Te Tari Taiwhenua
Internal Affairs

Digital Identity Services Trust Framework Rules

PROPOSED

APRIL 2024

Contents

Introduction

Purpose

The Department of Internal Affairs (the Department) seeks your views on the proposed Digital Identity Services Trust Framework Rules 2024 (the Rules). The Rules outlined in this paper to support the establishment of the Digital Identity Services Trust Framework (DISTF).

Overview

More and more services are moving online. Digital identity services give people the ability to securely share personal or organisation information (for example, a person's name, age, date of birth, qualifications, employment history or medical records) to access both online and face-to-face services. It's important that people can provide information about themselves digitally in a trusted, safe, and consistent way.

New Zealand's digital identity environment currently lacks consistent application of standards. This makes it difficult to provide reliable and secure services people feel they can trust.

The Digital Identity Services Trust Framework

The Digital Identity Services Trust Framework Act 2023 (the Act) comes into force on 1 July 2024. It enables the introduction of a new regulatory Trust Framework, which will establish rules and regulations for the provision of secure digital identity services.

The Digital Identity Services Trust Framework (the Framework) aims to give people more control over their own data, including what they choose to share about themselves and who they share it with. It sets out the legal requirements for accredited digital identity services, supporting New Zealanders to have more confidence in using online services.

Digital Identity Services Trust Framework Rules 2024

The Rules, which complement the regulations, establish the technical service requirements that providers will need to meet when designing and delivering accredited digital identity services. The focus of the Rules is to ensure that decentralised identity approaches are applied to support consistent, coherent, and trusted digital identity services.

The Digital Identity Services Trust Framework Administrative Bodies

The Act sets establishes a Trust Framework Board (TF Board) and a Trust Framework Authority (TF Authority) to administer the legislation. The Act also provides for a Māori Advisory Group to advise the TF Board on Māori interests and knowledge as they relate to the Framework and issues that raise matters of tikanga Māori or Māori cultural perspectives, as well as jointly establish with the TF Board an engagement policy covering how the two groups will work together and consult with iwi and hapū when necessary.

Digital Identity Services Regulations

To support the implementation of the Act, regulations are being developed to establish broader legal and administrative process requirements that either need to be met by regulated parties or clarify how the TF Board and the TF Authority will manage aspects of the regulatory system.

How to have your say

We are seeking your feedback on the proposed **Digital Identity Services Trust Framework Rules**.

Written submissions on the Rules outlined in this document are due **by 5pm, Friday, 3 May 2024.**

Please refer to the key questions throughout this to help guide your feedback on the proposed Rules. Enter your feedback in the submission form provided.

Your input will play an important role in ensuring the final Rules are effective in supporting the growth of trusted and secure digital identity services for New Zealanders.

Please send your submission to distf@dia.govt.nz.

Digital Identity Services Trust Framework Rules

About the Rules

Rules categories

The Rules provide a set of requirements across five categories, which are set out in the Digital Identity Services Trust Framework Act 2023[1].

Digital identity service providers must demonstrate their ability to meet the Rules, in order to become accredited digital identity service providers under the Trust Framework.

Rules Category	Description
Identification Management	Rules for determining the accuracy of personal or organisational information, binding that information to an individual or organisation, and enabling the secure reuse of the bound information.
Sharing and Facilitation	Rules for facilitating the sharing of information with relying parties including authorisation (consent) requirements.
Privacy and Confidentiality	Rules for trust framework providers to ensure the privacy and confidentiality of the information of individuals or organisations to whom the information relates is maintained.
Security and Risk	Rules ensuring information is secure and protected from unauthorised modification, use, or loss.
Information and Data Management	Rules for managing personal and organisational data to ensure a common understanding of what is shared.

Applying the Rules

To determine which Rules are applicable to a digital identity service provider:

- Identity what digital identity service(s) the provider is delivering.

[1] Section 20(1)

- Confirm **all** associated activities corresponding that digital identity service are activities the provider undertakes within their service.
- The corresponding Rules for those activities apply to the provider's specific service, and are set out in Identification Management, and Sharing and Facilitation sections.
- Rules under Authorisation, Privacy, Security and Information sections apply to **all** providers, unless stated otherwise.

