CredentialStatusService",
      "serviceEndpoint": "https://example.com/status"
    },
    {
      "id": "d5b8a9cb-e2f4-4bb2-a634-aaf3a2655d78",
      "type": "NotificationService",
      "serviceEndpoint": "https://example.com/notify"
    }
    ]
  }
}
```

6.8 Create Credential Request

Within the scope of this application, in order to obtain a credential, the migrant must submit a request to a trusted third party that is authorised to issue credentials, or whose credentials are recognised by the immigration authorities. This workflow takes place within the trusted third party's application, where the migrant creates a user account in order to obtain a VC.

Initially, the migrant needs to create a credential request by navigating to the Credential Request page. A nonce text will be displayed on this page. The migrant must then enter their DID and sign the nonce text using their private key (this process is explained in Section 6.19, Nonce Signing Process).

After this, the application attempts to resolve the DID to ensure that the entered DID is valid and published. The application then validates the signature of the nonce using the public key obtained from the DID specified by the migrant. This validation step ensures that the migrant is using the correct DID that they wish their credentials to be based on.

If either of these validations fails, the process cannot proceed, and the migrant is notified accordingly. If the validations are successful, the details are saved, and a credential request reference is generated. This reference is a randomly generated GUID prefixed with "VC-". It serves as an important identifier, as it is used during the credential issuance process and subsequently for tracking the validity status of the corresponding VC.

After this process, the migrant is directed to the Documents screen. If the migrant has previously uploaded any documents, they will be displayed, otherwise, they can upload new ones. The migrant can then select the documents that need to be verified. A single VC may contain information derived from multiple documents. The documents are encrypted using AES-256 during the upload process (see Section 6.21 for details). In the prototype, only PDF documents are allowed. These may be scanned versions of original documents (e.g. passport, payslip), compiled into a single PDF file, with each page of the document corresponding to one page in the PDF.

In the next step, the migrant can provide additional claims, referred to in the application as extra claims (for example, a claim such as "Salary is above $1000"). Once all the information is entered, the migrant can review and submit the credential request.Figure 6.11 illustrates a flow chart detailing this process.

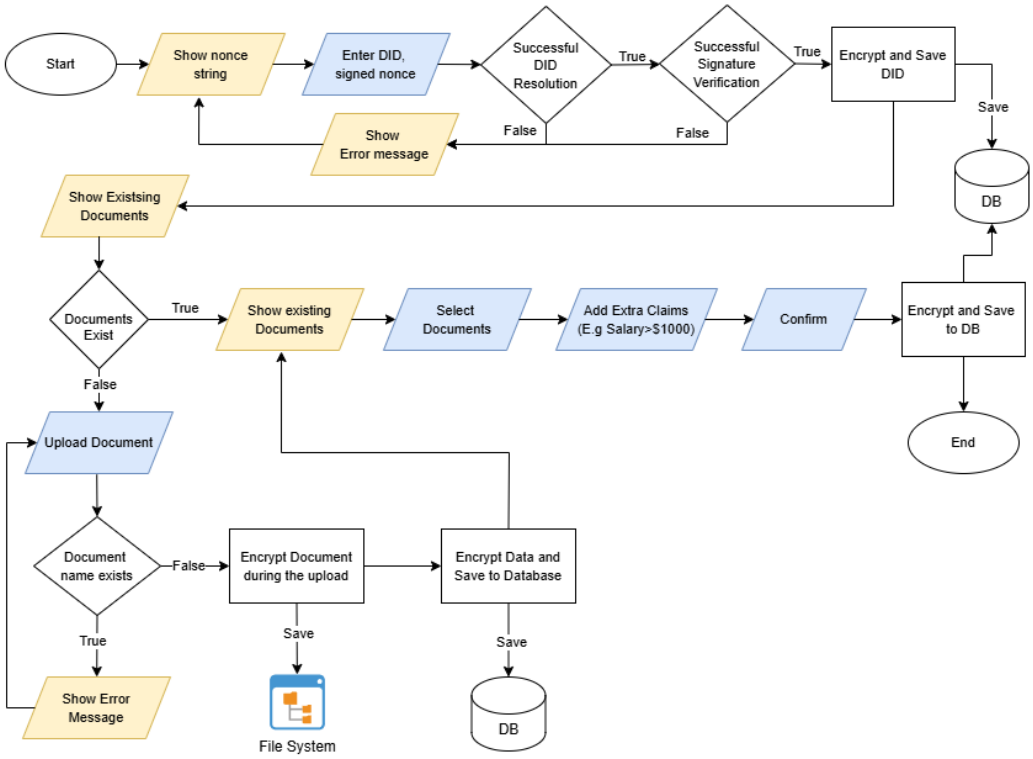


Figure 6.11: Flowchart of Credential Request.

The sequence diagram Figure 6.12 illustrates how the components of the application work together to create a credential request. Initially, when the user enters their DID and the signed nonce, the CardanoWeb application contacts the CardanoBridgeAPI to resolve the DID. If the DID is found, the application retrieves the corresponding public key. The CardanoWeb application then verifies the signature. If the signature is valid, the application stores the request data in the database. The migrant is then allowed to upload the documents. The documents are saved in the local file system, while the associated metadata is stored in the database.

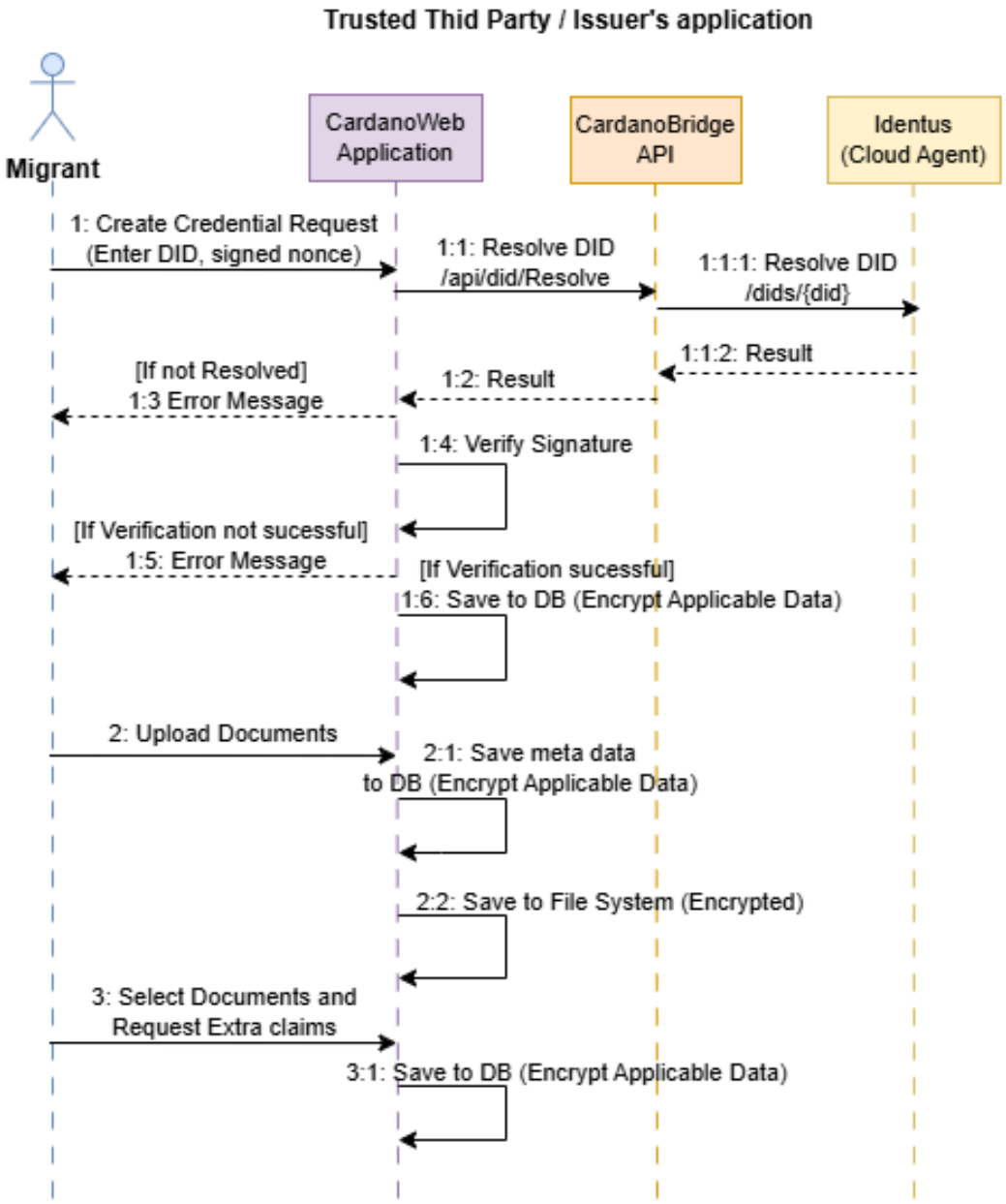


Figure 6.12: Sequence diagram of Credential Request.

6.9 Credential Request Processing

This workflow takes place within the trusted third party's application. When an officer who is authorised to issue credentials logs into the system and checks the Pending Credential Requests, they will be shown a list of requests. The officer can select a request and assign it to themselves. After this, they can review the documents attached to the request one by one and verify them. The verification process can be conducted according to the standards of the trusted third party. This may involve contacting the organisations that issued the original documents, or using any other verification method deemed appropriate.

If, after verification, the officer is not satisfied with the authenticity of the documents, they can reject the application, and the migrant will be notified. If the officer is satisfied with the verification results, they can issue a Verifiable Credential (VC) invitation to the migrant. Following this process, the documents relevant to the VC are added to the IPFS network. Figure 6.13 depicts this workflow in a flowchart.

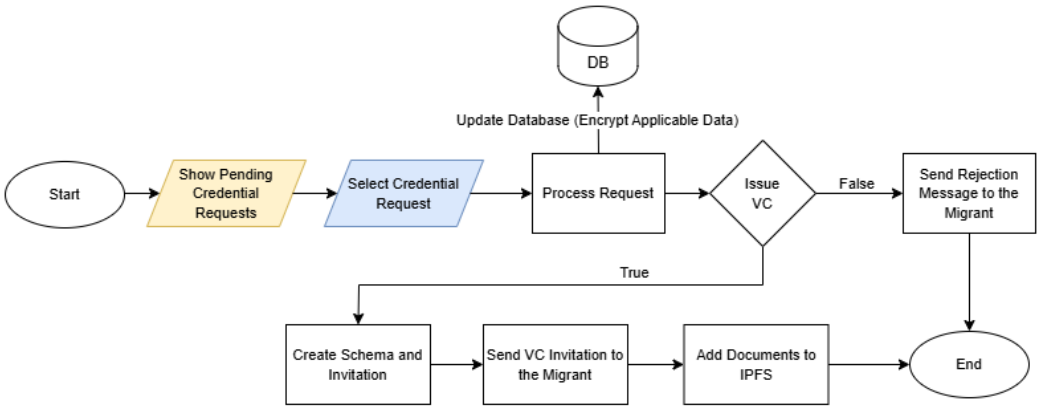


Figure 6.13: Flow Chart of Credential Request processing.

Figure 6.14 illustrates, in a sequence diagram, how the components of the prototype application operate during this process. When an officer checks the pending credential requests, the relevant documents are displayed to them. When a document is selected, it is read from the local file system, decrypted, and shown on the screen. The document cannot be downloaded or saved by the officer. If the credential request is rejected, the migrant will be notified

when they log into the system. If the credential request is accepted, an invitation is issued to the migrant in the same way.

In order to generate a credential offer invitation using the Identus Cloud Agent, a JSON schema first needs to be created to define the claims. This JSON schema is generated by the CardanoWeb application and then passed to the CardanoBridge API, which subsequently sends it to the relevant API endpoint of the Identus Cloud Agent. All communication occurs via REST APIs.

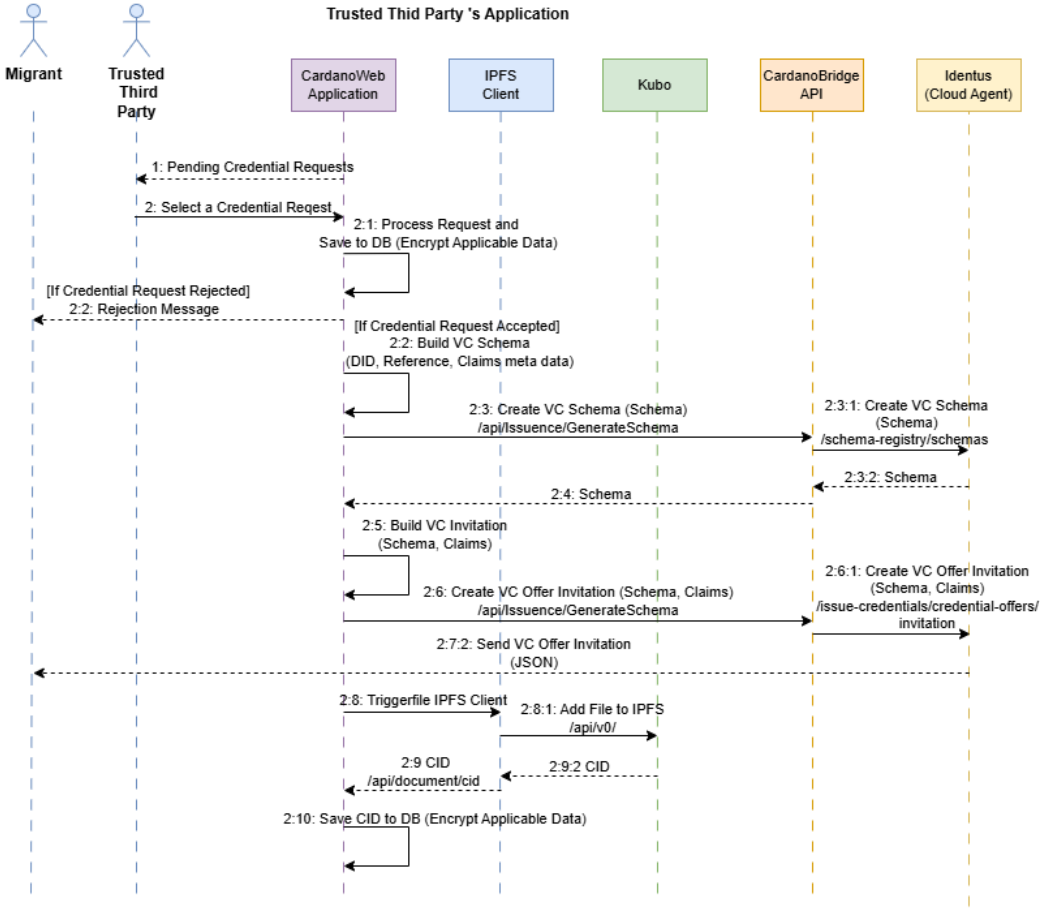


Figure 6.14: Sequence Diagram of Credential Request processing.

After creating the schema, the CardanoWeb application uses it to generate an invitation JSON, which follows a similar process to obtain the creden-

tial offer invitation from the Identus Cloud Agent. The resulting invitation is then shared with the migrant.

Below is an example of the JSON schema template. The author field contains a DID belonging to the issuing authority. The schema section defines the claims. In this example, a single VC combines the passport details and the migrant's job contract details. The fields givenName, familyName, dateOfIssuance, passportNo, and nationalStatus represent the passport attributes, while employerName, jobTitle, salary, and salaryAbove1000Dollars represent the employment-related claims derived from the job contract.

```
{
  "name": "passport-degree",
  "version": "1.0.0",
  "description": "Passport-Degree Schema",
  "type":
     "https://w3c-ccg.github.io/vc-json-schemas/schema/2.0/
  schema.json",
  "author":
     "did:prism:50d1adae855831a01a7f017d64688b6b99ae0c6a
  5fbfbecb77cd6c5d5ff89095",
  "tags": [
    "passport"
  ],
  "schema": {
    "$id": "https://example.com/passport-1.0.0",
    "$schema":
       "https://json-schema.org/draft/2020-12/schema",
    "description": "passport-salaryslip",
    "type": "object",
    "properties": {
      "givenName": {
        "type": "string"
      },
      "familyName": {
        "type": "string"
      },
      "dateOfIssuance": {
        "type": "string"
      },
      "passportNo": {
```

```
        "type": "string"
      },
      "nationalStatus": {
        "type": "string"
      },
      "employerName": {
        "type": "string"
      },
      "jobTitle": {
        "type": "string"
      },
      "monthlyPay": {
        "type": "string"
      },
      "monthlyPayAbove1000Dollars": {
        "type": "string"
      }
    },
    "required": [
      "givenName",
      "familyName",
      "dateOfIssuance",
      "passportNo",
      "nationalStatus",
      "employerName",
      "jobTitle",
      "monthlyPay",
      "monthlyPayAbove1000Dollars"
    ],
    "additionalProperties": true
  }
}
```

It is worth noting the field monthlyPayAbove1000Dollars. This is not a field directly taken from the contract. Within the application, migrants are allowed to create additional claims based on their documents, labelled as Extra Claims. This is one such example, where the migrant claims to earn more than $1000 based on their job contract. This information can be verified by the officer reviewing the request. If the document supports this claim, it can be added to the final VC issued to the migrant.

The JSON shown below serves as a template for creating a VC offer invitation. The claims and their corresponding values are included in this JSON structure to generate the VC offer invitation. The claims section follows the same structure and format as defined in the previously described schema. The credentialFormat field specifies whether the credential is of type SD-JWT or JWT. The issuingDID is the DID of the issuer, while the schemaId refers to the unique identifier of the generated schema, typically expressed as a URL path within the cloud agent application.

