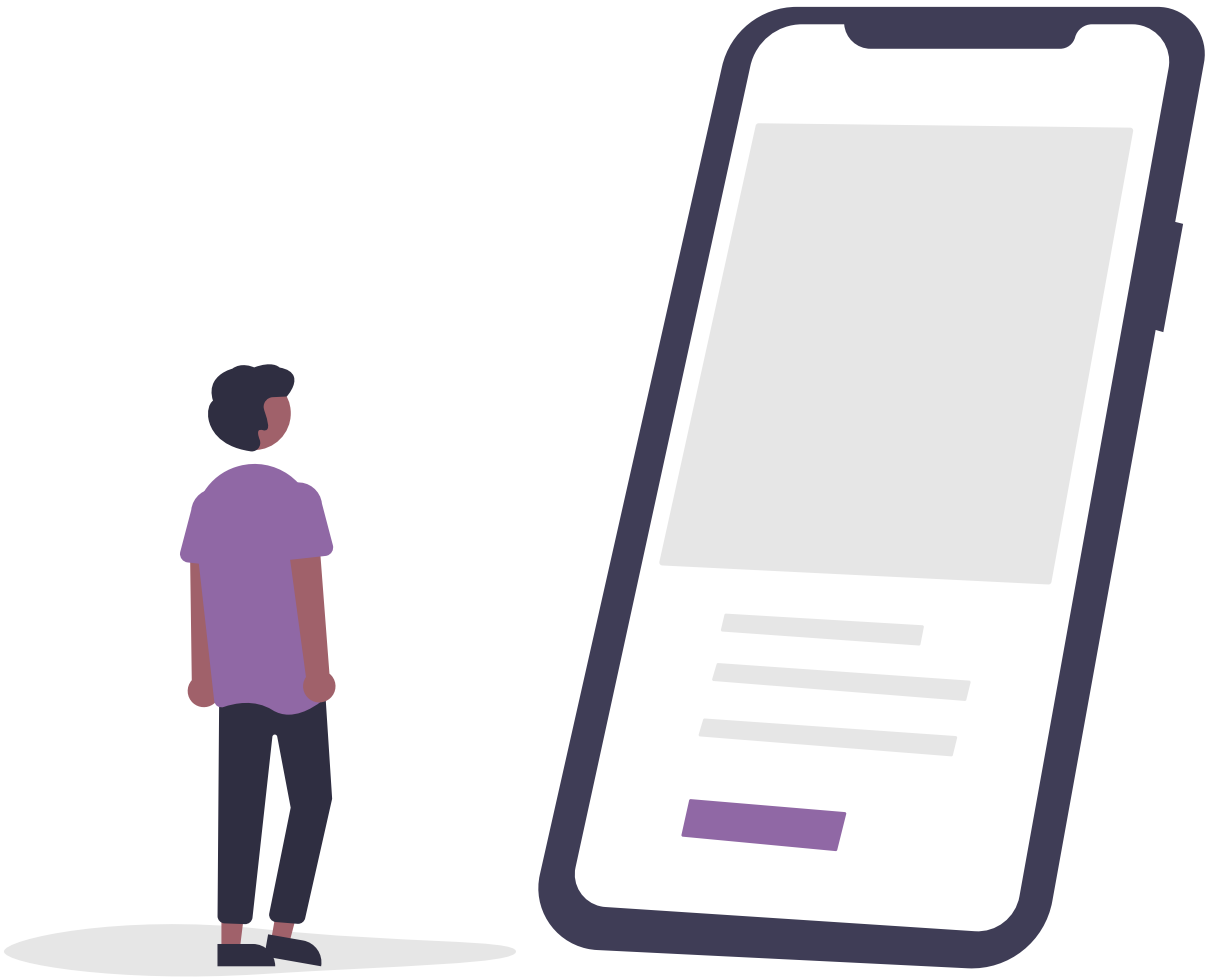
SEPTEMBER 25 V1.1

Verifiable Credentials **Sandbox 2024-25 Lessons Learnt**

Internal Affairs
Te Tari Taiwhenua



Contact us:

- Website: https://www.digitalidentity.dia.govt.nz/
- Email: verifiablecredentials@dia.govt.nz

1 SANDBOX 24-25

The Regulatory and Identity Services (RIS) branch of the Department of Internal Affairs (DIA) holds a wealth of information about New Zealanders. It is responsible for the registration of every birth, death and marriage in the country, managing the process for immigrants to gain New Zealand citizenship, issuing New Zealand Passports and other travel documents. It is also responsible for a suite of identity-related products including the RealMe Login, RealMe Verified Identity service, Identity Check and the Confirmation service.

We - the Product Innovation team within RIS - have a long-term view that identity products are moving in a digital-first direction, with a focus on being portable and privacy-respecting. We have been looking at how this will impact the services RIS currently delivers and how we will need to evolve what we offer moving forward. This report primarily looks at one of the workstreams we are running around our identity services – a Verifiable Credential Sandbox.

At a very high level, in a digital-first future, we want to enable our customers to be in control of their information. We want their information to be portable, to reduce oversharing of information, and allow them to share only what is needed and they consent too. Finally, we want to reduce the work others need to undertake to trust in the system. As such, we have been investigating the use of verifiable credentials as a key part of the suite of identity services RIS offers.

Verifiable credentials are a new technology in the identity space which are aligned with our goals. They are cryptographically secure, can hold a range of information, and can be provided to a customer's digital wallet to use as and where they see fit. They provide relying parties with the confidence to trust the information, and the ability to verify the data's integrity as needed.

Since 2019, we have completed a range of activities including prototypes and proof of concepts and reported on these via whitepapers. The current evolution of this work is the VC Sandbox. This test environment was set up in 2024 to:

- Test the issuance of credentials to third parties
- Test our ability to verify and bind credentials to people, and
- Explore the various uses cases for these within the 'digital identity ecosystem'.

When we conceived of the VC Sandbox, we decided to look beyond the purely technical side of credentials. In the grand scheme of things, if we are unable to build trust with agencies and users of our services and credentials, they will ultimately end in failure. As such, we took the opportunity presented by the sandbox to look outside of the Department towards a broad set of objectives.

TECHNICAL OBJECTIVES

- A practical idea of how to build a verifiable credentials issuance service within DIA.
- An understanding of how a verifiable credentials issuance model might work for the is-suing agency; the receiving organisations; and users/consumers.

