DRAFT V0.4, DECEMBER 2023

Verifiable Credentials
Proof of Concept Report: Age Verification

Te Tari Taiwhenua
Internal Affairs

Authors:
Tim Waldron
Senior User, Delivering the Future of Identity Services

Andrew Jones
Workstream Lead - Verifiable Credentials

Tim and Andrew are leading the work within DIA's Service Delivery and Operations Branch on how we can help customers get their information in a secure and safe manner, and share it in ways that are convenient and safe for them to do so.

The views in this report do not necessarily reflect those of the wider Department.

Please email VerifiableCredentials@dia.govt.nz if you are interested in providing feedback or interested in being involved in future work.

Special thanks to NEC (NZ) and SUSH Labs.

1 SUMMARY

With the passing of the Digital Identity Services Trust Framework Act 2023, The Digital Public Service branch of The Department of Internal Affairs are responsible for creating the rules and regulations (and the regulatory body), that would create a digital identity ecosystem within New Zealand.

From June to September 2023, Te Pou Manawa (a product innovation group within the Department of Internal Affairs) worked with NEC and SUSH Labs to evolve our understanding of this ecosystem and how it may operate in practical terms. This work, delivered under the auspices of the Delivering the Future of Identity Services (DFIS) programme looked to expand our understanding of Verifiable Credentials as a key component for the ecosystem.

Building on our previous exploratory work with digital wallets, we tested new concepts and explored how we could, in a technical manner, design and build a system based on our current understanding of the Trust Framework. We also wanted to prove that we were capable of issuing Verifiable Credentials based off information we held.

Our initial findings were presented to the DFIS Board on 14th October 2023, and are set out in this report. A Technical Discussion Whitepaper has also be published alongside this report

At a very high level, we achieved a greater understanding of the issuance and facilitation sides of the digital identity ecosystem. However, we still are still developing our understanding of the use of the information and it's lifecycle. We also expanded our understanding of the overall ecosystem, including exploring the various Trust Framework roles, determining how we can meet the rules, and demonstrating an end-to-end process in a decentralised manner.

Ko te pae tawhiti, whāia kia tata.
Ko te pae tata, whakamaua kia tīna.

CONTENTS

1	Summary	3
2	Background	4
3	Concept Outline	6
4	Project Findings	8
5	Future Work	12
6	Additional Reading	14

2 BACKGROUND

DIGITAL WALLET PROTOTYPE

In 2021, Te Pou Manawa, along with SUSH Labs and University of Auckland developed a prototype digital wallet system. It demonstrated how we could use Identity Check (then known as OTI or One Time Identity) to allow people to create a verified identity and store it in an app for sharing at a later point - in this case to enrol at university.

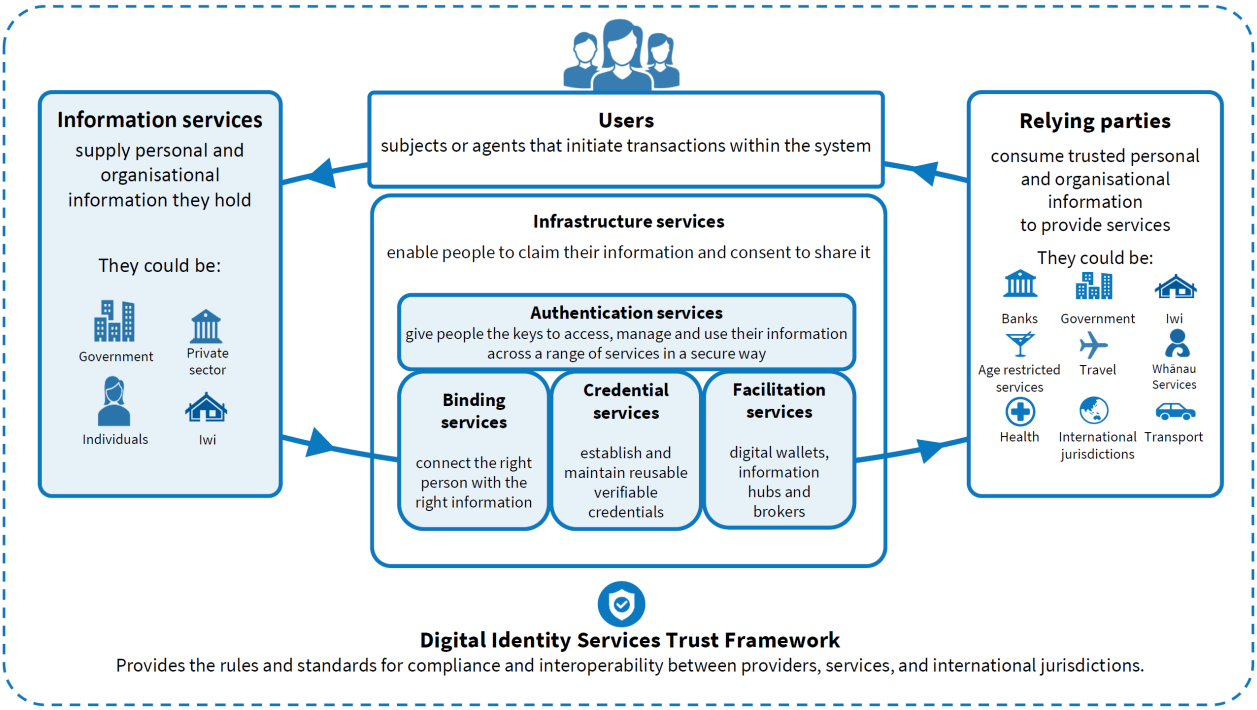
At the time, there was no legal framework to guide this, beyond using 'user consent' as the basis for all transactions. The model set up for the Digital Wallet system relied on a central information broker to do a lot of the heavy lifting, including authentication, credential issuance and facilitation of information between parties. It also required information sources and relying parties to integrate directly with it.