```
    {
  "claims": {
    "givenName": "Ada",
    "familyName": "Lovelace",
    "dateOfIssuance": "2025-01-01",
    "passportNo": "X123456",
    "nationalStatus": "United Kingdom",
    "employerName": "IT Corporation",
    "jobTitle": "Software Engineer",
    "monthlyPay": "2500",
    "monthlyPayAbove1000Dollars": "True"
  },
  "credentialFormat": "SDJWT",
  "issuingDID": "did:prism:
     did:prism:50d1adae855831a01a7f017d64688b6b99ae0c6a5fbfbec
  b77cd6c5d5ff89095",
  "schemaId":
     "http://host.docker.internal:8080/prism-agent/
  schema-registry/schemas/9b1aaf75-f06b-3bf2-84bf-74b8cd26b681",
  "validityPeriod": 36000
}
```

6.10 Accepting VC Invitation and Offer

When a migrant receives a Verifiable Credential (VC) invitation, it is provided in JWT format. The migrant copies this JWT and pastes it into the CardanoWeb application they control on the “Accept VC Invitation” page. Once this step is completed, a VC offer is generated and delivered to the application under the VC Offer page. The migrant can then choose to ei-

ther accept or reject the offer. If the offer is rejected, the credential issuance process ends.

In the prototype application, there is currently no option to update claims, though this could be implemented in future versions. When the migrant accepts the VC offer by providing their DID, the acceptance is sent from the CardanoWeb application to the CardanoBridge API, which forwards it to the Identus Cloud Agent. The Identus Cloud Agent then generates the credential offer in JSON format, which is returned to the CardanoWeb application. During the stage when the migrant confirms acceptance of the VC offer, the VC is issued and saved in their Identus wallet.

Behind the scenes, the migrant's Identus node communicates with the trusted third party's Identus node (see Figure 6.16). The first flowchart in Figure 6.15 shows the process of accepting a VC invitation, and the second shows the process of accepting a VC offer.

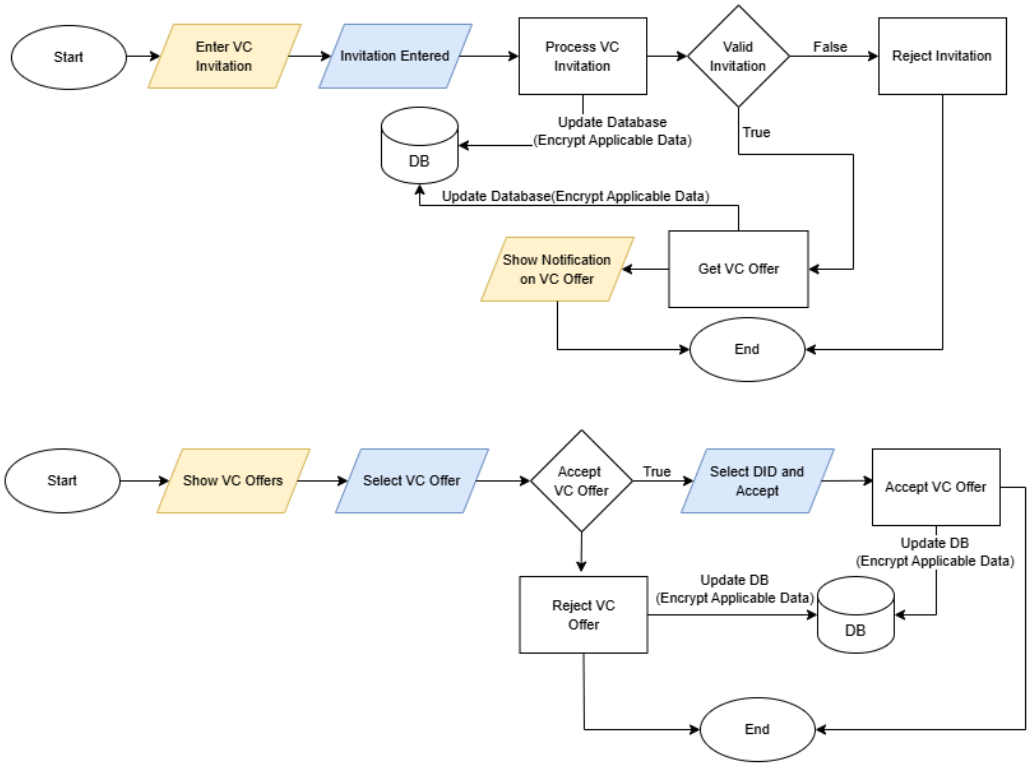


Figure 6.15: Flow Charts of Accepting VC Invitation.

The first sequence diagram Figure 6.16 illustrates the migrant receiving the VC offer invitation from the trusted third party's application. The second sequence diagram depicts the processes that occur within the migrant's application. The migrant provides the JWT formatted invitation, and the Cardano Web Application calls a REST endpoint in the Cardano Bridge API with this token. The token is then parsed and forwarded to the Identus Cloud Agent via a REST API. Behind the scenes, the Identus or Prism node operated by the migrant prepares to communicate with the trusted third party's node using the issuer's peer DID obtained from the invitation. The trusted third party's node then issues a VC offer, which will be exchanged over a secure Decentralised Identifier Communication version 2 (DIDComm v2) channel and can be retrieved via the Cardano Bridge API, then parsed to the Cardano Web Application. Once the user accepts the VC offer by supplying their DID, this information is again passed to the Cardano Bridge API and subsequently to the Identus Cloud Agent. The completed VC is then returned to the migrant's wallet following the same sequence. It is worth noting that the VC issuance process, including the invitation, offer, and issuance phases, relies on DIDComm v2 messaging as implemented within Hyperledger Identus.

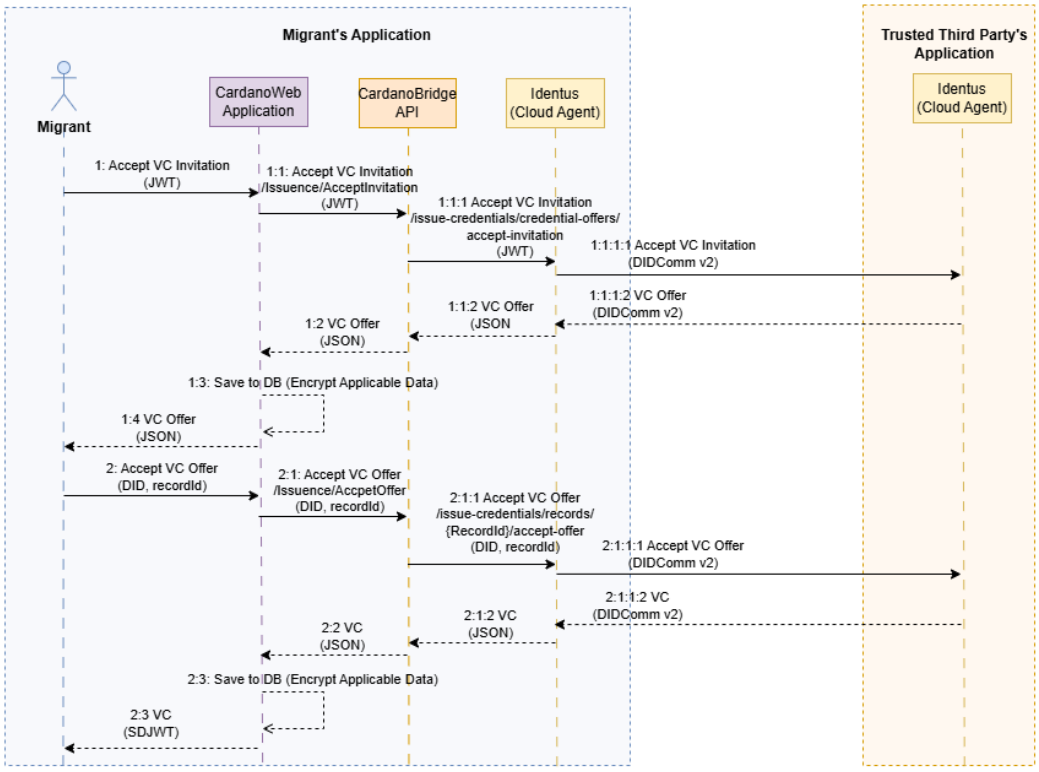


Figure 6.16: Sequence Diagrams of Accepting VC Invitation.

DIDComm is a messaging protocol used between two decentralised entities to establish secure, private, end-to-end encrypted communication. It uses DIDs as the basis for cryptographic operations between these entities. Hyperledger Identus utilises this protocol during the verifiable credential issuance process. The VC invitation, received in JWT format, contains the information required for the migrant's Identus agent to establish communication with the trusted third party's Identus agent.

6.11 Verification Process

When a migrant needs to apply for a visa or other migration related services, they can use their VC instead of presenting traditional physical documents. In the prototype implementation, the immigration authority operates its own instance of the CardanoWeb Application.

In order to begin the verification process, the migrant first selects their VC and selects the claims they wish to disclose. This process is done within the migrant's CardanoWeb Application. They navigate to the Credential Wallet page, where all VCs and their associated metadata are displayed. From there, the migrant selects the VC they intend to share with the immigration authority or other relevant entities. On the following page, they can choose which claims to disclose and then generate a presentation, which is an SD-JWT containing only the selected information. This presentation is later used by the immigration authority's application during the verification process.

The migrant then creates an account in the immigration authority's CardanoWeb Application and navigates to the Create Verification Request page. At this stage, a nonce is displayed. The migrant enters their Decentralised Identifier (DID) and their VC (in SD-JWT format) and digitally signs the nonce using their private key. This process, which ensures the authenticity of the request and the validity of the DID, is described in detail in Section 5.4.3, Digital Signatures. After completing these steps, the migrant submits the verification request. This process is illustrated in the first flowchart in Figure 6.17.

When the immigration authority logs into their CardanoWeb Application, they can view the list of pending verification requests under the Pending Verification Requests section. They can then select and assign a request to themselves. After doing so, the authority can view the claims contained in the VC. The system also verifies and displays whether the issuer's signature on the VC is valid and whether the subject of the VC matches the identity of the person submitting the verification request. This process is shown in the second flowchart in Figure 6.17.

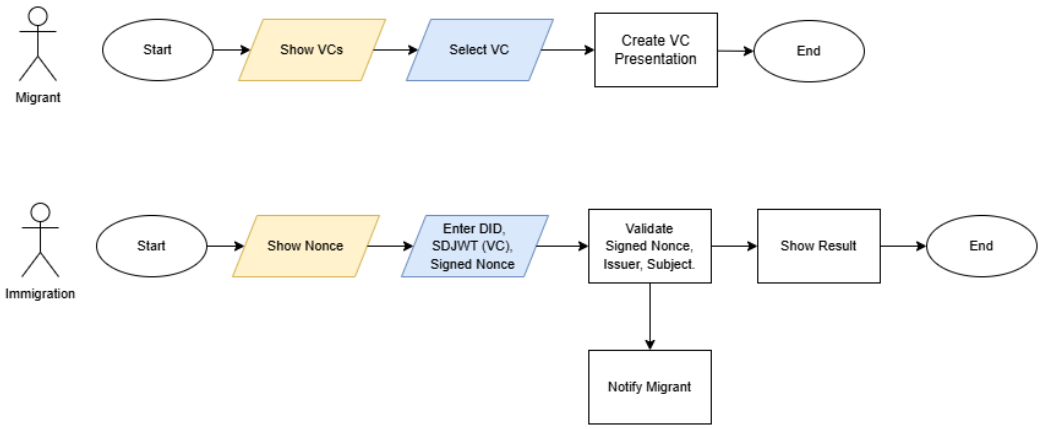


Figure 6.17: Flow Charts of Verification Process.

When a Verification Request is assigned to an officer, a notification is automatically sent to the migrant to whom the VC belongs. This is carried out using the Notification Endpoint specified in the migrant's DID document, under the Services section (see Figure 5.6). The Notification Endpoint is an API that forms part of the CardanoWeb Application. When a message is passed to this API, it appears in the migrant's notifications.

During the verification process, when the immigration authority reviews a verification credential request, the CardanoWeb Application first resolves the requester's DID by sending the DID details to the Cardano Bridge API, which forwards the request to the Identus Cloud Agent. The Identus Cloud Agent retrieves the corresponding DID Document and returns it to the Cardano Bridge API, which then relays it to the Cardano Web Application. Using the public key obtained from the DID Document, the application verifies the SD-JWT token associated with the VC. The sequence diagram in Figure 6.18 illustrates how the modules of the prototype application interact during this verification process.

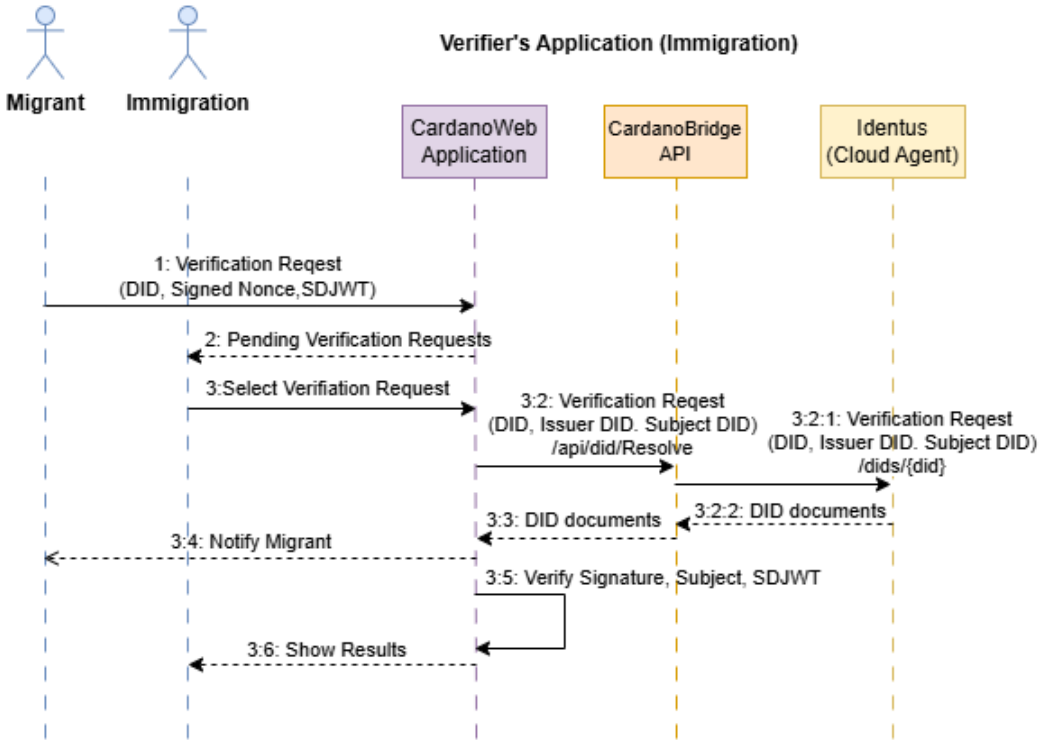


Figure 6.18: Sequence Diagram of Verification Process.

6.12 Document Re-verification

If, for any reason, the trusted third party needs to re-verify the documents for which a VC has already been issued, they can do so through the process. On the page, the VC reference must be entered. Once this is done, the CardanoWeb Application notifies the IPFS client to fetch the documents associated with the VC reference. The IPFS client, running in the background, communicates with Kubo and downloads the relevant files. These files are then decrypted and displayed to the trusted third party.

When a document re-verification is performed, a notification is automatically sent to the migrant to whom the VC belongs. This process occurs in a similar way as the notification process described in the Verification Process section.

The flow chart in Figure 6.19 and the sequence diagram in Figure 6.20 illustrate this process.

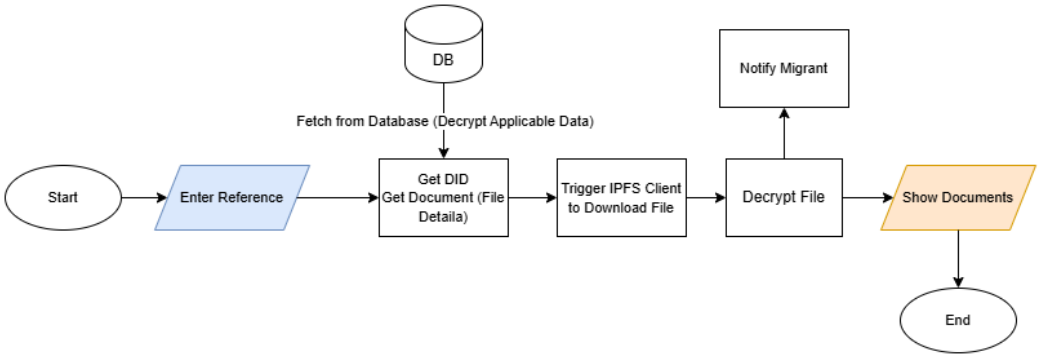


Figure 6.19: Flow Chart of Re-verification Process.

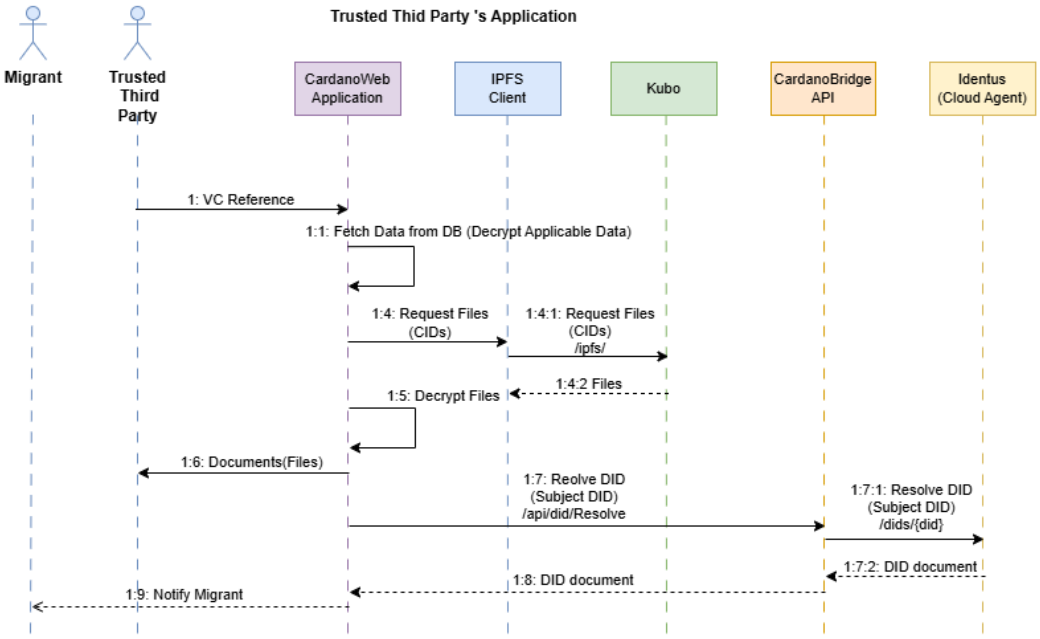


Figure 6.20: Sequence Diagram of Re-verification Process.

6.13 VC Status Check

If an immigration officer needs to check the status of a VC, for example to determine whether it has been revoked, they can do so using the status

check feature. During the verification process, the URL for the status check is displayed on the verification results page. This URL is obtained from the Status Endpoint listed under the Services section in the DID document of the VC issuer. The immigration officer can click this URL to access the status check page of the trusted authority, where they can enter the VC details and view the results. This process is illustrated in Figure 6.21 and Figure 6.22. This process occurs within the trusted third party's application.

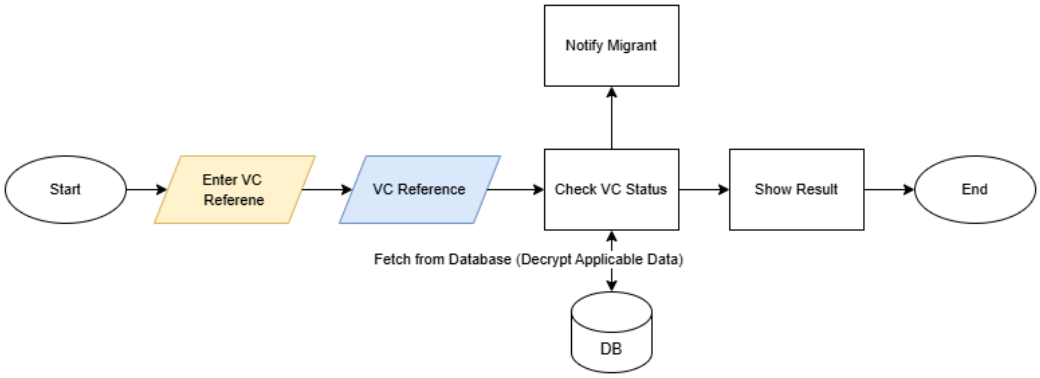


Figure 6.21: Flow Chart of Status Check Process.

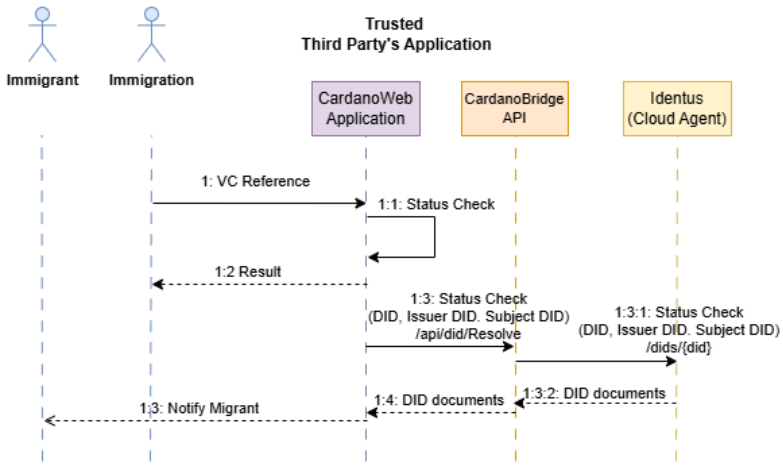


Figure 6.22: Sequence Diagram of Status Check Process.

When a status check is performed, a notification is automatically sent to

the migrant to whom the VC belongs. This process occurs in the same manner as the notification process described in the Verification Process section.

6.14 Artefact Uploading

The artefact related features become available when the application configuration in *appsettings.json* is set to "User". The individual or community that owns the artefact can upload content via the Create Artefact page. The artefact owner can provide a unique title and description, select the content type, and upload the file. The available content types include text, video, audio, and image.

During the upload process, the artefact is encrypted using a strong random key, and the associated metadata is stored in the local database. Subsequently, the IPFS client is triggered to add the file to the IPFS network. In the background, the IPFS client communicates with Kubo to perform this operation. Once the file is successfully added to the IPFS network, a Content Identifier (CID) is returned to the IPFS client. The client then sends this CID to the CardanoWeb Application via a REST API call. Before being stored in the local database, the CID is encrypted to enhance security.

Figure 6.23 illustrates the flowchart of this process, and Figure 6.24 presents the corresponding sequence diagram.

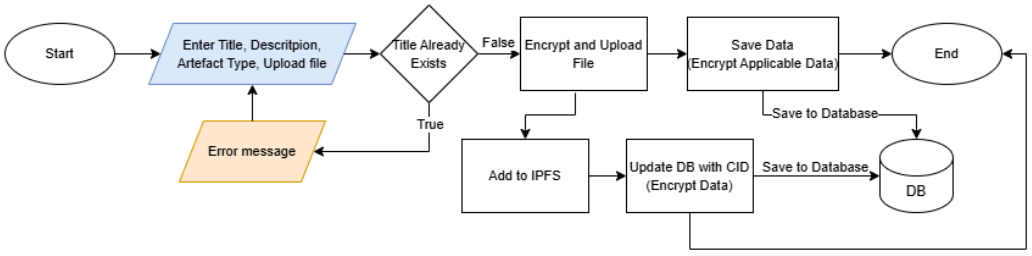


Figure 6.23: Flow Chart of Artefact Uploading Process.

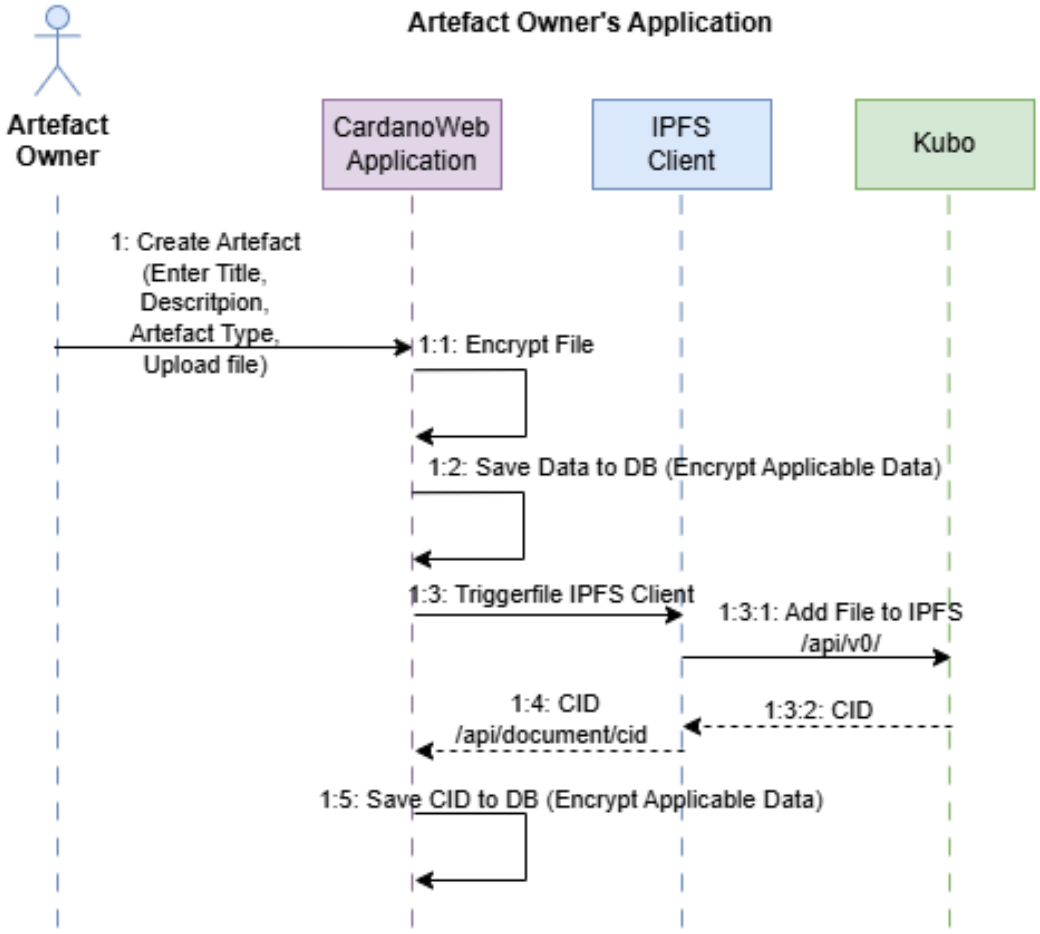


Figure 6.24: Sequence Diagram of Artefact Uploading Process.

6.15 Requesting Artefact

When an individual or organisation requires an artefact, they can create an account within the CardanoWeb Application hosted by the artefact owner. Once registered, the user can search for the required artefact via the Catalogue page by entering relevant keywords. When a search is initiated, the application searches for the specified keywords within the artefact titles and descriptions to identify matches. The matching artefacts are then displayed in a list, along with their corresponding metadata.

The user can then select the desired artefact, which redirects them to a page where they are required to enter their DID and sign a nonce. This step ensures that the requester is using the correct DID and allows the artefact owner to verify that the credential is being issued to the legitimate DID. Similar to the process used when a migrant creates a credential request (see Create Credential Request, Section 6.8), the system first checks whether the DID can be resolved, followed by verification of the signed nonce. The underlying technical processes and APIs used are identical to those described in Section 6.8.

If the validations are successful, the request details are stored, and a credential request reference is generated. This reference is a randomly generated Globally Unique Identifier (GUID) prefixed with "AVC-". It serves as an important identifier during the credential issuance process and is subsequently used to track the validity status of the corresponding VC.

Once the credential request reference has been generated, the individual or organisation is required to enter additional details related to the request, such as Duration, Scope of Use, and Territory. After completing these fields, the requester can submit the artefact request. The process flow is illustrated in Figure 6.25, and the corresponding sequence of operations is presented in Figure 6.26.

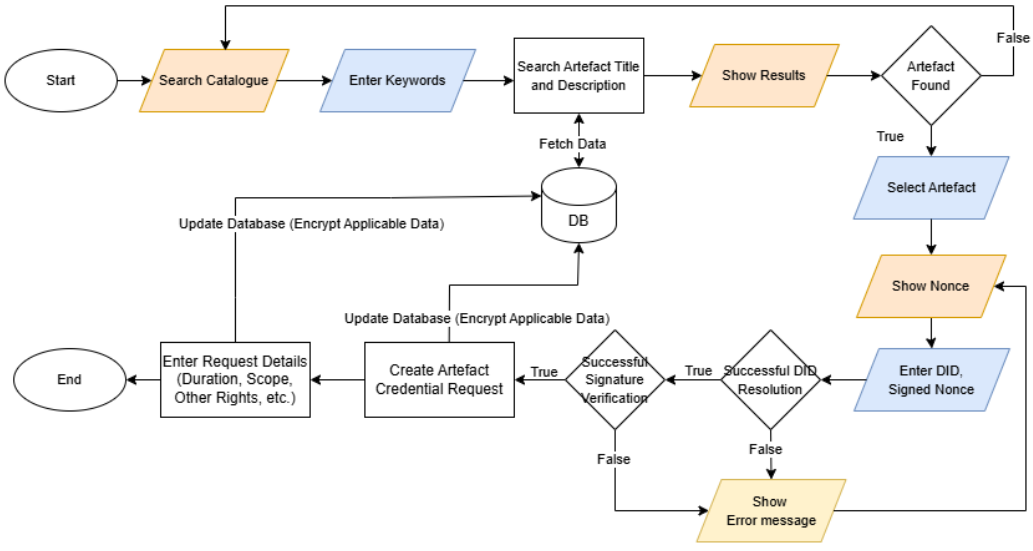


Figure 6.25: Flow Chart of Requesting Artefact Process.

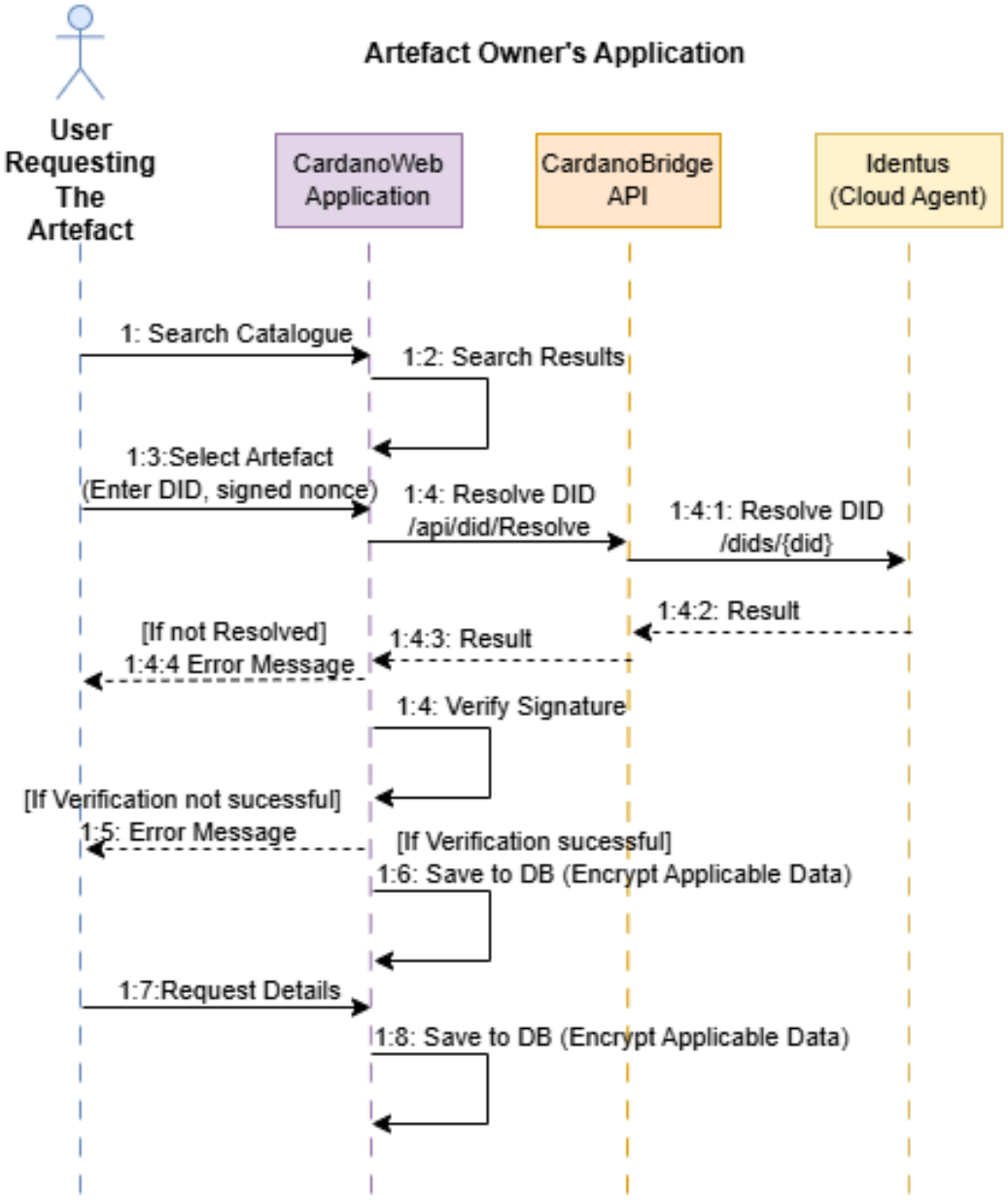


Figure 6.26: Sequence Diagram of Requesting Artefact Process.

It is worth noting that, for migrant related documents, the system allows a single VC to cover multiple documents, as these are typically issued by a central authority and are unlikely to change ownership or usage terms over

time. In contrast, artefacts are often individually or jointly owned (for example, by communities), and ownership may change, rights may be transferred, or heirs may inherit intellectual property. Therefore, each artefact requires a separate VC. This approach provides detailed access control, enabling artefact owners to manage permissions, validity periods, and VC revocation for each artefact independently. It also ensures that revoking the VC for one artefact does not affect access to other artefacts. Furthermore, different artefacts may require customised validity periods. For example, a song may have a VC valid for two years, whereas an image may only require a few months. Individual VCs also facilitate precise auditing and tracking of access, which is important for copyright management and legal compliance (for consideration in future versions). Overall, these considerations justify the decision to restrict one VC per artefact, while still allowing a single VC for multiple migrant related documents.

6.16 Artefact Credential Request Processing

When a request for a credential for an artefact is submitted, the processing is similar to the Credential Request Processing for migrant-related documents. Upon logging into the CardanoWeb Application, the artefact owner can view pending requests. The owner may then select a request and either reject it or issue a VC. The technical procedures are largely the same as those described in Section 6.9, Credential Request Processing. The main difference is that, instead of issuing an SD-JWT VC, a standard JWT VC is issued for artefacts. Figure 6.27 illustrates the flowchart for this process, while Figure 6.28 presents the corresponding sequence diagram.

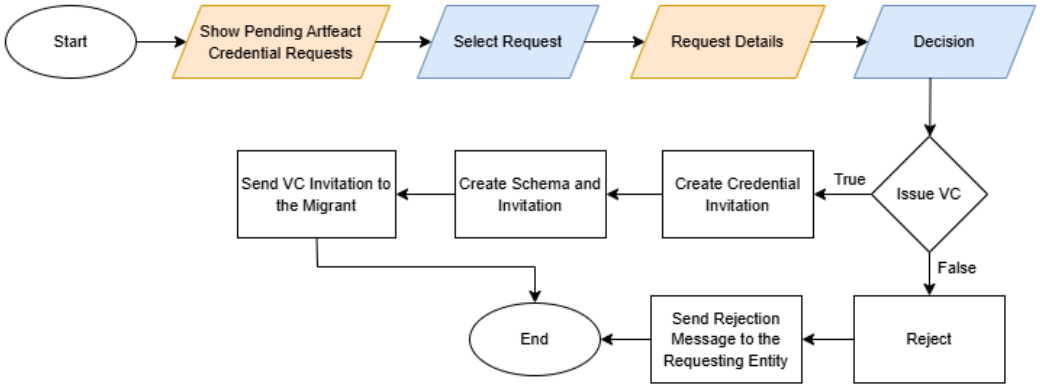


Figure 6.27: Flow Chart of Requesting Artefact Credential Request Processing.

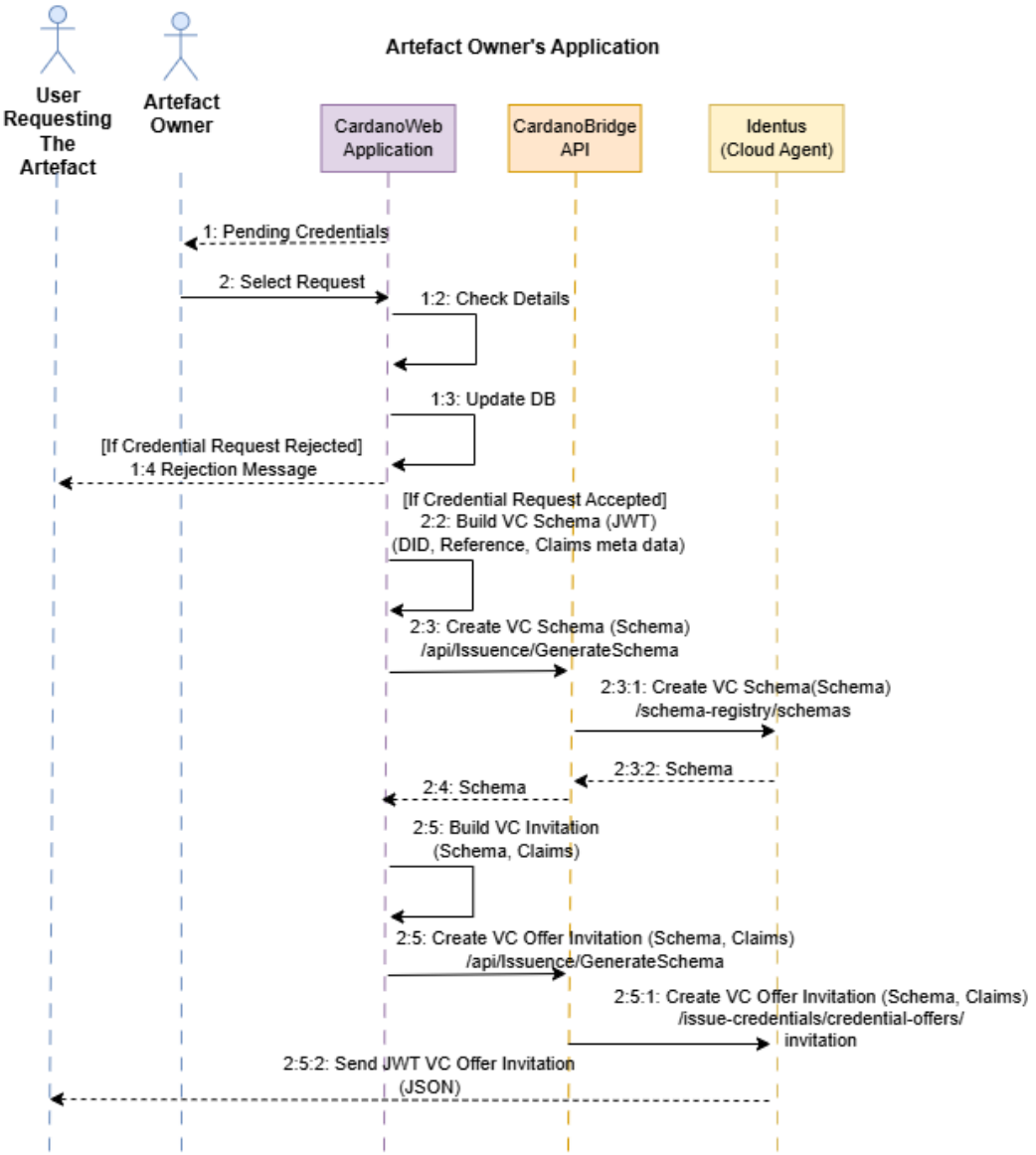


Figure 6.28: Sequence Diagram of Artefact Credential Request Processing.

6.17 Accepting Artefact VC Invitation and Offer

The process of accepting an artefact VC invitation and offer is similar to the procedure described in Section 6.10, Accepting VC Invitation and Offer. There are, however, two minor differences. First, in this case, a JWT-based VC is used instead of an SD-JWT-based VC. Second, after the credential offer invitation is issued, when the user logs into the Artefact Owner's CardanoWeb application, they will see a button to download the artefact on the All Credential Requests page, under their credential request. The user is expected to download the content after accepting the offer, otherwise, it is considered unauthorised use.

This approach allows users to access the artefact immediately after the invitation is issued. Although it would be possible to restrict downloads until after the offer is accepted, implementing such logic would significantly increase system complexity. More importantly, the primary purpose of the application is not merely to manage content, but to manage rights. By treating downloads without VC invitation and VC offer acceptance as unauthorised, the system enforces proper rights management while maintaining a practical and usable implementation. Furthermore, unless the user accepts the invitation and offer, they will not be able to present the VC when required to prove their rights to use the content.

6.18 Verification Process

The process of verifying an artefact is slightly different from the process of verifying a verifiable credential (VC) related to the migration process. In the case of an artefact, the VC will be JWT based rather than SD-JWT. Additionally, there is no verification request flow for artefact verification, unlike the migration process. However, the technical implementation is similar to the procedure described in Section 6.11, Verification Process. Therefore, a detailed explanation is not repeated here.

6.19 Nonce Signing Process

In certain processes, nonce signing may be required to prove ownership of the DI. To sign a nonce, the user navigates to the Sign Nonce page, where they enter their DID and the nonce text. If the DID exists in their wallet, the signed nonce will be displayed. This process is illustrated in the flowchart in Figure 6.29.

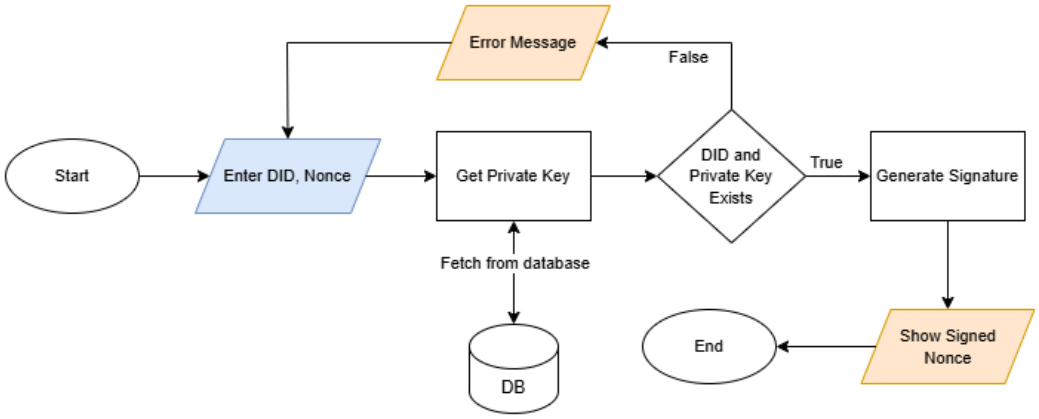


Figure 6.29: Flow Chart of Signing Processing.

During the signing process, the CardanoWeb Application sends the DID and nonce text to the CardanoBridge API via REST APIs. The CardanoBridge API then retrieves the private key associated with the DID from the Agent Database within the Identus Cloud Agent's database environment. The API signs the nonce text using the Ed25519 algorithm and returns the signed nonce to the CardanoWeb Application. The following sequence diagram is shown in Figure 6.30, which depicts this process in detail.

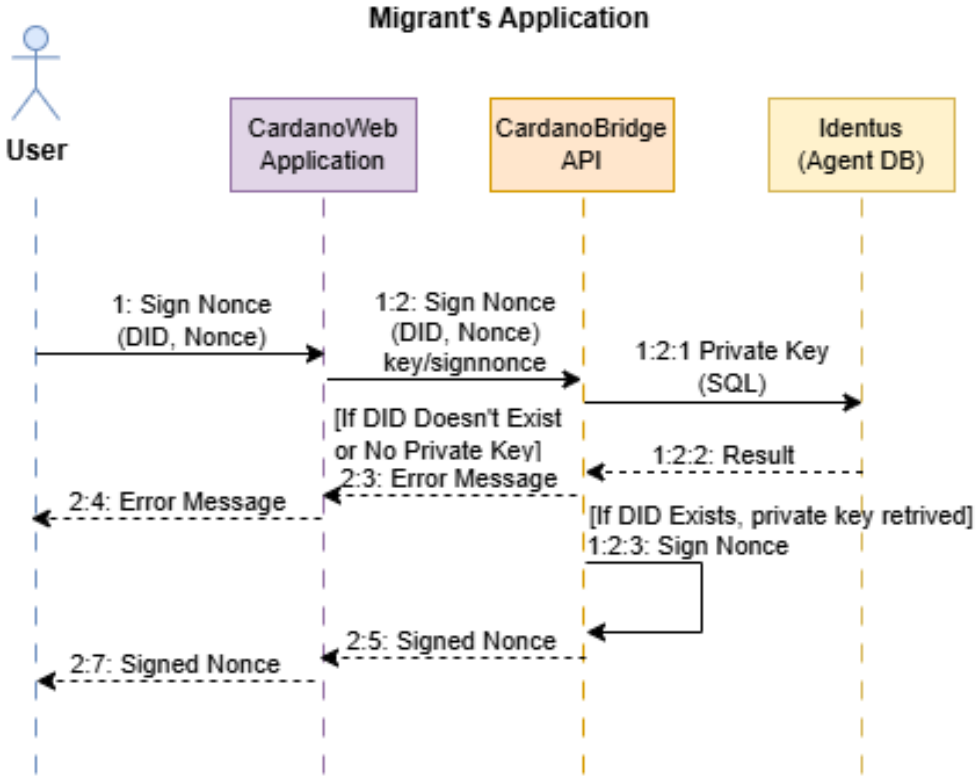


Figure 6.30: Sequence Diagram of Signing Processing.

6.20 The Database

The CardanoWeb application uses a relational data model implemented in a PostgreSQL database (version 17.5). The database is managed through Microsoft Entity Framework Core (version 9.0.8) and the Microsoft.EntityFrameworkCore.PostgreSQL provider to enable connectivity with PostgreSQL [83].

All fields within the tables that may contain personal or sensitive data are encrypted before being stored. Figures 6.31 and 6.32 present the Entity–Relationship (ER) diagram of the database. Tables 6.5 to 6.31 provide detailed information about the database tables, including their fields, key types, and encryption status.

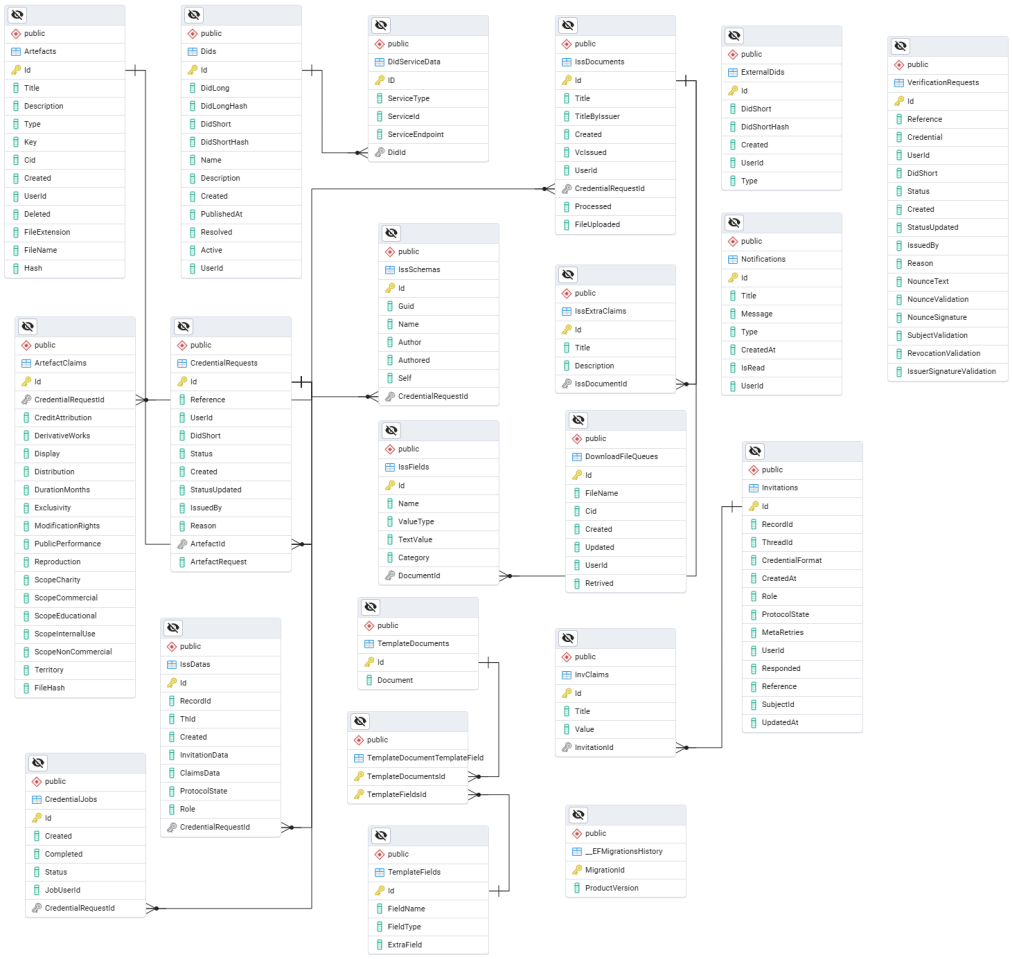


Figure 6.31: ER Diagram of the Database Part 1

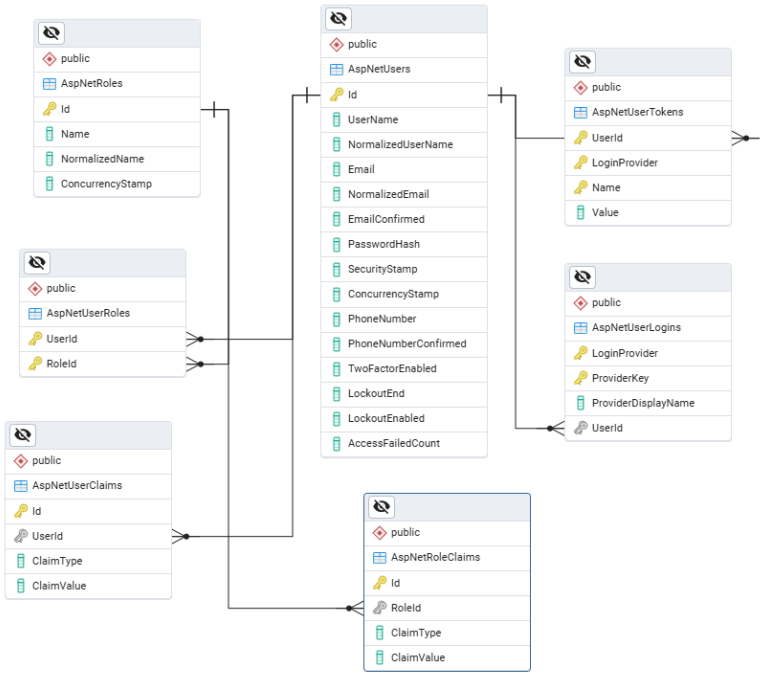


Figure 6.32: ER Diagram of the Database Part 2

6.20.1 Details of the database tables

ArtefactClaims: Stores information on artefact claims.

Field	**Type**	**Encrypted**
Id (PK)	integer	No
CredentialRequestId (FK)	integer	No
CreditAttribution	boolean	No
DerivativeWorks	boolean	No
Display	boolean	No
Distribution	boolean	No
DurationMonths	integer	No
Exclusivity	text	No
ModificationRights	boolean	No
PublicPerformance	boolean	No
Reproduction	boolean	No
ScopeCharity	boolean	No
ScopeCommercial	boolean	No
ScopeEducational	boolean	No
ScopeInternalUse	boolean	No
ScopeNonCommercial	boolean	No
Territory	text	No
FileHash	text	No

Table 6.5: Fields of the ArtefactClaims table

Artefacts: Contains information on artefacts.

Field	**Type**	**Encrypted**
Id (PK)	integer	No
Title	text	No
Description	text	No
Type	text	No
Key	text	Yes
Cid	text	Yes
Created	timestamp with time zone	No
UserId	text	No
Deleted	boolean	No
FileExtension	text	No
FileName	text	Yes
Hash	text	No

Table 6.6: Fields of the Artefacts table

CredentialJobs: Stores information about credential processing jobs.

Field	**Type**	**Encrypted**
Id (PK)	integer	No
Created	timestamp with time zone	No
Completed	timestamp with time zone	No
Status	integer	No
JobUserId	text	No
CredentialRequestId (FK)	integer	No

Table 6.7: Fields of the CredentialJobs table

CredentialRequests: Contains details of credential requests made by migrants.

Field	**Type**	**Encrypted**
Id (PK)	integer	No
Reference	text	No
UserId	text	No
DidShort	text	Yes
Status	integer	No
Created	timestamp with time zone	No
StatusUpdated	timestamp with time zone	No
IssuedBy	text	No
Reason	text	No
ArtefactId (FK)	integer	No
ArtefactRequest	boolean	No

Table 6.8: Fields of the CredentialRequests table

DidServiceData: Stores information about DID service details, such as endpoint information.

Field	**Type**	**Encrypted**
ID (PK)	integer	No
ServiceType	text	No
ServiceId	integer	No
ServiceEndpoint	text	Yes
DidId (FK)	integer	No

Table 6.9: Fields of the DidServiceData table

Dids: Contains information on DIDs and related metadata.

Field	**Type**	**Encrypted**
Id (PK)	integer	No
DidLong	text	Yes
DidLongHash	text	No
DidShort	text	Yes
DidShortHash	text	No
Name	text	No
Description	text	No
Created	timestamp with time zone	No
PublishedAt	timestamp with time zone	No
Resolved	boolean	No
Active	boolean	No
UserId	text	No

Table 6.10: Fields of the Dids table

DownloadFileQueues: Stores information about files queued for download, including metadata.

Field	**Type**	**Encrypted**
Id (PK)	integer	No
FileName	text	No
Cid	text	No
Created	timestamp with time zone	No
Updated	timestamp with time zone	No
UserId	text	No
Retrived	boolean	No

Table 6.11: Fields of the DownloadFileQueues table

ExternalDids: Stores information about external DIDs (DIDs from external parties) and their associated metadata.

Field	**Type**	**Encrypted**
Id (PK)	integer	No
DidShort	text	Yes
DidShortHash	text	No
Created	timestamp with time zone	No
UserId	text	No
Type	text	No

Table 6.12: Fields of the ExternalDids table

InvClaims: Stores information about individual claims associated with invitations.

Field	**Type**	**Encrypted**
Id (PK)	integer	No
Title	text	No
Value	text	No
InvitationId (FK)	integer	No

Table 6.13: Fields of the InvClaims table

Invitations: Contains details of invitations sent to users, including metadata and protocol state.

Field	Type	Encrypted
Id (PK)	integer	No
RecordId	text	No
ThreadId	text	No
CredentialFormat	text	No
CreatedAt	timestamp with time zone	No
Role	text	No
ProtocolState	text	No
MetaRetries	integer	No
UserId	text	No
Responded	boolean	No
Reference	text	No
SubjectId	text	No
UpdatedAt	timestamp with time zone	No

Table 6.14: Fields of the Invitations table

IssDatas: Stores issued data entries related to offer invitations and claims.

Field	Type	Encrypted
Id (PK)	integer	No
RecordId	text	No
ThId	text	No
Created	timestamp with time zone	No
InvitationData	text	No
ClaimsData	text	Yes
ProtocolState	text	No
Role	text	No
CredentialRequestId (FK)	integer	No

Table 6.15: Fields of the IssDatas table

IssDocuments: Contains information about migrant documents linked to credential requests.

Field	Type	Encrypted
Id (PK)	integer	No
Title	text	No
TitleByIssuer	text	No
Created	timestamp with time zone	No
VcIssued	boolean	No
UserId	text	No
CredentialRequestId (FK)	integer	No
Processed	boolean	No
FileUploaded	boolean	No

Table 6.16: Fields of the IssDocuments table

IssExtraClaims: Stores additional claims associated with documents attached to credential requests.

Field	Type	Encrypted
Id (PK)	integer	No
Title	text	No
Description	text	No
IssDocumentId (FK)	integer	No

Table 6.17: Fields of the IssExtraClaims table

IssFields: Contains fields associated with documents attached to credential requests, including type and value information.

Field	Type	Encrypted
Id (PK)	integer	No
Name	text	No
ValueType	text	No
TextValue	text	Yes
Category	integer	No
DocumentId (FK)	integer	No

Table 6.18: Fields of the IssFields table

IssSchemas: Stores schema definitions for VCs, including the associated credential request.

Field	Type	Encrypted
Id (PK)	integer	No
Guid	text	No
Name	text	No
Author	text	No
Authored	timestamp with time zone	No
Self	text	No
CredentialRequestId (FK)	integer	No

Table 6.19: Fields of the IssSchemas table

Notifications: Stores notifications for users, including message content and read status.

Field	Type	Encrypted
Id (PK)	integer	No
Title	text	No
Message	text	No
Type	text	No
CreatedAt	timestamp with time zone	No
IsRead	boolean	No
UserId	text	No

Table 6.20: Fields of the Notifications table

TemplateDocumentTemplateField: Links template documents with their template fields.

Field	Type	Encrypted
TemplateDocumentsId (PK)	integer	No
TemplateFieldsId (PK)	integer	No

Table 6.21: Fields of the TemplateDocumentTemplateField table

TemplateDocuments: Stores template documents used in the system (e.g., passport, bank statement).

Field	Type	Encrypted
Id (PK)	integer	No
Document	text	No

Table 6.22: Fields of the TemplateDocuments table

TemplateFields: Contains fields for template documents, including the field type and extra field flag.

Field	Type	Encrypted
Id (PK)	integer	No
FieldName	text	No
FieldType	text	No
ExtraField	boolean	No

Table 6.23: Fields of the TemplateFields table

VerificationRequests: Stores verification requests submitted by users, including credentials, DID information, and validation statuses.

Field	**Type**	**Encrypted**
Id	integer	No
Reference	text	No
Credential	text	No
UserId	text	No
DidShort	text	No
Status	integer	No
Created	timestamp with time zone	No
StatusUpdated	timestamp with time zone	No
IssuedBy	text	No
Reason	text	No
NounceText	text	No
NounceValidation	boolean	No
NounceSignature	text	No
SubjectValidation	boolean	No
RevocationValidation	boolean	No
IssuerSignatureValidation	boolean	No

Table 6.24: Fields of the VerificationRequests table

AspNetRoleClaims: Stores claims associated with roles.

Field	**Type**	**Encrypted**
Id	integer	N/A
RoleId	text	N/A
ClaimType	text	N/A
ClaimValue	text	N/A

Table 6.25: Fields of the AspNetRoleClaims table

AspNetRoles: Stores roles used in the identity system.

Field	Type	Encrypted
Id	text	N/A
Name	character varying	N/A
NormalizedName	character varying	N/A
ConcurrencyStamp	text	N/A

Table 6.26: Fields of the AspNetRoles table

AspNetUserClaims: Stores claims associated with users.

Field	Type	Encrypted
Id	integer	N/A
UserId	text	N/A
ClaimType	text	N/A
ClaimValue	text	N/A

Table 6.27: Fields of the AspNetUserClaims table

AspNetUserLogins: Stores login information for users.

Field	Type	Encrypted
LoginProvider	text	N/A
ProviderKey	text	N/A
ProviderDisplayName	text	N/A
UserId	text	N/A

Table 6.28: Fields of the AspNetUserLogins table

AspNetUserRoles: Stores the mapping between users and roles.

Field	Type	Encrypted
UserId	text	N/A
RoleId	text	N/A

Table 6.29: Fields of the AspNetUserRoles table

AspNetUserTokens: Stores authentication tokens for users.

Field	Type	Encrypted
UserId	text	N/A
LoginProvider	text	N/A
Name	text	N/A
Value	text	N/A

Table 6.30: Fields of the AspNetUserTokens table

AspNetUsers: Stores user information for authentication and identity management.

Field	Type	Encrypted
Id	text	N/A
UserName	character varying	N/A
NormalizedUserName	character varying	N/A
Email	character varying	N/A
NormalizedEmail	character varying	N/A
EmailConfirmed	boolean	N/A
PasswordHash	text	N/A
SecurityStamp	text	N/A
ConcurrencyStamp	text	N/A
PhoneNumber	text	N/A
PhoneNumberConfirmed	boolean	N/A
TwoFactorEnabled	boolean	N/A
LockoutEnd	timestamp with time zone	N/A
LockoutEnabled	boolean	N/A
AccessFailedCount	integer	N/A

Table 6.31: Fields of the AspNetUsers table

6.21 Privacy and Security Considerations

This research focuses on privacy and security, and one of the primary objectives of the prototype application is to implement robust security measures. Accordingly, the following precautions have been taken to ensure that best

practices and principles are followed to protect the data privacy of all stakeholders in the system.

- **Authentication and Authorization:** The system uses the Microsoft Identity Framework to manage authentication and authorization. Users are assigned roles with defined permissions, and claims-based access control is enforced to limit access to sensitive data. Users are only granted access to the data and functionality required for their role. Sensitive operations, such as credential issuance or verification, require appropriate role-based privileges. Strong password rules, including minimum length, complexity requirements, and account lockout on multiple failed attempts, are enforced to enhance account security. Although dedicated user interfaces for these operations are not implemented in the prototype, the design and infrastructure already support role-based enforcement and can be extended to the UI for active use [82].

- **Data Encryption:** All fields in the database that may contain personal or sensitive information are encrypted before storage using ASP.NET Core's Data Protection API in combination with Entity Framework Core Value Converters. This approach ensures that credentials, and sensitive DID information are automatically encrypted when written to the database and decrypted when read by the application. Due to this, even if an unauthorized access occurs at the database, still the encrypted data remains unreadable, while the application continues to operate transparently with plaintext values in memory. This method provides a secure, integrated mechanism for protecting sensitive data at rest without modifying the application logic elsewhere [84] [83].

  The encryption keys used by the Data Protection API are automatically generated, rotated, and stored securely. By default, keys are saved to the file system (protected using the operating system's cryptographic mechanisms, regardless of the operation system). Key rotation occurs periodically to limit the risk in case a key is compromised, and older keys remain available to decrypt existing data. The prototype application uses the default key rotation interval of 90 days. The Data Protection API ensures that keys are managed securely, and encryption or decryption operations are performed smoothly through the ValueConverters in Entity Framework Core. The application never directly handles raw encryption keys [85].

Furthermore, when documents are uploaded by migrants to the trusted third party's CardanoWeb application, or when artefacts are uploaded by their owners or communities on their own CardanoWeb application, the files are encrypted during the upload process and saved in storage in encrypted form. The files are encrypted using AES-256 with a randomly generated strong key. This encryption key is then stored in the database after being encrypted using the same Data Protection API mechanism described above. This ensures that both the file and the associated encryption key are protected at all times.

- **Data Minimization and Masking:** Personal identifiers are stored in hashed or encrypted forms whenever possible to minimize exposure. For example, full DIDs are either encrypted or hashed to prevent direct user identification. The application collects only the data necessary for its core functionality. Specifically, only an email address is required for the login process; no other personal information is collected or stored. Any personal or sensitive data that must be collected, primarily for issuing VCs to migrants, is encrypted or hashed before storage. This approach ensures that data is used solely for its intended purpose and reduces the risk of exposure in case of unauthorized access.

- **Notifications:** Whenever a migrant's documents are accessed for re-verification by a trusted third party, or when their credentials are accessed for verification by immigration authorities or other authorized entities, a notification is automatically sent to the migrant. This also applies when the status of their credential is checked, ensuring the migrant is informed of any access to their data.

- **Logging:** All critical actions, such as credential requests and re-verifications, are logged along with the user who performed the action. This ensures traceability and accountability, allowing administrators to monitor and review changes in an event of abuse or breach.

- **Selective Reveal of Information:** Unlike the current migration process, where migrants must share all the information in their documents even if only a single detail is required, the prototype application allows them to selectively share details via VCs based on SD-JWT. This prevents oversharing while cryptographically validating the authenticity and integrity of the data.

Chapter 7

Evaluation

The prototype application was informally evaluated by colleagues from the researcher's laboratory and department. Two instances of the prototype were set up, one representing a migrant and the other representing the trusted third party. The users were informed about how the application functions and were provided with guidance on its features and the processes involved.

The following application flows were examined:

- Creating and publishing a DID
- Requesting a VC
- Issuing a DID
- Creating a verification request for a VC
- Verifying a DID
- Creating an artefact
- Requesting an artefact
- Issuing a VC for an artefact
- Verifying the VC for an artefact

Several areas for improvement were identified during the evaluation.