All Trust Framework Rules use keywords MUST, SHOULD, MAY and their negatives, to signify different types of requirements:

- MUST: indicates an absolute requirement.
- SHOULD: indicates the recommended course of action. This Rule may not need implementing if the implications of doing so are mitigated or alternative actions are in place, which achieve the intention of the Rule.
- MAY: indicates a course of action that is optional. These Rules sometimes carry an ONLY IF statement which indicates the limited parameters for when the course of action could be taken.
- MUST NOT: indicates an absolute requirement that a particular course of action does not take place.

How the Rules will be assessed for accreditation

The Trust Framework Authority (TF Authority) will accredit applicants as a provider, **and** for at least one of the five accreditable services.

The accreditation process contains four sections:

- Provider – general information relating to the provider and their key personnel including information identified in the legislation and regulations.
- Privacy – evidence that the applicant meets the Privacy Rules and the provision of key documents including Privacy Incidence Response Plan, Complaints Process, and a Privacy Impact Assessment.
- Security and information management – evidence the applicant meets the Security, and Information and Data Management Rules, including evidence from an external security assessor that key risks have controls in place to manage them.
- Identification management – evidence of conformance to the relevant parts of the Identification Management Standards (IMS) as well as other information about the service, including the service name and description, what credential if any, what attributes, and the level of assurance for each attribute. Additional accreditation questions may be asked for Rules not addressed in the IMS. Note: assessment framework for this IMS conformance is currently in development.

The TF Authority assesses each accreditation application and may ask for further information or clarification during the assessment.

The TF Authority will decide to accredit the provider and their service(s) at the end of the assessment.

Successful applicants will receive a contract from the TF Authority, with the TF Authority's accredited provider terms and conditions. The contract outlines the accredited provider's requirements set out in the legislation and regulations, and the terms of use of the accreditation mark.

Once the provider accepts the accreditation contract, the TF Authority will list them on the Trust Framework Register as an accredited provider and for the accredited services.

Digital identity services

Digital identity services are services that organisations may seek to be **accredited** under the Trust Framework. Each digital identity service is a service available to consumers and relying parties as **standalone** service. There are five types of digital identity services that can be accredited:

1. **The Digital Identity Services Trust Framework Information Service** (information service) provides an assessment of the accuracy of personal or organisational information.

   An information service provides attributes and involves assessing the accuracy of personal or organisational information. It helps ensure that the information the individual or organisation is correct, reducing the risk of information errors and false associations (e.g., a bank providing a bank account number).

2. **The Digital Identity Services Trust Framework Binding Service** (binding service) provides an assessment of the accuracy of personal or organisational information and ensures the connection (entity binding) of personal or organisational information to an individual or organisation.

   Like information services, binding services also provide attributes and involve assessing the accuracy of personal or organisational information. In addition, the binding services focus on assuring the connection between personal or organisational information and the individual or organisation. It establishes a secure link between information and the entity it pertains to (e.g. associating bank account number to person claiming it as there one).

3. **The Digital Identity Services Trust Framework Authentication Service** (authentication service) ensures the connection of a user to an authenticator. It also secures the sharing of personal or organisational information between Trust Framework participants, by ensuring the authenticator(s) are possessed and controlled by an authorised holder.

An authentication service ensures a secure connection between a user and an authenticator. It also ensures the secure sharing of digital identity credentials by assuring the authenticator is still controlled by the user (e.g., a login service, two-factor authentication).

4. **The Digital Identity Services Trust Framework Credential Service** (credential service) combines bound information and an authenticator to establish (or issue) and maintain a reusable credential.

   Credential services verify and bind information about an individual or organisation and issue digitally verifiable credentials to them. This credential can be used to establish and maintain the user's information across various services, minimising the need to repeatedly share sensitive information (e.g., a university that issues a digital student ID card).