These were chosen to expand on the technical knowledge that we already had. In our previous work, we had covered each of the roles as described by the Government Chief Digital Office (GCDO) as part of a digital identity ecosystem (see the Trust Framework websitefor more information about the work done by the GCDO, and the roles digital service providers can play). For this work, we wanted to get others involved. We also wanted to ensure that when there is a need for credentials, we will be ready.

ENGAGEMENT OBJECTIVES

- Insight into market demand for verifiable credentials and their potential role in the digi-tal economy.
- An understanding of how DIA could work with other government agencies to help them issue their own credentials over time, e.g. Tertiary Education sector qualifications and/or NZTA's driver's licence.

These objectives were chosen to increase our understanding of the wider ecosystem from a service delivery point of view. For the VC Sandbox, we engaged with agencies from the following sectors:

- Finance (Banks, Payments and FinTechs)
- Tertiary
- Government
- Farming
- Sale of Alcohol (and other restricted products)

Our previous findings have been shared publicly with representatives from over 100 agencies, and both formal and informal feedback has been sought. From that, we met with 64 agencies to learn more about their business and how they could use identity credentials. We walked through technical aspects of the VC Sandbox with 12 agencies, ran one end-to-end proof of concept, and are working on one pilot from this work.

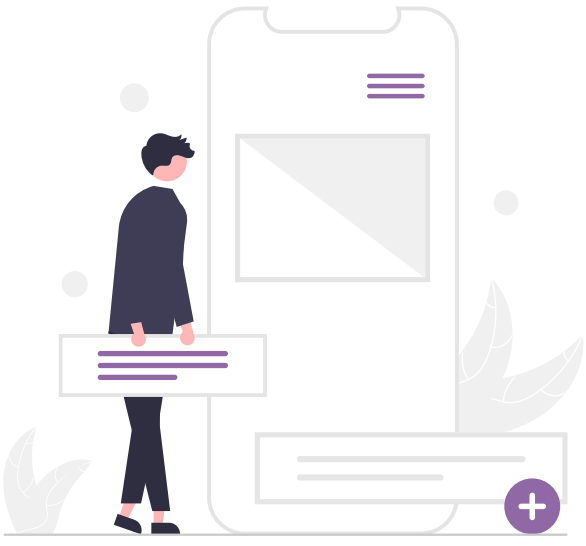
CUSTOMER OBJECTIVES

- Understand the social license and any other cultural implications of verifiable creden-tials.
- Understand the full end-to-end journey of a customer covering various parties (e.g. wal-let providers, getting and using credentials).

These objectives were chosen to build on our existing work in this customer space, such as Researching the Invisible Customer or Designing Proof of Identification That Works for Everyone, and to ensure that when RIS build systems, a holistic view is taken.

Overall, this report presents lessons for each objective and examines in detail what has been achieved for each. The report also states high level goals for the VC Sandbox over the 25/26 fiscal year.

It should also be noted that DIA is also the home of the Trust Framework Authority (TFA) – a regulator for digital identity services. While we work closely with the TFA, the TFA has a mandate to regulate the ecosystem that RIS would deliver services within. As such, this report should be read only from the service delivery perspective of RIS and may not reflect the views of the TFA.



2 KEY TAKEAWAYS

We have 10 key takeaways from the Sandbox in 2024/25.

1. RIS was able to successfully meet both technical objectives. RIS has a functioning sandbox and has proven it is technically feasible for DIA to issue a verifiable credential into a wallet, and have an external party verify and use the credential.
2. The sandbox shows it is possible for DIA to issue verifiable credentials in a safe, secure manner, and confirms the reliance on a digital wallet. It also has revealed that there will need to be additional service design work to be done, especially around accessibility.
3. There is a strong market demand for credentials that can be used transactionally (such as proving age), to show service eligibility (such as when enrolling in university), or to show ownership of assets (such as farm ownership or running a business).
4. There is demand for government issued identity credentials as they tend to attract higher levels of trust from the public than those provided commercially.
5. DIA better understands the role that DIA-issued credentials can fit within New Zealand's digital economy. For example – in the payments sector, there is a clear need for digital age verification for the purchase of age-restricted products.
6. DIA is clearer about how other government credentials, such as immigration status, will be needed over time, but also how more stakeholder engagement and testing will be needed.
7. New Zealanders are interested in using verifiable credentials though they want to better understand the technology and how it works, and how it keeps them safe.
8. The customer journey for issuing and receiving verifiable credentials is now clearer and government's understanding of how to make the service accessible for users who have disabilities.
9. Readiness of the sector to consume and/or use verifiable credentials varies greatly across industries and individual organisations, which is likely to have an impact on the uptake of verifiable credentials.
10. Testing verifiable credentials needed to work outside the sandbox. To do so, the "VC for Students" workstream was created to work with MyMahi to test the issuance of verifiable credentials to school students (16+) to assist them as they leave school and start to navigate the world as an adult.

3 DEFINITIONS

The following are terms/names used throughout this document.

- **Attributes** (Inc. Core Identity Attributes, Derived Attributes):

  An Attribute is a single piece of information about a person, such as their first name, age, date of birth or other information. Core identity attributes are a set that includes full name, date of birth and a photo.

  A derived attribute is one where a value is calculated based off another attribute – e.g. "Over 65" is derived from a person's date of birth.

- **MyMahi (**See www.mymahi.com):

  A private sector agency who provide services to students that extend a schools student management services.

- **Identity Check**: (See Identity Check for more)

  A service provided by RIS that enables an agency to confirm their customers identity online in real time against their passport or driver licence. for more information on how this service works.

- **Regulatory and Identity Services** (RIS, formerly Service Delivery and Operations/SDO):

  RIS is a branch of the Department of Internal Affairs. The branch has two main functions - the delivery of Identity Services including Identity Check, RealMe login and RealMe Verified Identity, Passports, Births and Marriages etc., and the delivery of Regulatory services in areas such as anti-money laundering (AML), gambling, racing and digital safety.

- **Trust Framework Authority, Trust Framework Board** (TFA, TFB):

  A pair of regulatory bodies established by the Digital Identity Services Trust Framework Act 2023, and run out of the Government Chief Digital Office in the Digital Services branch of DIA.

