Te Tari Taiwhenua
Internal Affairs

Transition to Verifiable Credentials

Technical Whitepaper v2.1

We make it EASY, we make it WORK

Contents

Introduction

Document purpose

This paper articulates connections with the identity-focused work undertaken in other public and private sector agencies and how a DIA issued Verifiable Credential will be helpful to the Future State New Zealand digital identity ecosystem and its relationship to other agency's identifying attributes or credentials. The purpose of this document is to:

- Describe DIA strategic approach and transition path for issuing Verifiable Credentials for New Zealanders and issuing Verifiable Credentials for verified personal attributes such as passport details, citizenship status, and child relationships, which are held in DIA's registers.
- Test the transition path strategic approach with Client Organisations and Service Providers within digital identity ecosystem.
- Gather feedback from policy, security, privacy, legal and technical teams and identify gaps and any potential alternative options in the proposed transition approach.

It is essential to point out that the proposed transition approach articulated in this paper would follow existing "trust" framework conditions which we have articulated in the *RealMe Service Operating Framework section*. We are acutely aware that DIA holds identity taonga on behalf of New Zealanders and those who attain New Zealand Citizenship by the grant. In this context, we are sensitive to and mindful of the future Digital Identity Services Trust Framework (DISTF) to ensure, when this receives permission, we would align, where required, with any requirements to meet the accreditation criteria to operate lawfully within the DISTF.

Furthermore, the paper draws connections with identity-focused work undertaken in other public and private sector agencies and how a DIA issued Verifiable Credential will support the digital identity ecosystem and its relationship to other agency's identity attributes or credentials.

This version of the paper (v.2.1) has been updated reflecting feedback provided by stakeholders following between February and April 2023. It is noted that this document will continue to evolve as the Department refines its design and implementation approach.

Executive Summary

The Department of Internal Affairs (DIA):

- Can technically ***issue and operate Verifiable Credentials for existing RealMe Verified customers*** within the current ***RealMe Operational Framework*** and test the approach with client organisations and the market whilst the future Digital Identity Services Trust Framework requirements are developed.
- Plans to conduct further ***policy, security, and privacy assessments*** to explore and confirm the proposed approach.
- Will continue to to engage ***client organisations and the market providers*** to test the proposed approach for issuing Verifiable Credentials. DIA is keen to iterate the approach based on the feedback.
- Will be commencing work to identify and work with various entities and people representing ***Māori to identify***, understand and respond to elements of this future work programme that may have implications for Māori, particularly as this relates to identity (acknowledging identity as Taonga) and more frequent use of facial biometric verification technologies.
- Can implement an approach to leverage the existing RealMe customer base that can build a bridge between the current state identity operating environment and transition state Verifiable Credentials through the ***Credential Assertion Service*** to speed up the digital services' ***uptake of Verifiable Credentials***.

Background

DIA manages the RealMe platform, RealMe services have been recently migrated to the cloud platform to allow RealMe to be fit for the future. We are committed to meeting the needs of the New Zealand identity ecosystem, recognising our role and experience issuing and maintaining identity records.

DIA's future transition state is to support a **Future State New Zealand Identity Ecosystem** through Verifiable Credentials, enabling **Portability**, **Control** and **Choice** for the customer. DIA is in a unique position to issue Verifiable Credentials to support the New Zealand identity ecosystem and uptake of digital services by New Zealanders.

Glossary of terms

The following terms are used in this document:

Term	Detail
API	API is the acronym for Application Programming Interface, a software intermediary that allows two applications to transfer personal information.
Azure AD B2C	Azure Active Directory B2C (Azure AD B2C) is a customer identity access management (CIAM). It provides the primary platform that supports RealMe services.
Client Organisations	Client organisations are the existing clients of RealMe, or the receivers of the DIA issued Verifiable Credentials through Holder App.
Credential	A set of one or more claims related to the customer made by an issuer.
Credential Issuance Service	Credential service issues Verifiable Credentials to the holder app.
Credential Repository	A Credential Repository is a storage vault deployed on a personal device or cloud service that stores and protects access to the holder's Verifiable Credentials.
Customer	A member of the public or user who enrols with the Client Organisation services for applying for entitlements or creating an account. Note that the customers can be enterprise workforce to get Verifiable Credentials from the issuers.
DID	Decentralised Identifier, A DID is a simple text string consisting of three parts: 1) the DID URI scheme identifier, 2) the identifier for the DID method, and 3) the DID method-specific identifier.

Holder app	Holder app is an example credential repository. Holder app acts as an agent for the Holder that receives, stores, presents, and manages Credentials and key material of the customer. There is no single deployment model for a Holder app. Credentials and keys can be stored/managed locally by the customer or by using a remote self-hosted or third-party service.
EIC	Electronic Identity Credential (EIC) represents the verified identity information, including Full Name, Date of Birth, Place of Birth, Photo and Registered Sex.
Issuer	An issuer is a role an entity can perform by asserting claims about one or more subjects, creating a Verifiable Credential from these claims, and transmitting the Verifiable Credential to a holder.
Holder	A holder is a role an entity might perform by possessing one or more Verifiable Credentials and generating presentations from them. Holders store their credentials in credential repositories. The Holder app app is an example of holder app.
ODIC	OpenID Connect is an identity layer on top of the OAuth 2.0 protocol. It enables the relying parties or client organisations to verify the identity of the customer based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the customer in an interoperable and REST-like manner.
SAML	Security Assertion Markup Language is an open standard for exchanging authentication and authorization data between an identity provider and a service provider aka relying party or client organisation.
Verifier	A verifier is a role an entity performs by receiving one or more Verifiable Credentials, optionally inside a Verifiable Presentation for processing. Other specifications might refer to this entity as a relying party or OAuth client.
Verifiable Credential	A Verifiable Credential is a tamper-evident Credential that has authorship that can be cryptographically verified. Verifiable Credentials can be used to build Verifiable Presentations, which can also be cryptographically verified.

Verifiable Credential Lifecycle Management	The Verifiable Credential lifecycle involves changing the credential status based on changes to the verified identity record or a notification from the Holder app regarding any changes to the device authentication etc.
Verifiable Credential Status Check	This is one of the future capabilities proposed as part of this whitepaper. Verifiers query DIA's status check capability to confirm the status of Verifiable Credential that they have received from the Holder App.
Verifiable Data Registry	A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as Verifiable Credential schemas, revocation registries, issuer public keys, and so on, which might be required to use Verifiable Credentials. Example of verifiable data registries includes trusted databases, decentralized databases, government ID databases, and distributed ledgers. Often there is more than one type of verifiable data registry utilized in an ecosystem.
Verifiable Identity Credential	It is a Verifiable Identity Credential with a credential type as "Identity Credential" and verified identity information of an individual, which includes Full Name, Date of Birth, Place of Birth, Photo and Registered Sex.
Verifiable Presentation	A Verifiable Presentation is a tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. Certain types of Verifiable Presentations might contain data that is synthesized from, but do not contain, the original Verifiable Credentials.
Verified Identity Store	DIA's register for saving the verified identity record for the customers. The customer's verified identity record contains their full name, place of birth, date of birth, registered sex and verified photo, and links to the authenticator (s).

Table 1: Glossary of Terms

Strategic Business Context

Strategic Vision

To support **Aotearoa's** digital economy and ecosystem operation by issuing trusted, secure, high-confidence verifiable identity credentials to everyone who wants one.

Note: The above vision statement aligns with Aotearoa’s Digital Strategy vision statement.

Strategic Drivers, Goals, Outcomes

The future state New Zealand Identity Ecosystem enables customers to **Control** their identity and attributes information, **Choice** about when, how and to whom it is asserted as proof of identity and **the Portability** of those attributes and credentials for ease of use. DIA and Client organisations need to invest and develop capabilities to support the Future State New Zealand Identity Ecosystem.

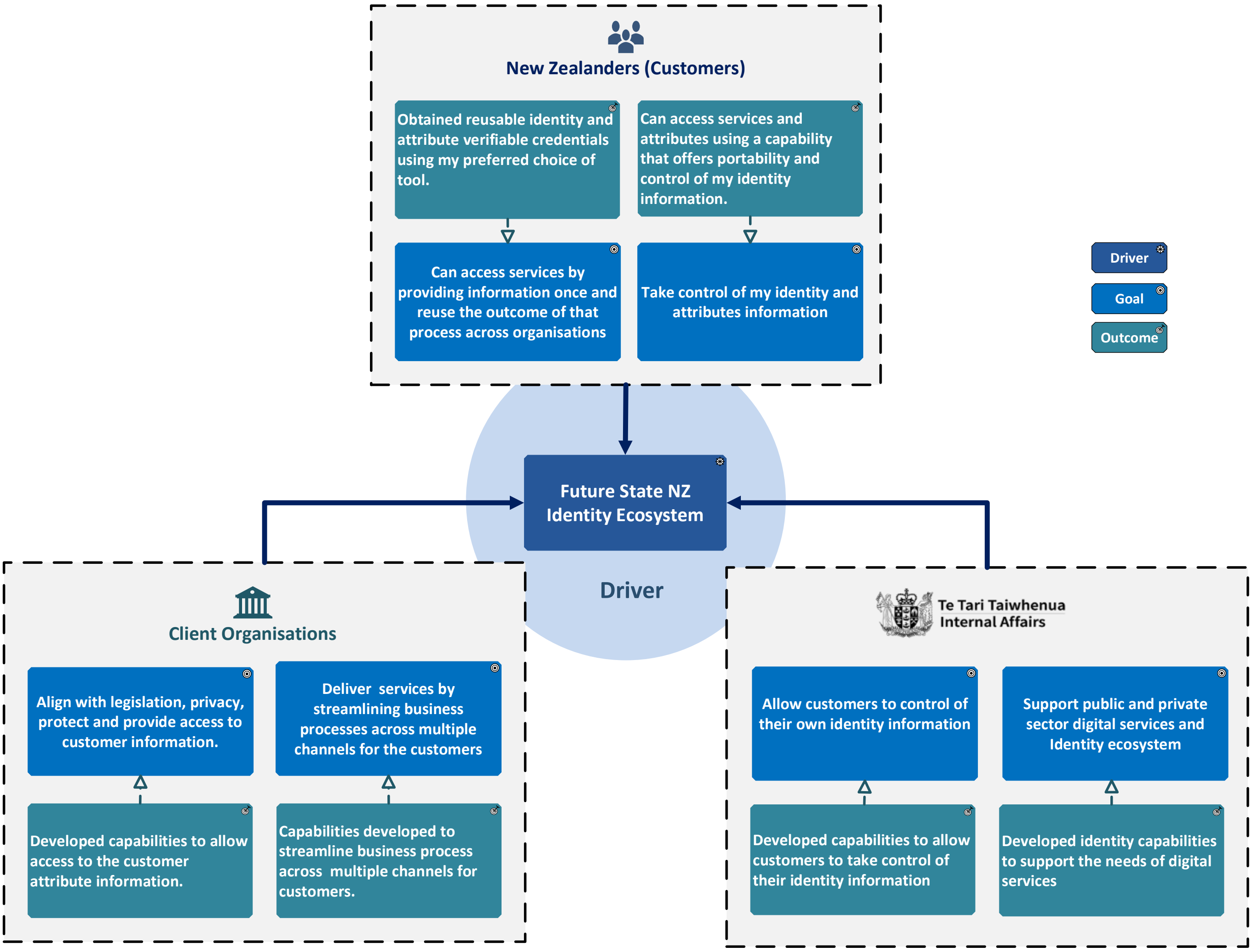
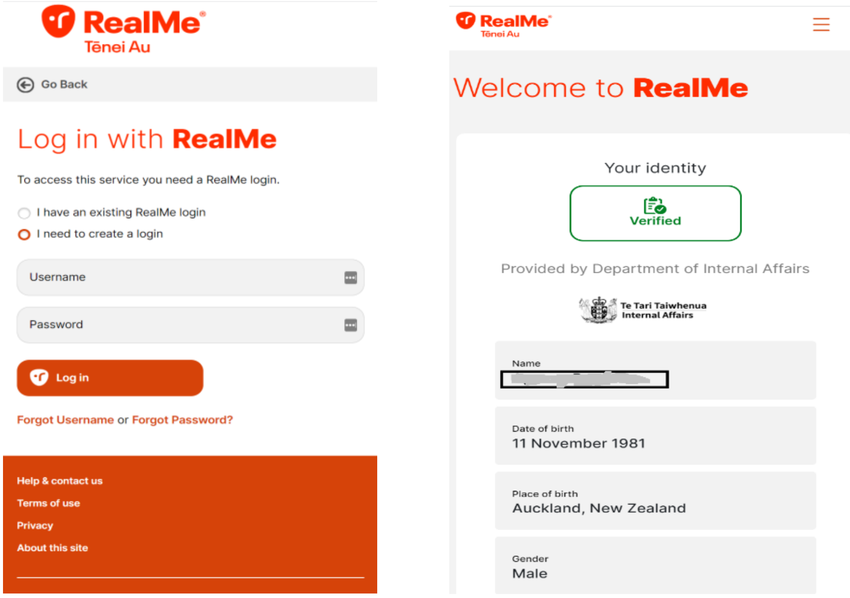