1. Users required guidance regarding the processes involved in the migration flow. The process flow had to be explained in detail because migration related procedures are not common and are typically only used by migrants, trusted third parties, and immigration authorities. Although the users explored the application from all perspectives and help text was available on the web pages, more comprehensive documentation would have been beneficial. The step-by-step wizard-style flow was seen as a positive feature. However, a dedicated help section or a chatbot-style assistant would provide additional support, especially for migrant users.

2. Several user interface related issues were identified. It was suggested that a clearer colour scheme could be used to better indicate the status of various requests, such as New, Pending, Approved, and Rejected. A few users found the grid columns confusing due to the absence of visible column borders. It was also recommended that sorting and searching functionality be available on all grids and implemented consistently across the application. In addition, the sidebar, which shifted during page navigation, was regarded as distracting. A static sidebar was therefore proposed as an improvement.

3. Accessibility options for users who require them were noted as missing in the prototype. Implementing accessibility features was recommended.

4. Users also noted that manually copying and pasting data between applications during certain flows (for example, copying an invitation from the trusted third party's application into the user's application) was inconvenient. They suggested enabling direct communication between the applications to eliminate the need for manual copying and reduce the time required.

5. Finally, some process names were considered too technical, such as "Invitation Offer". Users recommended replacing such terminology with more user-friendly, non-technical terms.

The following positive observations were noted by the users.

1. From the migrant's perspective, users appreciated that they only needed to submit their documents once in order to obtain digital credentials

that could be reused for any migration related process where VCs are accepted.

2. Users valued the ability to selectively reveal information, as this prevented them from disclosing unnecessary personal details.

3. The potential time savings were considered significant, since VCs can be cryptographically verified. This removes the need for authorities to contact each institution or employer individually to confirm the user's credentials. Some users, who were also migrants, mentioned that traditional manual verification processes were time consuming, frustrating, and at times privacy intrusive.

4. Users also appreciated the ability to receive notifications whenever their VC was accessed, as this allowed them to know when their credentials were being viewed.

5. The capability to protect cultural assets and hold parties accountable for their use, was also identified as a positive aspect of the system.

6. The users had inquiries about how the data was being stored and whether it was secure. After the security measures taken to protect user data were explained to them, the users expressed their appreciation.

Although the users identified several areas that required improvement, most of these were related to user experience. The evaluation provided valuable insights that can be used in future work to improve the prototype application. Overall, the users were positive about the proposed system due to its privacy-protecting features, the control it gives users over their personal and cultural heritage data, and the potential time and effort it could save during migration processes.

Chapter 8

Limitations

- **Updating and Deactivating DIDs:** The prototype system currently allows only the creation and publication of DIDs. There is no functionality to modify or deactivate a DID. Although the underlying infrastructure supports these actions, they were not implemented during the early development and experimentation stages, as they were not identified as essential features at the time.
- **User Control over DID Keys:** While the system generates strong cryptographic keys for creating and managing DIDs, users do not have the option to use their own keys or view the keys generated for them. This limits user control and visibility over their digital identity credentials.
- **Data Deletion:** The prototype does not provide users with the ability to delete their data. If a migrant wishes to remove their data from a trusted third party's system or the verifier's system, there is currently no mechanism to do so. Before implementing such functionality in the future, it will be important to consider the perspectives of other stakeholders, such as migration authorities and trusted third parties, to ensure compliance with their data retention policies and regulatory requirements.
- **No option to Update request:** Once a migrant submits a request for credentials, the system does not allow any amendments to be made. Any errors or changes require the user to restart the process entirely, which may affect usability and convenience.

- **No download progress shown:** When users request a file that needs to be fetched from the IPFS network, the application does not currently display real-time download progress. Only a message stating "Fetching file" is shown. Once the download is complete, the user can refresh the page to see the download button.

- **Clipboard Based Transfer of VC Invitations:** In the current prototype, when users receive a VC offer invitation, either as migrants or as artefact requesters, the invitation must be manually copied from the relevant third party or artefact owner's application and pasted into the user's own application. This reliance on clipboard-based transfer creates a security limitation. Although the application clears the clipboard after five seconds, there is a small risk that malware on the user's device, or software on a public computer, could access the clipboard contents within that time window. The VC offer invitation is encoded in JWT format, and a malicious program could potentially decode it. This issue is not addressed in the present implementation, but it could be mitigated through a more secure method of exchange in future development.

- **Risk of DID Substitution in the Issuance Process:** When a VC offer is received by a migrant, they accept the offer by providing their DID. However, if the migrant is a malicious actor, they may provide someone else's DID during this stage in order to receive the VC under a different identity or to commit fraud.

  For example, an individual A who holds a computer science degree could submit their documents (such as their certificate and passport), but provide B's DID during the issuance process. The trusted third party would verify A's documents, and the resulting claims would be attached to B's DID. Person B could then present these claims during verification and falsely appear to be the legitimate owner of A's credentials.

  However, this limitation does not enable misuse for immigration purposes. The VC does not function as a standalone travel document, and at a border crossing the VC would be checked against the traveller's passport. Any mismatch between the passport and the identity associated with the VC would be identified immediately, preventing fraudulent use. Furthermore, embedding biometric data in VCs, as

discussed in the future work section, could help prevent such risks of substitution by ensuring that the VC is cryptographically bound to the legitimate owner.

- **Possession of Artefact Without VC Acceptance:** When a party requests an artefact from a migrant or an organisation, and the request is approved, the issuance process for the VC begins. After this step, the requesting party can download the artefact. However, if the requester downloads the artefact but then fails to accept the issued VC, they are technically in possession of the artefact without an accompanying credential. At present, this scenario cannot be prevented in the prototype application. The purpose of the prototype is not to protect artefacts physically, but to issue credentials that govern their authorised use.

Chapter 9

Recommendation and Future work

9.1 Enhancements to the Prototype

- **Implement DID Update and Deactivation Functionality:** The underlying infrastructure to support DID updates and deactivation already exists within the prototype. However, these features were not implemented during the initial development stages. Future work should focus on enabling this functionality, even if it requires minor adjustments to existing workflows. Adding support for updating and deactivating DIDs would improve flexibility and align the system with decentralised identity best practices.

- **Provide options for users to manage or view their keys:** An option could be introduced during the DID creation stage that allows users to provide their own cryptographic keys, provided they meet the required security standards. Additionally, the application could offer the ability for users to view the keys associated with their DIDs. Any feature that exposes or handles user keys must follow strict security procedures to avoid introducing vulnerabilities. The current prototype already contains the foundational infrastructure necessary to support such enhancements.

- **User-driven data deletion:** Future work should explore the feasibility of allowing users to delete their data from trusted third-party or

verifier systems. This requires careful consideration, particularly when consulting with immigration authorities and trusted third parties, as each stakeholder may operate under specific data retention regulations. One potential approach could be to introduce configurable settings that allow organisations to enable or disable user driven data deletion depending on their policy requirements. The prototype includes the foundational capability for incorporating such functionality.

- **Allow modification of credential requests:** Providing users with the ability to amend credential requests after submission would significantly enhance usability. Implementing this feature may require changes to the current workflow, but the underlying infrastructure to support it is already present within the prototype. Future work should focus on integrating a secure and structured method for modifying requests without compromising data integrity.

- **Real-Time Progress Indicator for File Downloads:** Implementing a real-time progress indicator for file downloads would enhance the user experience by providing clear feedback on the download status and reducing uncertainty, particularly for large artefact files.

9.2 Security and Identity Integrity

- **Investigate methods to prevent DID substitution:** Future work should explore mechanisms to mitigate the risk of DID substitution during the credential issuance process. One potential approach is to incorporate image data or biometric information within the Verifiable Credential. This would enable a physical or biological link between the VC and its rightful holder, reducing the likelihood of fraudulent use. Incorporating biometrics may also support broader use cases, such as enabling the VC to function as a form of digital travel document. Further research is required to identify the most secure, ethical, and privacy-preserving methods for establishing this linkage.

- **QR Code, Image, or File Based VC Invitation Sharing:** Presently, VC invitations are manually copy-pasted from one application to another, which introduces potential security risks. To improve the system's security, VC offer invitations, which are currently encoded as

JWTs, could instead be transferred via QR codes, image files, or encrypted temporary files. Using QR codes or secure file transfer would eliminate reliance on the clipboard, reduce the risk of malware or public computer exposure, and provide a more user-friendly and standardised mechanism for transferring invitations. Furthermore, QR codes and temporary files could be designed with an expiry time and for single use, further enhancing security and privacy.

- **Ability to Embed Image or Biometric Data in the VC as a Selectively Revealable Attribute:** In the current prototype application, image or biometric data cannot be attached to a VC. In future work, enabling this feature could be highly valuable. Although the infrastructure to support this functionality exists in the prototype, it has not yet been implemented. Adding this capability in future versions would allow users to include images or biometric information as part of their credentials while maintaining the selective reveal and privacy preserving features of the system. In such a scenario, a VC could function similarly to a digital passport, allowing it to be validated at airports or other locations requiring identity verification without the need for a physical passport. This would be feasible provided a standard is established and adopted by relevant authorities and entities that require image or biometric linked credentials.

- **Preventing Unauthorised Artefact Redistribution:** In the prototype application, cultural-heritage-related artefacts are protected by issuing a VC. Once the VC is issued, the authorised individual or organisation can download the artefact. However, although any use of the artefact without a valid VC is considered unauthorised, the system cannot prevent a legitimately authorised user from sharing the artefact with others. Furthermore , there is currently no mechanism to identify how, or by whom, an artefact is redistributed once it leaves the system. To address this limitation, future work could explore the integration of techniques such as digital watermarking or steganography. Watermarking involves writing identifiable information onto an image or video, with the primary goal of ensuring that it cannot be removed without damaging the underlying content. Steganography, on the other hand, is "The art and science of hiding information within ordinary or unremarkable cover media in a way that avoids attracting suspicion"

[86]. A steganographic system embeds hidden information inside images, audio, video, or other media in such a way that the presence of the concealed data is not detectable to an observer. Investigating these mechanisms could enhance the system's ability to detect or trace unauthorised redistribution while maintaining usability and privacy for legitimate users.

- **Quantum Computers and Encryption:** According to the Quantum Threat Timeline Report, public key encryption algorithms could potentially be broken within the next 15 to 30 years. This would pose a threat to applications that rely on these algorithms, including the Cardano blockchain, which this prototype is based on. Although the Cardano organization is actively working on mitigating this risk, further research and adaptation of quantum-resistant cryptographic techniques will be necessary to ensure the long term security of the system.

9.3 Stakeholder Engagement and Adoption

- **Stakeholder Education and System Adoption:** An important factor in the success of any proposed solution is the acceptance of all stakeholders involved in the system. Both the formal study conducted for this thesis and the informal evaluation indicate that users, while initially sceptical about blockchain and decentralized technologies for migration related data sharing and cultural heritage preservation, became supportive once the concepts were explained. Users particularly appreciated features such as transparent data handling, control over who accesses their information, and the ability to selectively share data. Therefore, it is recommended that any future implementation include clear user education and demonstrations of these features to ensure trust and adoption.

  Acceptance from other key stakeholders, such as migration authorities, is also critical. Their adoption would encourage participation from trusted third parties, creating a supportive network around the solution. Future work should focus on educational initiatives to raise awareness of data privacy, security, and sovereignty, and on how decentralised technologies can address these issues. Workshops or educational programmes demonstrating the system in practice could further improve

stakeholder acceptance.

- **More automation (System to system communication):** During the informal evaluation, one suggestion from users was to automate the process of copying and pasting the VC invitation related workflow, or to allow it to occur in the background (for example, the migrant's system communicating directly with the trusted third party's system). Users noted that the manual copy and paste step was inconvenient and time-consuming.

  However, another user preferred to keep the process manual, as it gave them a greater sense of control over their actions and their data. While automation could simplify the workflow, this feedback emphasises the importance of allowing users to maintain control where they feel it is necessary. This aspect require further investigation, and the process could be refined accordingly.

Chapter 10

Conclusion

The goal of this research was to identify the challenges migrants face regarding the privacy, security, and ownership of their personal data, and to propose a Cardano-based blockchain solution supported by a working prototype. The objective was to design and evaluate a decentralised system that enables migrants to securely store, share, and manage personal and cultural heritage information while maintaining ownership and privacy. In order to achieve this, existing literature relating to migrant data management, self-sovereign identity, cultural heritage preservation, and decentralised technologies was examined. This was then followed by a formal study of migrants, combining survey data and short interviews. Building on the literature and findings from the study, a system architecture combining the Cardano blockchain, Hyperledger Identus, and IPFS was designed and implemented, resulting in a functional prototype deployed on the Cardano testnet. Informal feedback and technical evaluation were subsequently collected to assess the system's usability, security, and potential for future scalability.

Migrants represent a significant and diverse global population, and migration has played an essential role throughout human history. Individuals move across borders for a range of reasons, including the pursuit of better opportunities or the need to escape danger. These movements are shaped by political, security-related, and economic factors, and are governed by legal frameworks that vary from one country to another. Such regulations typically require extensive documentation and data collection. Migrants often have limited control over how this information is gathered, processed, or stored, yet they must comply in order to obtain visas or secure legal entry into a host country. Although host nations typically implement protocols and mechanisms

intended to manage migrant data securely and protect privacy, significant risks still remain. These include the potential for data breaches caused by malicious actors, outdated or insufficient systems, or simple carelessness, any of which may expose migrants to serious harm.

Existing literature on migrant data management, self-sovereign identity (SSI), cultural heritage preservation, and decentralised technologies provided a foundation for this research. Previous work emphasised key principles such as privacy, data ownership, SSI, Verifiable Credentials (VC), and Verifiable Presentations with selective disclosure, alongside the use of cryptography. However, much of this work remained theoretical or lacked practical implementation. Studies focusing specifically on migrant data or cultural heritage highlighted the need for secure documentation and protection of sensitive information, yet did not offer implementable, privacy-focused architectures or functioning prototypes. Therefore, by addressing these gaps, this research designed and implemented a decentralised system combining the Cardano blockchain, Hyperledger Identus, and IPFS, demonstrating a practical approach for securely storing, sharing, and managing personal and cultural heritage data while maintaining ownership and privacy.

A formal study was conducted with 20 migrants using online and paper-based questionnaires, along with short interviews. Participants originated from various parts of the world and had migrated for diverse reasons. A large portion of the sample was recruited through university networks, with most participants from Sri Lanka, which may represent a limitation of the study. Despite the small sample size and potential biases, the study was deemed sufficient for the purposes of this thesis. The findings provided valuable insights into participants' demographics, motivations for migration, attitudes towards personal data sharing, and perspectives on cultural heritage preservation. Participants expressed discomfort with sharing personal and sensitive data, emphasising the importance of minimal data collection, transparency, and retaining control over their information. Although familiarity with blockchain was limited, participants recognised its potential value in protecting personal and cultural heritage data once its advantages were explained. Cultural heritage was widely regarded as important to preserve, particularly traditions, historical knowledge, and cultural practices, with migration seen as a factor that increases the risk of cultural loss. Overall, the study highlighted two main concerns. The first was the need for stronger protections around personal data. The second was the desire to securely preserve cultural heritage. These findings were taken into consideration during

the design and development of the system, with maximum effort made to incorporate measures addressing these valid concerns in the prototype. Key features implemented based on the study included notification mechanisms when migrant credentials were accessed, security measures for storing data, data minimisation and masking, selective disclosure of information, and adherence to good security practices with strong encryption.

The proposed solution was initially planned to be developed directly on the Cardano blockchain using Haskell. However, due to the challenges associated with developing the system within the time frame of this thesis, as described in Appendix Section A, alternative options were considered. During this process, the existence of Hyperledger Identus, an SSI-based technology, was discovered. Hyperledger Identus could act as a second layer and is supported by industry leaders. After evaluating all options, it was decided that this technology would be used for the prototype application. To store migrant documents and artefacts, the IPFS network, a decentralised technology was employed. Documents and artefacts were encrypted prior to storage to ensure security. The main application was built using .NET Core, WebAPI and Razor Pages and was structured into three modules. The first module is the user-facing web application (CardanoWeb). The second module is an API suite (CardanoBridgeAPI) that enables communication between the web application and Hyperledger Identus. The third module is a console application designed to handle file operations and interact with IPFS. The application uses a PostgreSQL database to store metadata. Only minimal and necessary data were stored, and any personal data were encrypted prior to storage to ensure security. The application was designed with security in mind and incorporates multiple measures, including encryption of files during upload, periodic rotation of encryption keys, authentication and authorisation mechanisms, and adherence to other best security practices.

The prototype application was informally evaluated by colleagues of the researcher, representing migrant users, trusted third parties, and verifiers. Users were guided through the application flows, including creating and publishing DIDs, requesting, issuing, and verifying VCs, and managing artefacts. The evaluation identified areas for improvement, mostly related to user experience, such as clearer or less technical terminology, the inclusion of a help section, enhanced navigation, accessibility features, and more intuitive interfaces. Users also highlighted positive aspects of the system, including the ability to submit documents once and reuse digital credentials, selectively disclose information, receive notifications when credentials were accessed, and

securely protect cultural heritage data. Participants appreciated the privacy protecting features and the control provided over personal and cultural heritage data. Overall, the evaluation confirmed that the prototype successfully demonstrates a decentralised, secure system for managing migrant data and cultural heritage, while highlighting areas for future enhancement to improve usability.

Although the goal of the research was achieved, several limitations of the study and prototype were identified, providing opportunities for future work. The prototype application currently allows the creation and publication of DIDs but does not support updating, deactivation, or deletion of DIDs or user data, limiting users' control over their digital identity. Users cannot manage or view cryptographic keys and credential requests cannot be modified once submitted. While the system issues Verifiable Credentials for artefacts, it cannot prevent authorised users from redistributing them outside the system. In addition, the use of biometric or image data to strengthen identity verification has not yet been implemented. Future work could address these limitations by adding DID update and deletion functionality, enhancing cryptographic key management options, enabling modification of credential requests, incorporating secure image or biometric attributes, and investigating mechanisms to trace or prevent unauthorised artefact redistribution. Furthermore, long-term security considerations, such as quantum-resistant cryptography, and stakeholder engagement strategies to improve adoption and trust, are important areas for further research.

In summary, this research has investigated the issues faced by migrants regarding the privacy, security, and control of personal, sensitive, and cultural heritage related data. It identified gaps in the existing research on this subject and included a formal study with migrants to gather first-hand insights into these challenges. The findings from the user study and evaluation highlight both the importance of secure, transparent systems and the potential for decentralised technologies to empower migrants and protect cultural heritage. Based on the existing literature, the identified gaps, and the findings from the formal study, a prototype system was implemented. The implementation combined the Cardano blockchain, Hyperledger Identus, and IPFS, along with an application suite built using .NET Core, WebAPI, and Razor Pages.

Overall, this research provides practical groundwork for future work in privacy focused, decentralised identity management systems, with the potential to influence policy, stakeholder adoption, and the development of scalable

solutions for migrant communities.

Appendices

Appendix A

Development Approach

After the requirements gathering phase, the researcher developed an understanding of the knowledge migrants possess regarding their rights related to personal and sensitive data, as well as cultural heritage information. The researcher also examined their awareness of potential threats to their data and privacy, along with their ideas about the features a system should include to support them.

Since it was decided that the prototype software would be built using the Cardano blockchain, the researcher first developed a preliminary understanding of the system's technical details. The application would be based on the Cardano blockchain, potentially developed using Haskell, and might involve the use of smart contracts.

As the researcher was new to the Cardano ecosystem and its development practices, the following strategy was adopted.

1. Run a Cardano node locally, ideally by compiling it from the source code.

2. Build a very basic sample application to understand the development process and gain hands-on experience.

3. Begin development of the prototype application.

The researcher chose to build the Cardano node locally from the sources provided on the Cardano GitHub page, rather than using precompiled binaries. Building from source ensures access to the latest updates and features,

provides firsthand insight into the development process, and allows identification of potential compatibility or system related issues that may arise later during the prototype development, especially since the researcher was developing on a Linux environment running on top of Windows. In addition, experience with compiling from source benefits the future development of the prototype, as access to the source code can be crucial for debugging, understanding the overall system. In software development, the approach of building from the source usually exposes developers to build scripts, dependency management, and coding conventions, which are valuable skills for future development. In complex projects like Cardano, which have many interdependent components, building from source helps the researcher understand how dependencies interact and resolve issues independently, further preparing them for deeper involvement in the project.

One of the expected challenges in developing the prototype was that the researcher was not familiar with Haskell or Plutus, the framework used to develop smart contracts and had no prior experience with blockchain related development activities. Although the researcher had experience in general programming, primarily using modern programming languages and development tools, the blockchain domain and a new programming language presented an initial challenge. From personal experience, the researcher found that theoretical learning alone was insufficient to gain practical understanding, hands-on practice was essential. To address this, the researcher decided that, in addition to studying the language and associated concepts, building a few small applications would be beneficial for becoming familiar with the Cardano development environment and the highly technical aspects of blockchain development. As famously noted in the book "C Programming Language" by Brian Kernighan and Dennis Ritchie (1988, p. 9) [87], "The only way to learn a new programming language is by writing programs in it," a principle echoed by many programming experts.

It was anticipated that setting up the development environment, successfully building the Cardano source code, and developing a few sample applications would provide the researcher with sufficient exposure to proceed with the prototype software development.

A.1 Development

This section describes how the initial development was carried out, the challenges encountered during the research and experimentation with the technology, and the rationale behind certain choices and decisions.

A.1.1 The Development Machine

According to the report by the European Union Blockchain Observatory and Forum, applications related to blockchains are generally processor- and memory-intensive, although Cardano is reported to require fewer computational resources than many other blockchains. Therefore, it was assumed that the machine used to develop, run, and test the blockchain applications should possess slightly higher processing capabilities. The development and testing were conducted locally on a laptop, with the specifications outlined below [88].

- Operating System - Windows 11 Professional
- Processor - AMD Ryzen 7 (16 CPUs)
- Memory - 32 GB
- Hard Disk - 1TB SSD

A.1.2 Setting up Cardano Development Environment

The development machine was running Windows 11, however the Cardano development environment had to be done in Linux. According to the Cardano developer documentation at the time development commenced, Cardano recommended using WSL2 for development on Windows [89].

WSL2 (Windows Subsystem for Linux) is an open-source technology that allows developers to run a Linux environment on their Windows computer. This enables the developer to run most Linux-based applications and tools on their Windows machine without the need for dual booting or virtual machines [90].

WSL2 was successfully installed on the researcher's Windows machine. Furthermore, Ubuntu version 24.04.2 LTS was installed, and development was conducted within the Ubuntu environment.

A.1.3 Building Cardano from Source

As detailed in the earlier sections of this report, the researcher chose to build the Cardano node from the source code provided on the Cardano GitHub repository, rather than using precompiled binaries. According to the Cardano documentation, there are two primary methods for building the Cardano node [91].

1. Building via cabal
2. Building via Nix

Building via cabal: Cardano development is based on the Haskell programming language. According to the Cardano developer documentation, the recommended method for installing Haskell tools is GHCup, the primary Haskell installer. Following the installation instructions from the official GHCup page, the script below was executed in the Linux (Ubuntu) environment [92].