  The TFA is responsible for running an opt-in accreditation regime for digital identity services. The TFB is responsible for setting up the rules and regulations for the ecosystem.

- **Verifiable Credentials** (VCs):

  A verifiable credential is a generic term for a collection of attributes packaged up in a standard format. There are currently three main standards that can be considered as VCs. These are the W3C's VCDM, IETF's SD-JWT VCs and ISO's mDoc standard.

  At a high level, all three standards offer a tamperproof package of attributes that is bound to a person.

4 TECHNICAL LESSONS

TECHNICAL OBJECTIVES

The VC Sandbox has the following two technical objectives.

- **Objective A**: A practical idea of how to build a verifiable credentials issuance service within DIA.
- **Objective B:** An understanding of how a verifiable credentials issuance model might work for the issuing agency; the receiving organisations; and users/consumers.

OBJECTIVE A - CREDENTIAL ISSUANCE

Objective A covers the core technical work in the sandbox – issuance of credentials. There are two components required to do this – a service that can issue credentials, and a wallet to hold them. With these two capabilities we can demonstrate the end-to-end credential issuance process. In previous work, we built bespoke versions of both these components. For the sandbox, we wanted to move away from these bespoke builds towards open-source or out-of-the-box capabilities where possible. We chose the Walt.ID platform as it is an open source and has a range of capabilities that match what was required.

CREDENTIAL ISSUANCE SERVICE

The issuance service, at its core, is an orchestration service. It was designed to take requests from those who want a credential, such as a wallet provider, and undertake all activities required to get the requested credential back to the customer. This involved using Identity Check to confirm a person's identity, the creation of the credential, and returning it to the requestor.

The Issuance service has been set up to issue standards-based credentials. Prior to the sandbox, formats appropriate to the use case were included. When a wallet/user makes a request for a credential, they need to include what format they support. This will then be handled by the issuance service, returning an appropriately formatted credential.

The lessons here were primarily that credential issuance itself is relatively straight forward. Since we began work around VCs in 2019, we have moved from a fully bespoke, self-designed system to one that is based on open-source libraries and follows common protocols for the presentation and receipt of information. Globally, there has been a lot of work done on creating robust standards, such that now these capabilities can be easily accessed out of the box from a range of service offerings, rather than needing to be custom built.

In New Zealand, the difficulty in issuing credentials is therefore not the credential itself, but the parts of the service that wrap around the issuance. For example, the issuer needs to ensure that the information being issued is accurate, and that adequate assurance processes are used to identify and bind the holder to the information.

MYWAI - THE TEST WALLET

Prior to the sandbox, we had developed a test wallet called 'MyWai'. MyWai was designed to be a basic container for credentials in our early prototypes that could be reused later as required. As with the issuance service, it was originally a bespoke build as again, there were no readily available 'off the shelf' digital wallets tools.

With the Sandbox, MyWai was updated to use standard components provided by the Walt.ID platform. Currently, it provides a basic container to simulate binding to a person, request credentials from the Credential Issuance Service, and enable the sharing of these credentials.

For a credential-based system, the credential needs to be held or stored somewhere that is in the user's control. This rework of MyWai was initiated after our attempts to find a NZ-based wallet provider who was ready to work were unsuccessful. However, as RIS does not have a mandate to create a wallet, nor is seeking one. We will continue to look at what the market is delivering in the space, such as sector specific wallets, or a government services wallet.

UNTESTED CAPABILITIES

When building the sandbox, we determined that some capabilities should be investigated at a later stage. For example, while revocation is an essential capability, it didn't make sense for a sandbox implementation. Likewise, while the fully offline sharing of a credential (such as via NFC, or Bluetooth) does have some utility, RIS will primarily an issuer, which would be done online. Any offline sharing should be managed by the wallet and will therefore is a problem to be addressed outside of this work.

Some capabilities were excluded that will be provided externally to RIS such as a simulated Trust Register. We recognised these as essential to a functioning ecosystem, however they are not essential to a sandbox.

OBJECTIVE B: UNDERSTAND THE VC SYSTEM

In December 2023, we published a technical whitepaper "Verifiable Credentials in Action". A range of agencies provided feedback on the document, with the majority supporting the general direction. The biggest ask though, was that they wanted to see it in action. As such, we opened the sandbox capabilities to external agencies, both public and private.

We engaged with a range of agencies and started to understand how our credentials could fit into the wider digital identity ecosystem. Numerous examples were provided where proof of age would be beneficial, with many wanting a simple "18+" or "16+" proof, rather than a full document. There were also plenty of more complex interactions. Two standout examples of these are:

- **Enrolling in Tertiary Education**

  When young adults leave school, many decide to enrol for further study. For tertiary enrolment they need to repeatedly provide their name, citizenship status, National Student Number, school results, address, contact details and more. Along with these, they need to provide proof of each of these things.

  On the flipside, tertiary education providers must then undertake checks to verify each document or piece of information, as well as determining other factors such as if the person qualifies as a domestic student.

  For potential students, being able to collect all the information they need once then quickly present it was by far preferable. For tertiary education providers they could trust VCs with minimal additional work.

- **Getting a consent to farm your land**

  Farmers need consent to farm on their land, and to borrow money if required. To get consent, the farmer must prove they own the farming business, they own the land, and who they are. Once they provide proof of these to a consenting body, there is a long wait while everything is verified. Being able to provide all this electronically in a VC format should speed up the consenting process considerably and enable the reuse of this information with banks when applying for loans.

The Sandbox has provided us with a good understanding of where DIA issued credentials can fit into the wider ecosystem. We acknowledge there are other agencies that can provide people with a digital identity, however our binding and matching should provide the gold-standard in levels of assurance required, as we can do biometric matching against source documents. We are also looking to evolve our existing capabilities to support credential issuance. Further, we are well placed to provide credentials to those who may be excluded from digital channels if they are

unable to obtain physical documents to base them of. (e.g. if a person is unable to pass a vision test or can never travel overseas).

WORLDLINE INTEGRATION

Over November and December 2024, we worked with Worldline – a payments processor who provides eftpos services to merchants all over the country. Together, we aimed to test the idea of proving your age at the time you make a payment. The typical use case is:

> *As a merchant, if I use eftpos terminals provided by Worldline, I should be able to get proof my customer is old enough to purchase my service or product. I should be able to attach this proof to my Point-of-Sale system such that I meet any regulations related to proof of age for my product or service.*

With a long list of age-restricted products or services in this country*, there is an opportunity to reduce friction for consumers, while enabling merchants to meet their regulatory obligations.