New Zealanders (Customers)
Obtained reusable identity and attribute verifiable credentials using my preferred choice of tool.
Can access services and attributes using a capability that offers portability and control of my identity information.
Can access services by providing information once and reuse the outcome of that process across organisations
Take control of my identity and attributes information
Driver
Goal
Outcome
Future State NZ Identity Ecosystem
Driver
Client Organisations
Align with legislation, privacy, protect and provide access to customer information.
Deliver services by streamlining business processes across multiple channels for the customers
Developed capabilities to allow access to the customer attribute information.
Capabilities developed to streamline business process across multiple channels for customers.
Te Tari Taiwhenua
Internal Affairs
Allow customers to control of their own identity information
Support public and private sector digital services and Identity ecosystem
Developed capabilities to allow customers to take control of their identity information
Developed identity capabilities to support the needs of digital services

Figure 1: Strategic Drivers, Goals and Outcomes Mapping

Current State

Overview



Log in with RealMe

To access this service you need a RealMe login.

○ I have an existing RealMe login
○ I need to create a login

Username

Password

Forgot Username or Forgot Password?

Welcome to RealMe

Your identity

Provided by Department of Internal Affairs

Name
[redacted]

Date of birth
11 November 1981

Place of birth
Auckland, New Zealand

Gender
Male

Figure 2: RealMe login and verified identity landing pages

DIA has recently migrated key RealMe account service onto Microsoft's Azure platform utilising Azure AD B2C and other Azure PaaS components. The RealMe account offers two agency interfaces:

- **RealMe login service**: the customer can use the **same login** to access various government agencies.
- **RealMe assertion service** is a facilitation service that allows the customer to consent to share their **RealMe verified identity** and **RealMe verified address** details with the participating government and private sector organisation's digital services to open a bank account, apply for a student loan, apply for NZ passports, renew driver's license etc. The RealMe assertion service can potentially allow sharing other verified information from verified sources.

RealMe Verified Identity

DIA is responsible for issuing RealMe verified identity to New Zealanders (including permanent residents and other visa holders) to confirm their identity to a high level of confidence business process, enabling easy access to public and private sector client services. DIA has issued more than one million RealMe verified identities. DIA's intent is to make the RealMe verified identity more portable, easily accessible to the customer, and capable of use in different contexts and services. This paper provides a transition pathway that has the potential to achieve the intent.

The current RealMe verified identity data is stored within DIA's secure environment. It is not a credential under the control of the citizen. A RealMe verified identity can only be asserted or used with a public or private sector agency that uses RealMe as its identity verification tool. RealMe identity credential is held by the government that is not available to the citizen to roam with, control or have a choice about where they present the credential.

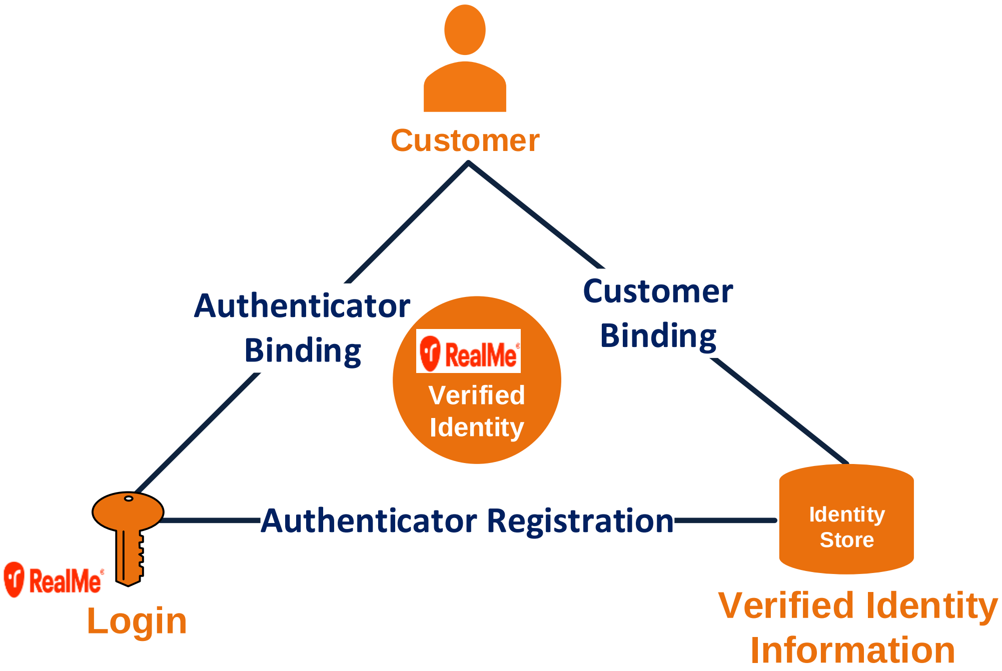


Figure 3: RealMe Verified Identity

This diagram represents the connection between the Customer, Authenticator (represented by a key) and Verified Identity Information (represented by the identity store).

The Customer and Verified Identity information relationship is marked as Customer binding. The Verified Identity Information and Authenticator relationship is marked as Authenticator Registration. The Authenticator and the Customer relationship is marked as Authenticator Binding. The triangulation of these entities represents the **RealMe verified identity**.

The following are the key points regarding the **RealMe verified identity**:

- The RealMe verified identity is known by its legislative term as an **Electronic Identity Credential (EIC).** The customers EIC (RealMe verified identity record) is stored in DIA's identity register.
- The customer is bound to the RealMe verified identity record through liveness, and biometric matching between a customer's facial live image and a source photo and DIA's verification of the RealMe verified identity application.
- The RealMe login (i.e. username, password, mobile based one-time password) is an authenticator method linked to the RealMe verified identity and bound to the customer.
- The RealMe verified identity is always accessed through RealMe and is not held in a persistent form on the customer's device.
- The customer consents to share their RealMe verified identity with the participating agency service through the RealMe assertion service.

RealMe Operational Framework

A Service Operational Framework is a common set of best practice standards-based rules that ensure minimum requirements are met for security, privacy, identification management and interoperability through accreditation and governance. The application of this framework enables the issuing of a trusted RealMe verified identity to the customers that meet legislative requirements and obligations under the Electronic Identity Verification Act 2012.

The RealMe Service Operational Framework was initially developed to guide the design and build of the service. The RealMe Service Operational Framework has been reviewed from time-to-time to ensure trust and confidence are maintained for New Zealanders to prove their identity online.

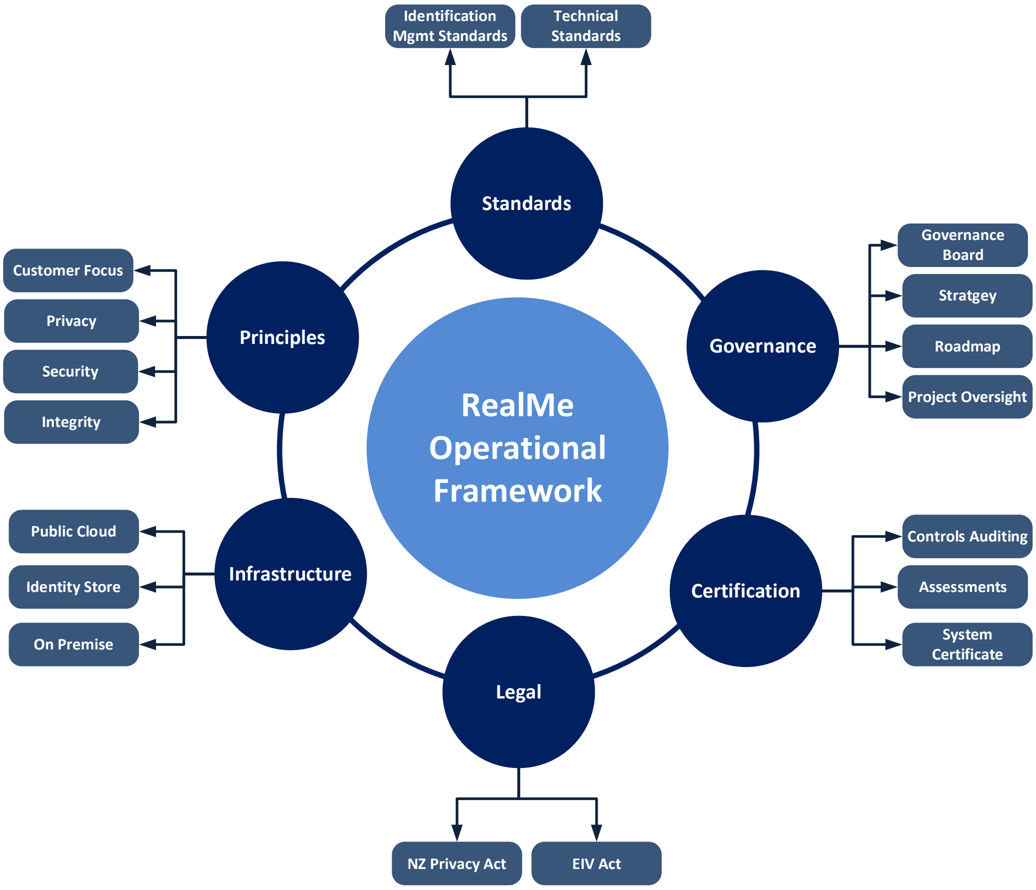


Figure 4: RealMe Operational Framework

Principles

The following key four principles are fundamental to the current RealMe architecture, and these principles constitute a primary reference for architectural governance to help projects deliver architecture consistently.