```
curl --proto    =https" --tlsv1.2 -sSf
   https://get-ghcup.haskell.org | sh
```

When the above script was executed, several prompts appeared, for which the default answers were selected. The Cardano documentation did not specify which options should be chosen. Although the script eventually displayed a message indicating successful installation, subsequent commands (given below) recommended in the Cardano documentation did not execute as expected.

```
ghcup install --set ghc 9.6.7
ghcup install --set cabal 3.12.1.0
```

After several attempts, including reinstalling the entire environment and restarting the Ubuntu WSL2 instance, the commands eventually executed successfully. However, running the commands generated the errors below indicating that they were using an outdated command style.

```
[ Warn  ] This is an old-style command for installing
   GHC. Use 'ghcup install ghc' instead.
[ Warn  ] New ghc version available. If you want to
   install this latest version, run 'ghcup install ghc
   9.12.2'
```

```
[ Warn  ] New cabal version available. If you want to
   install this latest version, run 'ghcup install
   cabal 3.16.0.0'
[ Warn  ] New stack version available. If you want to
   install this latest version, run 'ghcup install
   stack 3.7.1'
[ Error ] [GHCup-07140] Both installation and setting
   the tool failed.
[ ...   ] Install error was: Unable to find a download
   for GHC version 'ghc' on detected platform
   x86_64-linux-ubuntu-24.04
[ ...   ] Set error was: The version 'ghc' of the tool
   ghc is not installed.
[ Error ] Also check the logs in
   /home/vignes/.ghcup/logs
[ Warn  ] This is an old-style command for installing
   GHC. Use 'ghcup install ghc' instead.
[ Warn  ] New ghc version available. If you want to
   install this latest version, run 'ghcup install ghc
   9.12.2'
[ Warn  ] New cabal version available. If you want to
   install this latest version, run 'ghcup install
   cabal 3.16.0.0'
[ Warn  ] New stack version available. If you want to
   install this latest version, run 'ghcup install
   stack 3.7.1'
[ Error ] [GHCup-07140] Both installation and setting
   the tool failed.
[ ...   ] Install error was: Unable to find a download
   for GHC version 'cabal' on detected platform
   x86_64-linux-ubuntu-24.04
[ ...   ] Set error was: The version 'cabal' of the
   tool ghc is not installed.
```

The correct command, shown below, was identified with the assistance of online search resources.

```
ghcup install ghc 9.6.7
ghcup set ghc 9.6.7
```

However, the following error occurred after executing the command.

```
[ Info ] verifying digest of:
   ghc-9.4.8-x86_64-ubuntu20_04-linux.tar.xz [ Info ]
   Unpacking: ghc-9.4.8-x86_64-ubuntu20_04-linux.tar.xz
   to /home/vignes/.ghcup/tmp/ghcup-3da9b7235ce16361 [
   Info ] Installing GHC (this may take a while) [
   ghc-configure ] checking Setting up CFLAGS, LDFLAGS,
   IGNORE_LIN... [ ghc-configure ] checking Setting up
   CONF_CC_OPTS_STAGE0, CONF_G... [ ghc-configure ]
   checking Setting up CONF_CC_OPTS_STAGE1, CONF_G... [
   ghc-configure ] checking Setting up
   CONF_CC_OPTS_STAGE2, CONF_G... [ ghc-configure ]
   checking C++ standard library flavour... ./conf... [
   ghc-configure ] configure: error: Failed to compile
   test progra... [ Error ] [GHCup-00841] Process "sh"
   with arguments ["./configure", [ ... ]
   "--prefix=/home/vignes/.ghcup/ghc/9.4.8"] failed
   with exit code 1. [ Error ] Also check the logs in
   /home/vignes/.ghcup/logs "ghcup
   --metadata-fetching-mode=Strict --cache install ghc
   recommended" failed!
```

This error could not be resolved despite various attempts, including uninstalling and reinstalling the entire setup. The issue was investigated extensively, and multiple approaches were tried to identify and fix the cause; however, these efforts did not yield any results.

At a later stage, while documenting the implementation process, the researcher revisited the setup. On this occasion, the process progressed slightly further before failing again. By this time, both the Cardano documentation and the researcher's development environment had been updated, which may have contributed to the partial improvement observed.

The environment variables were configured to install the software versions specified in the official documentation. These same versions were used on the assumption that the documented configurations had been verified to function correctly. Afterwards, depending on project requirements or system constraints, the versions and configurations could be modified as necessary.

```
CARDANO_NODE_VERSION='10.3.1'
IOHKNIX_VERSION=$(curl
   https://raw.githubusercontent.com/IntersectMBO/cardano-node/
   $CARDANO_NODE_VERSION/flake.lock | jq -r
```

```
   '.nodes.iohkNix.locked.rev')
echo "iohk-nix version: $IOHKNIX_VERSION"
```

Sodium is a cross-platform and cross-language software library that provides functionality for encryption, decryption, digital signatures, password hashing, and other cryptographic operations. Cardano uses a customised version of *libsodium*, which must be obtained from the official repository maintained by IntersectMBO: `https://github.com/IntersectMBO/libsodium`

The Sodium version to be used was identified and selected.

```
SODIUM_VERSION=$(curl
   https://raw.githubusercontent.com/input-output-hk/iohk-nix/
$IOHKNIX_VERSION/flake.lock | jq -r
   '.nodes.sodium.original.rev')
echo "Using sodium version: $SODIUM_VERSION"
```

Then installed.

```
: ${SODIUM_VERSION:='dbb48cc'}
git clone https://github.com/intersectmbo/libsodium
cd libsodium
git checkout $SODIUM_VERSION
./autogen.sh
./configure
make
make check
sudo make install
```

Environment variables were added according to the documentation.

```
export LD_LIBRARY_PATH="/usr/local/lib:$LD_LIBRARY_PATH"
export
   PKG_CONFIG_PATH="/usr/local/lib/pkgconfig:$PKG_CONFIG_PATH"
```

secp256k1: According to the documentation, it was necessary to install secp256k1, an elliptic curve library used for cryptographic operations in blockchain systems. The specific version required for this project was identified and installed in accordance with the recommendations provided in the documentation.

```
SECP256K1_VERSION=$(curl
   https://raw.githubusercontent.com/input-output-
hk/iohk-nix/
```

```
$IOHKNIX_VERSION/flake.lock | jq -r
   '.nodes.secp256k1.original.ref')
echo "Using secp256k1 version: ${SECP256K1_VERSION}"
```

Then secp256k1 was installed.

```
: ${SECP256K1_VERSION:='v0.3.2'}
git clone --depth 1 --branch ${SECP256K1_VERSION}
   https://github.com/bitcoin-core/secp256k1
cd secp256k1
./autogen.sh
./configure --enable-module-schnorrsig
   --enable-experimental
make
make check
sudo make install
```

blst is a cryptographic library that implements the BLS12-381 signature scheme. This library is commonly used in blockchain systems and applications requiring efficient pairing-based cryptography. The specific version of blst required for this project was identified and installed in accordance with the recommendations provided in the documentation.

```
BLST_VERSION=$(curl
   https://raw.githubusercontent.com/input-output-hk/iohk-
nix/$IOHKNIX_VERSION/flake.lock | jq -r
   '.nodes.blst.original.ref')
echo "Using blst version: ${BLST_VERSION}"
```

The blst library was installed on the development environment according to the version specified in the documentation, ensuring compatibility with the Cardano build process.

```
: ${BLST_VERSION:='v0.3.11'}
git clone --depth 1 --branch ${BLST_VERSION}
   https://github.com/supranational/blst
cd blst
./build.sh
cat > libblst.pc << EOF
prefix=/usr/local
exec_prefix=\${prefix}
libdir=\${exec_prefix}/lib
includedir=\${prefix}/include
```

```
Name: libblst
Description: Multilingual BLS12-381 signature library
URL: https://github.com/supranational/blst
Version: ${BLST_VERSION#v}
Cflags: -I\${includedir}
Libs: -L\${libdir} -lblst
EOF
sudo cp libblst.pc /usr/local/lib/pkgconfig/
sudo cp bindings/blst_aux.h bindings/blst.h
   bindings/blst.hpp  /usr/local/include/
sudo cp libblst.a /usr/local/lib
sudo chmod u=rw,go=r
   /usr/local/{lib/{libblst.a,pkgconfig/libblst.pc},include/
{blst.{h,hpp},blst_aux.h}}
```

The Cardano node repository was cloned from GitHub to the local development environment to obtain the source code required for the purpose of building the node. The source code was cloned from this repository: `https://github.com/IntersectMBO/cardano-node.git`

A.1.4 Building with Nix

Nix is a package manager commonly used with languages such as Haskell. It was installed by following the instructions provided on the official Nix website, using the command shown below. This command is intended for use in a WSL2 environment.

```
$ sh <(curl --proto '=https' --tlsv1.2 -L
   https://nixos.org/nix/install) --daemon


git clone https://github.com/IntersectMBO/cardano-node
cd cardano-node
git tag | sort -V
git switch -d tags/<TAGGED VERSION>
nix build .#cardano-node

However, the following error occurred.
```

```
warning: ignoring the client-specified setting
   'trusted-public-keys', because it is a restricted
   setting and you are not a trusted user

In order to resolve the issue described above, several
   approaches were attempted, including adding the
   following configuration to the nix.conf file as
   suggested online.

substituters = https://cache.nixos.org
   https://cache.iog.io
trusted-public-keys =
cache.nixos.org-1:
6NCHdD59X431o0gWypbMrAURkbJ16ZPMQFGspcDShjY=
hydra.iohk.io:f/Ea+s+dFdN+3Y/G+FDgSq+a5NEWhJGzdjvKNGv0/EQ=
trusted-users = root vignes
```

However, despite numerous attempts, the issue could not be resolved. During this phase of the research, the direct development of the Cardano-based application using Haskell did not proceed as smoothly as expected. Consequently, alternative approaches were investigated. During this process the researcher came across the HyperLedger project.

A.1.5 HyperLedger Identus

The main challenge with Identus was that the documentation was somewhat difficult to navigate. The online documentation typically only supports the latest version, with limited guidance for older releases. Additionally, the documentation is not consistently categorised, which can be confusing for the reader.

The quick start guide was followed, as it provides practical examples. The first example involved cloning and running the Cloud Agent, which was successfully completed. Using this example, a long-form Decentralized Identifier (DID) could be created, and a credential schema could be defined. However, the guide did not provide instructions for DID resolution or the configuration of the Prism node, leaving some critical steps unclear.

The next example involved cloning the TypeScript SDK. According to the documentation, both Rust and Wasm-Pack were required to compile the TypeScript SDK. This command was intended to be executed within a WSL2

environment.

```
curl --proto '=https' --tlsv1.2 -sSf
   https://sh.rustup.rs | sh
```

According to the documentation, Wasm-Pack could not be installed. During the initial stages of the research, Wasm-Pack had been available; however, according to its GitHub page, the project is now discontinued. The functionality previously provided by Wasm-Pack has since been integrated into the wasm-bindgen project, which can be found at: `https://github.com/wasm-bindgen/wasm-bindgen` This command had to be run according to the documentation.

```
cargo install wasm-bindgen-cli
```

However the below error appeared.

```
Updating crates.io index error: cannot install package
   wasm-bindgen-cli 0.2.100, it requires rustc 1.76 or
   newer, while the currently active rustc version is
   1.75.0 wasm-bindgen-cli 0.2.92 supports rustc 1.57
```

To resolve the issue, the Wasm-Pack version was updated by uninstalling and reinstalling it. However, despite multiple attempts, an error occurred that could not be resolved within the development environment. The error, related to an incorrect path, persisted regardless of trying various troubleshooting techniques.

```
    npm warn cleanup Failed to remove some directories [
npm warn cleanup   [
npm warn cleanup
   '\\\\wsl.localhost\\UbuntuIdentus\\home\\vignes\\
test\\sdk-ts\\node_modules\\rxdb',
npm warn cleanup
[Error: EPERM: operation not permitted, rmdir
   '\\wsl.localhost\
UbuntuIdentus\home\vignes\test\sdk-ts\node_modules\
rxdb\src\plugins\flutter'] {
npm warn cleanup       errno: -4048,
npm warn cleanup       code: 'EPERM',
npm warn cleanup       syscall: 'rmdir',
npm warn cleanup       path:
   '\\\\wsl.localhost\\UbuntuIdentus\\home\\
```

```
vignes\\test\\sdk-ts\\node_modules\\rxdb\\src\\
plugins\\flutter'
npm warn cleanup     }
npm warn cleanup   ]
npm warn cleanup ]
npm error code EISDIR
npm error syscall symlink
npm error path
   \\wsl.localhost\UbuntuIdentus\home\vignes\
test\sdk-ts\externals\generated\jwe-wasm
npm error dest
   \\wsl.localhost\UbuntuIdentus\home\vignes\
test\sdk-ts\node_modules\jwe-wasm
---
npm error code EISDIR
npm error syscall symlink
npm error path
   \\wsl.localhost\UbuntuIdentus\home\vignes\
test\sdk-ts\externals\generated\jwe-wasm
npm error dest
   \\wsl.localhost\UbuntuIdentus\home\vignes\
test\sdk-ts\node_modules\jwe-wasm
npm error errno -4068
npm error EISDIR: illegal operation on a directory,
   symlink
   '\\wsl.localhost\UbuntuIdentus\home\vignes\test\
sdk-ts\externals\generated\jwe-wasm' ->
   '\\wsl.localhost\UbuntuIdentus\home\vignes\test\sdk-ts\
node_modules\jwe-wasm'
npm error A complete log of this run can be found in:
   C:\Users\Vignes\
AppData\Local\npm-cache\_logs\
2025-08-29T08_25_53_711Z-debug-0.log
```

A.1.6 Atala prism setup example

During the search for examples of Prism and Cloud Agent implementation, the researcher identified a YouTube video and accompanying sample code provided by Ley Lawrance. This proved to be the most useful example en-

countered throughout the research, particularly because the official documentation was difficult to navigate. The video clearly demonstrated the process of issuing verifications from an issuer to a holder. While the example was highly valuable, it did present certain challenges, which were subsequently addressed and resolved during the development process.[75]

This setup was executed within two Docker containers, using Docker Compose files named *docker-compose-cardano* and *docker-compose-prism*.

The *docker-compose-cardano* file contained the Docker images required to set up and run the Cardano node. The file specified the following images and their respective versions:

1. Postgres 14.10-alpine
2. Cardano-node 9.1.1
3. Cardano-wallet 2024.9.3
4. Icarus 2023-04-14

The *docker-compose-prism file* contained the Docker images required to set up and run the Prism node. The file specified the following images along with their respective versions:

1. postgres:13
2. pgadmin4
3. prism-node 2.2.1
4. prism-agent 1.28.0
5. Hashicorp vault – latest

The example included a script named *cardano-start.sh*, which was intended to initialise and start the setup. However, executing this script resulted in several errors.

```
./cardano-start.sh: line 21: lz4: command not found
tar: This does not look like a tar archive
tar: Exiting with failure status due to previous errors
./cardano-start.sh: line 21: jq: command not found
```

```
  % Total    % Received % Xferd  Average Speed Time
     Time Time Current Dload Upload Total Spent Left
     Speed
100   233  100   233    0     0    230      0  0:00:01
   0:00:01 --:--:--   230
curl: Failed writing body
```

However, the following error occurred.

```
./cardano-start.sh
  % Total % Received % Xferd Average Speed Time Time
     Time Current Dload Upload Total Spent Left Speed
  0 3478M    0  7102    0     0   6766Error 44 :
     Unrecognized header : file cannot be decoded
    0   6d 05h  0:00:01   6d 05h  6770tar: This does
       not look like a tar archive
tar: Exiting with failure status due to previous errors
  0 3478M    0  7102    0     0   5233      0   8d 01h
     0:00:01   8d 01h  5237
```

Based on the errors encountered, it was determined that the lz4 package was required. Therefore, it was installed along with jq using the following commands:

```
sudo apt update
sudo apt install lz4 jq
```

Despite executing the commands to install lz4, jq , the following errors were encountered.

```
./cardano-start.sh
  % Total % Received % Xferd Average Speed Time Time
     Time Current Dload Upload Total Spent Left Speed
  0 3478M    0  7102    0     0   6766Error 44 :
     Unrecognized header : file cannot be decoded
    0   6d 05h  0:00:01   6d 05h  6770tar: This does
       not look like a tar archive
tar: Exiting with failure status due to previous errors
  0 3478M    0  7102    0     0   5233      0   8d 01h
     0:00:01   8d 01h  5237
```

A manual download and decompression of the snapshot was then attempted. However, the startup.sh script did not execute as expected, and the snapshot could not be downloaded successfully. Even when the snapshot

was obtained, the commands in the script required modification. Consequently, a separate script was executed (as shown below) to download and configure the snapshot correctly.

```
# Get the snapshot filename
SNAPSHOT=$(curl -s
   https://downloads.csnapshots.io/testnet/
testnet-db-snapshot.json | jq -r .[].file_name)

# Download the snapshot
curl -L
   https://downloads.csnapshots.io/testnet/$SNAPSHOT -o
   snapshot.tar.zst

# Decompress it
zstd -d snapshot.tar.zst -o snapshot.tar

# Make sure the target directory exists
mkdir -p ./data/db

# Extract the snapshot
tar -xf snapshot.tar -C ./data/db
```

After this the below modified version of the cardano-start.sh script was then executed.

```
#! /bin/bash

set -euo pipefail

set -a; source .env-cardano; set +a

mkdir -p $NODE_DB

if [ "$(ls -A "${NODE_DB}")" ]
then
    echo "Node state is present, not downloading the
       snapshot."
else
    if [ $NETWORK == "mainnet" ]
    then
        # download the node-db snapshot, or wait for
```

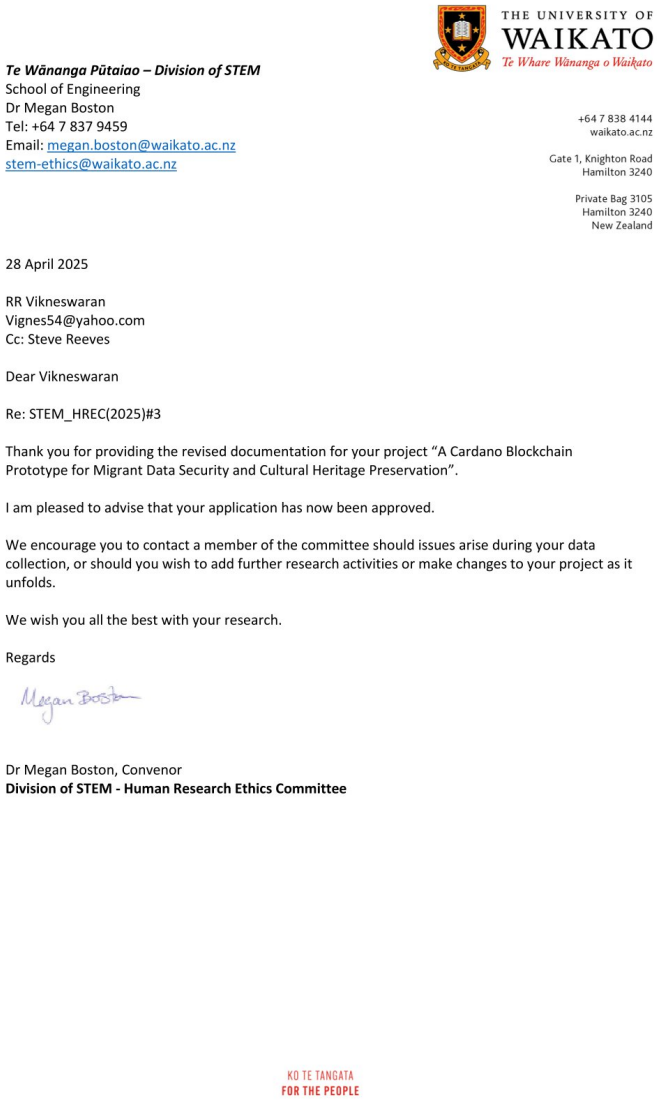
```
            the node to sync for a long time
        curl -o -
            https://downloads.csnapshots.io/mainnet/$(curl
            -s
        https://downloads.csnapshots.io/mainnet/
        mainnet-db-snapshot.json| jq -r .[].file_name )
        | lz4 -c -d - | tar -x -C $NODE_DB
        mv $NODE_DB/db/* $NODE_DB/
        rm -rf $NODE_DB/db
    elif [ $NETWORK == "preprod" ]
    then
        echo "Node state is present, not downloading
            the snapshot."
    elif [ $NETWORK == "sanchonet" ]
    then echo "no cache for sancho";
    else
        echo "NETWORK must be mainnet or preprod or
            sanchonet"
        exit 1
    fi
fi