This work was halted due to impacts from Covid-19.

DIGITAL IDENTITY TRUST FRAMEWORK

Fast forward to early 2023, and the passing of the Digital Identity Trust Framework Act (the Act). This Act established a Regulatory Board and agency (and Te Ao Māori Advisory group) to govern how personal information can be managed within a digital identity ecosystem. The board would set the rules and regulations for the ecosystem, which will come into effect from 1 July 2024, with accreditation under the framework required on an opt-in basis.

Image A: The Proposed Digital Identity Services Trust Framework



The Trust Framework (Image A) effectively sets out five important roles that we need to investigate (those highlighted blue) - Information providers and the 4 types of infrastructure providers. While relying parties and users are not regulated as such, they are still an important part of any investigation into how we might work in this space.

For the avoidance of doubt - the ecosystem such that it is, already exists. People are currently providing their personal information to companies to get goods and services. However, the manner in which this happens is often suboptimal. It is ripe for the over sharing of information, and can lead to doubling up of work when a person provides information to the company that then requires it to be separately verified.

One of the keys to the digital identity ecosystem is the concept that someone can issue a verified credential for identity. DIA's Service delivery and Operations (SDO) branch is the kaitiaki of source records (such as the birth and citizenship registry). As such, we believe that SDO should be that issuance agency. As such, we are working hard to determine what SDO's role can and will be, and how we are best placed to influence and lead within the emergent regulated ecosystem.

WHITEPAPER

In December 2022, we published a technical white paper on a transition to verifiable credentials. This document described a strategic approach and transition path for issuing Verifiable Credentials. The purpose of the paper was to test the transition path and strategic approach with client organisations and service providers within the digital identity ecosystem.

We received feedback from a range of interested parties covering both the public and private sectors (and even some individuals).

PROOF OF CONCEPT

From our engagement regarding the whitepaper, we were able to identify gaps in our understanding of the system. As a next step, we decided to run a series of proof of concepts to further investigate the system, and increase our overall understanding in relation to verifiable credentials.

This document outlines the first proof of concept. For it, we engaged with NEC and SUSH Labs to run a Proof of Concept to test one of the most simple, yet common requests - proof a person is over 18.

3 CONCEPT OUTLINE

For this proof of concept, we determined that a commonly cited use case - proving your age (over 18) would be an ideal testing ground. This use case would likely be one of the first fleshed out, as there is a high demand for confidence in a person's age when they purchase age restricted products such as alcohol or tobacco, while the current system forces an overshare of unneeded information.

OBJECTIVES

- Test our ability to issue verifiable credentials to a digital wallet in a manner consistent with the draft trust framework rules.
- Test various roles and responsibilities under the framework.

PARTICIPANTS

- NEC New Zealand would provide the digital wallet, binding and authentication services.
- SUSH Labs would evolve the previous existing infrastructure towards the decentralised model proposed by the Trust Framework.
- DIA would provide coordination and architectural oversight for the work.

RESOURCING

- NEC, SUSH Labs and DIA provided all project resources.
- Work was run as four 2 week sprints around July/August.