5. **The Digital Identity Services Trust Framework Facilitation Service** (facilitation service) assists users to share or present credentials with relying parties.

   This service provides a facilitation mechanism to assist users in sharing credentials or specific parts of credentials with relying parties. It simplifies sharing digital identity credentials with trusted parties while maintaining security and control (e.g., providing a digital wallet).

Components

Each digital identity service contains components. These components are known as activities and are required to be undertaken for the service to be considered a Digital Identity Services Trust Framework (DISTF) service.

Digital identity service activities

For a digital identity service to be accredited, the service must complete all the corresponding activities listed below, to achieve the expected outputs. The Trust Framework Rules set out the compliance requirements for undertaking each activity to reach the expected outputs.

Service	Activity	Output
Information Service	• Verifying information	• Provides attributes • Establishes level of information assurance

Service	Activity	Output
Binding Service	• Verifying information • Entity binding	• Provides bound attributes (bound to an entity) • Establishes level of information assurance • Establishes level of binding assurance
Authentication Service	• Authentication	• Provides authenticator(s) • Establishes level of authentication assurance
Credential Service	• Verifying information* • Entity binding* • Authenticator binding and registration • Authentication* • Credential establishment and issuance. *May use an accredited digital identity service to complete these activities.	• Provides digital identity/identification credential • Links entity and authenticator to entity information • Establishes levels of information, binding, authentication assurance
Facilitation Service	• Facilitation mechanism establishment • Authentication • Credential presentation	• Provides facilitation mechanism • Confirms entity relationship to their credential(s) • Links new authenticators associated with the mechanism. • Presents credential(s)

Activity descriptions

Below is a breakdown of each activity, the corresponding Rules, and the required compliance evidence to support accreditation.

Activity	Description
Verifying information	The process to establish the quality and accuracy of entity information. **Rules****: IM.1: Verifying Information. **Compliance evidence**: Certificate of conformance with the Information Assurance Standard.

Activity	Description
Entity binding	The process of ensuring the entity information belongs to the Entity that is using it. **Rules****: IM.2: Entity binding. **Compliance evidence**: Certificate of conformance with the Requirements for Entity Binding component of the Binding Assurance Standard.
Authenticator binding and registration	The process of ensuring the user of the authenticator is the same entity to which the entity information relates, and the process of creating and/or linking an Authenticator to the information about an Entity. **Rules****: IM.3: Authenticator binding and registration. **Compliance evidence:** Certificate of conformance with the Requirements for Authenticator Binding component of the Binding Assurance Standard.
Authentication	The process of ensuring the same entity is returning to access the system. **Rules****: IM.4: Authentication. **Compliance evidence:** Certificate of conformance with the Authentication Assurance Standard.
Credential establishment and issuance	The establishment of credentials for users across multiple contexts. **Rules****: IM.5: Credential establishment and issuance. **Compliance evidence:** Certificate of conformance with the Requirements for Credential Providers establishing Credentials component of the Federation Assurance Standard.

Activity	Description
Facilitation mechanism establishment	The establishment of a facilitation mechanism for users to hold and share credentials from. It includes confirming the relationship between the entity and their credentials and any new Authenticators associated with the mechanism. **Rules****: SF.1: Facilitation establishment (establishing a facilitation mechanism) **Compliance evidence**: Certificate of conformance with the Requirements for Facilitation Providers establishing facilitation mechanisms component of the Federation Assurance Standard.
Credential presentation	The steps for facilitating the presentation of credentials by users to relying parties. **Rules****: SF.2: Credential Presentation **Compliance evidence**: Certificate of conformance with the Requirements for the presentation of Credentials by Facilitation Providers component of the Federation Assurance Standard.
**Providers will additionally need to comply with Rules set in Authorisation Rules, Privacy and Confidentiality Rules, Security and Risk Management Rules, and Information and Data Management Rules sections.	