We provided Worldline with MyWai and test data so they could receive credentials. They tested the capability to add the ability into their payment terminals that would be able to accept these. This resulted in an eftpos terminal that could display a QR code that encapsulated a request (using the standard OpenID for Verifiable Presentations messaging standard), that a user could scan using MyWai, read the request and consent to sharing the information.

To progress this concept beyond a simple PoC, would require an update to regulations that outline what are acceptable forms of identity under the Sale of Liquor Regulations. Currently, it heavily relies on physical documents there is little appetite to start accepting credentials until this has been addressed. Work has been initiated to update these rules as part of a wider piece of work to improve alcohol regulation.

VC FOR STUDENTS PILOT

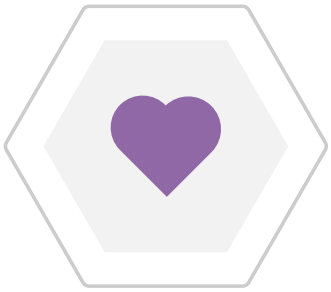
Our exploration into New Zealand based wallet providers introduced us to MyMahi - a New Zealand-based company that provide schools a platform to extend their student management services. MyMahi has a platform with wallet capabilities which they were using to hold credentials such as like loyalty cards. MyMahi had begun work with schools to issue a digital Student ID card. However, as there is no regulation around the issuance of

* including, and definitely not limited to voting, movies, tattoo, fireworks, firearms, pawnbrokers, ear-piercing, driving, child-fares/prices, energy drinks, alcohol, bulk fertiliser purchases, tobacco, adult magazines, gambling...

a student ID agencies were not willing to accept is as proof a person was a student or trust the info on it.

Outside the VC Sandbox, we have worked with MyMahi to develop a pilot credential for student use. This workstream is known as 'VC For Students'. In effect, we can add an additional step of assurance to their existing processes, using our Identity Check service, and can now offer a student an NZ Government verified eID credential. This credential contains name, date of birth and a photo that DIA has verified and credentialised and then given to the student for their use.

This work is expected to go live in late 2025 and has the potential to help students engage in the world in a digital manner. Initially, it will be limited to a small group of students, and we will expand on the pilot over time. Importantly, this work targets a cohort of people that often don't have other forms of official government ID that they can rely on.



MyMahi also offer their services internationally, and have been involved in trials for the Australian under-16 social media age restrictions. More information on this pilot can be found on our Digital Identity Services website.

ATTRIBUTES

When engaging with agencies and examining the use cases, people wanted a credential which has 'core identity attributes'. These are a full name, date of birth, and a confident match to an authoritative photo. We found broad support for a credential containing this information with a high level of assurance. This type of credential was often seen as pathway into a service, such as applying for finance.

During our engagements, we discussed the views on the acceptability of various documents, with a focus on what DIA provides. We received consistent feedback that many use cases would prefer something issued from an authorotative source specifically for the provision of identity. There is positive support for services such as the RealMe Verified Identity (often called the gold standard), and Identity Check Check (with agencies wanting a full rollout to consume the service in their binding processes). These services are seen as providing strong identity proofing processes in a unique space where it is easier for us to bind information to people. In many cases, it was preferable to have the government as the issuer.

We sought to understand the need for derived attributes. For example, when purchasing an age-restricted product a user could share an 'over 18' attribute derived from their date of birth, rather than the specific date. The agencies we engaged with were generally in support of this. However, some noted their existing systems would expect an exact date, so moving

towards a derived attribute would require additional change. This type of operational problem will need to be addressed by each agency as part of their journey to accept credentials.

To date, we have not examined what processes we would need to put in place to issue credentials based on other registers DIA holds. For example – there is an appetite for a citizenship credential, or a parent/child credential. Both these cases will require additional exploration to ensure that we are providing the appropriate verified information and that the user is bound to it.

CITIZENSHIP

A citizenship credential is valuable to the ecosystem. It is the basis of proof for people to work in New Zealand, or receive state-funded health care, among other uses. This credential would need to hold:

- If a person has New Zealand citizenship – likely a true/false value but could potentially also have status such as 'waiting for ceremony'.
- The type of citizenship - birth, grant or descent
- The date it was received or granted
- If citizenship has been renounced.

Each of the items listed here will require a further investigation to confirm if they will add value to the overall ecosystem. For example – the 'Renounced' status will likely always be 'false', though its presence removes any doubt about the citizenship. There is some debate about this credential being able to exist solely containing citizenship information, and if it would also need to replicate the identity information for the person it is bound to.

To issue a citizenship status credential, we would need to confidently bind a person to their record in one of three separate registers and confirm they have not renounced their citizenship (or otherwise lost it). Further investigation will be undertaken in the 25/26 fiscal year to understand how a citizenship credential should be constructed to meet the needs of relying parties and their use cases.

RELATIONSHIPS

Many agencies that provide services to children (or for their Many agencies that provide services to children (or for their benefit) wanted a credential of the connection between a parent and their child. Use cases included enrolling children in school or with doctors. There are also some use cases for younger people needing to prove a link to their parents, such as when signing up for Kiwisaver while aged 16-18. There is also

value in credentials that show a relationship between parties (such as married couples).

A relationship credential from DIA would likely need to hold:

- Something to identity the credential holder
- Something to match them to another identity
- The relationship between the two parties – Parent, Child, Sibling, Married, etc.
- A potential part of this service could be showing how one person can act on behalf of another. However, some sources of such authorisation (e.g. power of attorney or court order), cannot be verified by DIA alone.

While the establishment of a relationship may seem to be relatively simple on the face of it – i.e. if it is something that is recorded in records DIA holds – a large portion of the value in these credentials comes from showing the power to act on behalf of others.

When it comes to the parent-child relationship, it is not as simple as being listed on the birth record to prove guardianship. The Family Court can remove or add guardians externally to the birth registration process, and people not on the birth record can hold guardianship of a child. This area deserves deeper consideration, and we will look to what opportunities can be explored with relevant agencies over the 25/26 fiscal year.