# start the services
NETWORK=${NETWORK} NODE_DB=${NODE_DB} docker compose -p
   cardano -f ./docker-compose-cardano.yml --env-file
   .env-cardano up -d
```

The script then produced more errors. After investigation, it was determined that the issue was caused by the Cardano node being outdated. Consequently, the node was upgraded to the latest version at the time, 10.5.1. Following this upgrade, the Cardano node operated successfully.

Appendix B

Survey

B.1 Approval Letter from the STEM Ethics Committee



THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

Te Wānanga Pūtaiao – Division of STEM
School of Engineering
Dr Megan Boston
Tel: +64 7 837 9459
Email: megan.boston@waikato.ac.nz
stem-ethics@waikato.ac.nz

+64 7 838 4144
waikato.ac.nz

Gate 1, Knighton Road
Hamilton 3240

Private Bag 3105
Hamilton 3240
New Zealand

28 April 2025

RR Vikneswaran
Vignes54@yahoo.com
Cc: Steve Reeves

Dear Vikneswaran

Re: STEM_HREC(2025)#3

Thank you for providing the revised documentation for your project "A Cardano Blockchain Prototype for Migrant Data Security and Cultural Heritage Preservation".

I am pleased to advise that your application has now been approved.

We encourage you to contact a member of the committee should issues arise during your data collection, or should you wish to add further research activities or make changes to your project as it unfolds.

We wish you all the best with your research.

Regards

Dr Megan Boston, Convenor
Division of STEM - Human Research Ethics Committee

KO TE TANGATA
FOR THE PEOPLE

Figure B.1: Approval from the STEM Ethics Committee

B.2 Email Sent During Questionnaire Distribution

Hi,

Thank you very much for your willingness to participate in this study!

I've attached the participant information sheet. **Please take a moment to read through it**.
If you have any questions about the questionnaire, feel free to contact me using the details provided in the information sheet.

The questionnaire will take approximately 20 minutes to complete. You do not need to save anything manually; it will be saved automatically. After completing the questionnaire, you can close your browser window after a short 5-second delay.

You may skip any questions or answers that are not applicable to you.

Please click the link below to access the questionnaire. When prompted, enter the password provided.

Password - ##########
https://drive.proton.me/urls/##########

Kind regards,

R R Vikneswaran.

Figure B.2: Email sent to participants

B.3 Questionnaire Used in the Survey

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

Research Consent Form

HECS Human Ethics Committee

A Cardano Blockchain Prototype for Migrant Data Security and Cultural Heritage Preservation

Consent Form for Participants

I have read the **Participant Information Sheet** for this study and have had the details of the study explained to me. My questions about the study have been answered to my satisfaction, and I understand that I may ask further questions at any time.

I also understand that I am free to withdraw from the study before 2 weeks from the date of the study, or to decline to answer any particular questions in the study. I agree to provide information to the researchers under the conditions of confidentiality set out on the **Participant Information Sheet**.

I agree to participate in this study under the conditions set out in the **Participant Information Sheet**.

Signed:

Name:

Date:

Researcher's Name and contact information:

Vikneswaran Rengasamy Rajamanikkam

vr141@students.waikato.ac.nz

0226514964

Supervisor's Name and contact information: (if applicable)

Professor Steeve Reeves
steve.reeves@waikato.ac.nz

This questionnaire is conducted as a partial requirement for the Master of Science (Research) in Computer Science. The goal of this research project is to build a decentralized application to securely store migrant data and cultural heritage related information.

If you take part in the study, you have the right to:

- **Refuse to answer any question and withdraw from the study within two weeks of your participation.**
- **Ask any further questions about the study that occur to you during your participation.**
- **Receive a summary of the study's findings once the study is concluded.**

Figure B.3: Page 1

If you have any questions or concerns about the project, either now or in the future, please feel free to contact us using the contact information provided in the participant information sheet.

Questionnaire

1. What is your age group? *(choose one)*
   - ☐ 18-24
   - ☐ 25-34
   - ☐ 35-44
   - ☐ 45-60
   - ☐ Above 60

2. What is your country of origin?

3. What was your reason for migration? *(choose one or more)*
   - ☐ Climate change / Natural Disasters
   - ☐ Conflict / Persecution
   - ☐ Cultural / Religious / Lifestyle Reasons
   - ☐ Education
   - ☐ Employment
   - ☐ Family
   - ☐ Improved quality of life
   - ☐ Marriage / Partner
   - ☐ Other (Please specify)

4. How long have you been in your new country? *(choose one)*
   - ☐ Less than 1 year
   - ☐ 1-3 years
   - ☐ More than 3 years

5. The list below contains some personally identifiable information. During your migration process, which of the following were you asked to provide? And how comfortable were you in providing such information? (choose one for each row)

Personal information	Not Sure	Comfortable	Not very comfortable	Uncomfortable
Full name	☐	☐	☐	☐
Date and place of birth	☐	☐	☐	☐
Address	☐	☐	☐	☐
Phone number	☐	☐	☐	☐
Former phone numbers	☐	☐	☐	☐
Email address	☐	☐	☐	☐
Former email addresses	☐	☐	☐	☐
Social media profiles	☐	☐	☐	☐
Passport / Licence / ID card numbers	☐	☐	☐	☐
Photograph	☐	☐	☐	☐
Employment history	☐	☐	☐	☐

Figure B.4: Page 2

Educational history	☐	☐	☐	☐
Any other personal information?				

6. The list below contains some sensitive personal information. During your migration process, which of the following were you asked to provide? And how comfortable were you in providing such information? *(choose one for each row)*

(Sensitive personal information can be any information that has significance to you and something you may wish to keep private and revealing it might result in you being treated in a particular way or can put you at risk or unease).

Sensitive personal information	**Not Sure**	**Comfortable**	**Not very comfortable**	**Uncomfortable**
Gender	☐	☐	☐	☐
Race / Ethnicity	☐	☐	☐	☐
Religious beliefs	☐	☐	☐	☐
Sexual Orientation	☐	☐	☐	☐
Facial recognition data	☐	☐	☐	☐
Fingerprint data	☐	☐	☐	☐
Genetic Data	☐	☐	☐	☐
Iris Data	☐	☐	☐	☐
Citizenships, Residencies you hold or previously held.	☐	☐	☐	☐
Medical records	☐	☐	☐	☐
Travel history	☐	☐	☐	☐
Bank account numbers	☐	☐	☐	☐
Financial history	☐	☐	☐	☐
Salary/ Income details	☐	☐	☐	☐
Tax numbers	☐	☐	☐	☐
Wealth / Asset details	☐	☐	☐	☐
Criminal / conviction history	☐	☐	☐	☐
Affiliations or association to governments or other organizations that were involved in criminal	☐	☐	☐	☐

Figure B.5: Page 3

behaviour or advocated criminal behaviour				
Affiliations or association to the government or political parties	☐	☐	☐	☐
Age when the conflict in your country ended	☐	☐	☐	☐
History of support for any liberation groups	☐	☐	☐	☐
Information on being witnessed or participation of ill treatment of people	☐	☐	☐	☐
Military / Law enforcement / Intelligence service history	☐	☐	☐	☐
Any information related to your marriage or relationship?				
• Marriage Certificate	☐	☐	☐	☐
• Information on children together	☐	☐	☐	☐
• Evidence of time spent together (Travel / Meetings /Events)	☐	☐	☐	☐
• Photos / social media posts together.	☐	☐	☐	☐
• Chat / text / email / call history	☐	☐	☐	☐
• Joint property / asset, rental agreements	☐	☐	☐	☐
• Bank account information	☐	☐	☐	☐
• Utility bill information	☐	☐	☐	☐
Any other sensitive personal information?				

7. Did you have to provide any personal information of your family members? *(choose one)*
   - ☐ Yes
   - ☐ No

8. If you answered "Yes" to question no 7, Which of the following were you asked to provide on your family members? *(choose one for each row)*

Personal information	Not Sure	Comfortable	Not very comfortable	Uncomfortable

Figure B.6: Page 4

behaviour or advocated criminal behaviour				
Affiliations or association to the government or political parties	☐	☐	☐	☐
Age when the conflict in your country ended	☐	☐	☐	☐
History of support for any liberation groups	☐	☐	☐	☐
Information on being witnessed or participation of ill treatment of people	☐	☐	☐	☐
Military / Law enforcement / Intelligence service history	☐	☐	☐	☐
Any information related to your marriage or relationship?				
• Marriage Certificate	☐	☐	☐	☐
• Information on children together	☐	☐	☐	☐
• Evidence of time spent together (Travel / Meetings /Events)	☐	☐	☐	☐
• Photos / social media posts together.	☐	☐	☐	☐
• Chat / text / email / call history	☐	☐	☐	☐
• Joint property / asset, rental agreements	☐	☐	☐	☐
• Bank account information	☐	☐	☐	☐
• Utility bill information	☐	☐	☐	☐
Any other sensitive personal information?				

7. Did you have to provide any personal information of your family members? *(choose one)*
   - ☐ Yes
   - ☐ No

8. If you answered "Yes" to question no 7, Which of the following were you asked to provide on your family members? *(choose one for each row)*

Personal information	**Not Sure**	**Comfortable**	**Not very comfortable**	**Uncomfortable**

Figure B.7: Page 4

Full name	☐	☐	☐	☐
Date and place of birth	☐	☐	☐	☐
Address	☐	☐	☐	☐
Phone number	☐	☐	☐	☐
Email address	☐	☐	☐	☐
Social media profiles	☐	☐	☐	☐
Passport / Licence / ID card numbers	☐	☐	☐	☐
Photograph	☐	☐	☐	☐
Employment history	☐	☐	☐	☐
Educational history	☐	☐	☐	☐
Any other personal information?				

9. Do you know who or which organizations have access to your information? *(choose one)*
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

10. Do you know who or which organizations have accessed or used your information? *(choose one)*
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

11. Do you know how, or for what purpose, your information will be used by the organization or each organization that has access to it? *(choose one)*
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

12. Are you worried that your information could be misused by those who have access to it? *(choose one)*
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

13. Would you prefer to know who accessed your data and how your information will be used by each party? *(choose one)*
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

14. Would you prefer to have the ability to grant access only to the organizations you trust with your data? *(choose one)*
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

Figure B.8: Page 5

15. Do you know how and where your information will be stored? *(choose one)*
- ☐ Yes
- ☐ No
- ☐ Unsure

16. Are you worried that your information could be accessed and misused by unauthorized entities? *(choose one)*
- ☐ Yes
- ☐ No
- ☐ Unsure

17. Did you know that your data could be stored anywhere in the world, and that in certain regions the government or specific entities have legal right to access your data? *(choose one)*
- ☐ Yes
- ☐ No

18. Would it make you comfortable if you knew how and where your information is stored? *(choose one)*
- ☐ Yes
- ☐ No
- ☐ Unsure

19. Are there any countries or regions where you would prefer or not prefer your data to be stored?

20. Do you use a smartphone / tab / laptop / pc regularly? *(choose one)*
- ☐ Yes
- ☐ No

21. Do you have access to internet regularly? *(choose one)*
- ☐ Yes
- ☐ No

22. Would you prefer having a mobile application or a website where you could store your data and grant access to others? *(choose one)*
- ☐ Yes
- ☐ No
- ☐ Unsure

23. What features would you like in a system designed to protect and manage your personal data?

24. Do you know about blockchain technology? *(choose one)*
- ☐ Yes
- ☐ No
- ☐ Unsure

25. (If you answered “No” or “Unsure” to question no 24, you can skip this question.) Would you be comfortable in having your data stored in a blockchain based system? *(choose one)*
- ☐ Yes
- ☐ No
- ☐ Unsure

Figure B.9: Page 6

26. Do you think having no control over your personal or sensitive data could put you at risk or make you vulnerable to exploitation? *(choose one)*
- [ ] Definitely
- [ ] Probably
- [ ] No
- [ ] Unsure

27. Do you have anything you would like to share about data privacy, having control over your own data, or any other topics related to the questions above?

28. How important is it for you to preserve your cultural heritage information? *(choose one)*
- [ ] Not important
- [ ] Important
- [ ] Very important
- [ ] Unsure

29. If your answer to question no 28 is "Important" or "Very Important", it is because, *(choose one or more)*
- [ ] It contains unique or important knowledge or traditions that could be useful for all.
- [ ] It contains unique or important knowledge or traditions that could be of monetary worth.
- [ ] This information can be passed down to your future generations.
- [ ] The community's history should be preserved.
- [ ] Of Other reasons (Please specify).

30. What type of unique or important knowledge do you intend to preserve? *(choose one or more)*
- [ ] Artistic / Creativity
- [ ] Culinary
- [ ] Historical
- [ ] Medical / Herbal
- [ ] Philosophical
- [ ] Scientific
- [ ] Skills (E.g. Woodwork, masonry)
- [ ] Others (Please specify)

31. Do you think your cultural heritage information is misused or exploited by anyone? *(choose one)*
- [ ] Yes
- [ ] No
- [ ] Unsure

32. If you answered "Yes" to question no 31, how?

33. Would you prefer if you or your community can store cultural heritage information digitally and control access based on your or community's preferences? *(choose one)*
- [ ] Yes
- [ ] No
- [ ] Unsure

Figure B.10: Page 7

34. If you answered “Yes” to question no 33, storing in which formats do you think would be useful? *(choose one or more)*

- ☐ Audio
- ☐ Images
- ☐ Text
- ☐ Video
- ☐ Others (Please specify)

35. Do you think having no control over your cultural heritage information could put yourself and your community into disadvantage? *(choose one)*

- ☐ Definitely
- ☐ Probably
- ☐ No
- ☐ Unsure

36. Do you have any opinions you would like to share about digitally preserving cultural heritage information?

Figure B.11: Page 8

Appendix C

Setting up the prototype

The source code of the prototype and supporting applications can be downloaded from the following repositories:

- `https://github.com/vignes5454/Test` – Contains the Cardano and Prism setup packages, including the CardanoWebAPI and the Cardano Web Application.
- `https://github.com/vignes5454/IPFSClient` – Contains the IPFS client (Console Application).
- `https://docs.ipfs.tech/install/ipfs-desktop/#windows` - IPFS Desktop client

The CardanoWebAPI, CardanoWeb, IPFS Client, and IPFS Desktop Client must be run in a Windows environment. The CardanoWebAPI, CardanoWeb, and IPFS Client can either be built from the source code or installed from precompiled binaries from the Application folder.

C.1 Running the Cardano Node and Hyperledger Identus

The Cardano Node and Hyperledger Identus must be run inside an Ubuntu environment in WSL2. Instructions to install WSL2 and Ubuntu 24.04.2 can be found here: `https://learn.microsoft.com/en-us/windows/wsl/install` .

After setting up the WSL2 environment, follow the steps below.

1. Download the repository `https://github.com/vignes5454/Test`.
2. Navigate to the *preprod* directory. This is where the Cardano setup is located.
3. Run the following commands (Figure C.1):

```
chmod +x download-testnet-snapshot.sh
./download-testnet-snapshot.sh
```

4. Once the script finishes, install Docker. Instructions to install Docker can be found here: `https://docs.docker.com/engine/install`
5. Then, run these commands :

```
chmod +x cardano-start.sh
./cardano-start.sh
```

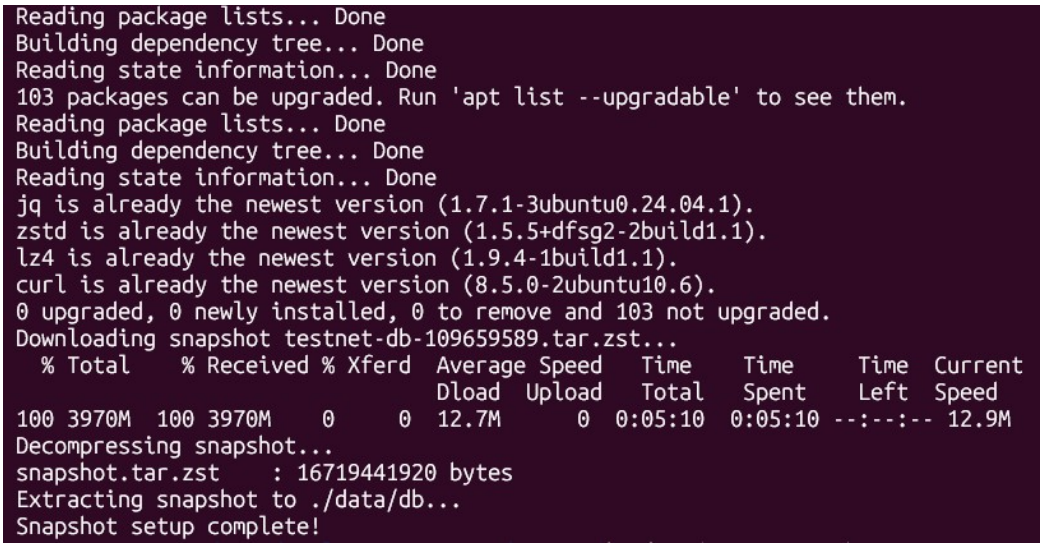


Figure C.1: Running download-testnet-snapshot.sh

This will run the Cardano node and synchronise it with the Cardano network. This process may take some time (potentially several hours, depending on the internet speed and the computer's performance).

Once the Cardano node has fully synchronised, run the following commands to start the Prism nodes for the Issuer, Holder, and Verifier. Note that running only the Issuer and Holder nodes is sufficient to perform a full cycle of the features.

Important: Ports can be changed if needed. However, any changes must also be reflected in the appsettings of the CardanoWebAPI and CardanoWeb applications.

Issuer:

```
./prism-start.sh -e .env-issuer -d host.docker.internal
   -n issuer -p 8080 -b
```

Holder:

```
./prism-start.sh -e .env-holder -d host.docker.internal
   -n holder -p 8090 -b
```

Verifier:

```
./prism-start.sh -e .env-issuer -d host.docker.internal
   -n verifier -p 8092 -b
```

Once the nodes are up and running, you can create Cardano wallets using the API below. This can be done by sending a POST request. A sample request is provided:

Endpoint: http://localhost:7090/v2/wallets

Headers: Content-Type: application/json

Payload:

```
{
  "name": "HolderWallet",
  "mnemonic_sentence": [
"repeat", "install", "device", "milk", "canal", "slam",
   "merry", "weasel", "poverty", "north", "correct",
   "whip", "document", "junk", "hundred"
    ],
  "passphrase": "xxxxxxx"
}
```

A mnemonic sentence can be generated using the following tool: `https://iancoleman.io/bip39`

The wallet details generated above must be added to the respective environment files .env-holder, .env-issuer and .env-verifier (if the verifier node is used). Each component requires a separate wallet, so ensure that a unique wallet is created and correctly configured in each file (Figure C.2).

```
PRISM_AGENT_VERSION=1.28.0
PRISM_NODE_VERSION=2.6.1
PORT=8090
VAULT_DEV_ROOT_TOKEN_ID=root
PG_PORT=5438
PGADMIN_PORT=5052
WALLET_ID=xxxxx
WALLET_PASSPHRASE=xxxxx
WALLET_PAYMENT_ADDR=xxxxx
```

Figure C.2: Example Environment File

C.2 Running the CardanoWebAPI

To run the CardanoWebAPI, CardanoWeb, and IPFSClient console applications, you need the .NET 8 runtime installed on your system. This can be downloaded from `https://dotnet.microsoft.com/en-us/download/dotnet/8.0` . Ensure that it is installed and available in your system PATH.

The CardanoWebAPI can be started using the following command from its published folder:

```
dotnet .\CardanoBridgeAPI.dll
```

C.3 Running the CardanoWeb Application

The CardanoWeb application can be started from its published folder using the following command:

```
dotnet .\CardanoWeb.dll
```

C.4 Running the IPFS Client Console Application

The IPFS Client Console Application can be started by double-clicking the IPFSClientConsole.exe file in the published folder.

Alternatively, you can run it from the command line using:

```
dotnet .\IPFSClientConsole.dll
```

C.5 Running the IPFS Desktop Client

After downloading the IPFS Desktop Client, it must be installed. Once the installation is complete, the application can be launched.

Appendix D

User Guide

A demonstration video of the application can be downloaded from the OneDrive link below.

`https://1drv.ms/f/c/a28ebb2c74013744/IgAneYUe5SiqSZZPzx73fQ6rAbhLAoMjmtHKFfM5zmEFs6A?e=zlC1DI`

D.1 Immigration Related Data Handling

D.1.1 User Registration and Login

The *login* page (Figure D.1) enables users to access the application by entering their username and password. Entering the correct credentials will successfully log the user into the system (Figure D.2). If a migrant doesn't have an account, for example when a migrant seeks to have their documents verified and to receive a VC from the Trusted Third Party, they may visit the login page of the Trusted Third Party's application and select *Register as a new user* in order to create an account (Figure D.3).

The *registration* page (Figure D.3) allows the user to provide an email address and a chosen password that will be used to create the account. Once the registration form has been submitted, an email containing an activation link is sent to the user. Access to the account is enabled when the user clicks this link.

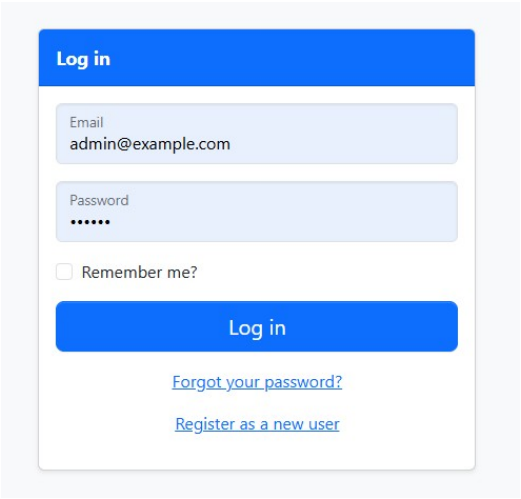


Figure D.1: Login Page

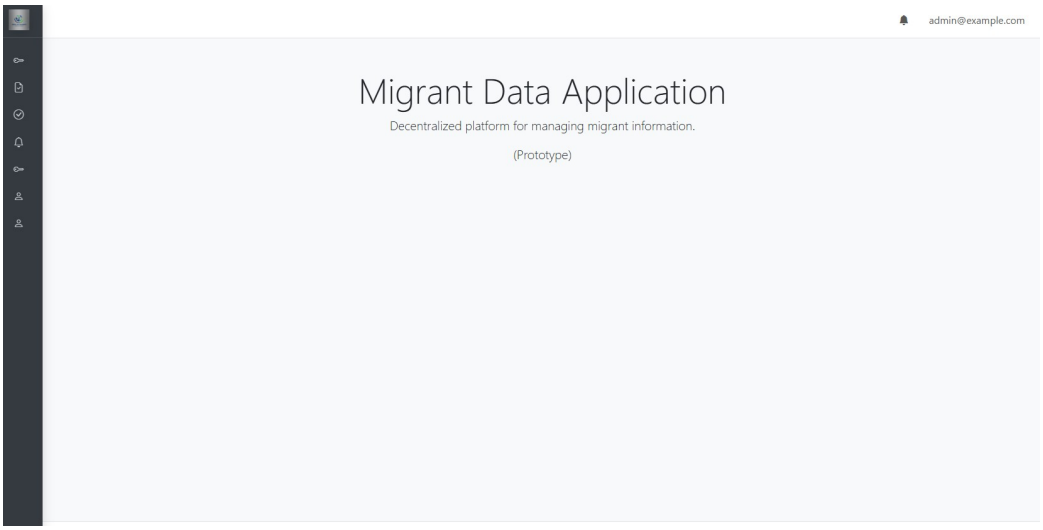


Figure D.2: User Successfully Logged In

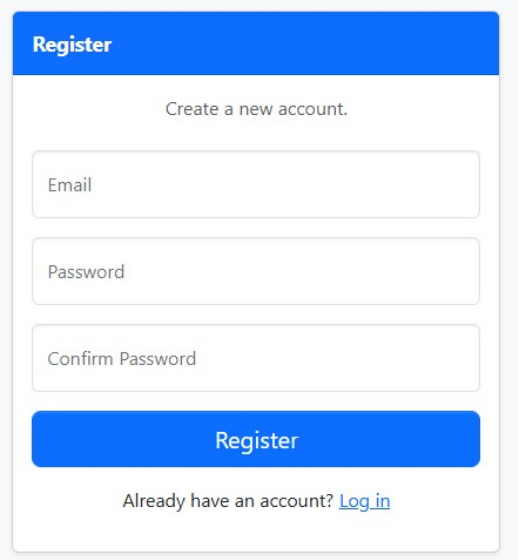


Figure D.3: User Registration Page

D.1.2 DID Creation and Publishing

From the side menu, the user can navigate to *DID Management* and then to the *All DIDs* page (Figure D.4). This page displays all DIDs owned by the user. It also presents the DID metadata, including the name and the resolution status. Users can edit any DID by selecting the *edit* button next to the DID they wish to modify.

If the user wishes to create a new DID, they can select *Create New DID* (Figure D.5). On the next page, the user can enter a DID name, which acts as a label that helps to identify the DID. The user may also add a description that explains the purpose of the DID, for example how it will be used. After this, endpoint details can be provided. One endpoint is used to validate any credentials that are issued using this DID. The notification endpoint is used to inform the DID owner when their Verifiable Credentials or documents have been accessed.

After entering the required information, the user can select *Create* button to generate the DID. Once the DID has been created, both the long DID and the short DID are displayed at the bottom of the page. Selecting the *publish* button will publish the DID on the Cardano Testnet (Preprod).

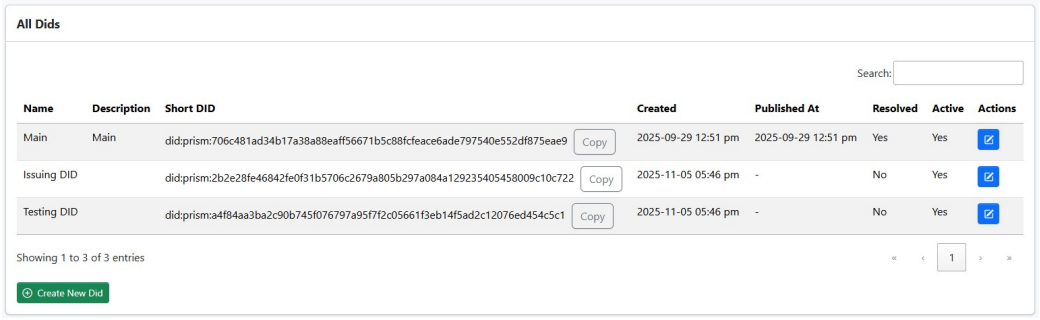


Figure D.4: All DIDs Page

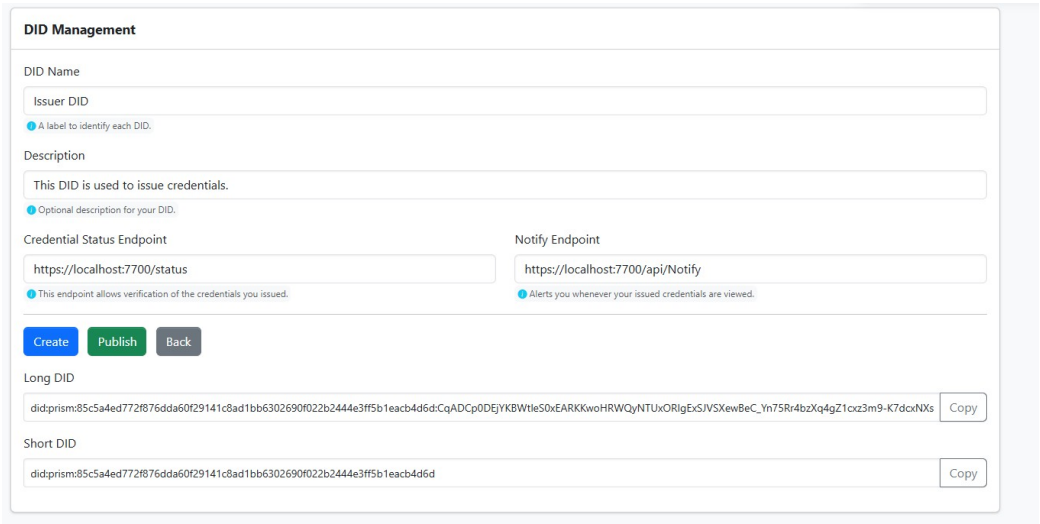


Figure D.5: DID Creation Page

If the DID has been successfully published to the Cardano Preprod network, the transaction hash from the publication process can be tracked using Cardano monitoring websites, such as Cardano Scan (https://preprod.cardanoscan.io). In Figure D.6, the transaction hash is highlighted in yellow. In Figure D.7, this hash was queried on the Cardano Scan website, and its successful publication was confirmed.

Figure D.6: Transaction Hash

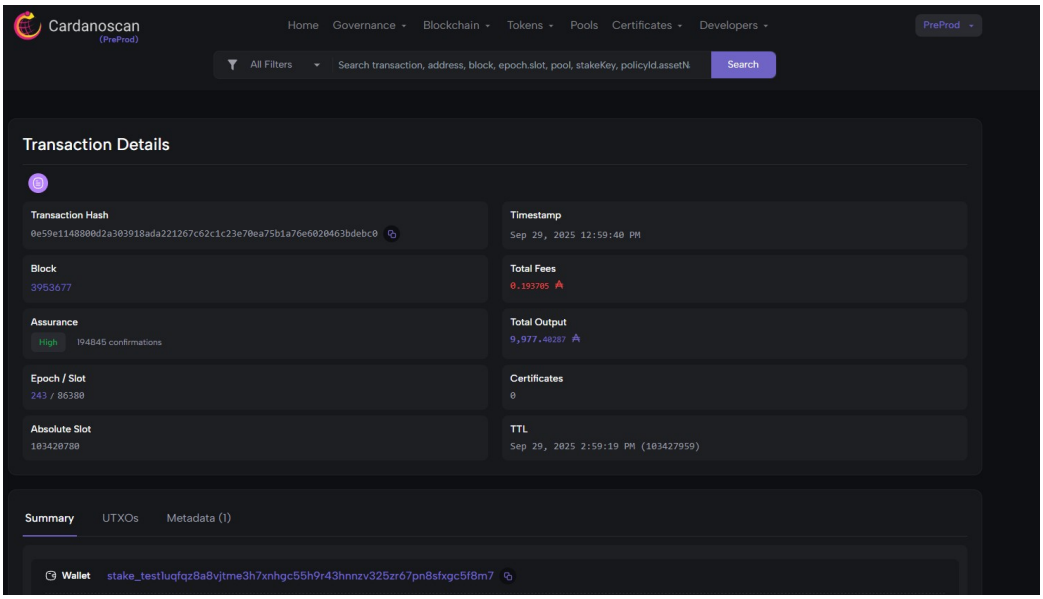


Figure D.7: Transaction Found In Cardano Scan

D.1.3 Requesting a Credential

After the migrant creates an account in the Trusted Third Party's application, they can request a credential by navigating to the *Credentials* menu and selecting *Create Request* (Figure D.8). On this page, the migrant is required to provide their short DID. They must then sign the nonce to confirm that

they are using the correct DID for this process. It is recommended that migrants use the copy and paste buttons provided on the page, as this reduces the risk of errors and ensures secure handling of the data.

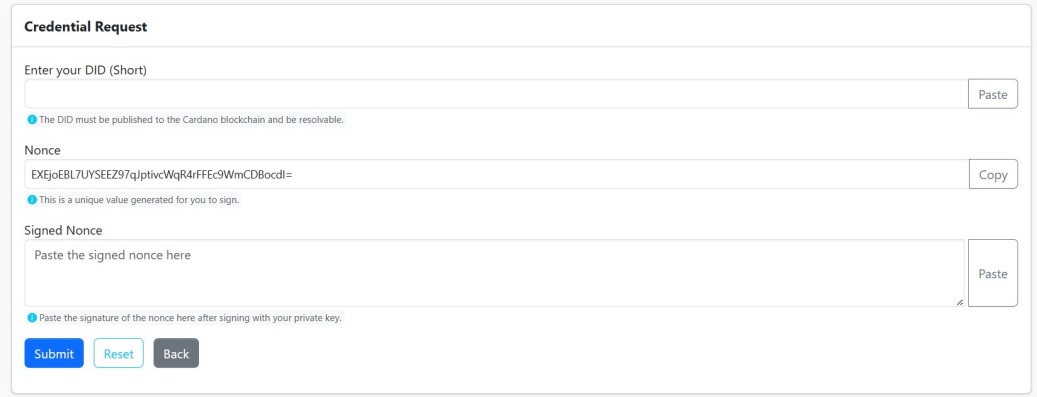


Figure D.8: Creating a Credential Request

After completing these steps, the migrant can select *Submit* to proceed to the next stage of the credential request process. If the signed nonce is correct, the migrant will be able to move to the a stage (Figure D.9). If the signed nonce is invalid, the migrant will not be able to proceed (Figure D.10).

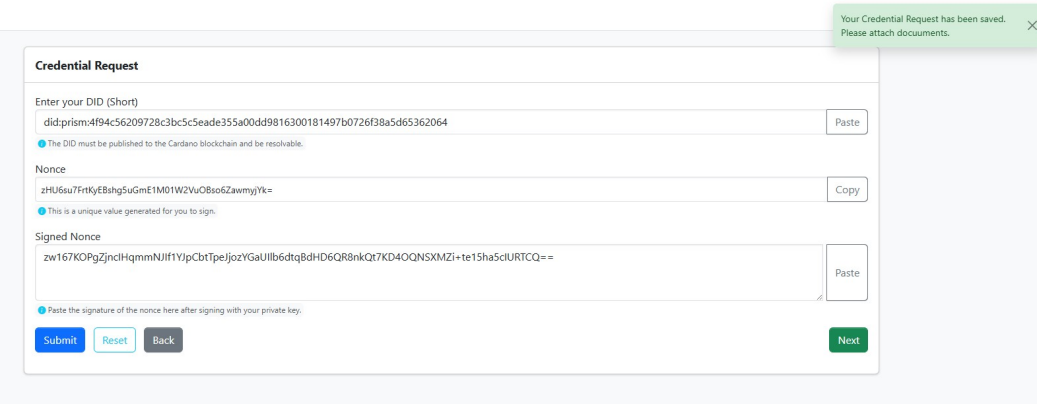


Figure D.9: Creating a Credential Request - Valid Nonce

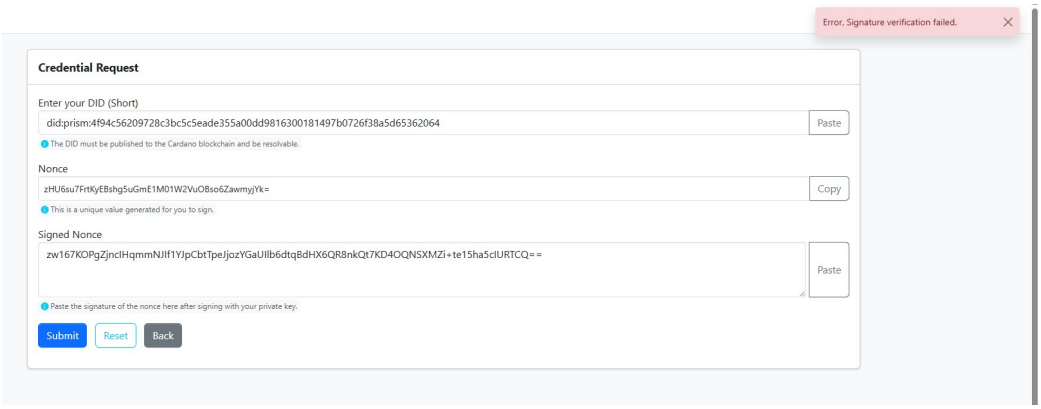


Figure D.10: Creating a Credential Request - Invalid Nonce

After successfully submitting the nonce, the migrant will land in the *Attach Documents* page (Figure D.11). On this page, the migrant should attach the documents they wish to have verified. If they already have documents that have not been verified, these will be displayed on this page. If not, the migrant can select *Create New Document*.

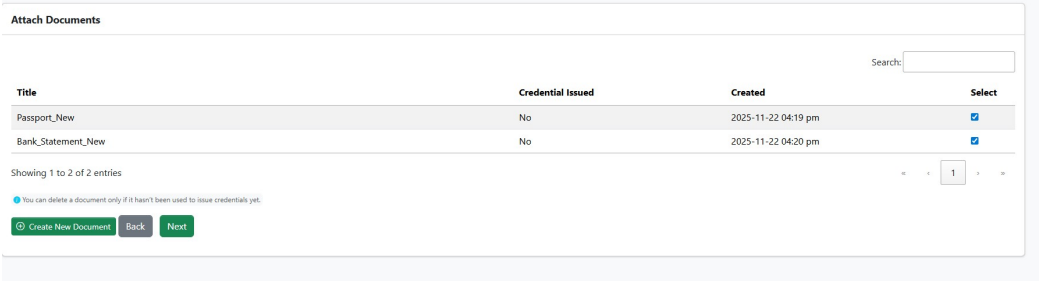


Figure D.11: Attach Documents Page

If the migrant selects *Create New Document*, they will be taken to the Upload Document page, where they can choose a file to upload (Figure D.12). The file should be in PDF format. Once the file is selected, the migrant can click *Submit* to complete the upload process.

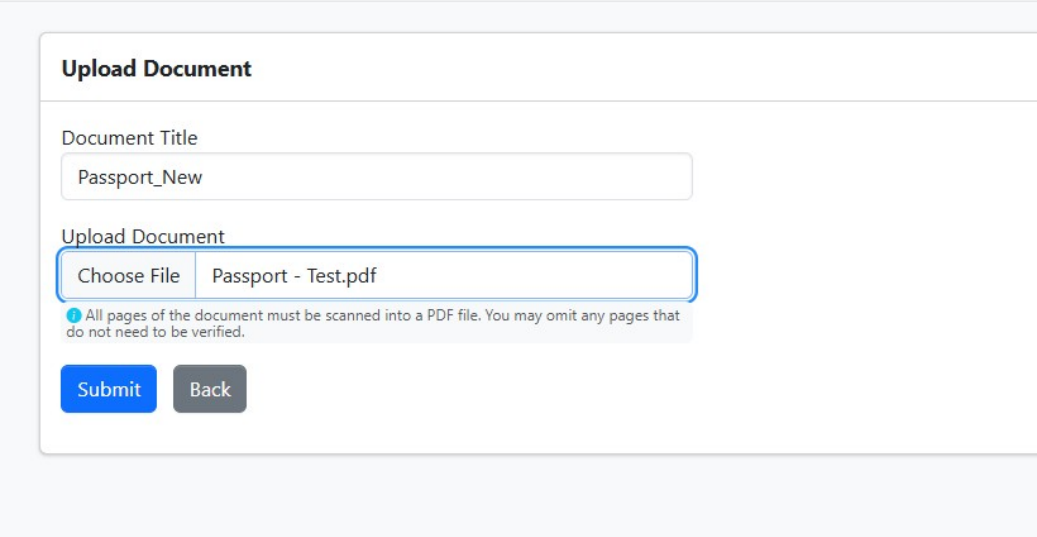


Figure D.12: Upload Documents Page

Once the migrant has uploaded the documents they wish to have verified, they can select the relevant documents and click Next to proceed to the *extra claims* page (Figure D.13).

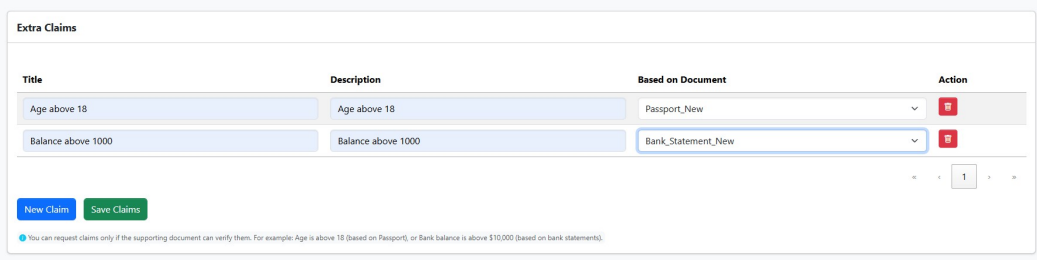


Figure D.13: Extra Claims Page

On the *extra claims* page, the migrant can enter the claims they wish to have verified and then select the document on which those claims should be based. After doing so, the migrant should click the *Save Claims* button, after which they will be directed to the *confirmation* page (Figure D.14). Here, the migrant can either confirm or cancel the credential request. Once the request is confirmed by clicking the *Submit* button, it is sent to the trusted third party for verification.

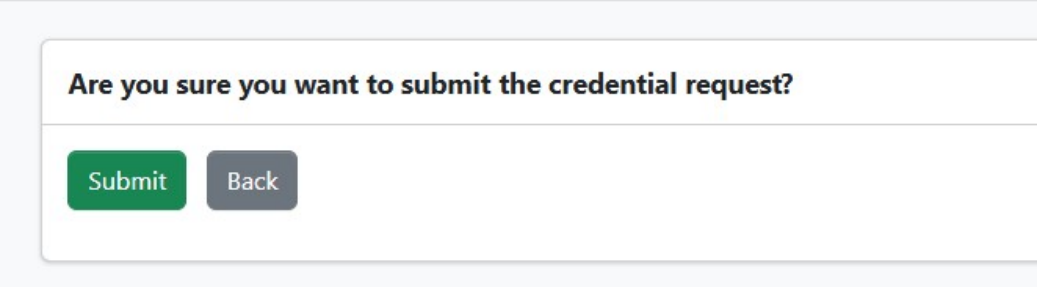


Figure D.14: Confirmation Page

D.1.4 Processing Credential Requests

The trusted third party is responsible for verifying migrant documents and issuing VCs based on this information. When the trusted third-party officer logs into their application, they can access the pending credential requests under the *Credential Issuance* menu by selecting the *Pending Credential Requests* option. This will open the *pending requests* page (Figure D.15).

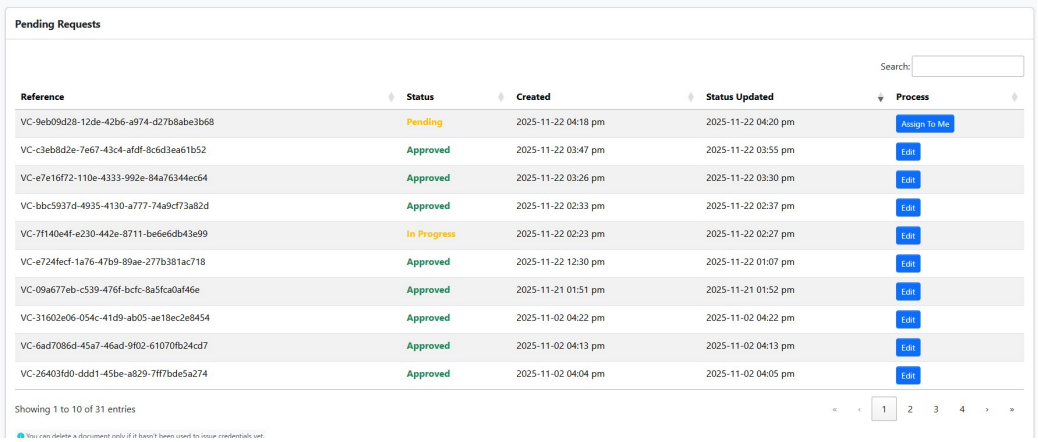


Figure D.15: Pending Credential Requests Page

Under *Pending Requests*, the trusted third-party officer can view all outstanding credential requests. The first column presents the request reference, and the second indicates the current status, which may be Pending, In Progress, Approved, Rejected, or Revoked. The interface also displays the

date and time the request was created and the most recent status update. The officer may assign a request to themselves by selecting *Assign to Me*.

Once a request has been assigned, the application displays all documents associated with that request (Figure D.16).

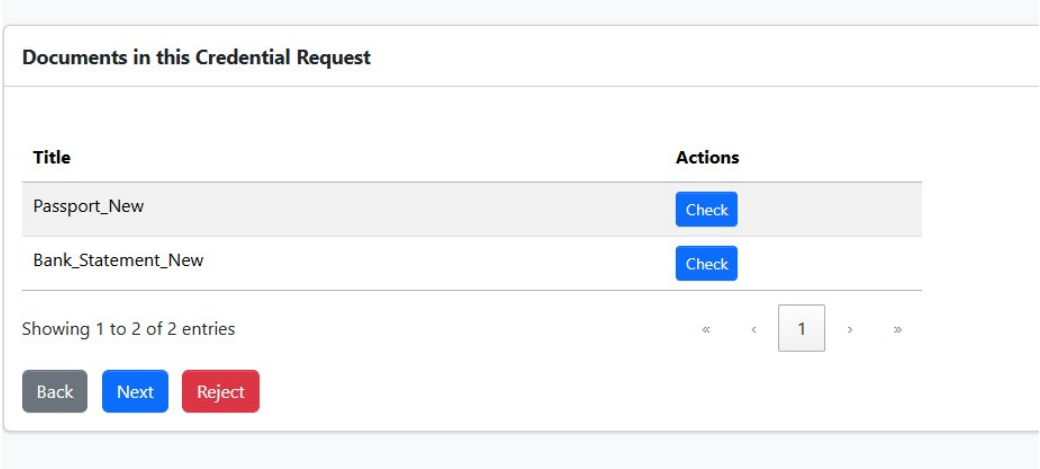


Figure D.16: Documents for the Credential Request

The officer can then select the *Check* button. Upon doing so, the respective document will be displayed. In this example, a passport and a bank statement have been provided. Figure D.17 illustrates the passport being processed.

The officer is required to enter the title of the document and subsequently type the fields contained within the passport. Common fields that appear in migration-related documents are automatically suggested as the officer types (autocomplete). If any fields need to be removed, the officer may select the *Remove* button.

Once all fields have been entered, any extra claims related to the particular document are displayed below as check boxes. If a claim is confirmed to be true according to the document, the officer can select the corresponding check box. After completing this process, the officer may click *Next*.

The same procedure should be followed for all documents. Figure D.18 illustrates the processing of a bank statement.

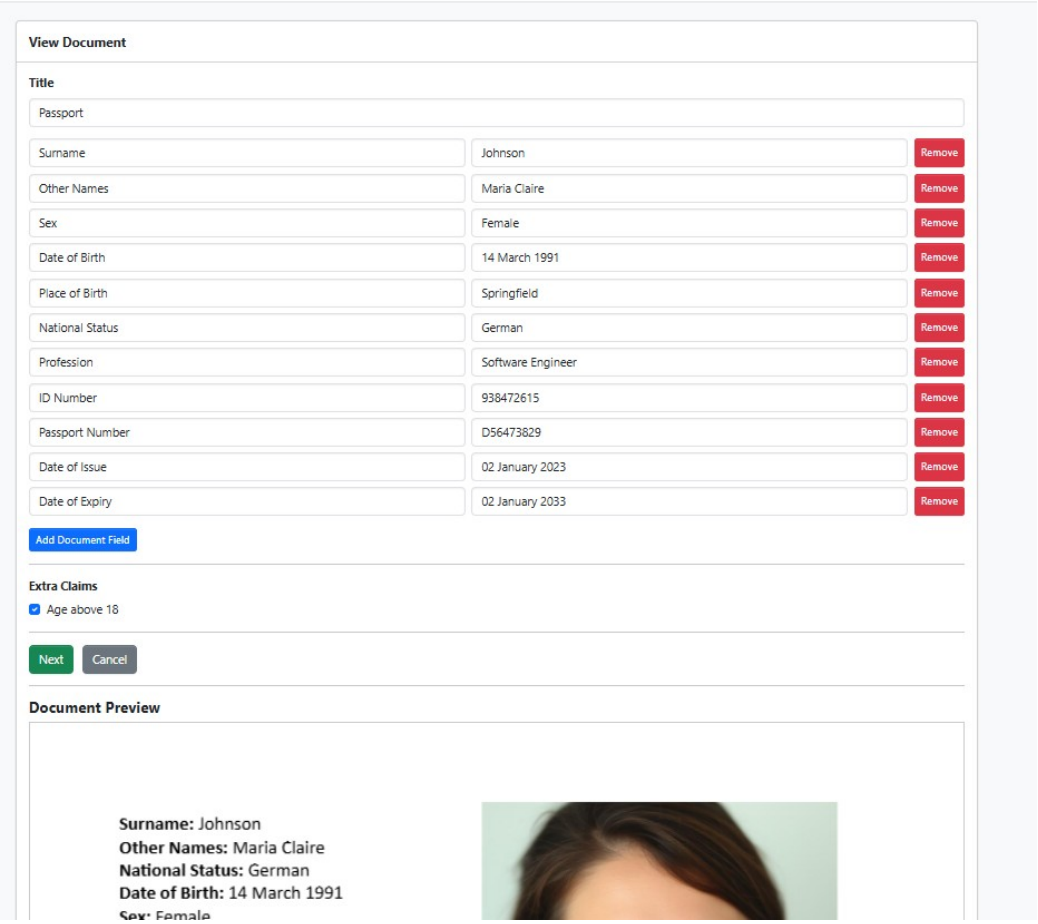


Figure D.17: Passport Being Processed.

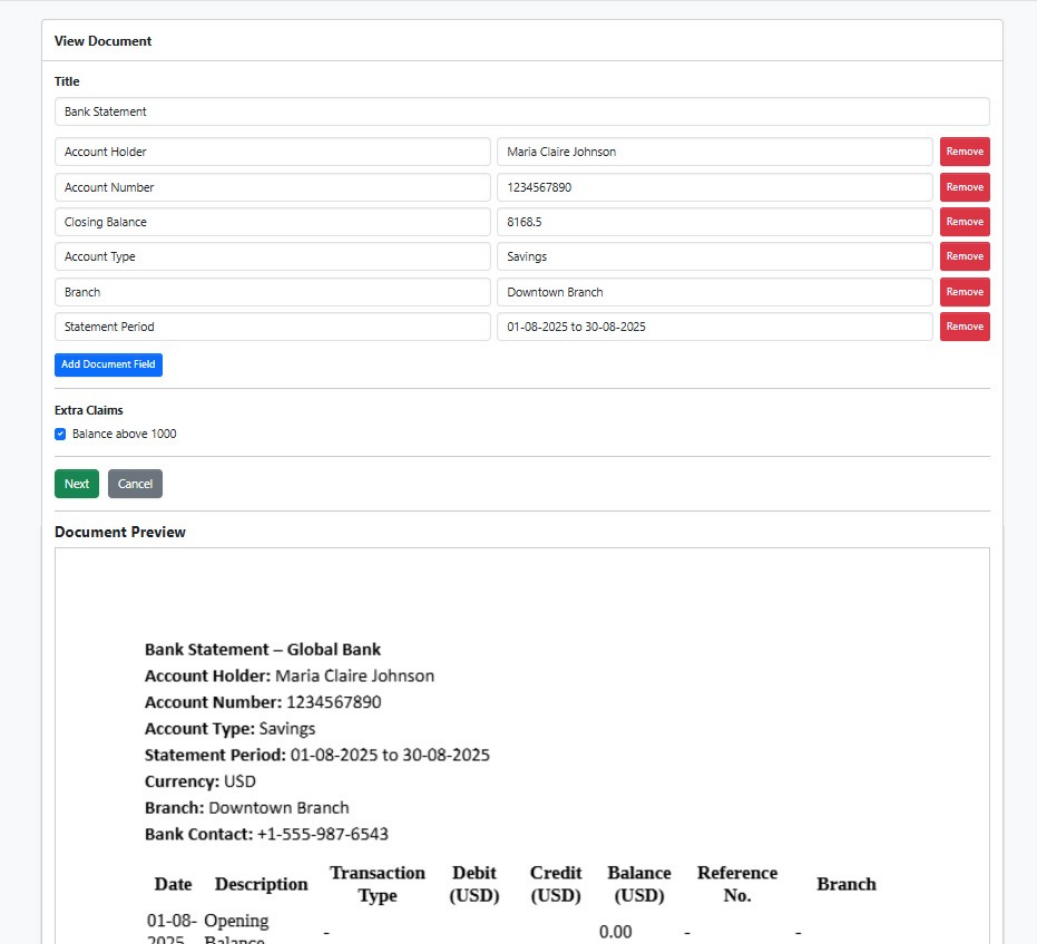


Figure D.18: Bank Statement Being Processed

After all documents have been processed, the officer may click *Next* on the *Documents in this Credential Request* page. A confirmation message will then be displayed (Figure D.19). If the officer is satisfied with the information, they may select *Yes* to confirm the credential issuance. Once confirmed, the application will send the invitation for the verifiable credential (VC) offer.

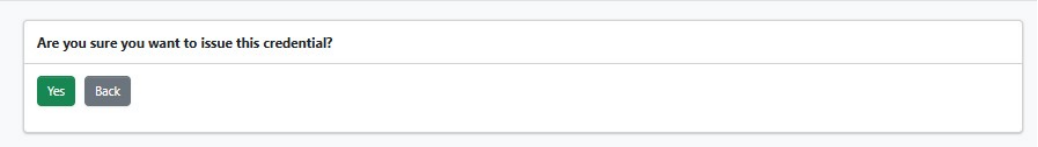


Figure D.19: Confirmation Message for VC Issuance

Credential Request Rejection : If, for any reason, the officer decides to reject a credential request, they may select the *Reject* button. The officer is then required to provide a reason for the rejection during the confirmation process (Figure D.20). Once the rejection is confirmed, the credential request is formally rejected, and the migrant is notified accordingly.

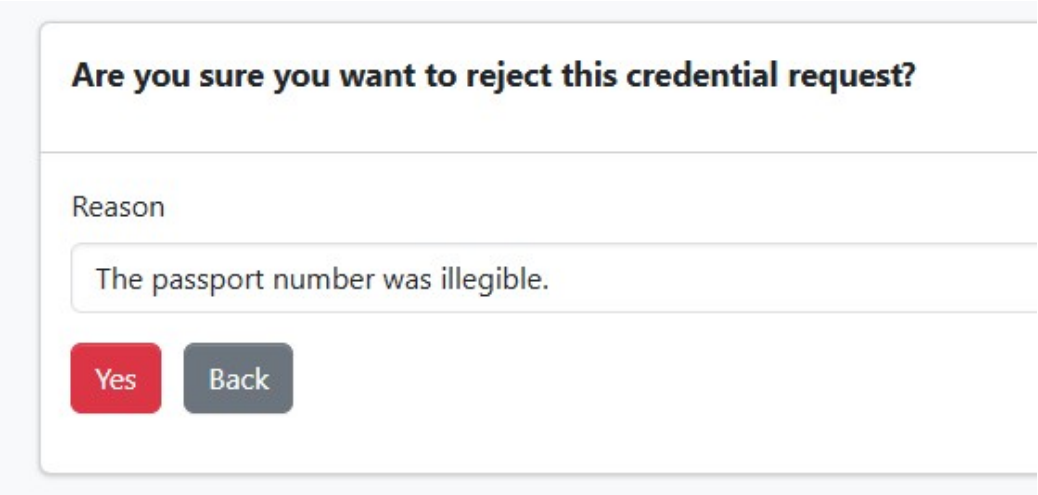


Figure D.20: Credential Request Rejection

Revoking a Credential : If the trusted third party needs to revoke a credential at any point, they should navigate to the *Pending Requests* page (Figure D.21).

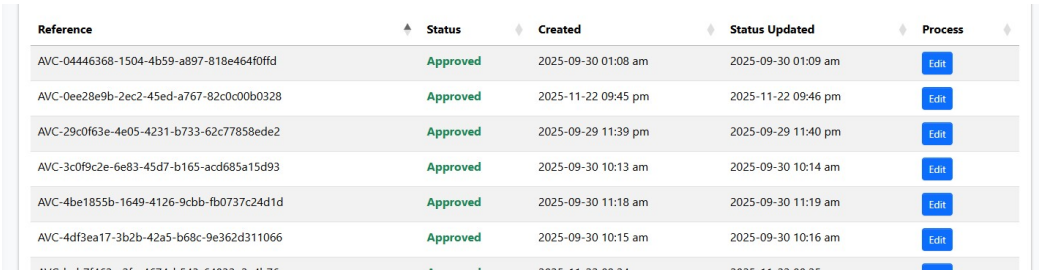


Figure D.21: Approved Credential Requests

They must then click the *Edit* button next to the credential they wish to revoke. This will display all documents related to that request, along with a *Revoke* button (Figure D.22).

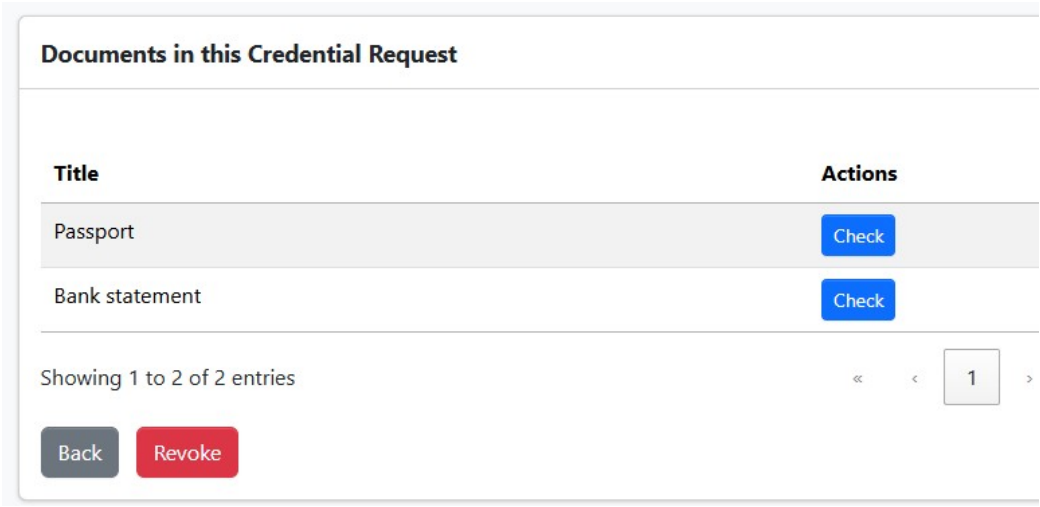


Figure D.22: Revoke Option

Clicking the *Revoke* button prompts the officer to confirm the revocation. The officer is required to enter the reason for revocation and then click *Yes* to complete the process (Figure D.23).

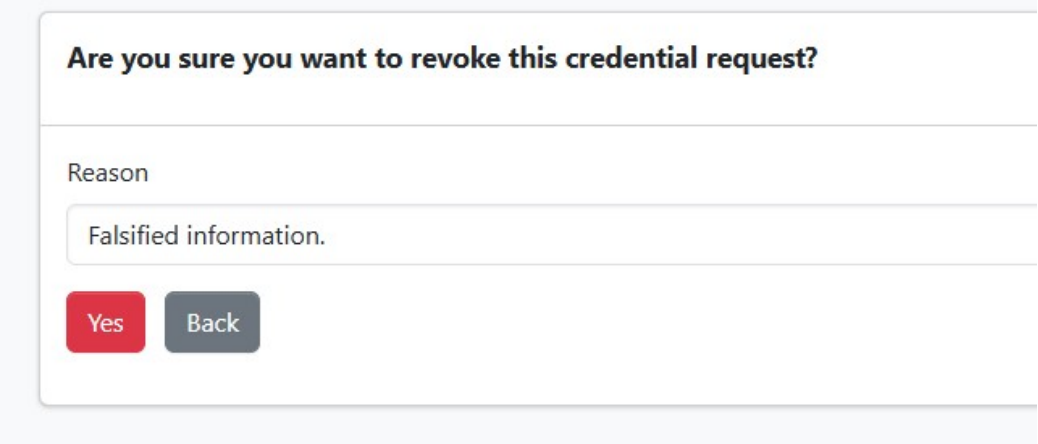


Figure D.23: Confirmation

D.1.5 Accepting a VC Invitation and Offer

When the migrant logs into the trusted third party application, they will be notified of the outcome of their credential request. The notification screens are presented in Section D.1.11.

To accept a VC offer, the migrant should navigate to the *Credentials* menu and select *Credential Requests*. They will then be presented with all their credential requests, including the status, creation date, and most recent status update (Figure D.24). The migrant can identify a specific credential request either by its reference number or by the creation date.

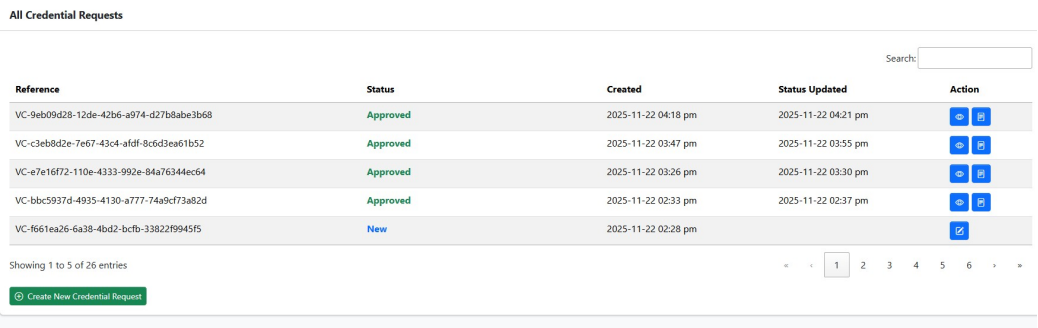


Figure D.24: All Credential Requests

To view the details of a credential request, the migrant may click the

View button (eye symbol), which will display the full request details (Figure D.25). If the migrant chooses to accept the credential request, they may click the *Credential Request Invitation* button (file symbol) to get the invitation (Figure D.26).

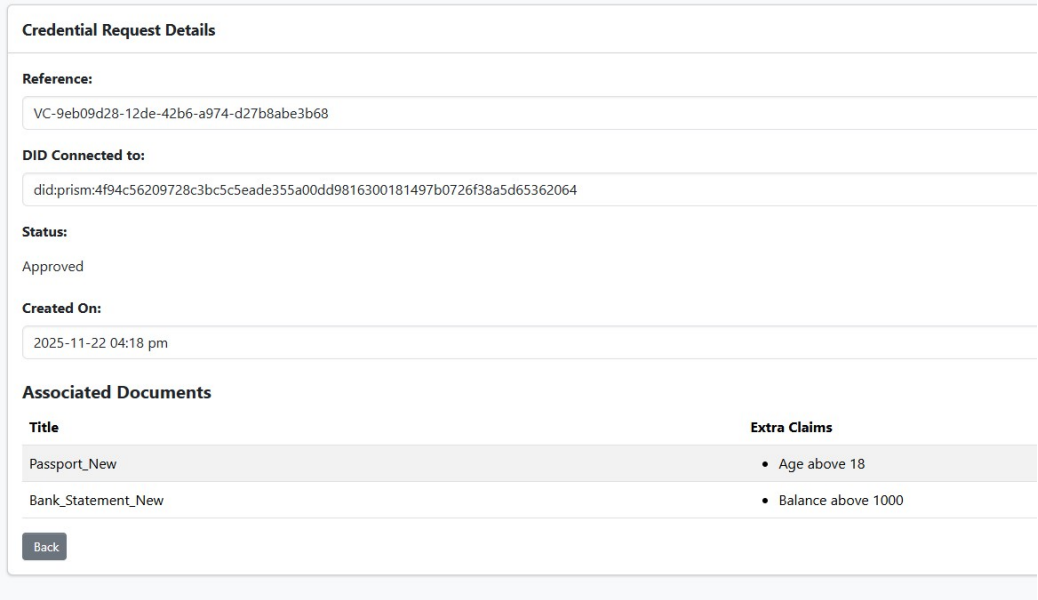


Figure D.25: Credential Request Details

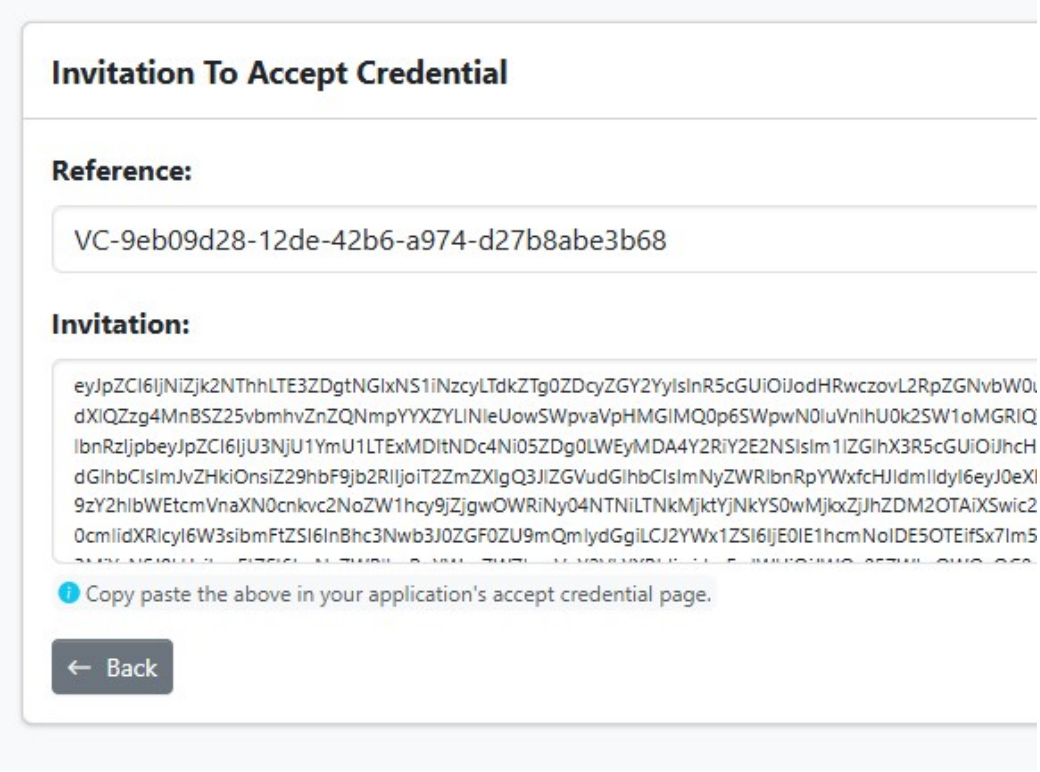


Figure D.26: VC Offer Invitation

To accept the VC offer invitation, the migrant must copy the invitation from the trusted third-party application and paste it into their own application. This can be done by navigating to the *Invitation* menu and selecting *Accept Invitation*. The *Accept Credential Offer Invitation* page will then be displayed (Figure D.27). After pasting the invitation, the migrant should click *Accept Invitation*.

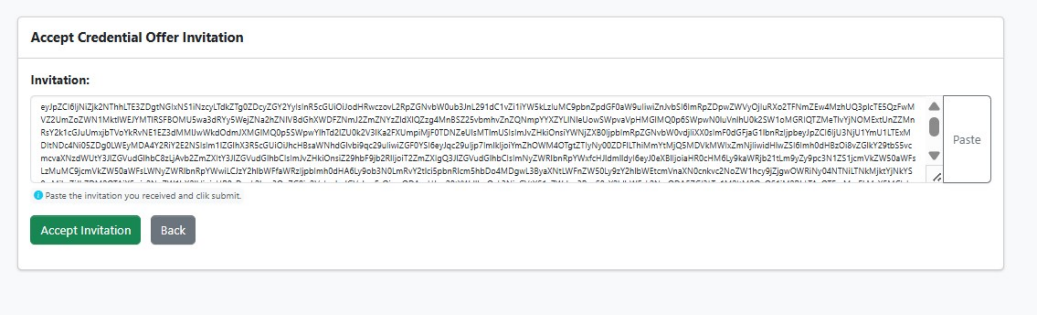


Figure D.27: Accept Credential Offer Invitation

Once the VC offer invitation has been accepted, the migrant will receive the VC offer within their application. This can be accessed under *All Credential Offers* in the *Invitation* menu, which displays all credential offers received by the migrant (Figure D.28). To accept a VC, the migrant should click the *View* button (eye symbol) to display the details of the offer. The credential offer will show all claims contained within the VC, as well as the migrant's DID in a drop-down list. The migrant can select their DID and click *Accept Claim* to accept the VC (Figure D.29).

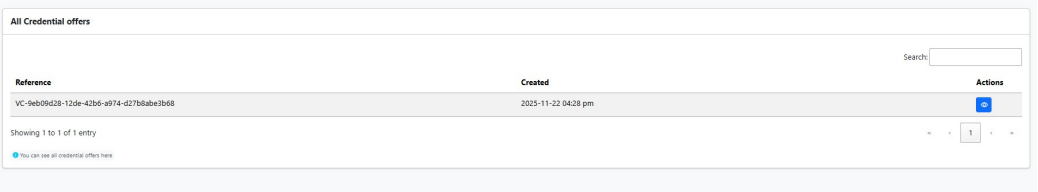


Figure D.28: All Credential Offers

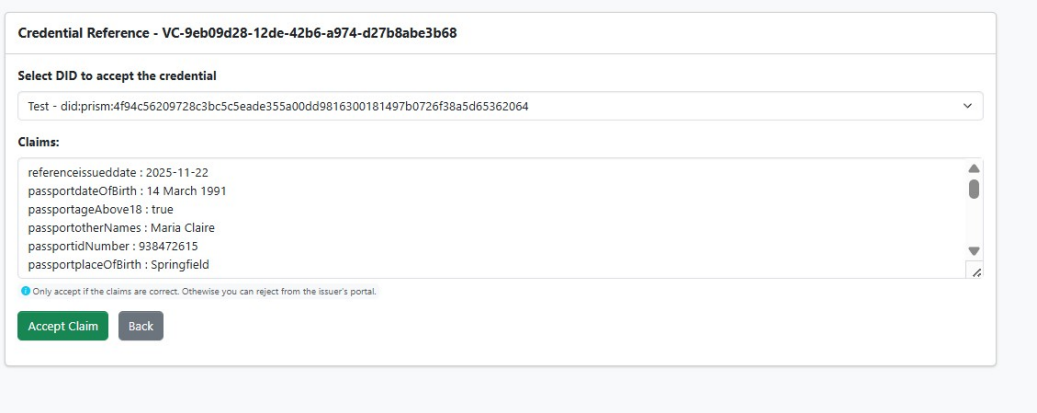


Figure D.29: Accepting the Offer (Claim)

After accepting the claim, the migrant will receive the verifiable credential. To view their VCs, the migrant should navigate to the *Credential Wallet* menu. On the A*ll Verifiable Credentials* page, the migrant can view all credentials they have received. On the list of VCs, migration document related VCs can be identified either by the type **Documents** or by the reference prefix **VC**. By clicking the *View* button (eye symbol), the migrant can access the details of each verifiable credential (Figure D.31).

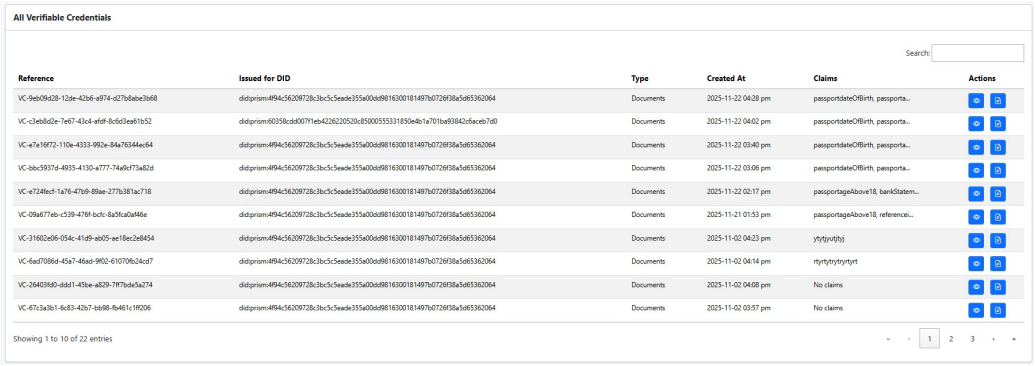


Figure D.30: Credential Wallet

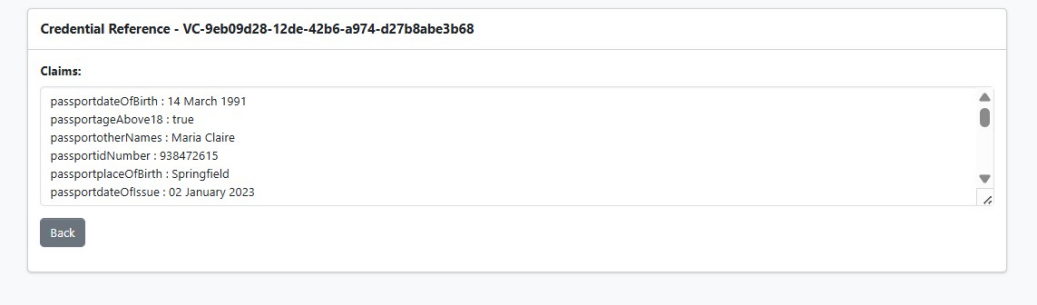


Figure D.31: VC Details

D.1.6 Creating a VC Presentation

To create a VC presentation, the migrant should navigate to the Credential Wallet page in their application by selecting *Credential Wallet* from the menu. They should then click the *Create Presentation* button (file symbol) on the VC they wish to use. The application will display all claims contained within the selected VC (Figure D.32).