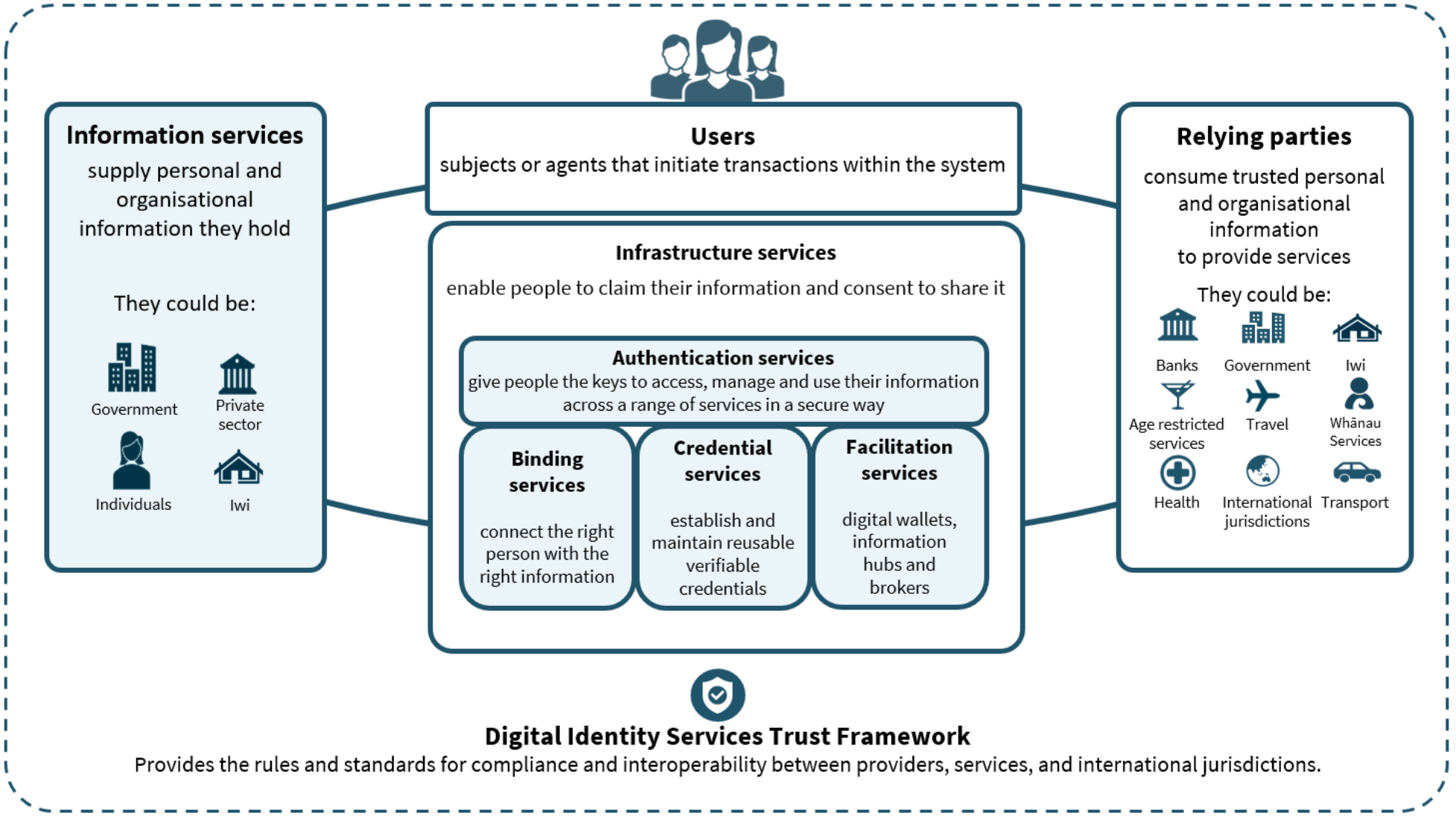
Digital Identity Services Trust Framework roles

The Digital Identity Services Trust Framework compromises multiples roles. The table below describes the different roles and participants.