Further to this, DIA is limited in the type of relationships it may be able to credentialise. For example, there is no database or established way to gain trust from an authoritative source for a 'power of attorney' type of arrangement. While this type of service has been suggested multiple times, it is outside the current scope of the services DIA provides. Potentially, the GCDO could establish a work program in this space.

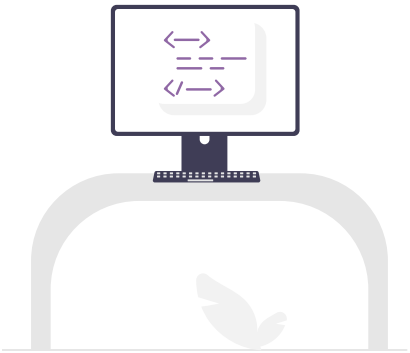
TRAVEL CREDENTIALS

The Department has been a strong advocate for the use of Digital Travel Credentials (DTCs). Since 2015, DIA has been heavily involved in the development of DTC standards with the International Civil Aviation Organisation (ICAO).

DIA will soon need to look towards the issuance of a DTC, even if just as a pilot. However, DTCs have significant differences from other credentials. For example – they aim to digitally replicate a full secure document with specific high-trust use cases.

CREDENTIAL FORMATS

When we began work on VCs, there were no standards published. There are now three major standards that are of interest.



VCDM (V1.1, V2.0) BY THE W3C CONSORTIUM.

This standard was designed to be a flexible and extensible, and used in decentralized identity systems. The W3C consortium has recommended for widespread adaptation. The standard is open and freely online (Verifiable Credentials Data Model v1.1, Verifiable Credentials Data Model v2.0).). The W3C also promotes its use to be royalty free and was the first of the major standards to be developed.

We used v1.1 in the Proof of Age PoC. While at the time, it was not fully developed in key areas such as selective disclosure, it is still available in the sandbox. The VCDM 2.0 has been published as of 15 May 2025.

SD-JWT VC BY THE INTERNET ENGINEERING TASK FORCE (IETF)

This standard was designed to have strong privacy-preserving features, such as how it handles selective disclosure. It has been developed by the IETF and is currently in a publication queue undergoing a final edit. It is an open standard freely available online (Selective Disclosure for JWT Verifiable Credentials).

This is the format that MyMahi have built their credential infrastructure around, and therefore the format used in the VC for Students Pilot. It is also available in the VC Sandbox.

mDL/mDoc BY ISO/IEC

The mDL (Mobile Driver License, ISO/IEC-18013, Mobile Document ISO/IEC-23220) format has risen to prominence over the last several years due to the key position that a driver licence holds in some parts of the world as proof of identity.

Its primary benefit is that it was designed with the ability to share in an offline manner as a core function (i.e. when pulled over where there is no cell coverage). The mDL standard was published by ISO between 2021 and 2025 and contained a technical description of mobile documents (mDoc) format.

The mDoc format has since been extracted into a separate standard - ISO/IEC-23220. This more generic standard is currently under development with the first two parts published in 2024/25. The

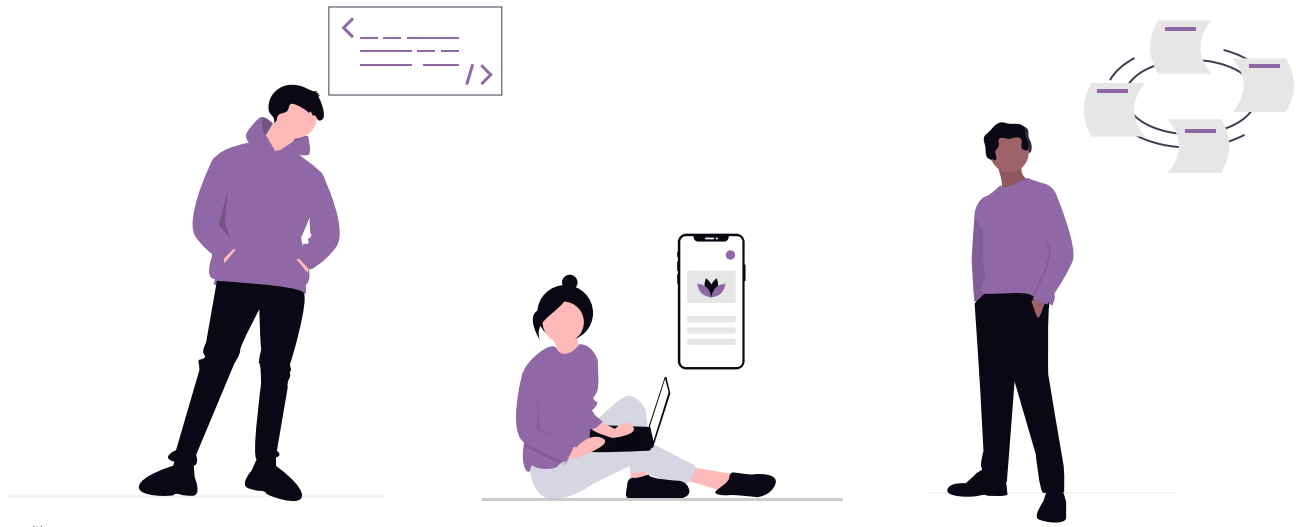
mDoc standard is looking to generalise various documents, including electronic IDs (eIDs) into the same underlying format.

In the 25/26 financial year, we will look to include mDocs as part of our sandbox capabilities.

These standards have risen to prominence separately, but all share at least the following three important things in common:

1. They all follow the same 'Issuer – Holder – Verifier' pattern of use. This means that they all strive to achieve the same outcomes, though in diverse ways.
2. The EUDI Reference Wallet/Architecture includes all three as primary standards for credentials (with updates on the road maps for when new versions are published). Support in the EUDI wallets indicates that they are seen as a viable credential format long term for widespread adoption.
3. The Open ID for Verifiable Presentation (OID4VPs) messaging standard has profiles for all three to ensure that no matter how the request is made, it can handle a response. All major wallet suppliers seem to be converging on using this standard for messaging.

In essence, the issuance platform DIA uses will need to be able to issue credentials in any of these three formats to ensure that it can issue to any wallet provider. However, currently the DISTF Rules only support mDL/mDoc and VCDM 1.1/2.0 for accreditation. The TFB has advised that SD-JWT VC will be included for comment and possible inclusion in the rules in a future round of consultation on the DISTF rules.