IN SCOPE

- Using a wallet/holder app to:
  - Binding a user to the wallet, not the device.
  - Make requests for a credential from a provider.
- A credential issuance service that issues a credential for an 18+ proof of age that is bound to a person at a high level of confidence and meets the W3 Verifiable Credential standard.
- An examination of the security and privacy aspects of this system
- A roadmap of potential development for this concept.
- Engagement with Digital Identity New Zealand, for transparency reasons, and to gain their feedback on the work.

OUT OF SCOPE

- Proof of age credentials for other age points than 18 – (i.e., no 15+, 16+ or 65+ credentials).
- Credentials derived from documents without verification or signing from the source agency.
- Commercial models.
- Creation of regulations relating to this system.
- Anything to do with delegated powers (i.e. credentials for children).

SUCCESS CRITERIA

- Greater understanding of DIA's role as an information provider and issuer of verifiable credentials.
- Technical capability to issue credentials.
- Greater understanding of the infrastructure roles.
- Demonstrable prototype showing the full flow across roles defined in the digital identity ecosystem.

Note: The draft Trust Framework rules were not widely shared or published. As such, we have not provided a link to these in the additional reading. We worked off draft rules from around January 2023. While we have received indications that any changes will be relatively minor, the rules are still under consultation.

NOTES ON PROJECT EVOLUTION

The original intent was to use an NEC provided wallet. However, the prototype wallet developed as part of that previous work was sufficient, with some updates, to meet the criteria, including the biometric binding of the user to the wallet.

When deciding the specific credentials to issue, we decided to use biographic details (name, date of birth, place of birth, gender), photo and 18+ credentials in a one-attribute per credential format. This allowed us to further explore the concept of 'selective disclosure'.

We performed a privacy impact assessment threshold check and determined that a full impact assessment was unnecessary. As this work was exploratory in nature, it was not connected to any databases of personal information. Test records (including photos of project members used with their consent) were created as needed. For similar reasons, a security assessment was not completed.

4 PROJECT FINDINGS

The following provides an overview of key learnings from the Proof of Concept. These learnings were developed in retrospective sessions with SUSH Labs and NEC. Each item is rated on a maturity scale. On this scale, a 9 implies we are production ready and could perform this role within the next 6 months. A 1 implies we know very little, and would be 18 months or more away from being ready in this space. A 5 would imply that we are generally well versed in this area, but still need to do more work before we would be ready to provide this as a service.

GENERAL FINDINGS

General Maturity

- The design as set out in the Transition to Verifiable Credentials white paper has provided a good foundation for developing a working proof of concept. The approach of detailing this has provided much benefit, rather than going straight to some form of proof of concept.
- Building from existing work, and the use of an experienced Digital Identity Architect provided a solid base for this work, allowing much faster progress.
- The process of a customer claiming a verifiable credential (from the Department) and sharing it into a third-party wallet (provided by SUSH Labs and NEC) then sharing it with a relying party is technically possible. This was the primary goal of the Proof of Concept and this has been achieved.

BINDING SERVICES

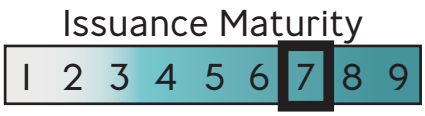
Binding Maturity

Biometric binding, both to a customer's identity record and the digital wallet, is necessary to ensure trust. There are options around how this can be done. Clarity around our approach to this will be important, particularly if this is an expectation/standard required by accredited digital wallet providers. Additionally, while not tested, binding at the time of sharing may also be required for certain attributes.

Binding within the digital wallet itself potentially provides a more robust security approach and greater portability than device-based biometric authentication (such as an iPhone's FaceID). It also supplies greater transparency. Binding service providers often are assessed against the NIST framework and publish their results. Typically, device-based services do not.

This is an area that requires more testing and monitoring of direction of other jurisdictions. For example, in Australia, binding services are meant to be able to report on the rates of false or fraudulent identities, accuracy and other relevant stats.

CREDENTIAL ISSUANCE

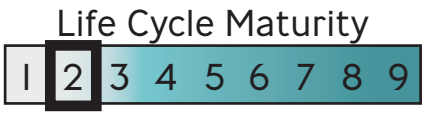


The capabilities provided by Identity Check (liveness/FR matching and biographic matching) are critical capabilities required if the Department seeks to transition to the issuance of Verifiable Credentials. Doing this well is central to any transition towards supporting the issuance of Verifiable Credentials. Furthermore, we need to ensure that there is a common standard being used across the ecosystem to ensure that interoperability and portability of credentials.