Role	Description
User	A User is an individual who initiates a digital identity service. They may be the subject, or an agent. Where the subject is an organisation, the user will be an agent.
Subject	A subject is the entity that is the focus of the personal or organisational information being shared through a digital identity service. This maybe an individual or organisation.
Agent	An agent is an individual who acts on behalf of the subject to initiate digital identity transactions.
Relying Party	Relying parties consume personal and organisational information to provide one or more functions of their business.

Role	Description
Credential Provider	Credential providers deliver a Digital Identity Services Trust Framework Credential Service.
Facilitation Provider	Facilitation providers deliver a Digital Identity Services Trust Framework Facilitation Service.
Information Provider	Information providers deliver a Digital Identity Services Trust Framework Information Service.
Binding Provider	Binding providers deliver a Digital Identity Services Trust Framework Binding Service.
Authentication Provider	Authentication providers deliver the Digital Identity Services Trust Framework Authentication Service.
Trust Framework Provider	Trust Framework providers deliver one or more DISTF accredited services.

The diagram on the following page visually represents the digital identity system. More information on the digital identity system can be found on www.digital.govt.nz.


Information services
supply personal and organisational information they hold
They could be:
Government
Private sector
Individuals
Iwi
Users
subjects or agents that initiate transactions within the system
Infrastructure services
enable people to claim their information and consent to share it
Authentication services
give people the keys to access, manage and use their information across a range of services in a secure way
Binding services
connect the right person with the right information
Credential services
establish and maintain reusable verifiable credentials
Facilitation services
digital wallets, information hubs and brokers
Relying parties
consume trusted personal and organisational information to provide services
They could be:
Banks
Government
Iwi
Age restricted services
Travel
Whānau Services
Health
International jurisdictions
Transport
Digital Identity Services Trust Framework
Provides the rules and standards for compliance and interoperability between providers, services, and international jurisdictions.

Identification Management Rules

Category Scope

All personal and organisation information transacted through the Digital Identity Services Trust Framework needs to go through robust process to ensure its level of accuracy and quality.

This category sets out the requirements for verifying and binding personal information and establishing a credential, including providing levels of assurance for the information being presented.

This category requires the application of the following standards:

Standard, protocol, or data model	Version
Information Assurance Standard	Version 1 (effective 1 March 2021) or later
Binding Assurance Standard	Version 1 (effective 1 March 2021) or later
Authentication Assurance Standard	Version 1 (effective 1 March 2021) or later
Federation Assurance Standard	Version 2 (1 February 2022) or later
W3C Verifiable Credential Data Model	Version 1.1 or later
ISO/IEC 18013-5:2021 Personal identification ISO-compliant driving licence Part 5: Mobile driving licence (mDL) application	Status: Published (September 2021 or later)

Detailed guidance for implementing the Identification Management Standards is also available to support conformance.

When applying the Identification Management Standards, the TF provider acts in place of the relying party when referenced in the standards.

Category Outcomes

- Users and relying parties of digital identity services have confidence that personal and organisational information shared is secure, supports privacy protection, and is known to be accurate.
- Trust Framework providers share personal and organisational information that includes declared levels of assurance to ensure relevancy and security.

- The levels of assurance cover information assurance, binding assurance, and authentication assurance.

- Trust Framework providers can establish relevant levels of assurance for information which enable and support te ao Māori approaches to identity.
- Trust Framework providers can **establish** and **manage** credentials through trusted, people-centred, and inclusive services.

Category Rules

IM.1: Verifying information.

Objective: The accuracy for information is determined.

Rule no.	Rule
IM1.1	All attributes MUST have a level of information assurance established in accordance with the *Information Assurance Standard* under the *Identification Management Standards.*

IM.2: Entity binding.

Objective: The strength of binding between the information and the subject is known.

Rule no.	Rule
IM.2.1	All attributes MUST have a level of binding assurance established in accordance with the *Binding Assurance Standard* under the *Identification Management Standards.*
IM.2.2	Attributes where the subject is an organisation, do not require a level of binding assurance. The level of binding assurance should be blank in this instance.

IM.3: Authenticator binding and registration.

Objective: The strength of authenticator is sufficient for the bound information.