5 ENGAGEMENT LESSONS

The VC Sandbox had the following two Engagement objectives.

- **Objective C**: Insight into market demand for verifiable credentials and their potential role in the digital economy.
- **Objective D**: An understanding of how DIA could work with other government agencies to help them issue their own credentials over time, e.g. Tertiary Education sector quali-fications and/or NZTA's driver's licence.

During the Sandbox, we have engaged with around 60 New Zealand agencies to discuss a range of topics around VCs and determine if and how we could work together. We talked to a range of range of public and private entities who were the people who either hold information or would want to consume it.

We also completed some targeted engagement towards wallet providers, with this engagement leading to the VC for Students pilot noted prior.

OBJECTIVE C: MARKET DEMAND

There is a consensus that VCs are more than likely to be where information sharing is heading, though there is still a lot of discussion around what that means in practice. Using the sandbox as an educational tool was invaluable as many of the people and agencies we talked to were, by and large, still determining "where do I fit". Agencies were trying to decide if they are just a consumer or whether they need to be an issuer as well.

Overall, we found it is still an emerging market with varying levels of understanding. For some the tech problems were considered solved, and the questions were more focused around policy, while others were still very new to the concept. RIS is in the fortunate position that we started to look at VCs early and we have been able to share what we know and have learnt from others about their own journeys in this space.

During these discussions, the following topics and uses for VC were commonly identified.

USE OF VCS FOR ENROLMENT

Agencies can easily see themselves on the receiving side of VCs. They see clear benefits of being able to accept information digitally that they implicitly trust. They look at their processes that include applications or enrolment forms and can see how a verifiable package of data

containing exactly what they need, without needing to subsequently verify it, can save them time and money.

TRANSACTIONAL USE OF CREDENTIALS

There is a clear demand in some sectors for a safe and easy way to verify a person's information in a transactional manner. Their users do not want to sign up for an account, they just need proof of something when they need it. This type of transactional proof is often a burden that carries with it a lot of regulatory weight and cost to the agency, though from the customers viewpoint is over in seconds.

REGULATIONS

When it comes to the usage of credentials, many saw the potential that they can provide to help meet requirements set out in regulation, operational policy, legislation etc. However, this proved to be a double-edged sword. While agencies acknowledge they could trust a credential, if regulations do not allow their use, then even experimenting was generally out of scope. For example – agencies didn't want to lose their liquor licence if a credential wasn't listed as acceptable ID. Finance companies loved the idea, but until guidance on how to meet AML regulations include VCs, it is too big a risk to take. Overall, there is a clear need for regulators to review their rules regarding how information can be accepted. Fortunately, change has begun in both these areas with potential updates to the various regulatory instruments being considered.

ISSUANCE OF CREDENTIALS

It was less common for an agency to want to issue a credential, rather than just consuming them. Most of these were Public Service agencies who hold data about people (or entities) and want to make it easier for them to use it. Often, these discussions came alongside transformation projects where if felt like VCs would be a side thought for the work, if a valuable one. There were no agencies that were ready to issue credentials to our sandbox.

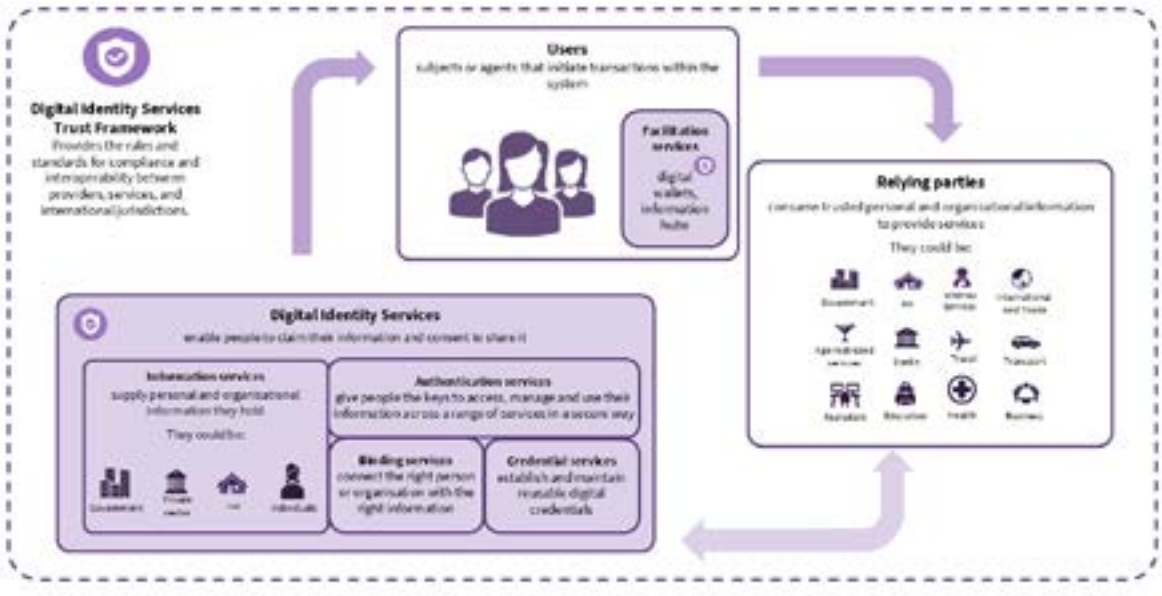
OBJECTIVE D: ECOSYSTEM BUILDING

As part of the sandbox, we set out to understand how we could help the development of the ecosystem mapped out by the DISTF (shown to the right), and if we could potentially offer capabilities to other government agencies.

This was a relatively new idea when we started the sandbox. In effect, we wanted to explore if the capabilities we had built could be leveraged by others too, and if we could use it as a tool to help take government from an emerging level of maturity to an aligned and unified approach.

Simultaneously, the TFB was undertaking similar engagement work, and came to a similar conclusion. Within the public sector, it would be wasteful for each agency to procure their own services for credential issuance, and that the government should provide a single issuance platform to all public sector agencies. This All of Government (AoG) issuance platform would help with the ecosystem's development and reduce the overall cost to the public. It would also reduce the work required for accreditation under the DISTF. It is important to note that the AoG issuance capability would focus solely on the credentialization of government information, and not the other tasks such as binding or information assurance.