- **Security**: RealMe architecture aligns with NZISM and ensures that RealMe uses the best security standards, practices, and guidelines available to protect the security of information held and used. The security of the service is achieved by implementing many safeguards to protect the overall RealMe platform, services, data, and customers.
- **Privacy**: The RealMe solution complies with the Privacy Act 2020, considering the 13 information privacy principles at the core of the Act. These principles determine how organisations may collect, store, use and disclose personal information.
- **Customer Focus**: RealMe ensures the recommended solutions are convenient, easy to use and non-intrusive for New Zealanders. RealMe ensures that the proposed authentication approach is generally acceptable to potential customers, considering the different needs of people and emerging industry standards, and avoids creating barriers.
- **Integrity**: RealMe ensures transparency in action, demonstrates reliability and trustworthiness, and is committed to customers and client organisations.

Standards

The following standards are implemented in RealMe to provide a framework for achieving economies, efficiencies, and interoperability.

RealMe implements many of the controls listed in the following identification management standards:

- **Information Assurance Standard:** RealMe has specific information management controls to ensure the information collected is suitable for issuing a RealMe verified identity and determining a person's eligibility.
- **Binding Assurance Standard:** RealMe has implemented specific controls such as biometric matching, liveness, and back-office verification to ensure uniqueness i.e. a person cannot have more than one verified identity, the person is appropriately bound to their verified identity record and multifactor authenticator to prevent identity theft.
- **Authentication Assurance Standard**: RealMe ensures many of the controls listed by the Authentication Assurance standard to allow legitimate access to RealMe verified identity.
- **Federation Assurance Standard**: RealMe involves establishing and using a mechanism that can facilitate the presentation of one or more Credentials in response to a request from a client organisation through secured and privacy-protected communication using open federation standards (SAMLv2.0, OpenID Connect).

Technical standards promote interoperability and enhances technical and business trust with the agencies. RealMe complies with world-class authentication management solution tailored to the New Zealand environment, based on the OASIS SAML 2.0 and OpenID Foundation's Open Id Connect, New Zealand Government Web Standards, New Zealand Government API Standards and New Zealand Security Manual (NZISM).

Note that these standards reflect the current state, and RealMe will adopt new standards, as required, to support the transition path to Verifiable Credentials and alignment with Digital Identity Service Trust Framework Act in future. This legislation has recently been passed (Royal Assent on 05/04/2023) with an enactment date of 1 July 2024.

Legal

RealMe is governed by the Electronic Identity Verification (EIV) Act 2012. This includes verifying the validity of human identity before binding them to a digital credential. Relationships between the parties (including integrating clients) are governed in a way that provides legal certainty.

RealMe also complies with the principles of the New Zealand Privacy Act 2020. RealMe has been awarded the Privacy Trust Mark for its data minimisation design.

Infrastructure

RealMe infrastructure is a combination of public cloud and on-premises platforms. The NZ Government cloud adoption strategy directs services to use 'cloud first' where appropriate to drive faster development and reduce upfront and ongoing costs. DIA has recently migrated RealMe integration services onto a public cloud platform, and the high confidence RealMe verified identity store is hosted on the on-premise platform. DIA ensures that the hybrid RealMe infrastructure delivers trustworthy, affordable, quality, accessible and cost-effective RealMe services for the client organisations and the customers.

Certification

The RealMe platform is regularly monitored and audited, and all changes, enhancements, and controls are assessed through security and privacy auditing. A third-party security provider prepares system audit reports and issues a system security certificate based on assessment and remediation activities. DIA shares its updated security certificate with the integrated/ integrating client organisations to enable business trust in the RealMe solution.

Governance

DIA has defined policies governing the RealMe solution, which requires oversight, and enables, governance boards to make decisions concerning business trust, strategy, roadmap, investments, enhancements, improving operational efficiencies etc.

Potential Future State

DIA want customers to have **Control** over their identity information, **Choice** about when, how and to whom it is asserted as proof of identity and **the Portability** of those attributes and credentials for ease of use. DIA believe issuing these life data attributes is a fundamental anchor for the digital services ecosystem which then has the potential to enable customers to bind their identity attributes to other credentials they might want from other private and public sector agencies.

The Department needs to issue the authoritative Verifiable Credential for the customers with their core life data information (name, date of birth, place of birth, registered sex, and photo) to enable a customer-centric identity ecosystem, and the economy, to function productively and make customers' lives easier. Issuing Verifiable Credentials with identity information goes through a rigorous identity-proofing process, binding it to the customer's biometric information is a fundamental element of the issuance process.

This section describes:

- Key Roles involved in delivering Future State New Zealand identity ecosystem. DIA will be the Issuer of Verifiable Identity Credentials in the future state identity ecosystem.
- Customers getting their Verifiable Credential with verified identity claims from DIA.
- Customers getting other Verifiable Credentials
- Businesses and client organisations consuming Verifiable Credentials

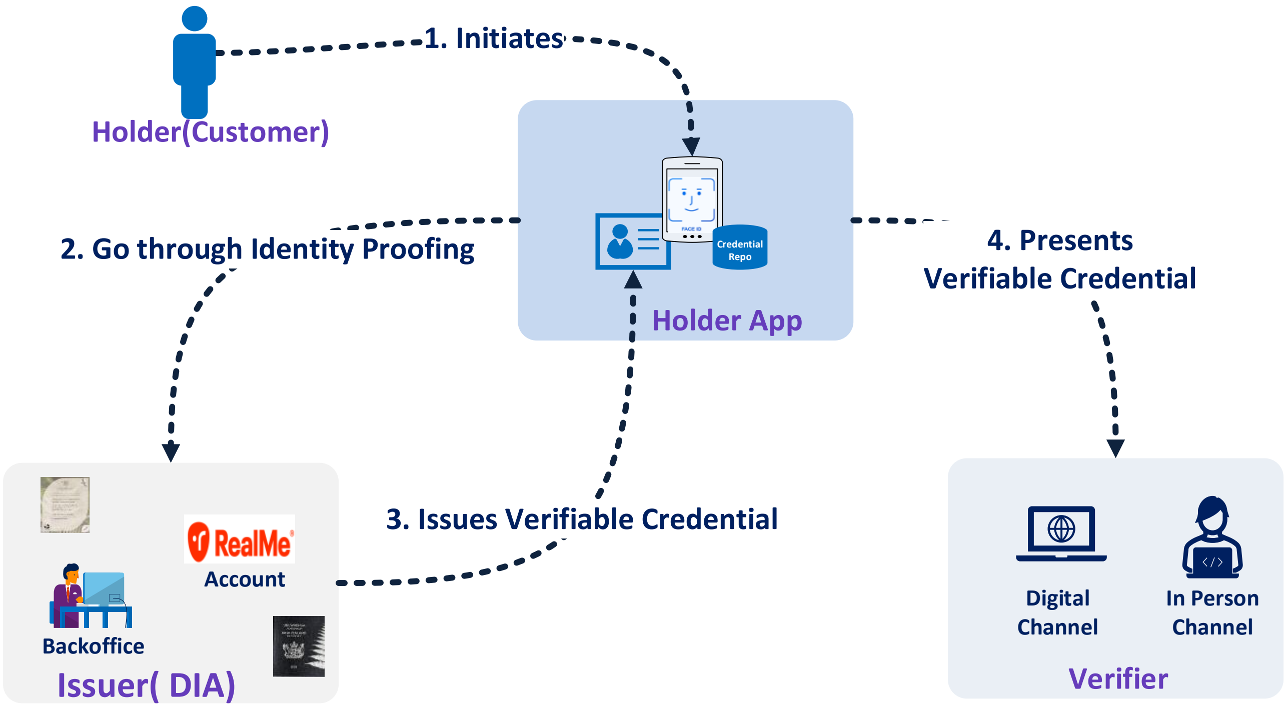


Figure 5: Verifiable Credentials Issuance and Presentation – Key Roles

Key Roles

- **Holder/ Customer:** A customer or holder is a person who initiates the transactions for obtaining Verifiable Credentials from issuers and provides consent for presenting Verifiable Credentials to the verifiers.
- **Issuer**: DIA acts as an issuer by creating a Verifiable Credential from the RealMe verified identity information and transmitting the Verifiable Credential to the customer's preferred wallet. It has the potential to be fully automated and/or may require back office manual checks.
- **Holder App**: A holder app is a holder app with one or more Verifiable Credentials and can generate presentations of the credentials, as appropriate. Holders store their credentials in credential repositories (i.e. device or cloud-based identity hubs).
- **Verifier**: A verifier is a relying party that receives a Verifiable Credential from the holder, optionally inside a Verifiable Presentation for processing.

How can customers get Verifiable Credentials in future?

DIA has identified the following transition pathways for customers to get Verifiable Credentials and wants to test these pathways with the client organisations and market. The following Verifiable Credentials list is based on DIA's identity register or sources.

Get Verifiable Credential if you are existing RealMe verified customer

While browsing the verifier's home page or RealMe home page, the customer comes across a holder app that can obtain Verifiable Credentials from DIA/RealMe. The customer downloads the holder app and uses their device to set their password less authenticator (e.g. device based biometrics) for the wallet. The customer is taken to DIA's credential issuance service. After successful authentication of the customer and association of holder app at RealMe, and consenting to their Verifiable Credential being transmitted, the customer returns to the wallet with their Verifiable Credential, which contains Full Name, Date of Birth, Place of Birth, Registered Sex and Photo verified claims.

Get Verifiable Credential if you are NZ Passports holder or NZ Citizenship by Grant

While browsing the verifier's home page or RealMe home page, the customer comes across a holder app that can obtain Verifiable Credentials from DIA. The customer downloads the holder app and uses their device to set their password less authenticator (e.g. device based biometrics) for the wallet. The customer is taken to DIA's credential issuance service. The customer enters their NZ passport or NZ citizenship details, and DIA's credential service confirms NZ passport or NZ citizenship details and matches the customer's live-captured facial image against the passport or citizenship image via a biometric facial verification process. Upon successful confirmation, the customer returns to the wallet with their Verifiable Credential, which contains Full Name, Date of Birth, Place of Birth, Registered Sex and Photo verified claims.

How can customers get other Verifiable Credentials?

A Verifiable Credential with verified identity claims can be one of the enablers for obtaining other Verifiable Credentials from other issuers. One of the options could be the customer receiving Verifiable Credentials with identity claims from DIA using their holder app before obtaining other Verifiable Credentials from the other issuer. DIA has identified the following key Verifiable Credentials that could be useful for the Future State New Zealand identity ecosystem.

It is noted that the options provided below are provided as illustrative only for the purposes of progressing thinking within this paper. They do not reflect planned implementation by agencies that are named.

Parents and Children relationship Verifiable Credential

Parents may have to prove their identity and relationship with their children to support eligibility or access to digital services (e.g. Work & Income, open bank account for children, etc.). Parents can obtain child relationships as a Verifiable Credential from DIA based on successful identity verification at DIA. The customer can use their Verifiable Identity Credential as one of the options for Identity Proof. The Department matches the customer's identity details against children's birth records and performs other eligibility checks before issuing a child relationship Verifiable Credential to the customer. This process will be automated, and manual intervention may be required if the verified identity details don't match the childbirth record parent's details to issue a relationship Verifiable Credential. It is yet to be determined the success rate of the automation.