Rule no.	Rule
IM.3.1	Authenticator binding and registration MUST be in accordance with the *Binding Assurance Standard – Requirements for Authenticator Binding* under the *Identification Management Standards* for all attributes.

IM.4: Authentication.

Objective: The authenticator remains solely in the control of its holder (the user).

Rule no.	Rule
IM.4.1	All attributes MUST have a level of authentication assurance established in accordance with the *Authentication Assurance Standard* under the *Identification Management Standards.*

IM.5: Credential establishment and issuance.

Objectives:

- Established credentials are trusted, verifiable, reusable, and interoperable.
- Credentials are managed and maintained to ensure ongoing reliability and safe use.

Rule no.	Rule
IM.5.1	All attributes on a credential MUST be verified at the time the credential is established.
IM.5.2	All attributes on a credential MUST be bound to an entity at the time the credential is established.
IM.5.3	All attributes on a credential MUST have an authenticator registered to them.
IM.5.4	All credentials MUST be revocable by the credential provider.
IM.5.5	Users MUST be able to request revocation of a credential issued to them. Revocation must occur as soon as practicable after the user has made the request.
IM.5.6	Subjects MUST be able to request revocation of a credential containing their personal information, or organisational information, if the subject is an organisation.
IM.5.7	Revocation MUST occur as soon as practicable after the user has made the request.
IM.5.8	When issued, credentials MUST not require users to adopt a specific facilitation mechanism.
IM.5.9	All credentials MUST be verifiable for authenticity by relying parties.
IM.5.10	Credential verification methods MUST be encrypted.
IM.5.11	Credential verification activity MUST not be tracked or correlated by the credential provider.

Rule no.	Rule
IM.5.12	All credentials MUST be formatted in accordance with the specifications, controls, models and standards set out in: • W3C Verifiable Credential Data Model v1.1 (or newer version holding recommended status); or • ISO 18013-5: Mobile driving licence (mDL) application (published version).
IM.5.13	All credentials MUST conform with the controls set out in the **Federation Assurance Standard - Requirements for Credential Providers establishing Credentials** with the following additional modifications: • Control FA3.02 is MUST (expiry date) • Control FA5.07 is MUST (selective disclosure).
IM.514	Credential providers MUST publish the standards and formats their service supports on a publicly available website.

End of Identification Management Category.

Sharing and Facilitation Rules

Category Scope

All digital identity service transactions need to be authorised by an individual that has the relevant authority to do so. Users need to be appropriately informed of what they are authorising, and authorisations should be recorded by Trust Framework providers. The sharing and facilitation category sets out requirements for:

- obtaining user authorisation to undertake a digital identity service.
- establishing a facilitation mechanism (a service such as a digital hub, or a tool such as a digital wallet) to help the user claim and share their credentials.
- facilitating the sharing (presenting) of credentials to relying parties.

This category requires the application of the following standards:

Standard, protocol, or data model	Version
Federation Assurance Standard	Version 2 (1 February 2022) or later
W3C Verifiable Credential Data Model	Version 1.1 or later
ISO/IEC 18013-5:2021 Personal identification ISO-compliant driving licence Part 5: Mobile driving licence (mDL) application	Status: Published (September 2021 or later)

Category Outcomes

- Facilitation mechanisms established by Trust Framework providers are well managed, trusted, people-centred, and inclusive.
- Users of digital identity services have confidence that personal and organisational information is only shared with their authorisation.

Facilitation Rules

SF.1: Facilitation establishment (establishing a facilitation mechanism)

Objective:

- Relying parties can trust the relationship between a user, an authenticator, and the information being collected, held, and maintained through the mechanism.
- Users can securely hold credentials in a facilitation mechanism accessible only to them.

Rule no.	Rule
SF.1.1	Facilitation mechanisms MUST be established in accordance with the **Federation Assurance Standard - Requirements for Facilitation Providers establishing facilitation mechanisms.**
SF.1.2	Facilitation mechanisms MUST be able to hold credentials of a at least one of credential formats listed in **Rule IM.5.12.**
SF.1.3	Users MUST be able to remove a credential a facilitation mechanism at any time.
SF.1.4	Facilitation providers MUST publish the standards and formats their service supports on a publicly available website.