We also assessed if we could create a 'Sandbox 2.0', extending the existing sandbox capabilities to other agencies. Ultimately, this idea was not progressed. RIS, like other public sector agencies, will be able to leverage capabilities provided by the GCDO in an AoG manner.



A map of the opt-in ecosystem as regulated by the Digital Identity Services Trust Framework, showing the relation between Identity services, Users and Relying Parties. The shaded boxes indicate services that can be accredited.

6 CUSTOMER LESSONS

The VC sandbox had the following two customer focused objectives.

- **Objective E**: Understand the social license and any other cultural implications of verifiable credentials.
- **Objective F**: Understand the full end-to-end journey of a customer covering various parties (e.g. wallet providers, getting and using credentials).

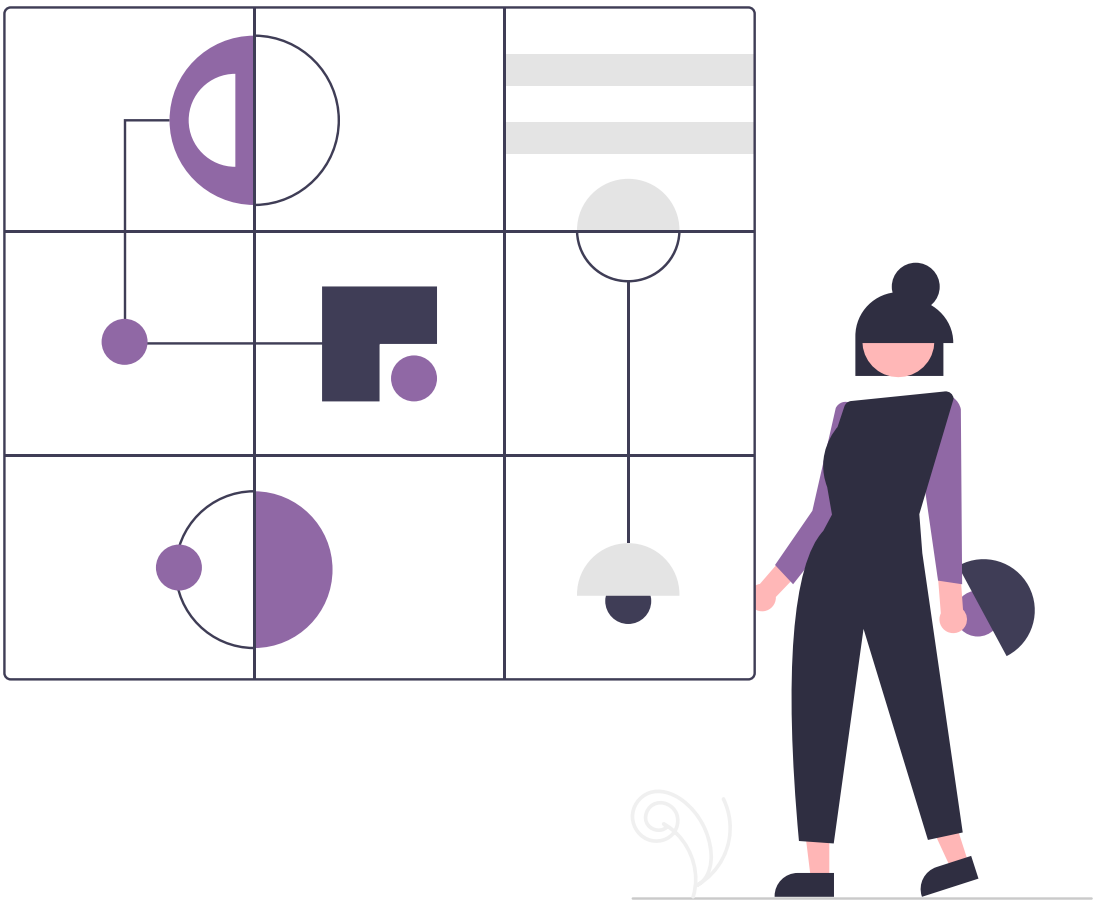
While the sandbox was running, we undertook a range of activities to explore these objectives. This included desk research, targeted interviews and surveys. The key findings are replicated below.

> *The full report into these activities is available here: Perceptions of Verifiable Credentials in Aotearoa*

Overall, if and how people use credentials will depend on a range of factors including practical need, personal comfort with technology and online services, and how useful or applicable it is in their everyday lives. In the research report, we have identified potential opportunities and challenges including:

- Technology and digital services are evolving, and people are evolving with them. Doing things online or digitally is becoming an expectation, with people looking to it for ease and convenience.
- New Zealanders have generally high trust in government and there is increasing interest in controlling their own information. For some though, this trust must be earned or is more on a 'need to' basis, to access the services they require.
- Proving identity via verifiable credentials has the potential to make it easier and faster through real-time information sharing, to make more services available fully online, and having identity documents on hand on a mobile device, ready to go.
- Digital exclusion impacts a large portion of society, ranging from access, trust, motivation and digital capability. Accessibility issues and the cost of mobile devices, internet connection and obtaining a NZ passport could present barriers to those already left behind.
- With increases in scams, privacy breaches, and the use of AI, people's behaviour is shifting. People are becoming more aware and more cautious of what they are doing online and with technology.

- We need to keep in mind how easy and practical verifiable credentials are perceived, especially when there are other readily available identity documents such as a physical Student ID or Kiwi Access Card, which will remain as easily presented options in person.
- The usability and accessibility of the end-to-end experience is crucial, especially for those that need more support.
- There is potential for the current perceptions of the RealMe service to impact on uptake of verifiable credentials as people have mixed views and experiences.
- Piloting verifiable credentials with a group where there can be several applicable situations e.g. students, may help increase uptake.



7 NEXT STEPS

Over the next year, we will progress our work with verifiable credentials as outlined in the following sections. In practical terms, this work will likely begin a shift over the next year towards being ready for a full service offering.

POLICY AND LEGISLATION

Throughout this work, it has become apparent that DIA will need to ensure there is a clear authorising environment for the issuance of credentials. This would likely take the form of new or amended legislation to include or enable VCs. Over the 2025/26 fiscal year, we will look to work with the Policy group (and others within DIA where appropriate) around how to correctly enable VCs.