Citizenship Status Verifiable Credential

The customer may have to share their citizenship status with the verifiers to support eligibility or access to digital services. The customer can obtain citizenship status as a Verifiable Credential from DIA based on successful identity verification at DIA. The customer can use their Verifiable Identity Credential as one of the options for Identity Proof. DIA matches customer identity details against birth or citizenship record before issuing the citizenship status Verifiable Credential to the customer. This process will be automated, and manual intervention may be required if the verified identity details don’t match the citizenship or NZ birth record to issue the citizenship status Verifiable Credential. It is yet to be determined the success rate of automation.

Immigration Status Verifiable Credential

The customer may have to share their immigration status with the verifiers to support eligibility or access to digital services. The customer can obtain immigration status as a Verifiable Credential based on identity verification at the Ministry of Business Innovation & Employment (MBIE). The customer can use their Verifiable Identity Credential as one of the options for Identity Proof. On successful identity verification, the ministry can issue immigration status Verifiable Credential to the customer.

Sector Identifier Verifiable Credential

People can obtain sector identifier credentials such as National Health Identifier (NHI) for the health domain, New Zealand Business Number (NZBN) for the business domain, and IRD tax number for the tax domain through the respective identity verification business processes. These sector identifier credentials will help people seamlessly access the respective sector services.

Act on Behalf (Role Association with Other Entities) Credential

People with a Verifiable Credential could be onboarded to roles where they are required in their personal or professional capacities to undertake tasks on behalf of an entity, i.e., filing company accounts as a company director or trustee.

How can businesses and client organisations consume Verifiable Credentials?

The customers can get a Verifiable Credential with verified identity claims from the Department of Internal Affairs using the customer's preferred holder app. The customer can also get Verifiable Credentials with verified attributes from other issuers, the holder retains **Control** of all Verifiable Credentials. The holder app offers **Choice** about when, how and to whom the Verifiable Credentials are asserted as a proof of identity and the **Portability** of those attributes and credentials for ease of use. These holder app providers may have to be accredited under the future digital identity trust framework.

The following are the key business processes categorised for Verifiable Credential assertion:

Category: Digital Channel

Applying for a student loan

Verifying and approving student loan applications can be significantly simplified with a Verifiable Credential. Students can share their Verifiable Credential with identity claims as identity proof using their holder app with the Study Link digital service. The Ministry of Social Development receives the student's Verifiable Credential and performs checks related to application processing.

Applying for a loan

Verifying and approving loan applications can be significantly simplified with Verifiable Credentials. Applicants can share their Verifiable Credential with identity claims as identity proof using their holder app with a financial institution. The organisation receives the applicant's Verifiable Credential and does other background checks to decide whether the loan should be approved.

Student Enrolment at Tertiary Education Institutes

Students (i.e., customers) can prove their identity online to enrol for tertiary education/university courses. They are also required to share other credentials issued by the government, such as citizenship or visa status credentials to support their enrolment application. Students can securely, seamlessly, and consistently share these trusted credentials with tertiary education providers and universities using Verifiable Credential technologies.

New Employee Onboarding

Many companies require prospective employees (i.e., customers) to go through a background check before they are offered a position, and trusted Verifiable Credentials can streamline the employee onboarding process. They may have to present their professional qualifications Verifiable Credentials along with the Verified Credential with verified identity claims.

Applying for Utility Connections

People applying for new utility connections or changing the name on the existing account such as internet and electricity must share their verified identity information, including residential address. Using trusted Verifiable Credentials can streamline the business processes and reduce time to access numerous services.

Key Government Services

People can digitally apply for a NZ passport and replacement of their NZ driver's licenses using their existing RealMe verified identity. Using trusted Verifiable Credentials can streamline the entitlement processes and issuance time for numerous key government services.

Category: in Person Channel

Opening a bank account

Opening a bank account is something that everyone does in their lifetime, sometimes more than once and with different banks. To open a bank account, the customer should prove their identity digitally or in person by visiting the bank branch using their government-issued identity documents. The current state RealMe service supports a digital channel offered by a bank, but the customer should carry their physical identity documents when visiting the bank to use the in-person channel. Carrying physical identity documents is risky because they can be lost in transit which may enable identity theft, and these documents need to be stored appropriately by the bank as well as managing data-entry issues/errors translating information from paper records into databases. A more secure, seamless, and consistent way to share trusted identity information through digital or in-person channels for opening a bank account is through Verifiable Credentials. The customer uses their holder app to share verifiable credentials by scanning a QR code in digital or in-person channels.

Registering with a General Practitioner/ Medical Facility / In person health services

A person (i.e., customer) should prove their identity to register with a GP, medical facility, or in-person health services. They can provide their identity by visiting the medical centre they are enrolling in. The person may have to share other credentials issued by the government, such as citizenship or visa status, to support their registration with a GP.

Category: Zero Knowledge Proof

Over 18 years

An individual must prove their age, that they are over 18, to avail of certain services like skydiving, entry to licensed premises, etc. (i.e., in-person channels). Presenting a derived value from the verified identity credential from their wallet is a convenient and trusted way to confirm that the individual is over 18 years.

How to issue Verifiable Credential?

The Verifiable Credential is a key enabler for the **Future State New Zealand Identity Ecosystem**, enabling **Portability**, **Control** and **Choice** for the customer of their identity and other attributes. DIA's contribution is to support the **Future State New Zealand Identity Ecosystem** and key customer outcomes by issuing Verifiable Credentials with the authoritative life data attributes we hold for New Zealanders.

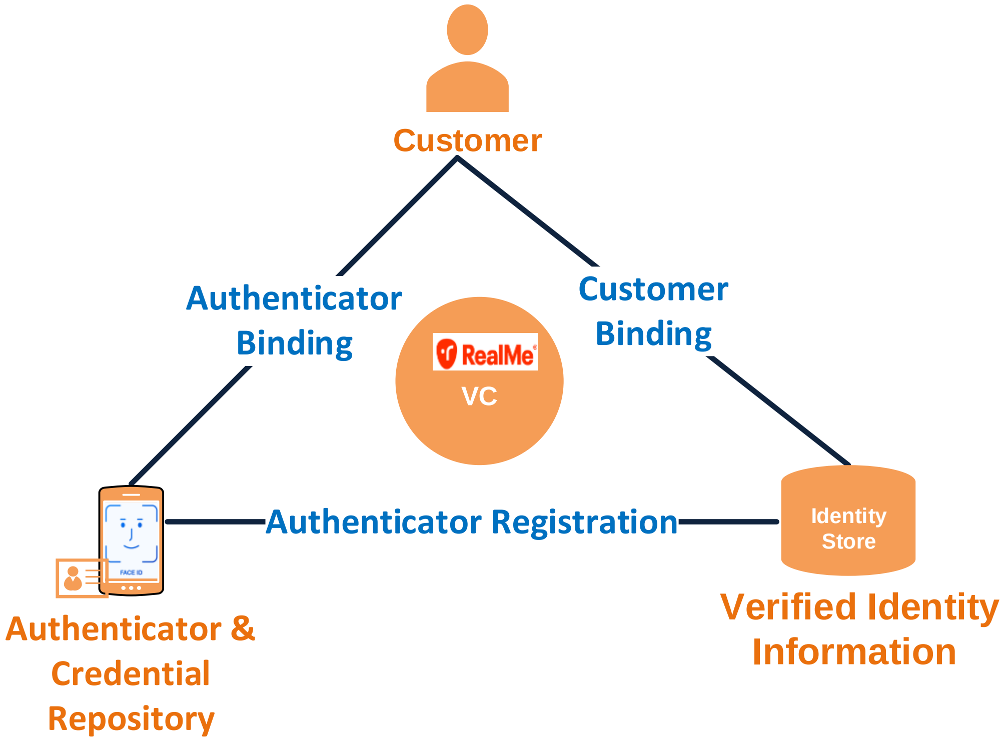

Customer
Authenticator Binding
Customer Binding
RealMe
VC
Authenticator Registration
Identity Store
FACE ID
Authenticator & Credential Repository
Verified Identity Information

Figure 6: Verifiable Credential

This diagram represents the connection between the Customer, Authenticator (represented by a holder app) and Verified Identity Information (represented by the identity store).

The Customer and Verified Identity information relationship is marked as Customer binding. The Verified Identity Information and Authenticator relationship is marked as Authenticator Registration. The Authenticator and the Customer relationship is marked as Authenticator Binding. The triangulation of these entities represents the **Verifiable Credential**.

The following are the key points regarding the **Verifiable Credential**:

- The customer's RealMe verified identity record is stored in DIA's identity register as per current state.
- The customer is bound to the RealMe verified identity record through liveness and biometric matching between facial live image and source photo and DIA verification of application details as per current state.
- The holder app is an authenticator linked to the RealMe verified identity and bound to the customer.
- The Verifiable Credential with identity claims is persistent on the customer's device and cannot be altered as DIA signs the Verifiable Credential using DIA's signing key.

Capabilities needed for DIA to issue Verifiable Credentials?

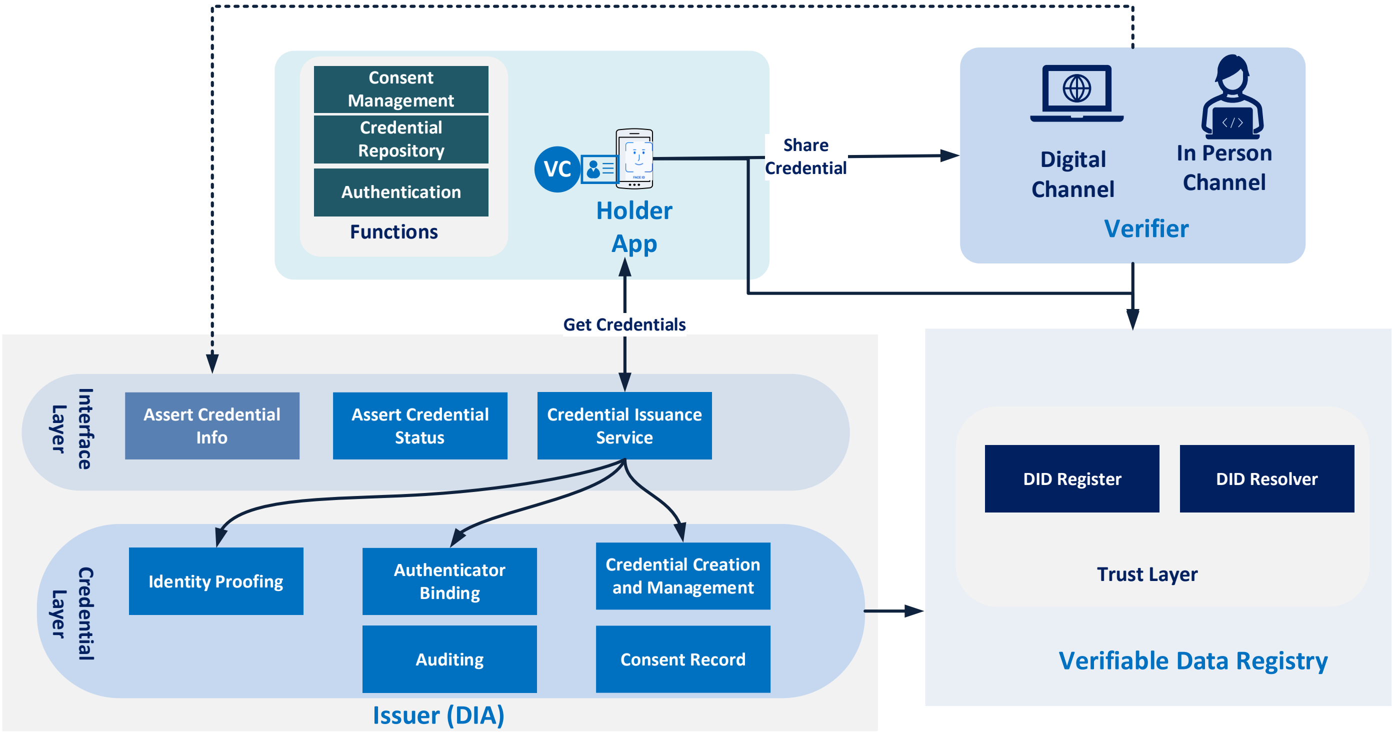


Figure 7: Capabilities

The following capabilities are required to issue Verifiable Credentials:

- The customer needs a holder app on their device to hold the Verifiable Credentials.
- The credential issuing authority (i.e., DIA) needs these capabilities to issue Verifiable Credentials:
  - Identity Proofing
  - Authenticator binding
  - Credential creation and management
  - Credential Issuance Interface
  - Sharing Credential Status
  - Assert Credential Info (Optional)
- Verifiable Data Registry: A capability to host issuer identifier, associated public keys, and Verifiable Credential schemas to support issuing Verifiable Credentials.

This section describes each capability's objectives, current and future transition state.

DIA Capability - Identity Proofing

Objectives

The following are the key objectives of this capability:

- Establishing that a person is a subject of either the identity information they have provided or are claiming. This is fundamental to preventing the impersonation of a person to gain a benefit or avoid an obligation.
- Verified identity information is expected to be specific to a single person, therefore only one person can have a legitimate association or binding with an instance of verified identity information.
- Each instance of identity information is distinguishable and unique from another in DIA's identity store.
- Ensuring that one person claims each instance still allows them to claim multiple instances of the same identity information, i.e. the verified identity information is linked to one or more verifiable credentials.

Current State

DIA issues a RealMe verified identity to a person using its identity proofing capability. The following are the key responsibilities of the capability:

- Verifying the customer’s identity to a high level of confidence,
- Binding the person with an identity record using biometrics and other manual checks,
- Persistence of the identity record for supporting identity lifecycle management, such as updating the identity status based on name changes, death checks, fraud detection etc.

DIA also developed an "Identity Check" capability for unverified RealMe customers. This capability confirms the person's identity in real-time based on either NZ passports or NZ citizenship documents and binds the person against them using biometrics.

Future Transition State

- There are no additional capabilities required to support Verifiable Credential issuance other than recording new authenticator(s) against verified identity information.

DIA Capability - Authenticator Binding

Objectives

The following are the key objectives of this capability:

- A person can trust that their information and the services they are enrolled in are being adequately protected from unauthorised access and use.

- Verified identity information is specific to a single person, therefore only one person can have a legitimate association or binding with an instance of verified identity information.
- Authenticator binding can occur during identity proofing or later during a subsequent transaction. In either case, it is essential to ensure that the person has been bound to the identity information at the required level of assurance before attempting to bind to an Authenticator.
- Authenticator strength is consistent with the level of authenticator binding and the identity proofing binding, ensuring the same person remains associated with their identity information. If one of the processes is weaker, it reduces the overall assurance and increases the opportunity for a takeover of account by another person.
- A person has control of the authenticator. Ensure that the person has control of an authenticator while associating with identity information. Without this assurance there is an increased risk of impersonation.
- For an authenticator to be successfully used by the person returning in the future, there needs to be enough information recorded in DIA's verified identity store to facilitate this.

Current State

- RealMe multi-factor login (i.e. something you know and something you have) is an authenticator associated with a person, along with the RealMe verified identity record created through the RealMe verified identity application process.
- A person has to login with multi-factor authentication to access RealMe verified identity information and share an instance of it with the agency services and private sector clients.
- The customer's email address and mobile phone number are verified during the application process for a RealMe account to prove that they have access to these.
- The multi-factor RealMe authenticator is linked to the RealMe verified identity to support the returning customer scenarios.

Future Transition State

- The holder apps use their own (e.g. device biometrics, server based biometrics etc) authentication to obtain Verifiable Credentials, from DIA. The holder app will become an authenticator for obtaining Verifiable Credentials.
- Existing RealMe verified customers must bind their holder app (implicitly mobile device) as an authenticator with the RealMe verified identity, to obtain Verifiable Credentials from DIA's proposed credential issuance service. Credential Issuance Service can also obtain an attestation along with the passkey from an inbuilt device FIDO authenticator to allow the customers to login to RealMe using their device as an authenticator.
- The holder app, acting as an authenticator must be bound to the verified identity information, to support the authentication binding objectives listed above.
- Binding the verified identity information with the holder app authenticator enables DIA to manage the Verifiable Credential lifecycle.

DIA Capability - Credential Creation and Management

Objectives

The following are the key objectives of this capability:

- Issue identity credentials which are trustworthy and acceptable to the agencies and identity ecosystem.
- Once a Verifiable Credential is issued, DIA manages the credential's life cycle, such as updating, suspending, and revoking the credential to maintain its integrity. DIA **monitors** the **credential issuance process** to detect suspicious activity and fraud.

Current State

- DIA creates a RealMe verified identity on successful processing of the RealMe verified identity application, and the credential is saved in DIA's verified identity store.
- Every time a RealMe verified identity is shared, a transaction is logged and monitored. DIA suspends or revokes the RealMe verified identity in the case of suspicious activity or fraud, to maintain the integrity of the credentials.

Future Transition State

- The capability registers DIA's Decentralised Identity (DID) Document with a Verifiable Data Registry.
- The credential creation capability verifies the holder app and issues Verifiable Credentials to the holder app. The capability registers credential metadata, and creates identity and holder app mapping, for credential life-cycle management.
- DIA doesn't monitor any transactions between the holder app and verifier and only **monitors** Verifiable Credential issuance process.
- The Holder App notifies of any changes (e.g., DID:key change) to Verifiable Credentials on the device to the credential management capability, which will update the credential status accordingly.
- DIA suspends or revokes the Verifiable Credential in case of suspicious activity or fraud, to maintain integrity of the credentials.
- If the device is lost, the person can call DIA helpdesk to revoke their existing verifiable credentials.

DIA Capability - Credential Issuance Service

Objectives

The following are the key objectives of this capability:

- Standards based interface to orchestrate customer and functional flows for RealMe verified identity customers to receive a Verifiable Credential to their holder app(s).
- Enabling customers greater control of their data.

Current State

- N/A

Future Transition State

- The interface capability orchestrates a process of binding the holder app with the RealMe verified identity information and issuing Verifiable Credentials to the holder app(s).
- Integration requirements between holder apps and the interface will need to be established.

DIA Capability – Assert Credential Status

Objectives

The following are the key objectives of this capability:

- Meeting client regulatory and legislative obligations such as Anti Money Laundering (AML), Counter Financing of Terrorism (CFT), etc.
- Establish trust with Verifiers (i.e., relying parties) regarding Verifiable Credential issuance and lifecycle management.

Current State

- N/A

Future Transition State

- This capability provides a Unique Identifier (i.e., RealMe Federated Identity Tag (FIT)) for a person's identity for the Verifier privacy domain and credential status (i.e., active, revoked etc.) based on the query from the Verifier to allow them to meet regulatory obligations.
- Holder apps share credential status changes related to the authenticator or metadata associated with Verifiable Credentials. This allows DIA to manage credential status accordingly.
- The capability provides credentials status based on a query from the holder app to allow the holder app to update credential status accordingly.

DIA Capability – Credential Assertion Service

Objectives

The following is the key objectives of this capability:

- Develop a bridge between the current state identity operating environment in RealMe and transition state Verifiable Credentials to speed up the digital services' uptake of Verifiable Credentials.
- Remove technology barriers for Verifiers and existing RealMe Clients to adopt Verifiable Credentials with their digital services.

Current State

- N/A

Future Transition State

- DIA can offer this capability and share Verifiable Credentials to create a bridge between the current state identity ecosystem and future transition state.

Trust Capability – Verifiable Data Registry

Objectives

The following are the key objectives of this capability:

- Provide a capability to host issuer, holder app (optional), and verifiers (optional) identifiers, associated public keys, and Verifiable Credential schemas to support issuing Verifiable Credentials.
- Provide a capability which can work in the existing operational environment for the New Zealand identity ecosystem.

Current State

- N/A

Future Transition State

- DIA hosts this capability in public cloud platform to persist DIA (as ***issuer)***, holder app (as ***holder)***, Client services (as a ***verifier***) DID document with their public signing key.
- Shares DID document key role (one of ***Issuer***, ***Holder,*** and ***Verifier***) based on a query from the other key role.

Holder Capability – Holder App

Objectives

The following are the key objectives of this capability:

- Enable/promote customers to control their data.
- Support customers to access digital and in person channels.
- Reduces customers needing to carry and present hard copy identity documents.
- Reduces potential for identity theft and data misuse.

Current State

- N/A

Future Transition State

- All customers receive Verifiable Credentials from DIA's credential service capability using their holder app and saves the credential in their device.
- Holder app(s) is an authenticator and supports authentication binding with verified identity information to receive Verifiable Credentials.
- Holder app(s) interact with the Verifiable Data Registry capability for saving its identifier and querying issuer and verifier's identifier (optional).
- Holder app(s) share Verifiable Credentials with Verifiers directly.

Verifier Capability

Objectives

The following are the key objectives of this capability:

- Provide seamless digital and in person services for the customers.
- Improve trust in providing access to the services.
- Reduces the need to retain hard copy identity documents or personal information, which is unnecessary for a verifier to retain.
- Reduces a verifier risk of privacy breaches or hacks designed to access and publicise personal information creating identity theft opportunities.

Current State

- N/A

Future Transition State

- Verifiers must do security and privacy assessments to understand the risks they will inherit due to the holder apps, and they may prefer particular holder app providers.
- Verifiers invest in Verifiable Credentials technology to:
    - receive Verifiable Credentials from holder apps,
    - register their DID document with the Verifiable Data Registry,
    - provide a digital and/or in person channel to receive Verifiable Credentials from the holder apps.
    - establish trust with the holder apps(s),
    - verify the authenticity of the holder app by querying the Verifiable Data Registry (optional),
    - query DIA's "share credential status" capability to verify the status of an identity credential as per regulatory obligations.

Consent Management and Auditing

Objectives

The following are the key objectives of the consent and auditing capabilities:

- Capture customer consent to protect the privacy of personal information, align with the regulations and offer a choice for the customer to share their data between parties.
- A record of consent enhances the ability to maintain and manage permissions of personal information by the customer and organisation and services.
- Audit every transaction between the parties to support non-repudiation.