This PoC has shown that the issuance of a verifiable credential can be achieved using OpenID Connect to provide a messaging protocol, and the expected W3C Verifiable Credential (v1.1) standard. As DIA is currently a leader in this space, we must be ready to provide advice and support to enable other agencies to issue credentials based on their own information.

Note: DIA does not intend to become a credential issuer on behalf of others. We would aim to be able to issue credentials from our own information and services. For example, we could using Identity Check to issue an identity credential based on a passport or driver license, but would not seek to issue a Driver License credential via the NZTA driver license API.

CREDENTIAL LIFE CYCLE (USE AND MANAGEMENT)



Demonstrating 'selective disclosure', through age verification has been a valuable undertaking. How this is most efficiently supported is important to understand, as much of the promise around Verifiable Credentials is supporting sharing the minimum amount of personal information required to support a particular use case.

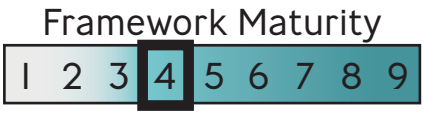
We decided to manage selective disclosure by issuing credentials with only a single piece of information. This allowed a very granular approach to relying parties requesting just what they needed (e.g. photo and '18+ credentials). This approach may be superseded soon, as there are indications that V2 of the verifiable credential standard will enable selective disclosure of parts of credentials chosen by the user, without needing to resign the credential.

More work required with relying parties to manage the transition from a possible over-supply of personal information to that which is specifically required for that use case. For example - at liquor stores, they often have to enter a full date of birth before their system allows the sale. More work will be required around this to ensure the Department designs it's credential issuance to meet relying party needs.

The life cycle of a credential is relatively complex. There will be requirements for service, such as status of credential, that will need to be understood and factored into our future design. Further exploration around this will be required to understand what can operationally be supported.

As with the previous work completed, management of the credentials was not primary focus. For example - due to the limited nature of a PoC, we did not need tools to enable us to manage a credential's status. Development of these tools will be required to enable the proper management of credentials from a customer and business viewpoint.

TRUST FRAMEWORK RULES



We examined a January 2023 draft version of the Trust Framework rules at a high level. We have assessed that around 70% of the rules were clearly met by the PoC, or could be met with small changes. Of the remaining rules, around half fell outside the scope of what we were testing (e.g. interoperability and credential management). This left around 15% that we were unable to meet with this current design. These results carried through when compared to the ecosystem roles tested within the PoC.

Examining the rules did raise some questions. Generally these were not related to the service itself, but to how the company is run. For example - for a large international company - would the whole entity need accreditation, or just the New Zealand branch? What is required to prove certain things, such as risk assessments being completed? How do you show you have people performing specified roles such as a privacy officer or someone responsible for managing security risks?

In April 2024, DIA's Digital Public Service branch are planing to publish the rules publicly for consultation. We also expect more information regarding the accreditation process to be published at about the same time. We expect at that time to conduct a similar exercise regarding the rules for future iterations of this work. We also expect to undertake a trial accreditation to test the process and determine how much such a process would cost.

TECHNICAL DESIGN

One of the outputs from this work is a technical discussion white paper, which evolved from the simple architecture documents drafted for the PoC. In it, we outline what design decisions were made for this concept and why. We also describe a very high level ecosystem design, and try to articulate the capabilities that we expect are required for a functioning digital identity ecosystem.

Image B: An example of the information held within a W3C Verifiable Presentation for proof of age (Over 18)

The capabilities we outline fall into three broad capabilities - the Issuer, the Holder App and the Verifier. The Issuer and Holder App cover the Digital Identity Services that would be regulated by the Trust Framework - the Information and Issuances services for the Issuer, and the Binding, Authentication and Facilitation services for the Holder.

As the white paper has been developed based purely on our findings, we will need to iterate and develop this document further. After internal review and feedback, we have made our first updates to the document. The Paper was published Dec 2023 and is available for comment and feedback.

Development of this artefact has also shown that while we have simulated a relying party in our tests, our next steps need to include a real relying party. It has also highlighted some aspects that facilitation providers will need to account for when looking at the system as a whole.

A copy of the white paper can be obtained by contacting us (see inside front cover for contact details).

5 FUTURE WORK

We are working on the next steps for this work. This section outlines what we expect those tasks to be, and have had general approval from the DFIS board to continue this work.