Potentially, this could take the form of updated legislation that could be a broad enabler of services, while addressing issues and restrictions that currently exist within the Electronic Identity Verification Act 2012, Identity Information Confirmation Act 2013, and other Acts that DIA administers. A single enabling act could form a base for DIA to offer identity services over the next 20 years, and ensure any future services are included.

VC SANDBOX 2026

The VC sandbox will continue to be valuable to this work, with a range of items to test and capabilities to explore. These are likely to include:

- Examination of the mDoc credential format (ISO/IEC 23220), to ensure that RIS are prepared to issue credentials in this format in the future.
- Exploration of the issuance of a an eID based on a passport or RealMe Verified ID, or the issuance of a Digital Travel Credential.
- Investigation of how RIS could issue relationship, citizenship and other credentials based on data held by DIA.
- Creation of other test capabilities as needed, such as using the sandbox as testing environment for modern technologies.

CONTINUE PILOT WORK

During 2025, we had a successful PoC with Worldline regarding proof of age at time of payment and have launched a pilot for VCs for Students, which will run over the first half of 2026. We will also look to achieve a more generalised pilot for DIA-issued credentials, beyond just the student use case, utilising AoG capabilities where available.

While the sandbox will techinically available if an external provider wishes to integrate with it, these will be considered on a case-by-case basis.

SUPPORT AOG INITIATIVES

During 2025, several initiatives have begun in this space to cover the wider ecosystem led by the GCDO, with procurement processes underway or compelte. These include a government issuance platform, wallet and other central services. Over the next year, we will aim to align with and use the various initiatives:

- **AoG Issuance Platform:** When an AoG Issuance Platform becomes available, we will look towards utilising it for our issuance both in the sandbox and elsewhere as appropriate.
- **Govt.NZ/AoG Wallet:** Would look to issue credentials into the AoG wallet to provide a core DIA-issued identity credential (eID/electronic ID) that all New Zealand citizens would have access to.
- **Trust Service/NZ Verify:** We will look to utilise these tools once it is feasible to do so.

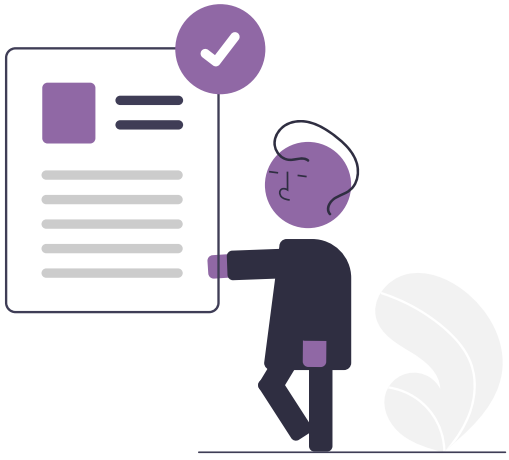
REGULATORY CHANGE WHERE NEEDED

The TFB undertakes a DISTF rules updates twice a year – in December and May. The GCDO also occasionally puts out consultation on the Identification Management Standards. We will participate these when announced, and provide input and commentaray on any changes.

We also will look to work with regulators for sectors where identity (or other information) needs a high level of assurance. In essence, we would like to inform them of the work completed and show the steps we have taken to ensure the credentials are of a high strength. We will also work proactively with regulators around the acceptance of VCs.

The primary sectors of interest are:

- Age verification
- AML/CFT and financial services.
- Tertiary study



8 FINAL WORD

On the technical front, we have met our objectives. The Worldline PoC, the VC For Students Pilot and engaging with external experts have led to a greater understanding of the technical requirements. We have obtained further clarity on what we need to do to issue credentials. We also have a clearer view of where to focus our efforts, such as a citizenship or relationship service.

Our engagement with interested parties has provided valuable insights into demand and readiness. We have a clearer understanding of what consuming agencies would like to see in a credential - government signed with a high level of assurance.

For our research into the social aspect of credentials, we have produced a comprehensive report outlining the benefits around the use of credentials. The interviews, surveys and other activities have provided valuable insights that can be carried forward as we complete activities like the VC for Students Pilot and work towards other pilots. We have a clear understanding of:

- what people want such as the credentials being free and easy to use.
- how they want to use them – many use cases were suggested.
- where some of the gaps are in our processes (e.g. some accessibility issues or education issues).

From the above insights, we can confidently move forward to ensure we can issue credentials that work for as wide a cross section of the New Zealand population as possible.

As a final statement, a highly trusted verifiable credential is essential to a functioning digital identity ecosystem. We are committed to providing all New Zealanders with an easy to access, high strength identity credential as part of the suite of identity products we offer, and to giving them the power back when it comes to interacting with the world in a digital manner.

We look forward to a seeing you in the VC Sandbox.

9 ACKNOWLEDGEMENTS

We would like to acknowldge and thank the following agencies who we have engaged with as part of the VC Sandbox 24/25 work.

- Accenture
- Ahau
- Air New Zealand
- SMLHub
- ANZ
- AplyID
- ASB
- Authsignal
- BNZ
- Canterbury University
- Centrix
- Cloudcheck
- CV Check
- Datacom
- Department of Internal Affairs
- Deloitte
- Entrust
- Financial Markets Authority
- Fintech NZ
- Foodstuffs
- Foodstuffs South Island
- Futureverse
- Hospitality NZ
- Horowhenua District Council
- ID Verse
- Immigration
- IRD
- Junctn
- Kiwibank
- Liqourland
- Mattr
- Ministry of Business, Innovation and Employment
- Ministry of Education
- Ministry of Health
- Ministry for Primary Industries
- Ministry of Social Development
- MyMahi
- NEC
- NZ Banking Association
- NZ Police
- NZ Post
- NZ Transport Agency
- NZTIER
- Otago University
- Payments NZ
- PWC
- Quid Est Veritas
- Reserve Bank of New Zealand
- Servian
- SeniorNet (Manawatū group)
- Simpon Grierson
- Spinika
- Super Liqour
- TAB
- Tasmon Liquor
- Te Pukenga
- Te Whatu Ora
- Trust Alliance
- VJMC Consulting/RegTech
- Whaikaha (Ministry of Disabled People)
- Westpac
- Woolworths/Countdown
- Worksafe
- Worldline