The migrant can choose which claims to include in the presentation by selecting the check boxes next to the relevant claims. After making their selections, they should click *Create Presentation*, which will generate a presentation containing only the selected claims.

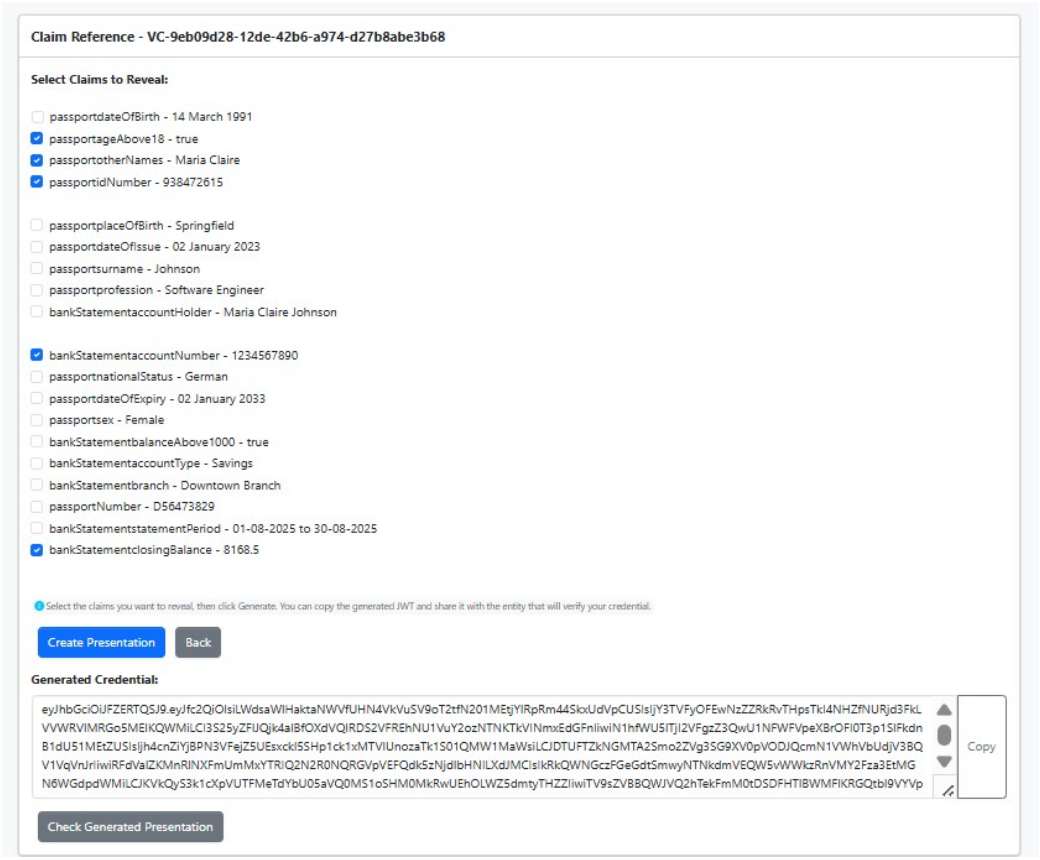


Figure D.32: Create VC Presentation

The migrant can then copy the presentation and use it as required. To review the claims included in the generated presentation, the migrant may click the *Check Generated Presentation* button (Figure D.33).

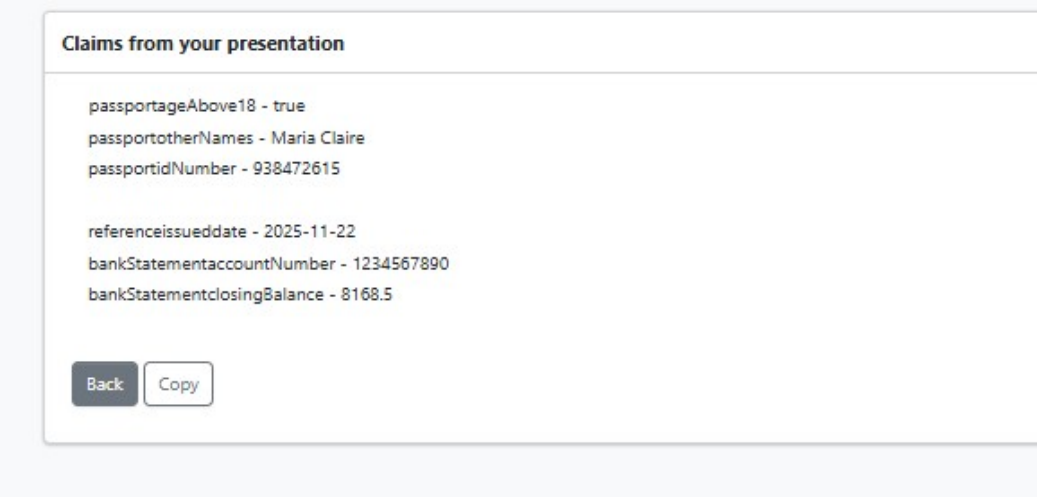


Figure D.33: Check Generated Claims

D.1.7 Creating a Verification Request

To create a verification request, the migrant must first create an account in the immigration application. They should then navigate to the *Verification* menu and select *Create Verification Request*.

On the Verification Request page (Figure D.34), the migrant is required to provide their DID and sign a nonce, as described in Section D.1.3. They must then paste the VC presentation into the Credential field and click *Submit*. Once submitted, the immigration authority will receive the VC verification request.

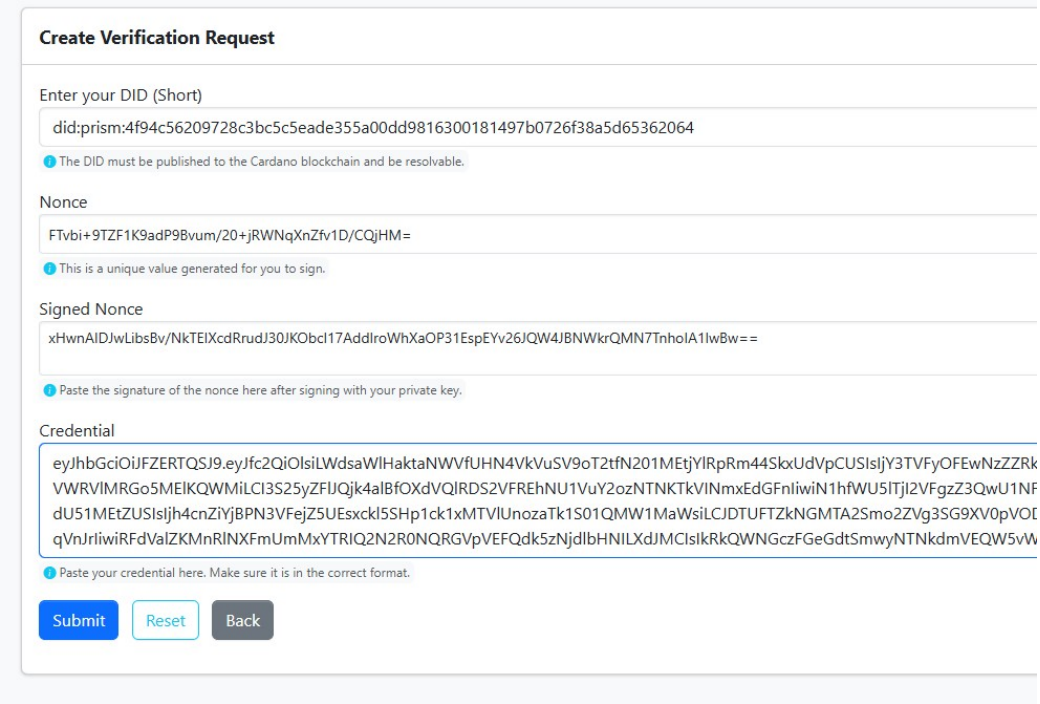


Figure D.34: Creating a Verification Request.

D.1.8 Processing a Verification Request

The immigration officer can access pending VC verification requests in their application under the *Verification* menu by selecting P*ending Verification Requests*. On this page, all pending verification requests are displayed (Figure D.35). The officer may assign a request to themselves by clicking the *Assign to Me* button.

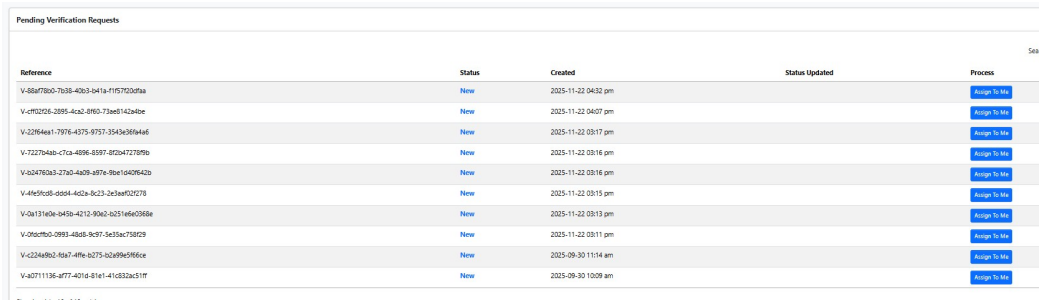


Figure D.35: Pending Verification Requests

Once a request has been assigned, the officer is taken to the Credential Information page (Figure D.36). This page displays the claims contained in the migrant's VC and indicates whether the VC issuer's signature is valid and whether the VC subject is correct.

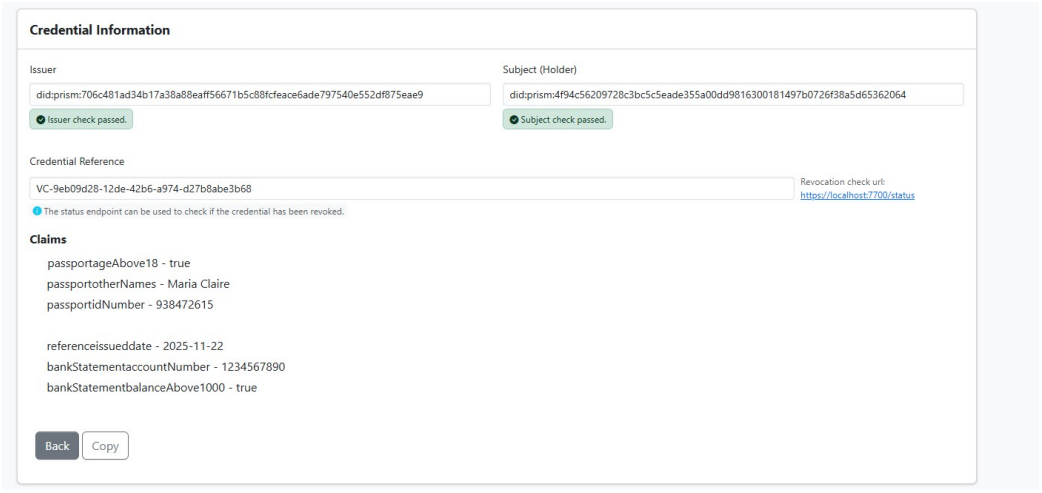


Figure D.36: Credential Information

Next to the credential reference, the officer will find a URL to check the revocation status of the VC. By clicking this link, the officer is directed to the trusted third party's portal, where they can enter the VC reference and click Check Status to verify the current status of the VC (Figure D.37).

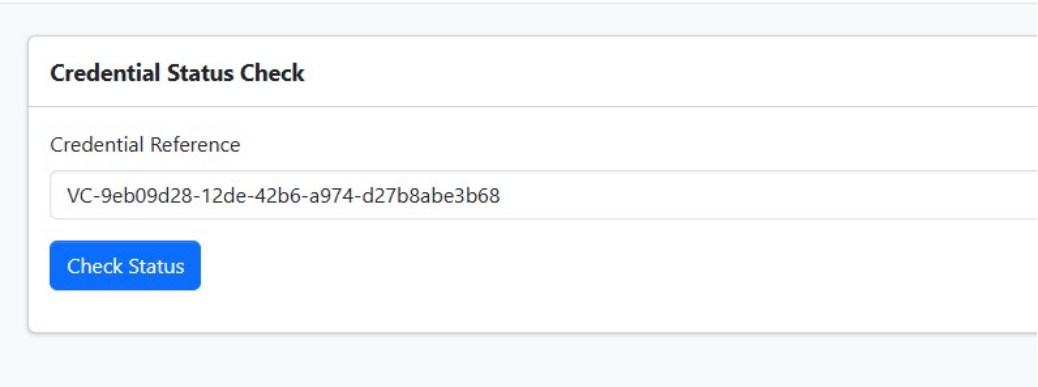


Figure D.37: Credential Status Check

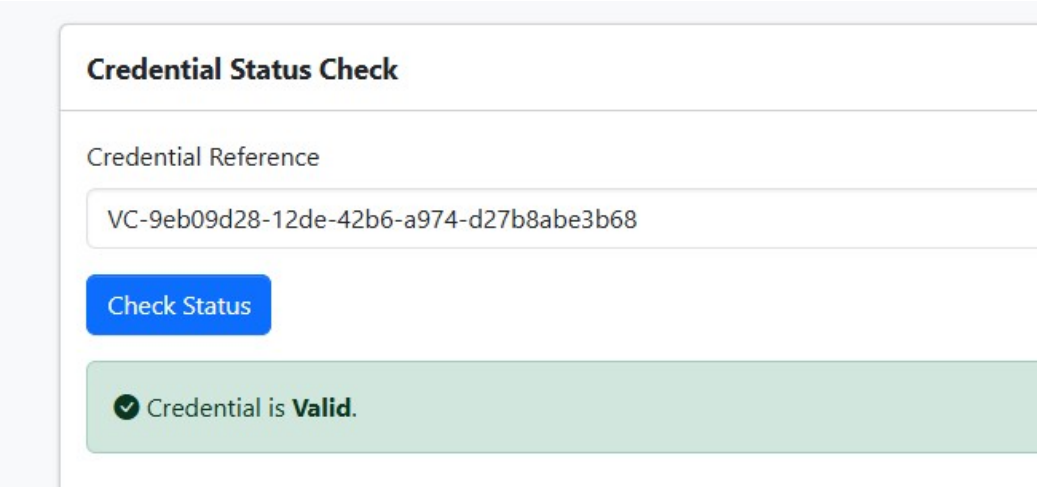


Figure D.38: Credential Status Check (Valid)

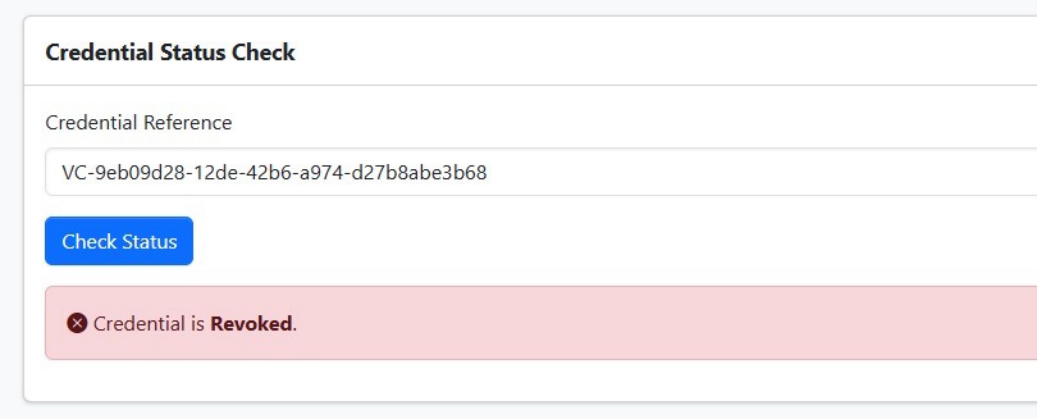


Figure D.39: Credential Status Check (Revoked)

D.1.9 Re-verification

If, for any reason, the trusted third party needs to re-verify the documents associated with a particular VC, this functionality can be used. The officer should select *Document Verification* from the menu. On the Document Verification page, they can provide the VC to be re-verified. The application will then display all documents related to the specified VC for verification (Figure D.40).

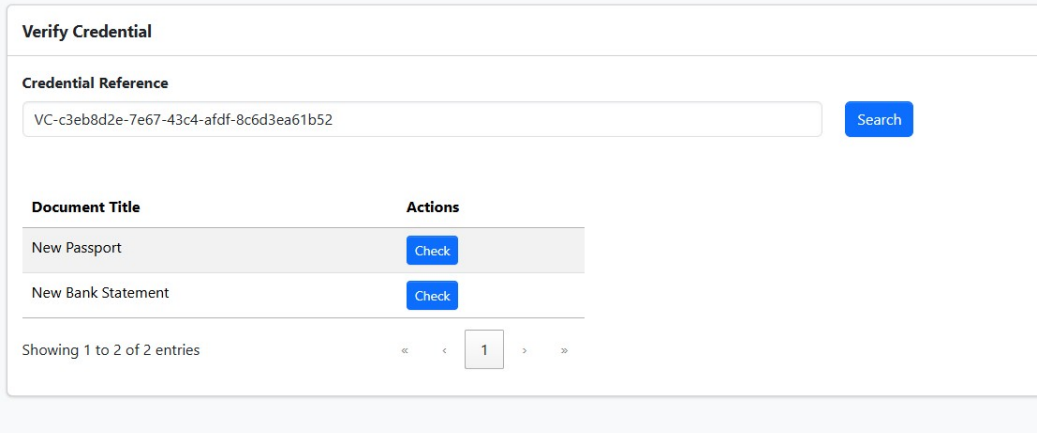


Figure D.40: Re-verification

D.1.10 Signing a Nonce

To sign a nonce, the user should navigate to the *Verification* menu and select *Sign Nonce*. On the Sign Nonce page (Figure D.41), they must enter the DID they wish to use for the signing process, along with the nonce text. They should then click *Sign*. If the DID exists in the user's system, the nonce will be successfully signed.

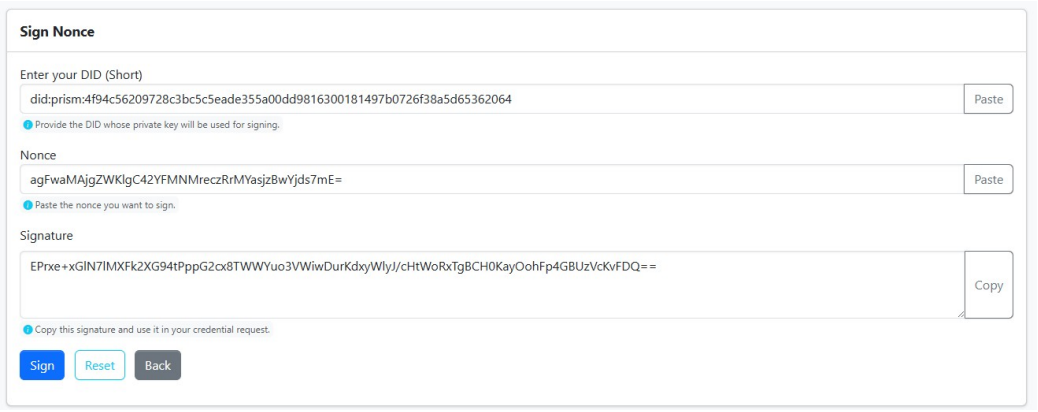


Figure D.41: Sign Nonce

D.1.11 Notifications

Whenever the user logs into the system, the number of unread notifications is displayed on the bell icon in the top-right corner (Figure D.42). The user can view their notifications by selecting the *Notifications* menu. Within this menu, unread notifications are explicitly labelled "unread". The user may click the *View* button (eye symbol) to read a notification and may delete any read notification by selecting the *Delete* button (bin symbol).

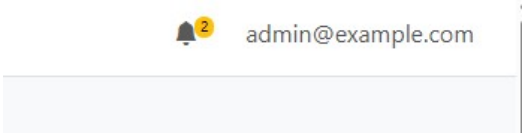


Figure D.42: Bell Icon Showing the Number of Unread Notification

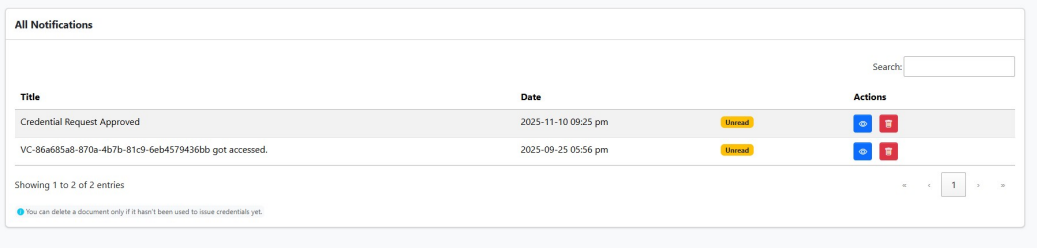


Figure D.43: All Notifications

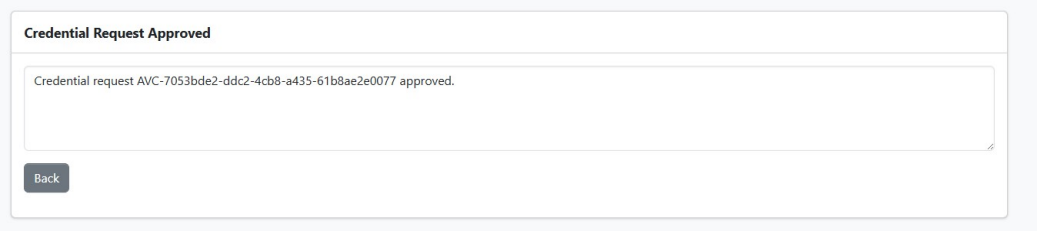


Figure D.44: Notification Details

D.2 Artefact Related Data Handling

D.2.1 Creating an Artefact

To create an artefact, the artefact owner should log into the application and navigate to the *Artefacts* menu, then select *Create Artefact*. This opens a page where the owner can upload the artefact (Figure D.45). An artefact may be a text file, video, audio file, or image. The owner can provide a title, description, and type for the artefact before clicking *Submit*.

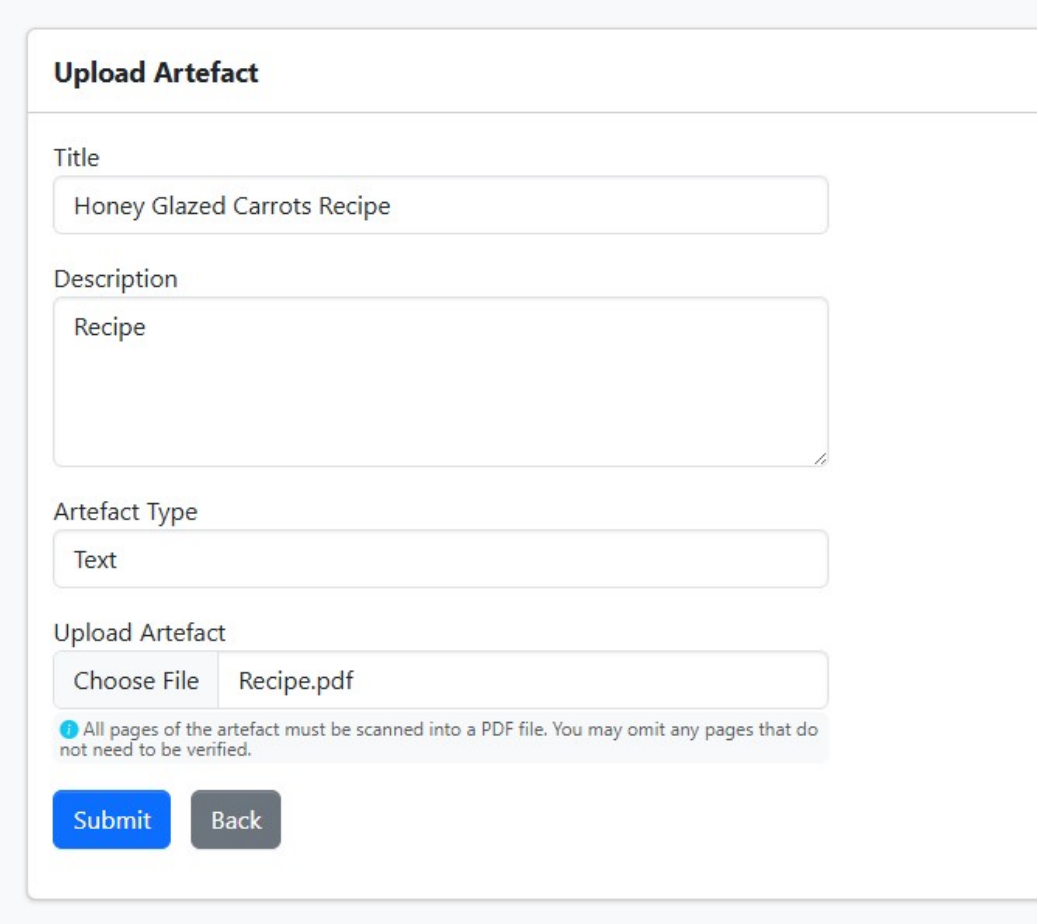


Figure D.45: Create Artefact Page

After uploading, the artefact will be available for users to browse in the catalogue. The artefact owner can view the artefacts they own by going to the *Artefacts* menu and selecting *All Artefacts* (Figure D.46).

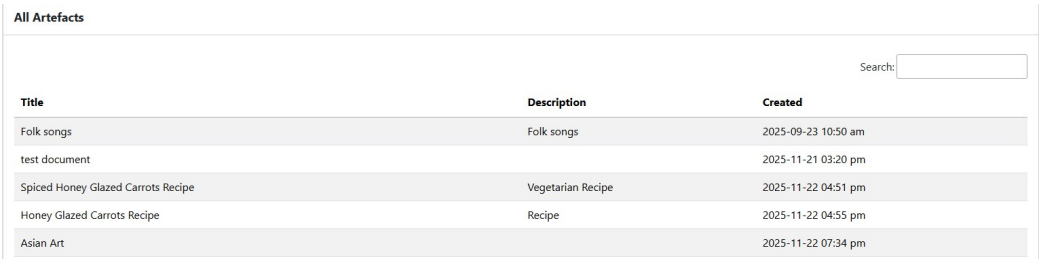


Figure D.46: All Artefacts Page

D.2.2 Requesting an Artefact

An individual or organisation that requires permission to use an artefact must first create an account in the artefact owner's application. They can then browse for artefacts by navigating to the *Artefacts* menu and selecting *Catalogue* (Figure D.47). There, they can search for an artefact using keywords. Once they locate the required artefact, they can click the *Request Artefact* button (arrow symbol) and the Artefact Credential Request page will then appear (Figure D.48).

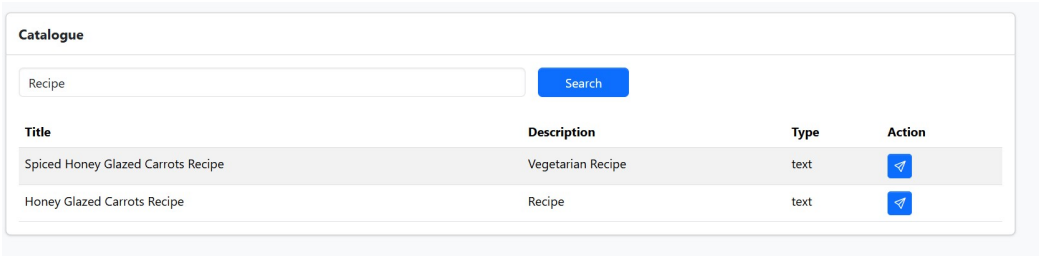


Figure D.47: Browser for the Artefact

On the *Artefact Credential Request* page (Figure D.48), the user must enter their DID and sign the nonce, as described in Section D.1.3, before clicking *Submit*. After submitting this information, if the nonce signature is valid, the Artefact Request Details page will be displayed (Figure D.49).

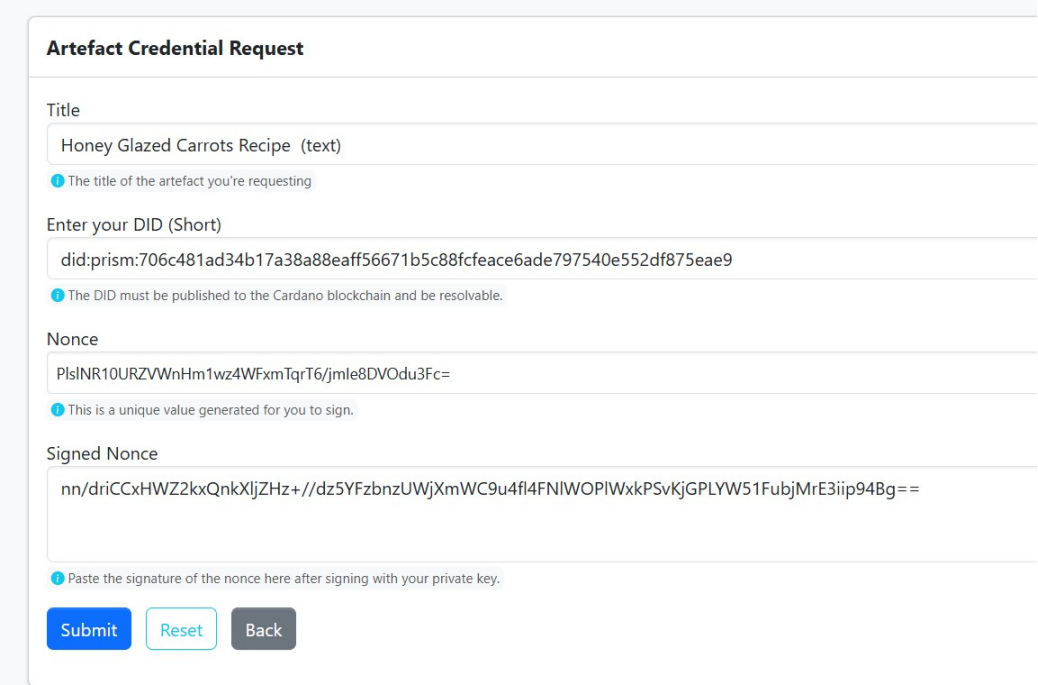


Figure D.48: Artefact Credential Request Page

On the Artefact Request Details page (Figure D.49), the user can enter details such as the duration for which they are requesting permission to use the artefact, as well as any other rights-related information. Once this form is completed, they can click *Submit*. The request will then be sent to the artefact owner.

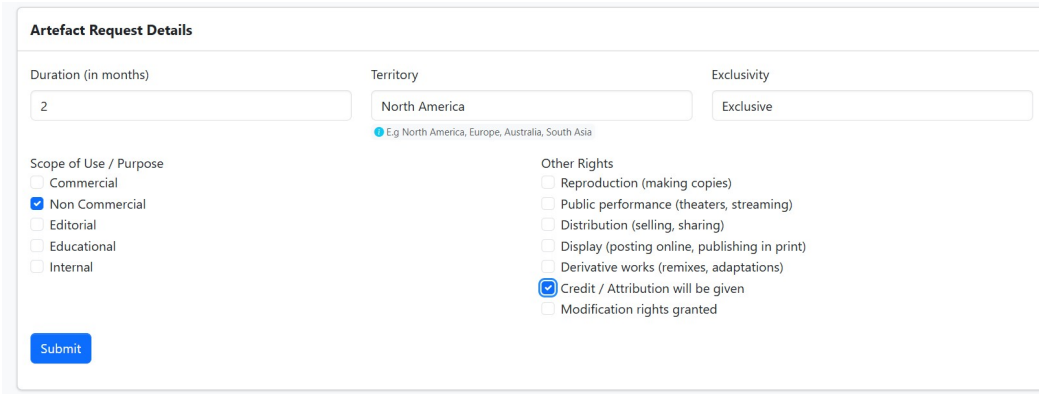


Figure D.49: Artefact Request Details

The user can view their credential requests under the *Artefact* menu by selecting *All Credential Requests*. On this page, the user will find a list of all the artefact requests they have submitted (Figure D.50). Each request is displayed along with its status, creation date, and most recent status update. They can view the full details of a request by clicking the *View* button (eye symbol) (Figure D.51).

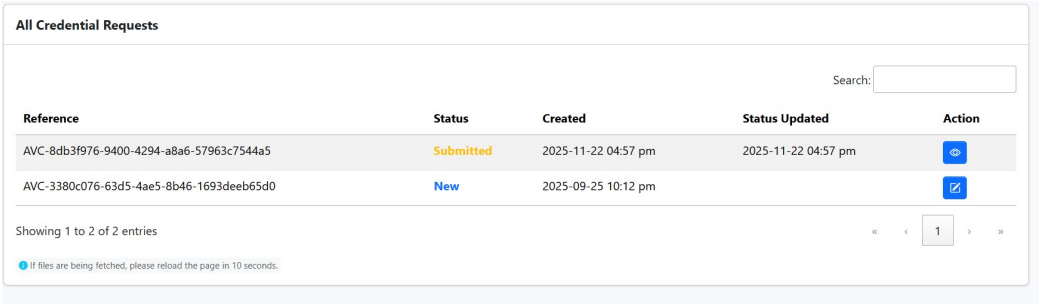


Figure D.50: All Credential Requests

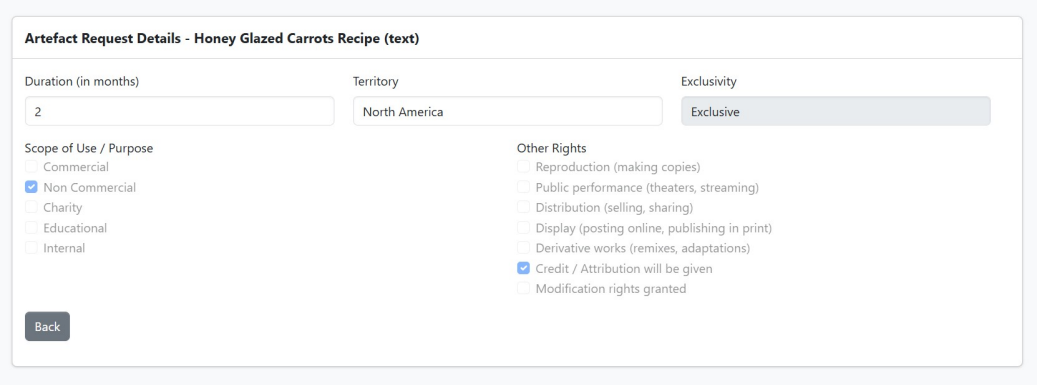


Figure D.51: View Artefact Request Details Page

D.2.3 Processing an Artefact Credential Request

The artefact owner can view credential requests by navigating to the *Credential Issuance* menu and selecting *Pending Credential Requests*. This will display all pending artefact requests (Figure D.52). The artefact owner can click Assign to me on a request to process it, then they will be able to see the requested rights for the artefact (Figure D.53).

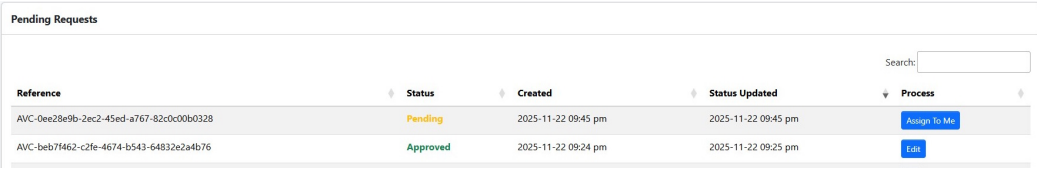


Figure D.52: Pending Requests Page

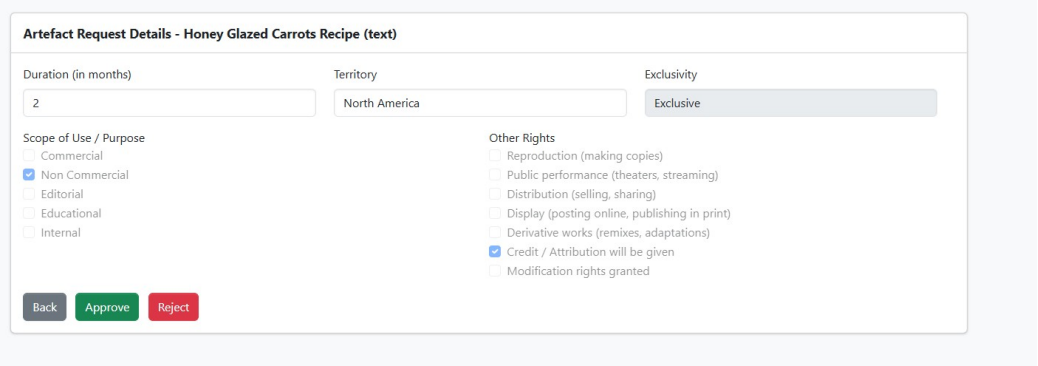


Figure D.53: Requested Rights

Based on the request details, the artefact owner can either reject the request by clicking the *Reject* button or approve it by clicking the *Approve* button.

If the artefact owner wishes to approve the request, they can click *Approve*. A confirmation message will then appear, prompting them to click *Yes* to confirm the issuance of the VC for the artefact (Figure D.54). Once confirmed, a VC offer invitation will be sent to the user who submitted the request.

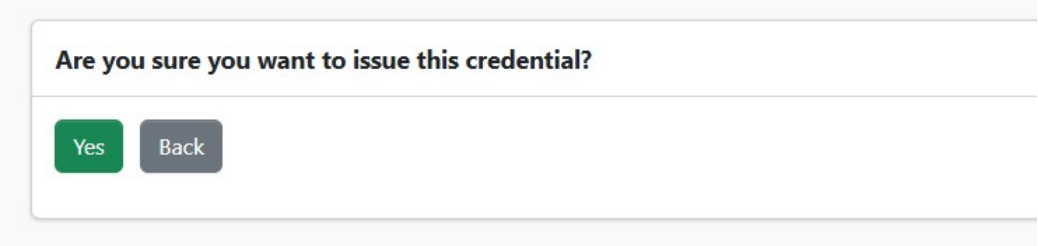


Figure D.54: Confirmation Message for Artefact VC Issuance

If the artefact owner chooses to reject the request, they can click the *Reject* button and they will be taken to a page where they can provide a reason for the rejection. This process is similar to rejecting a migrant's credential request, as described in Section D.1.4. Similarly, revoking an artefact VC follows the same procedure as revoking a migrant's credential, also explained in Section D.1.4.

D.2.4 Accepting a VC Invitation and Offer

Similar to how a migrant accepts their VC offer, the user will be notified upon logging into the artefact owner's application about the status of their artefact credential request. The user can then review their request by navigating to the *Artefact* menu and selecting *All Credential Requests* (Figure D.55).

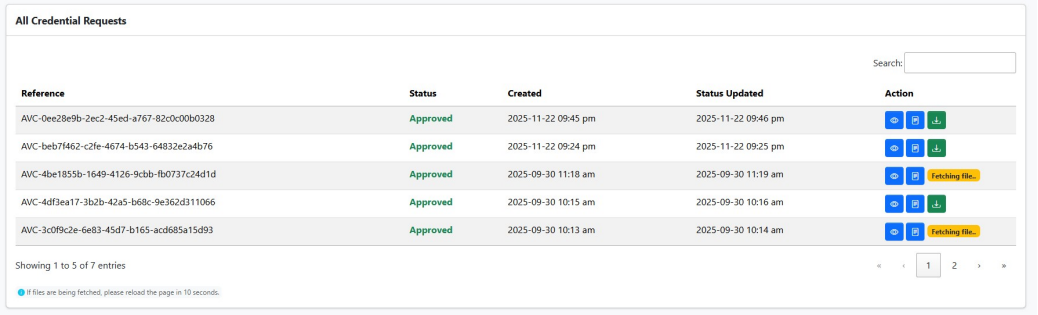


Figure D.55: All Credential Requests

If the VC invitation has been issued, a *Download* button (green download symbol) will appear next to the relevant credential request, allowing the user to download the requested artefact. If the file is not found on the server and must be retrieved from the IPFS network, a message indicating that the download is being fetched will be displayed. The user may then refresh the page after a short period to download the file once it becomes available.

The user can view the VC invitation offer by clicking the *Credential Request Information* button (file symbol). The remaining steps for accepting the VC invitation and the VC offer follow the same process as described for a migrant accepting a VC invitation and offer in Section D.1.5.

D.2.5 Creating an Artefact VC Presentation

Unlike the workflow for creating a presentation in a migrant's verification process, where the migrant can select which claims to include, the artefact presentation workflow does not allow the user to choose individual claims. All claims must be shared. The user can navigate to the *Credential Wallet* menu and, on the *All Verifiable Credentials* page, select the VC to share (Figure D.56). They can then click the *Create Presentation* button (file icon) to copy

the VC. On the list of VCs, artefact VCs can be identified either by the type **Artefact Usage** or by the reference prefix **AVC**.

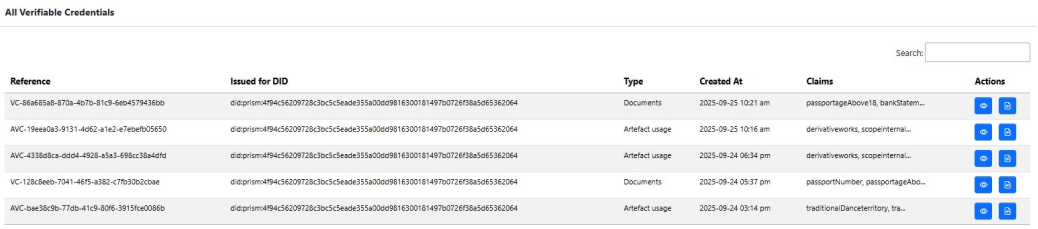


Figure D.56: Credential Wallet

D.2.6 Creating a Verification Request

The process for creating a verification request is similar to that described in Section D.1.7.

D.2.7 Processing a Verification Request

The process for processing a verification request is similar to that described in Section D.1.8.

Bibliography

[1] C. M. Schlebusch and M. Jakobsson. Tales of human migration, admixture, and selection in africa. *Annual Review of Genomics and Human Genetics*, 19:405–428, 2018. https://doi.org/10.1146/annurev-genom-083117-021759.

[2] International Organization for Migration. World migration report 2024, 2024. https://worldmigrationreport.iom.int/msite/wmr-2024-interactive/. Accessed: 2025-10-02.

[3] United Nations High Commissioner for Refugees. Global trends: Forced displacement in 2023, 2023. https://www.unhcr.org/global-trends-report-2023. Accessed: 2025-10-02.

[4] International Labour Organization. Ilo global estimates on international migrant workers: International migrants in the labour force. Technical report, International Labour Organization, 2024. https://researchrepository.ilo.org/esploro/outputs/report/995625051702676. Open access. Accessed: 2025-10-02.

[5] International Organization for Migration. International students trends, 2022. https://www.migrationdataportal.org/themes/international-students-trends. Accessed: 2025-10-02.

[6] Zhe Wang, Natalya Hanley, Joonghyun Kwak, Ilka Vari-Lavoisier, Mira Al Hussein, Lorena Sanchez Tyson, Ahmad Akkad, and Maia Chankseliani. How do international student returnees contribute to the development of their home countries? a systematic mapping and thematic synthesis. *International Journal of Educational Research*, 125:102330, 2024. https://www.sciencedirect.com/science/article/pii/S088303552400017X.

[7] United Nations. Universal declaration of human rights, n.d. https://www.un.org/en/about-us/universal-declaration-of-human-rights. Accessed: 2024-10-22.

[8] National Cyber Security Centre. Quarter four cyber security insights 2023, 2023. https://www.ncsc.govt.nz/insights-and-research/insights-reports/quarter-four-cyber-security-insights-2023/. Accessed: 2025-10-02.

[9] US Congress. H.r. 4943 – to promote the rights of migrant children and families, 2018. https://www.congress.gov/bill/115th-congress/house-bill/4943. Accessed: 2025-10-02.

[10] Z. Obermeyer, B. Powers, C. Vogeli, and S. Mullainathan. Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 366(6464):447–453, 2019. https://doi.org/10.1126/science.aax2342.

[11] J. Dastin. Insight: Amazon scraps secret ai recruiting tool that showed bias against women, 2018. https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG. Accessed: 2025-10-02.

[12] Royal Society Te Apārangi. Mana raraunga: Data sovereignty. Technical report, Royal Society Te Apārangi, Wellington, New Zealand, 2023. https://www.royalsociety.org.nz/assets/Mana-Raraunga-Data-Sovereignty-web-V1.pdf. Accessed: 2025-10-15.

[13] Alejandro Portes and Ruben G. Rumbaut. *Immigrant America: A Portrait (5th ed., Revised, Updated, and Expanded)*. University of California Press, Berkeley, CA, 2014.

[14] W. Omole. Impact of migration on identity formation: A study of second-generation immigrants. *International Journal of Humanity and Social Sciences*, 2(5):1–13, 2024. https://doi.org/10.47941/ijhss.1883.