Current State

- According to the RealMe privacy design, an individual's explicit consent is required for RealMe to broker sharing of their personal information with the client organisation services.
- Customers can view and manage their transactions by logging in to RealMe (www.realme.govt.nz).
- RealMe audits every transaction, and the customers can view the audit history by logging in to RealMe (www.realme.govt.nz).

Future State

- DIA credential service captures explicit customer consent for issuing verifiable credential to the holder app. Customers can view their consent by logging in to RealMe (www.realme.govt.nz).
- RealMe audits the verifiable credential issuance process, and the customers can view the audit history by logging in to RealMe (www.realme.govt.nz).
- The holder app captures explicit customer consent for sharing the verifiable credential presentation with verifiers services. The customers may view their sharing consents through the holder app, and the holder app may offer consent management and view audit history functionalities.
- Verifier audits verifiable credential presentation transactions from the holder app. The verifiers may offer view audit history functionality through their services.

Potential Future State Architecture View

Conceptual View

DIA can issue Verifiable Credentials based on the RealMe verified identity process as it stands but require new capabilities and interfaces to support Verifiable Credentials issuance and assertion of Verifiable Credentials. The following diagram depicts the high-level conceptual architecture of RealMe, Verifiable Credentials issuance, and sharing of Verifiable Credentials.

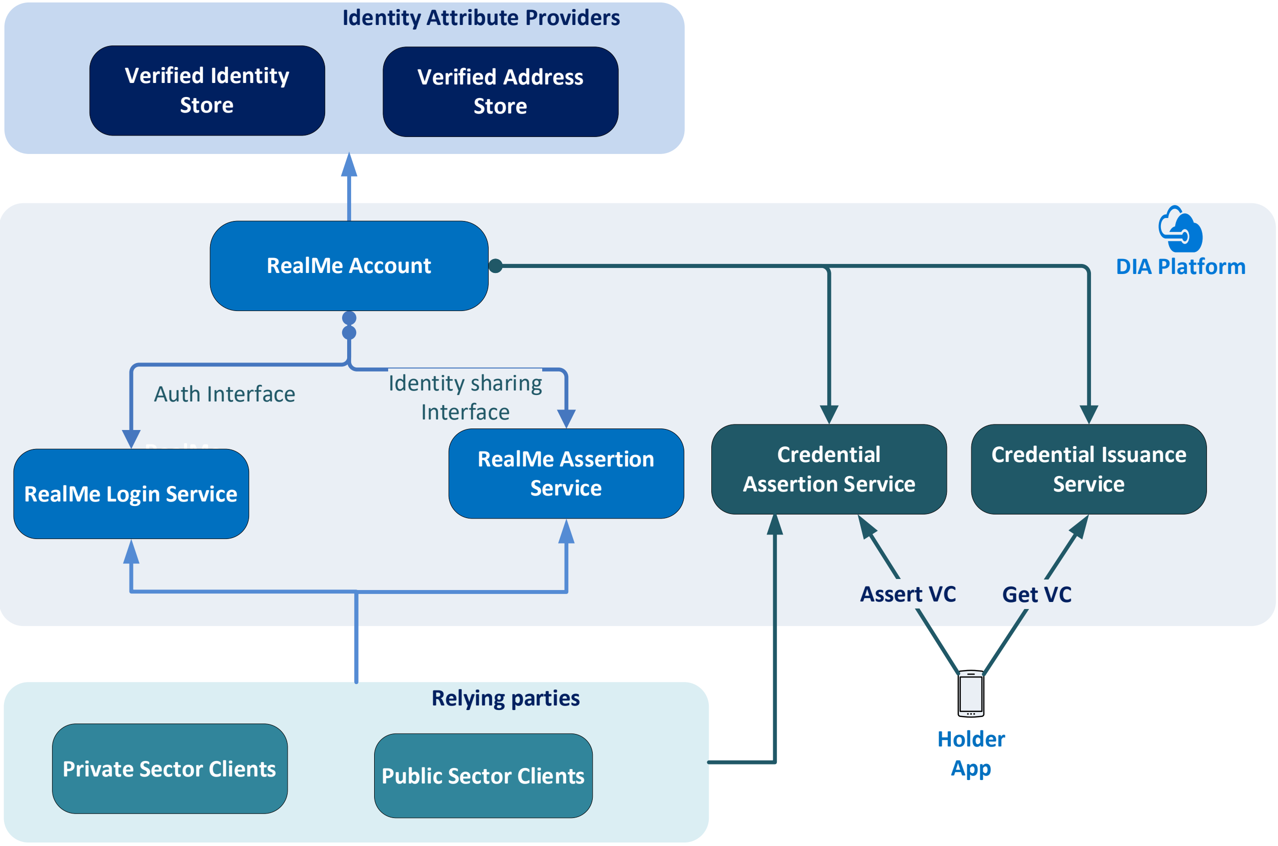


Figure 8: Integration View

The following are the key points regarding integration architecture view:

- DIA can provide additional interfaces for issuing Verifiable Credentials to the holder apps and asserting Verifiable Credentials through the RealMe platform.
- RealMe can build a bridge between the existing operational environment and the Verifiable Credentials transition state through a credential assertion service, and relying parties are not required to invest in Verifiable Credential technology. Verifiers can use existing Federation Protocols (SAML, Open ID Connect) to receive Verifiable Credentials. The credential assertion Service bridge will allow faster uptake of Verifiable Credentials by the existing RealMe integrated clients.

Verifiable Credentials – Conceptual Architecture

Get Verifiable Credential if you are existing RealMe verified identity customer

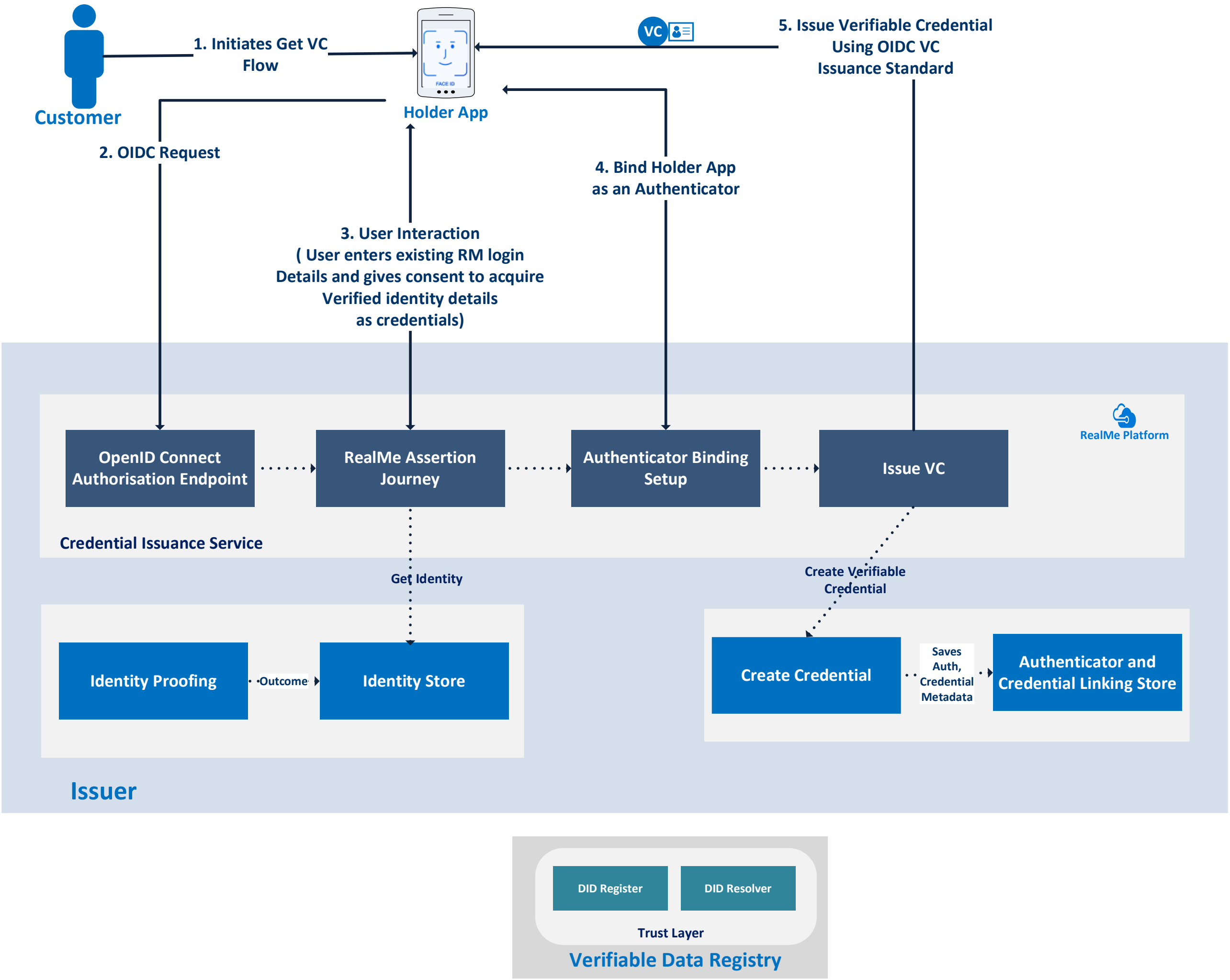

Customer
1. Initiates Get VC Flow
Holder App
VC
5. Issue Verifiable Credential Using OIDC VC Issuance Standard
2. OIDC Request
4. Bind Holder App as an Authenticator
3. User Interaction (User enters existing RM login Details and gives consent to acquire Verified identity details as credentials)
RealMe Platform
OpenID Connect Authorisation Endpoint
RealMe Assertion Journey
Authenticator Binding Setup
Issue VC
Credential Issuance Service
Get Identity
Create Verifiable Credential
Identity Proofing
Outcome
Identity Store
Create Credential
Saves Auth, Credential Metadata
Authenticator and Credential Linking Store
Issuer
DID Register
DID Resolver
Trust Layer
Verifiable Data Registry

Figure 9: Issuing Verifiable Credentials for existing RealMe verified identity customers

The following are the key points regarding above diagram:

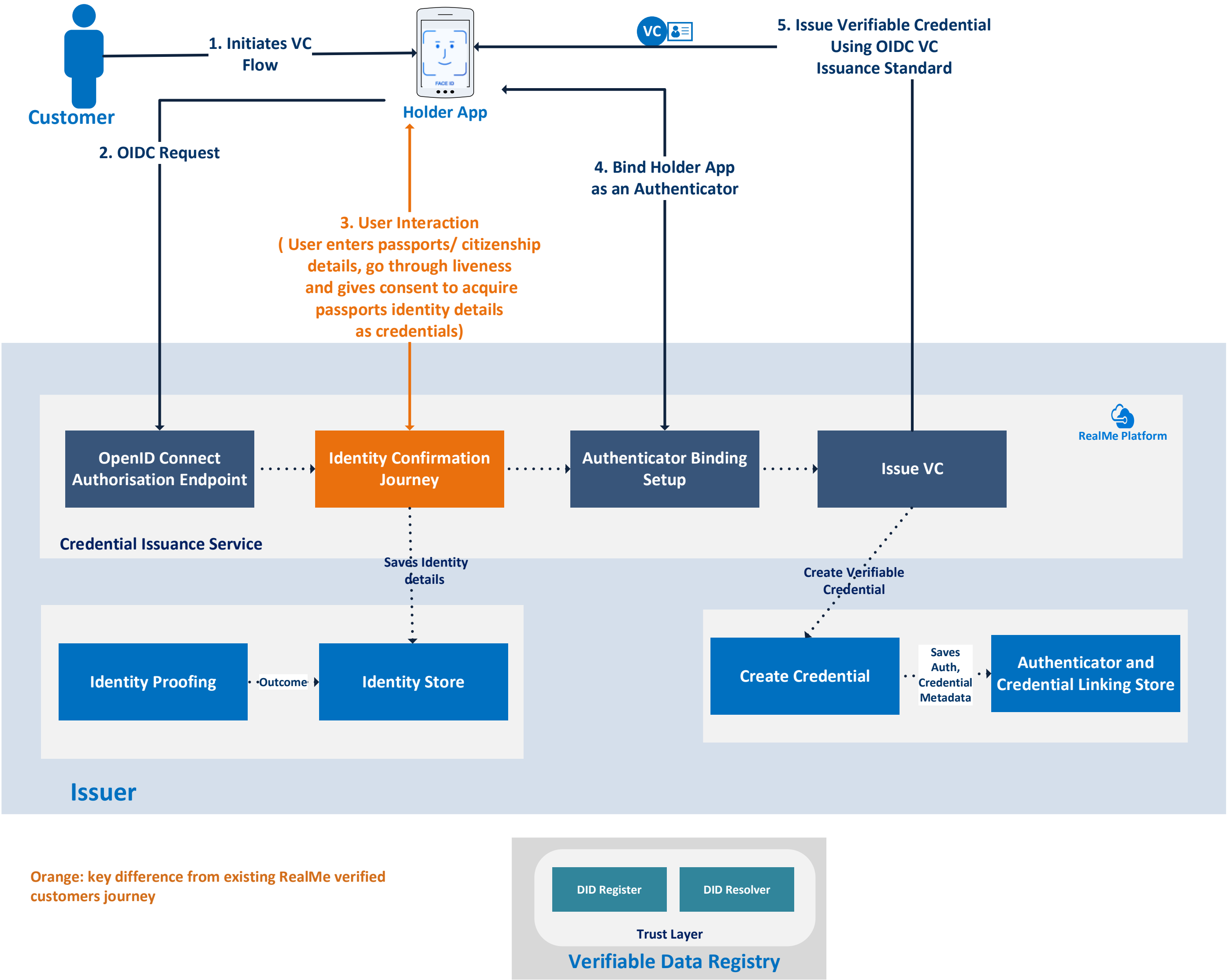
1. The customer downloads the **holder app** and uses their device to set the wallet's authenticator (e.g. password-less). One of the authentication options is that the holder app authenticates the customer using the Web Authentication (or "WebAuthn") standard, which uses public key cryptography (Passkey) using a device-based authentication method (e.g. Face ID). On successful authentication, the holder app generates a public-private key pair and associated did:key and saves them in the device's secure location. The customer initiates obtaining Verifiable Credentials from DIA.
2. The holder app redirects the customer to DIA’s **credential issuance service** with the OpenID Connect request.
3. The credential issuance service takes the customer through the RealMe verified assertion journey. The customer logs in to the RealMe assertion journey using multifactor authentication (username, password, SMS) and gives consent to issue verifiable credentials to the holder app.

4. The credential issuance service binds the holder app as an authenticator based on the signature proof provided as defined in Open ID connect Verifiable Credential issuance standard. Optionally the credential issuance service can also bind the customer's device using the Web Authentication (or "WebAuthn") standard to allow the customer to access RealMe using device (i.e. without password). The credential issuance service binds did:key, FIDO Key (optional) with verified identity record. DIA will support other DID methods for the holder apps once they are assessed and evaluated against the Digital Identity Trust Framework.
5. The credential service creates the customer's Verifiable Credential with:
    a. Full name, Date of Birth, Place of Birth, Gender, and Photo.
    b. Subject of the credential as did:key of the holder app
    c. Signed with the issuer DID, which is registered to a verifiable data registry. The Verifiable Data Registry is a public cloud platform which saves DIA's DID (did:web).

    The credential service returns the customer Verifiable Credential to the holder app as defined in Open ID connect Verifiable Credential issuance standard. The holder app securely saves the Verifiable Credential in the credential repository (e.g. device).

Note: The customer can use multiple holder apps to obtain Verifiable Credentials from DIA's credential service. These holder apps may have to be accredited under the future Digital Identity Trust Framework.

Get Verifiable Credential if you are not RealMe verified customer (NZ Passports holders or NZ Citizen by Grant)


Customer
1. Initiates VC Flow
Holder App
VC
5. Issue Verifiable Credential Using OIDC VC Issuance Standard
2. OIDC Request
4. Bind Holder App as an Authenticator
3. User Interaction (User enters passports/ citizenship details, go through liveness and gives consent to acquire passports identity details as credentials)
RealMe Platform
OpenID Connect Authorisation Endpoint
Identity Confirmation Journey
Authenticator Binding Setup
Issue VC
Credential Issuance Service
Saves Identity details
Create Verifiable Credential
Identity Proofing
Outcome
Identity Store
Create Credential
Saves Auth, Credential Metadata
Authenticator and Credential Linking Store
Issuer
DID Register
DID Resolver
Trust Layer
Verifiable Data Registry

Orange: key difference from existing RealMe verified customers journey

Figure 10: Issuing Verifiable Credentials for NZ Passports Holders flow

The following are the key points regarding above diagram:

1. The customer downloads the **holder app** and uses their device to set the wallet's authenticator (e.g. password-less). One of the authentication options is that the holder app authenticates the customer using the Web Authentication (or "WebAuthn") standard, which uses public key cryptography (Passkey) using a device-based authentication method (e.g. Face ID). On successful authentication, the holder app generates a public-private key pair and associated did:key and saves them in the device's secure location. The customer initiates obtaining Verifiable Credentials from DIA.
2. The holder app redirects the customer to DIA's credential issuance service with the OpenID Connect request.

3. The credential issuance service takes the customer to the Identity Confirmation journey for non RealMe customers. The journey validates customer entered NZ passport or NZ citizenship identity details, validates the customer's liveness, matches live image against passport photo, and obtains customer consent to issue Verifiable Credentials to the holder app. The credential service saves verified identity details in DIA's verified identity store.
4. The credential issuance service binds the holder app as an authenticator based on the signature proof provided as defined in Open ID connect Verifiable Credential issuance standard. Optionally the credential issuance service can also bind the customer's device using the Web Authentication (or "WebAuthn") standard to allow the customer to access RealMe using device (i.e. without password). The credential issuance service binds did:key, FIDO Key (optional) with verified identity record. DIA will support other DID methods for the holder apps once they are assessed and evaluated against the Digital Identity Trust Framework.
5. The credential service creates customer's Verifiable Credential with:
    a. full name, date of birth, place of birth, gender, and live photo.
    b. subject of the credential as did:key of the holder app
    c. Signed with the issuer DID, which is registered to a verifiable data registry. The verifiable data registry is a public cloud platform which saves DIA's DID (did:web).

The credential service returns the customer Verifiable Credential to the holder app as defined in Open ID connect Verifiable Credential issuance standard. The holder app securely saves the Verifiable Credential in the credential repository (e.g. device).

Get Verifiable Credential if you are not RealMe verified customer (NZ Citizen by birth or NZ Immigrant)

The customer is a natural NZ citizen or an NZ immigrant who applies for a RealMe verified identity from the RealMe website. DIA issues RealMe verified identity to the customer on successful verification of the RealMe verified identity application. The customer receives an email confirmation from RealMe that the user can get a Verifiable Credential based on the RealMe verified identity and instructions for getting it. The customer downloads the holder app app and uses their device's biometrics to set their password less authenticator for the wallet. The customer is taken to DIA's credential issuance service. After successful authentication of their holder app at RealMe, and consenting to their Verifiable Credential being transmitted, the customer returns to the wallet with their Verifiable Credential, which contains Full Name, Date of Birth, Place of Birth, Registered Sex and Photo verified claims.

Verifiable Credentials Presentation – Conceptual Architecture

VC Assertion through DIA's Credential Assertion Service (Cross device use case)

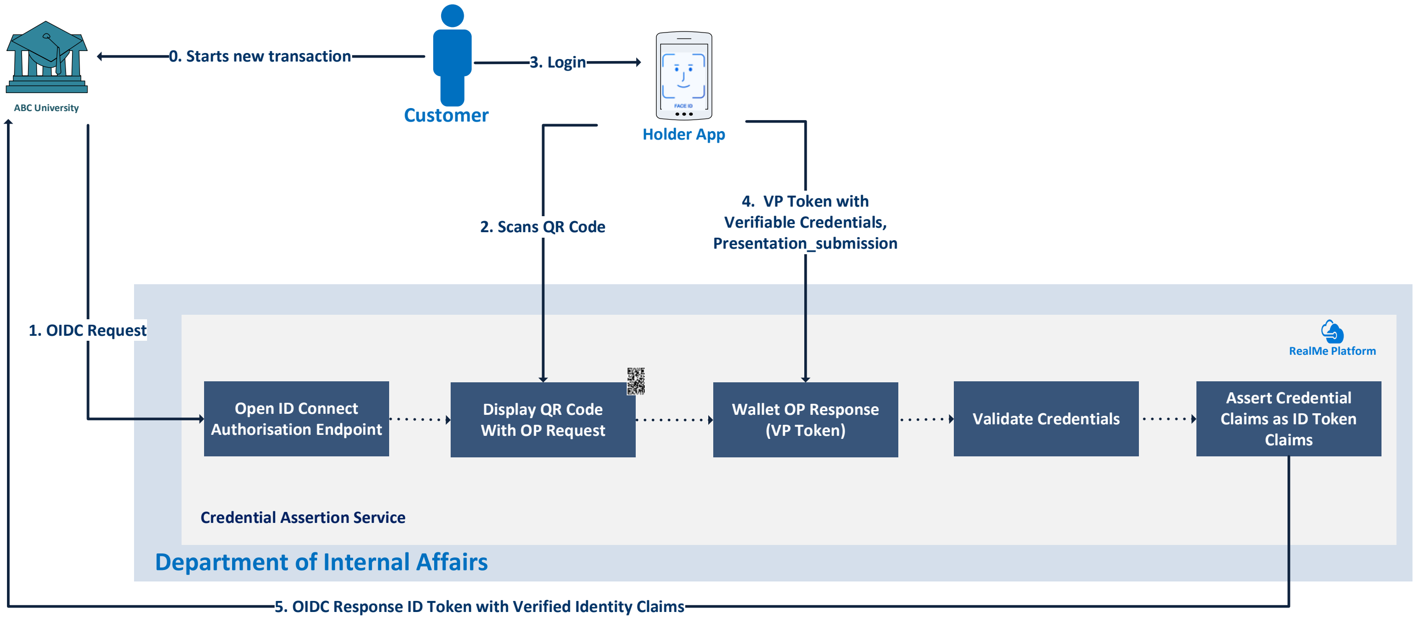

ABC University
0. Starts new transaction
Customer
3. Login
Holder App
2. Scans QR Code
4. VP Token with Verifiable Credentials, Presentation_submission
1. OIDC Request
RealMe Platform
Open ID Connect Authorisation Endpoint
Display QR Code With OP Request
Wallet OP Response (VP Token)
Validate Credentials
Assert Credential Claims as ID Token Claims
Credential Assertion Service
Department of Internal Affairs
5. OIDC Response ID Token with Verified Identity Claims