NEXT STEPS

When we published the first the white paper in Dec 2022, we had tacit approval to seek out 2-3 proof of concepts. The Proof of Age concept was the first, we the intent that the other two flow based on that. We are now confident we know what the next will need to be.

Essentially, the two areas that are least understood are the life cycle of the credentials, and the relying parties. To address this, we need to further evolve the technical work done so far to move beyond the closed system with just SUSH Labs and NEC, and instead open up our prototype credential issuance service for use by other parties. Towards this end there are three major steps.

1. Publish the Technical Discussion White paper for feedback
2. Consolidate all engagement/commercial work with feedback on the white paper, and build a technical sandbox that reflects our technical design
3. Run the sandbox for 3-6 months to gauge the effectiveness of the design, and make any changes required along the way.

1 - TECHNICAL DISCUSSION WHITEPAPER

The technical whitepaper based on the PoC architecture was published in December 2023 (See 'Section 6 - Additional Reading' for a copy). The intended audience is split between those we engaged for the original white paper at a policy/strategic level, and the technical staff that would be tasked with delivery of any such capabilities within their agencies.

We will actively seek feedback from those we engage with on the details as we iterate towards an design that works for all parties. We expect that the feedback will help inform and drive engagement with the sandbox once up and running. We are also directly engaging with interested parties in person or virtually to gather additional feedback.

When this is complete, we will have a shared understanding of how and where we fit within the ecosystem created by the Trust Framework, and how this all fits within our business context, and the wider ecosystem.

2 - CONSOLIDATION OF WORK

So far, we have done technical work with a small group of partners. However, separately, we have been engaging progressing exploratory work within the market. Separate discussions have been had with over 40 interested parties, from relying parties, to AML/CFT vendors, identity intermediaries, banks, public agencies and more.

These agencies and more are the audience for the technical whitepaper, and we will work to get those who are interested into the sandbox.

This part of the project would also see the inclusion of internal pieces of work around accreditation under the framework, engagement with Māori, legal, policy, privacy, security and risk. These would cover off a range of tasks and would feed into any business case that may be needed for future work.

3 - SANDBOX EVOLUTION

This technical PoC would have us evolving the work done to date and expanding who have worked with. There would be three major parts to this work.

- A gap analysis to determine what parts of the system we haven't built, and the development to fill those gaps and create the sandbox.
- Inviting select groups into the sandbox and get their feedback on how the system works and if we have built things correctly.
- A wider engagement with any interested parties. In particular we would want to engage facilitation providers and relying parties.

When this PoC in complete, we should be in a strong position to carry this work forward towards a productionalised service where we can supply the market with high quality, trusted verified credentials.

The sandbox will be available for 3 months. There is also potential for the sandbox to be extended as a useful tool for engagement with future parties or as a testing ground for new use cases.

6 ADDITIONAL READING

The following documents provide additional information on the work conducted by Te Pou Manawa in this area.

VERIFIABLE CREDENTIALS DOCUMENTS

These documents have been published by Te Pou Manawa and document our thinking and exploration in the verifiable credential space.

This document lists the findings of the original MyWai project in 2021. It was intended for an internal audience, and listed next steps for the work. Ultimately, this work didn't move forward due to Covid-19.

Link: Digital Wallet Project Report

In late 2022, we published the following white paper to explore how we could transition into a state where we used verifiable credentials in the future. This version contains updates based on feedback received over the course of 2023.

Link: Transition to Verifiable Credentials Technical Whitepaper v2.1

In late 2023, we published the following white paper to create discussion around the technical design of the system. it sets out the capabilities that we believe the three major areas of the trust framework will need.

Link: Verifiable Credentials in Action Technical Whitepaper3.0

DIGITAL IDENTITY TRUST FRAMEWORK

The following link to websites published by the Digital Public Service branch of DIA. The explain the Digital Identity Programme and the work that has been conducted within that area.

Link: Digital Identity Programme
Link: Digital Identity Services Trust Framework

STANDARDS

The following are links to the various standard documents that are referenced in this document.

The identification management standards provide a set of rules to help organisations to apply bet practice to their systems.

Link: Identification Management Standards

The W3C Verifiable Credentials and Presentations standards are the currently favoured standard for packaging personal information ins verifiable manner.

Link: https://www.w3.org/TR/vc-data-model/ (Recommended version)
Link: https://www.w3.org/TR/vc-data-model-2.0/ (Working Draft)