[15] J. Staletovich. Famed snake trackers from india latest weapon in florida war on pythons, 2017. https://www.miamiherald.com/news/local/environment/article128233064.html. Accessed: 2025-10-15.

[16] BBC. The snake people of southern india, 2018. https://www.bbc.com/travel/article/20180918-the-snake-people-of-southern-india. Accessed: 2025-10-15.

[17] Ashifa Kassam. Louis vuitton accused of cultural appropriation of romanian blouse. The Guardian, 2024. https://www.theguardian.com/fashion/article/2024/jun/05/louis-vuitton-accused-of-cultural-appropriation-over-romanian-blouse. Accessed: 2025-10-02.

[18] Norbert Nemes. Inspiration or appropriation? a win for romania as louis vuitton pulls folk items from collection. Radio Free Europe/Radio Liberty, 2024. https://www.rferl.org/a/romania-folk-dress-credit-louis-vuitton-ia/33013244.html. Accessed: 2025-10-02.

[19] Stuart Haber and W. Scott Stornetta. How to time-stamp a digital document. *Journal of Cryptology*, 3(2):99–111, 1991. https://doi.org/10.1007/BF00196791.

[20] Dave Bayer, Stuart Haber, and W. Scott Stornetta. Improving the efficiency and reliability of digital time-stamping. In R. Capocelli, A. De Santis, and U. Vaccaro, editors, *Sequences II: Methods in Communication, Security and Computer Science*, pages 329–334. Springer, 1992. https://doi.org/10.1007/978-1-4613-9323-8_24.

[21] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. https://ssrn.com/abstract=3440802 or http://dx.doi.org/10.2139/ssrn.3440802. Accessed: 2025-10-16.

[22] Cardano. Relevant research papers, 2024. https://docs.cardano.org/about-cardano/explore-more/relevant-research-papers/. Accessed: 2025-10-16.

[23] Cardano Foundation and Crypto Carbon Ratings Institute (CCRI). Ccri & cardano release mica sustainability indicators, 2024. https://cardanofoundation.org/blog/ccri-cardano-release-mica-sustainability-indicators. Accessed: 2025-10-15.

[24] G. Sadlier, D. Dixon, M. Luczak-Roesch, M. Galster, and D. Eyers. National data infrastructure - blueprint for aotearoa new zealand. Technical

report, Open Access Te Herenga Waka – Victoria University of Wellington, 2024. https://doi.org/10.25455/wgtn.26132434. Accessed: 2026-01-04.

[25] Quinten Stokkink and Johan Pouwelse. Deployment of a blockchain-based self-sovereign identity. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1336–1342, 2018. https://doi.org/10.1109/Cybermatics_2018.2018.00230.

[26] Françoise Vasselin. Blockchain for migrants: Promoting self-sovereign identity and financial inclusion. *International Journal of Business Administration*, 15(4):39–52, 2024. https://doi.org/10.5430/ijba.v15n4p39.

[27] Sovrin Foundation. Mainnet ledger shutdown likely on or before march31,2025. https://sovrin.org/sovrin-foundation-mainnet-ledger-shutdown-likely-on-or-before-march-31-2025, 2025. https://sovrin.org/sovrin-foundation-mainnet-ledger-shutdown-likely-on-or-before-march-31-2025. Accessed: 2025-10-30.

[28] Rosa M. Garcia-Teruel and Héctor Simón-Moreno. The digital tokenization of property rights: A comparative perspective. *Computer Law & Security Review*, 41:105543, 2021. https://doi.org/10.1016/j.clsr.2021.105543.

[29] Denis Trček. Cultural heritage preservation by using blockchain technologies. *Heritage Science*, 10(1):6, 2022. https://doi.org/10.1186/s40494-021-00643-9.

[30] Cardano Foundation. 20.2.18 – cardano foundation and z/yen explore threat of quantum computing to blockchain security. https://forum.cardano.org/t/20-2-18-cardano-foundation-and-z-yen-explore-threat-of-quantum-computing-to-blockchain-security/8495, February 2018. Accessed: 2025-11-24.

[31] Michele Mosca and Marco Piani. Quantum threat timeline report 2024. Technical report, Global Risk Institute, December 2024. https://glob

alriskinstitute.org/publication/2024-quantum-threat-timeline-report/.

[32] Marcus White. Cyber attackers steal personal data from council, June 2025. https://www.bbc.com/news/articles/c2k1dyql37ko. Online; Accessed: 2025-06-25.

[33] Liv McMahon. Uk watchdog fines 23andme for 'profoundly damaging' data breach, June 2025. https://www.bbc.com/news/articles/c4grggw4n56o. Online; Accessed: 2025-06-25.

[34] International Organization for Migration. Migration factsheet 2: Migrants, 2020. https://www.iom.int/sites/g/files/tmzbdl2616/files/documents/migration_factsheet_2_migrants.pdf. Accessed: 2025-07-03.

[35] Federal constitution of the swiss confederation, article 13: Protection of privacy, 1999. https://www.fedlex.admin.ch/eli/cc/1999/404/en#art_13. Accessed: 2025-06-26.

[36] Proton Technologies AG. Why switzerland? an analysis of swiss privacy laws, 2014. https://proton.me/blog/switzerland. Blog post, Accessed: 2025-06-26.

[37] Proton Technologies AG. Proton mail security, 2023. https://proton.me/mail/security. Web page, Accessed: 2025-06-26.

[38] Proton Technologies AG. Proton drive security, 2023. https://proton.me/drive/security. Web page, Accessed: 2025-06-26.

[39] Irina Marcopol. Openpgpjs security audit, 2018. https://proton.me/blog/openpgpjs-protonmail-security-audit. Blog post, Accessed: 2025-06-26.

[40] VFS Global. About us. Online, 2025. https://www.vfsglobal.com/en/general/about.html. Accessed: 2025-11-04.

[41] Roberto A Pava-Díaz, Jesús Gil-Ruiz, and Danilo A López-Sarmiento. Self-sovereign identity on the blockchain: contextual analysis and quantification of ssi principles implementation. *Frontiers in Blockchain*, 7:1443362, 2024. https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2024.1443362/full.

[42] National Institute of Standards and Technology. Secure hash standard (shs). FIPS PUB 180-4, August 2015. Information Technology Laboratory. Available at http://dx.doi.org/10.6028/NIST.FIPS.180-4.

[43] Annie Badman and Matthew Kosinski. What is symmetric encryption?, August 2024. https://www.ibm.com/think/topics/symmetric-encryption. Accessed: 2025-10-20.

[44] Annie Badman and Matthew Kosinski. What is asymmetric encryption?, August 2024. https://www.ibm.com/think/topics/asymmetric-encryption. Accessed: 2025-10-20.

[45] National Institute of Standards and Technology. Digital signature standard (dss), February 2023. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf. Accessed: 2025-10-20.

[46] IOHK and Cardano Foundation. Cardano node documentation, 2025. https://docs.cardano.org/about-cardano/learn/cardano-node. Accessed: 2025-10-22.

[47] Cardano Foundation. Time in cardano. Cardano Documentation, n.d. https://docs.cardano.org/about-cardano/explore-more/time/. Accessed: 2025-11-05.

[48] IOHK / Cardano Foundation. Consensus and staking, 2025. https://developers.cardano.org/docs/operate-a-stake-pool/basics/consensus-staking/. Accessed: 2025-12-05.

[49] Edsko de Vries, Thomas Winant, and Duncan Coutts. The cardano consensus and storage layer. Technical report, IOHK, 2025. https://ouroboros-consensus.cardano.intersectmbo.org/pdfs/report.pdf. Accessed: 2025-08-30.

[50] IOHK and Cardano Foundation. Consensus explained, 2025. https://docs.cardano.org/about-cardano/learn/consensus-explained. Accessed: 2025-10-22.

[51] IOHK and Cardano Foundation. Ouroboros overview, 2025. https://docs.cardano.org/about-cardano/learn/ouroboros-overview. Accessed: 2025-10-22.

[52] IOHK and Cardano Foundation. Stake pools, 2025. https://docs.cardano.org/about-cardano/learn/stake-pools. Accessed: 2025-10-22.

[53] IOHK and Cardano Foundation. Smart contracts, 2025. https://developers.cardano.org/docs/smart-contracts/. Accessed: 2025-10-23.

[54] Vitalik Buterin. "i quite regret adopting the term 'smart contracts'. i should have called them something more boring and technical, perhaps 'persistent scripts'.". Twitter post, Oct 2018. https://x.com/VitalikButerin/status/1051160932699770882. Accessed: 2025-08-30.

[55] Ethereum Foundation. Introduction to smart contracts, 2025. https://ethereum.org/developers/docs/smart-contracts/. Accessed: 2025-10-28.

[56] Input Output Global (IOG). Extended utxo model – cardano docs. https://docs.cardano.org/about-cardano/learn/eutxo-explainer, 2025. Accessed: 2025-08-30.

[57] MDN contributors. W3c, 2025. https://developer.mozilla.org/en-US/docs/Glossary/W3C. Accessed: 2025-10-25.

[58] World Wide Web Consortium. About us, 2025. https://www.w3.org/about/. Accessed: 2025-10-23.

[59] Manu Sporny, Michael B. Jones, Dave Longley, Markus Sabadello, Drummond Reed, Orie Steele, and Christopher Allen. Decentralized identifiers (dids) v1.0: Core architecture, data model, and representations, July 2022. https://www.w3.org/TR/did-1.0/.

[60] Manu Sporny, Michael B. Jones, Dave Longley, Markus Sabadello, Drummond Reed, Orie Steele, and Christopher Allen. Controlled identifiers v1.0, May 2025. https://www.w3.org/TR/cid-1.0/.

[61] Manu Sporny, Dave Longley, David Chadwick, Ivan Herman, Gabe Cohen, and Michael B. Jones. Verifiable credentials data model 2.0, May 2025. https://www.w3.org/TR/vc-data-model/.

[62] J. Bradley M. Jones and N. Sakimura. Json web token (jwt), May 2015. https://www.rfc-editor.org/info/rfc7519.

[63] JWT.io. What is json web token structure?, 2025. https://www.jwt.io/introduction#what-is-json-web-token-structure. Accessed: 2025-10-23.

[64] Jones, M. and Bradley, J. and Sakimura, N. Json web signature (jws). RFC 7515 7515, Internet Engineering Task Force (IETF), 2015. https://www.ietf.org/rfc/rfc7515.html.

[65] Fett, D. and Bradley, J. and others. Selective disclosure for json web tokens (sd-jwt). Internet-Draft draft-ietf-oauth-selective-disclosure-jwt-22, Internet Engineering Task Force (IETF), 2025. https://datatracker.ietf.org/doc/html/draft-ietf-oauth-selective-disclosure-jwt-22.

[66] IPFS Docs. Ipfs documentation, 2025. https://docs.ipfs.tech/. Accessed: 2025-10-30.

[67] IPFS Docs. Nodes — ipfs docs, 2025. https://docs.ipfs.tech/concepts/nodes/. Accessed: 2025-10-30.

[68] Mozilla Developer Network. What is a url?, 2025. https://developer.mozilla.org/en-US/docs/Learn_web_development/Howto/Web_mechanics/What_is_a_URL. Accessed: 2025-10-30.

[69] Mozilla Developer Network. How browsers work, 2025. https://developer.mozilla.org/en-US/docs/Web/Performance/Guides/How_browsers_work. Accessed: 2025-10-30.

[70] IPFS Docs. The lifecycle of data in ipfs – content-addressing / merkleizing, 2025. https://docs.ipfs.tech/concepts/lifecycle/#_1-content-addressing-merkleizing. Accessed: 2025-10-30.

[71] IPFS Docs. The lifecycle of data in ipfs – providing, 2025. https://docs.ipfs.tech/concepts/lifecycle/#_2-providing. Accessed: 2025-10-30.

[72] IPFS Docs. Distributed hash tables (dhts) — ipfs docs, 2025. https://docs.ipfs.tech/concepts/dht/. Accessed: 2025-10-30.

[73] Intersect MBO. What is intersect?, 2025. https://www.intersectmbo.org/about-intersect. Accessed: 2025-10-22.

[74] Docker, Inc. What is docker?, 2025. https://docs.docker.com/get-started/docker-overview/. Accessed: 2025-11-04.

[75] Lley154. Atala prism setup, 2025. https://github.com/lley154/atala-prism-setup. Accessed: 2025-10-28.

[76] IPFS Docs. Ipfs and the problems it solves — ipfs docs, 2025. https://docs.ipfs.tech/concepts/ipfs-solves/. Accessed: 2025-10-30.

[77] Microsoft. Introduction to .net, 2024. https://learn.microsoft.com/en-us/dotnet/core/introduction. Accessed: 2025-10-31.

[78] Microsoft. What's new in the .net 8 runtime, 2024. https://learn.microsoft.com/en-us/dotnet/core/whats-new/dotnet-8/runtime. Accessed: 2025-10-31.

[79] Microsoft. .net open source project, 2025. https://github.com/dotnet. Accessed: 2025-10-31.

[80] Hyperledger Foundation. *Hyperledger Identus Agent API Documentation*, 2025. https://hyperledger-identus.github.io/docs/agent-api/. Accessed: 2025-08-30.

[81] Rick Anderson, Dave Brock, and Kirk Larkin. Introduction to razor pages in asp.net core. Microsoft Learn Documentation, n.d. https://learn.microsoft.com/en-us/aspnet/core/razor-pages/?view=aspnetcore-8.0&tabs=visual-studio. Accessed: 2025-11-05.

[82] Microsoft Corporation. Introduction to identity in asp.net core. Microsoft Learn Documentation, n.d. https://learn.microsoft.com/en-us/aspnet/core/security/authentication/identity?view=aspnetcore-8.0&tabs=visualstudio. Accessed: 2025-11-05.

[83] Microsoft. Entity framework core, 2025. https://learn.microsoft.com/en-us/ef/core/. Accessed: 2025-11-13.

[84] Microsoft. Value conversions in efcore, 2025. https://learn.microsoft.com/en-us/ef/core/modeling/value-conversions?tabs=data-annotations. Accessed: 2025-11-05.

[85] Microsoft. Introduction to data protection in asp.net core, 2025. https://learn.microsoft.com/en-us/aspnet/core/security/data-protection/introduction?view=aspnetcore-8.0. Accessed: 2025-11-05.

[86] Niels Provos and Peter Honeyman. Hide and seek: An introduction to steganography. *IEEE Security & Privacy*, 1(3):32–44, 2003. https://doi.org/10.1109/MSECP.2003.1203220.

[87] Brian W Kernighan and Dennis M Ritchie. *The C Programming Language*. Prentice Hall, Englewood Cliffs, NJ, 1988.

[88] European Union Blockchain Observatory Forum. Energy efficiency of blockchain technologies. Tech. Report 1.0, European Commission, September 2021. https://blockchain-observatory.ec.europa.eu/publications/energy-efficiency-blockchain-technologies_en. Accessed: 2025-10-23.

[89] Cardano Developers. Cardano wallet documentation, 2025. https://developers.cardano.org/docs/get-started/cardano-wallet/cardano-wallet/. Accessed: 2025-07-28.

[90] Microsoft. About windows subsystem for linux (wsl), 2025. https://learn.microsoft.com/en-us/windows/wsl/about. Accessed: 2025-07-28.

[91] Cardano Developers. Installing cardano node, 2025. https://developers.cardano.org/docs/operate-a-stake-pool/node-operations/installing-cardano-node/. Accessed: 2025-07-28.

[92] GHCup. Installation - ghcup, 2025. https://www.haskell.org/ghcup/install/. Accessed: 2025-08-28.