Figure 11: Asserting Credentials through DIA's Credential Assertion Service

The following are the key points regarding above diagram:

1. The customer wants to enrol with a university and must digitally prove their identity. The customer clicks the "Prove Identity Online" button at ABC University to share their Verifiable Credentials. The university redirects the customer to DIA's credential assertion service with an OIDC request.
2. The credential assertion service creates a request for the holder app and renders it as a QR code as per Self Issued OpenID Provider protocol. The customer scans QR code with the holder app.
3. The customer logins to the holder app using device-based authentication (Face ID) and gives consent to assert Verifiable Credentials with the credential assertion service.
4. The holder app creates a Verifiable Presentation token, defined in OpenID Connect for Verifiable Presentation protocol. The Verifiable Presentation token contains Verifiable Credentials and signs the Verifiable Presentation using its private key to obtain Verifiable Credential. The holder app redirects to the credential sharing service with the Verifiable Presentation token.
5. The credential assertion service verifies the Verifiable Presentation token signature, validates the Verifiable Credential, creates an ID token with the Verifiable Credential claims, and redirects the customer with the ID token to the university. The credential assertion service shares a unique pairwise identifier (also known as RealMe Federated Identity Tag (FIT)) as part of ID token.
6. The university validates the ID token, does other checks, and takes the customer to the next step in the enrolment process.

VC Presentation directly to verifiers (Cross device use case)

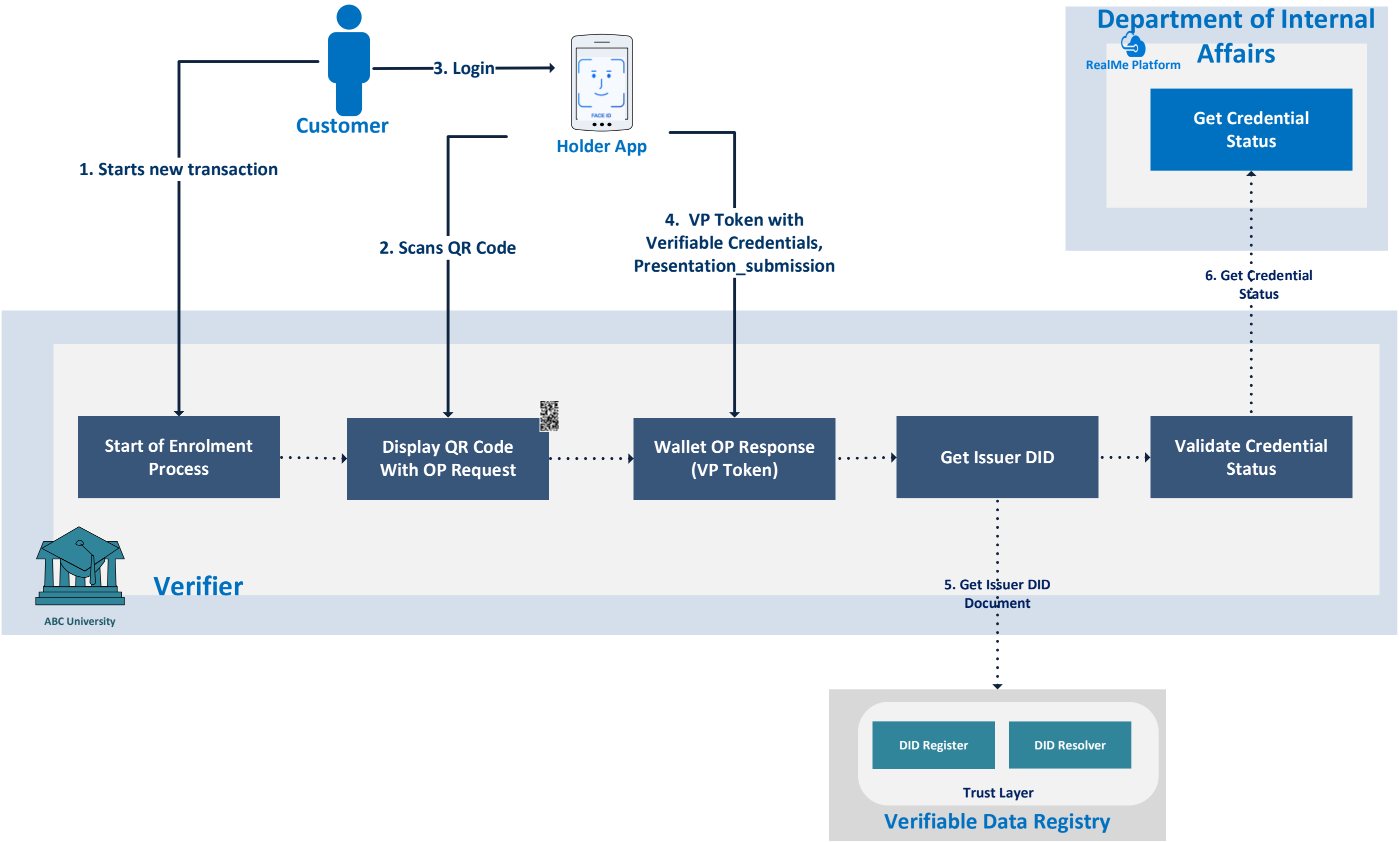

Customer
3. Login
Holder App
Department of Internal Affairs
RealMe Platform
Get Credential Status
1. Starts new transaction
2. Scans QR Code
4. VP Token with Verifiable Credentials, Presentation_submission
6. Get Credential Status
Start of Enrolment Process
Display QR Code With OP Request
Wallet OP Response (VP Token)
Get Issuer DID
Validate Credential Status
Verifier
ABC University
5. Get Issuer DID Document
DID Register
DID Resolver
Trust Layer
Verifiable Data Registry

Figure 12: Sharing Credentials directly to verifier web application

The following are the key points regarding above diagram:

1. The customer wants to enrol with a university and must digitally prove their identity.
2. The Verifier web service creates a Self-Issued OP request and renders it as a QR code as per Self Issued OpenID Provider protocol. The customer scans the QR code with the holder app.
3. The customer logins in to the holder app using device-based authentication (e.g. Face ID) and gives consent to share Verifiable Credentials with the Verifier service.
4. The holder app creates a Verifiable Presentation token, defined in OpenID Connect for Verifiable Presentation protocol. The Verifiable Presentation token contains Verifiable Credentials and signs the Verifiable Presentation using its private key. The holder app redirects to the Verifier web service with Verifiable Presentation token.
5. The Verifier web service invokes verifiable data registry DID resolver API to obtain DIA's DID document. The Verifiable Data Registry is a public cloud platform to save issuer DIDs (DID: web). The Verifier web service gets the issuer's public key from the issuer's DID document and verifies the signature of the Verifiable Credential using the issuer's public key.

6. On successful signature verification, the verifier web service invokes DIA's Credential Status API to check the status of the Verifiable Credential. The Credential status API provides the credential status as "Active" or "Revoked" and a unique pairwise identifier (also known as RealMe FIT) which is the customer's identifier related to the Verifier web service. The university takes the customer to the next step in the enrolment process if the credential status is "Active". The user takes the customer to the alternative identity verification options if the credential status is "revoked".

Security Considerations

The following are the key security considerations for issuing Verifiable Credentials to the holder app:

- The holder app must save its private key in a device-secured location and only be accessible to the holder app on successful device-based authentication.
- The holder app may have to support device-based biometric authentication as an authentication method for providing access to Verifiable Credentials.
- The holder app should save Verifiable Credentials in a device-secured location.
- The holder app must erase Verifiable Credentials if the device is rooted, a new biometric is enrolled, or malicious third-party wallets are present. The holder app should notify DIA regarding the deletion of the credentials on the device, and the Department must update the credential status as "Revoked".
- The holder app should provide App Attestation to the credential issuance service to obtain the Verifiable Credential, provided by the mobile's operating systems, which allows DIA to ensure it is communicating to a legitimate instance of the genuine holder app. This will allow DIA to validate the internal integrity of the wallet (as a whole).
- The lifetime of a Verifiable Credential needs to be confirmed during the implementation phase.
- The Verifiers should query the Department's credential status API regarding the status of a Verifiable Credential before accepting the credential.

Privacy Considerations

The holder app creates its identifier (e.g. *DID:key:abcdty78u9b*) using public key cryptography and shares it with issuers and Verifiers as part of Verifiable Credentials. Whilst this hasn't been assessed, it is possible that the proposed **sharing of verifiable credentials directly to the verifier** approach may be inconsistent with Privacy Act Information Privacy Principle 13 – Unique identifiers.

"An organisation cannot assign a unique identifier to a person if that unique identifier has already been given to that person by another organisation. For example, this prevents the Government from giving you one personal number to use in all your dealings with government agencies."

This proposed approach, we believe, would not contravene Information Privacy Principle 13 if:

- The holder app is installed on the customer's mobile and controlled by the customer,
- The holder app creates an identifier and shares it with issuers and Verifiers,
- The customer gives consent to get Verifiable Credentials for saving in the holder app and to share them with the Verifiers using their holder app,
- The holder app identifier will be used for authentication binding verification and Verifiable Presentation signature verification.

This approach needs privacy and legal assessment and views of the Office of Privacy Commissioner as to whether it is acceptable for a customer controlled holder app to share its identifier with issuers and Verifiers in the way described.

Impact on Electronic Identity Verification Act

RealMe is governed by the Electronic Identity Verification (EIV) Act 2012. This includes verifying the validity of human identity before binding a person to a digital credential. Relationships between the parties (including integrating clients) are governed in a way that provides legal certainty.

DIA assumes the following to issue Verifiable Credentials:

- RealMe Identity Proofing will continue to operate under the EIV Act, i.e., creating a verified identity record for the customer in DIA's identity store,
- The customer will be receiving RealMe Verified Identity (aka EIC) in the of form a Verifiable Credential which is an output of RealMe Identity Proofing,
- The third-party holder app providers are the facilitation providers for receiving Verifiable Credentials, who can be listed under the participation agency (i.e., integrating clients) class and will be governed through the EIV Act.
- The EIV Act is indifferent regarding how the identity information is exchanged with the integrating clients. DIA can assert identity information as SAML attributes, OIDC ID Token claims or Verifiable Credential Claims.

Legal and policy perspectives are required to determine whether these assumptions are accurate. DIA will ensure this assessment is conducted in due course.

What Next?

Next Steps

The Department of Internal Affairs will:

- Continue to engage partner agencies regarding the architecture approach and get their feedback.
- Progress Proof of Concept opportunities with partner agencies to test and refine/revise the architecture approach.
- Continue refining and understanding our approach in preparation for implementation.