SF.2: Credential Presentation

Objective: Trust Framework providers facilitating the sharing of credentials can:

- support users to make informed decisions about sharing their personal or organisational information to access relying party services.
- facilitate the exchange of information in secure, and privacy-preserving ways.
- support the user's option to choose which services they engage to share their personal or organisational information with relying parties.

Rule no.	Rule
SF.2.1	All credential presentations MUST be authorised by the user to be presented**.**
SF.2.2	All credential presentations MUST comply with the following: - W3C Verifiable Credential Data Model v1.1 - ISO 18013-5: Mobile driving licence (mDL) application (published version).
SF.2.3	Credential presentations MUST meet the **Federation Assurance Standard - Requirements for the presentation of Credentials by Facilitation Providers.**
SF.2.4	Credential presentation MUST only present attributes the user has chosen to present.

Authorisation Rules

AN.1: Requirement to authorise

Objective: Users are confident that no digital identity service will be undertaken without their authorisation.

Rule no.	Rule
AN.1.1	The following digital identity service activities MUST be authorised by users: • Verifying information • Entity binding • Credential establishment and issuance • Facilitation mechanism establishment • Credential presentation.
AN.1.2	Trust Framework Providers MUST receive valid authorising before undertaking activities that require authorisation under Rule AN.1.1

AN.2: Valid authorisation

Objective: Users and Trust Framework providers are confident that the authorisations are valid.

Rule no.	Rule
AN.2.1	An authorisation for a digital identity service activity to be undertaken MUST ONLY be considered valid if: • The authorisation is provided by a user permitted to authorise the digital identity service to be undertaken; and • The user has been informed about what they is authorising; and • The Trust Framework provider who sought the authorisation, has recorded the details of the authorisation.
AN.2.2	Trust Framework providers MUST NOT require the user to provide authorisation, consent or permission for any activity not directly related to the digital identity service being undertaken.

AN.3: Permitted user

Objective: Authorisations are given by users who have the appropriate authority to provide them.

Rule no.	Rule
AN.3.1	A user MAY be considered **permitted** to authorise a digital identity service to be undertaken, ONLY if: • The subject is the user providing the authorisation, or • The subject is an individual or organisation for whom the user has authority to act on behalf of.
AN.3.2	An authorisation to present a credential MUST only be provided by the user the credential has been established for (or issued to).

AN.4: Informed authorisation

Objective: Users are informed by Trust Framework providers of relevant information before providing an authorisation.

Rule no.	Rule
AN.4.1	All Trust Framework providers requesting an authorisation for verifying information and/or entity binding from a user MUST notify the user of the following: • the digital identity service(s) that will be undertaken; and • the personal or organisational information that will be collected or used to undertake the service(s); and • the organisations will be carrying out each service, including their accreditation status; and • where personal or organisational information and related data may be stored and processed.
AN.4.2	All Trust Framework providers requesting an authorisation to establish a credential from a user MUST notify the user of all the following: • the digital identity service(s) that will be undertaken. • the personal or organisational information that will be collected or used to undertake the service(s). • the digital identity providers will be carrying out each service, including their accreditation status. • the details of credential that will be established. • the terms of use for the credential. • where personal or organisational information and related data is stored and processed. • when the credential will be established and available for the user. • how to cancel or revoke the credential from further use. • how to report misuse of the credential.

Rule no.	Rule
AN.4.3	When a user initiates to present a credential, the facilitation mechanism MUST notify the user of all the following: • the credential to be shared. • the relying party whom the credential is being presented to (if not being [presented in person). • any authentication or binding checks that may happen, including which provider(s) will be carrying out each process, and their accreditation status. • appropriate warning about sharing their information, including their obligations for keeping their information safe.

AN.5: Authorisation record

Objective: Appropriate records of authorisations are retained.

Rule no.	Rule
AN.5.1	All Trust Framework providers MUST record sufficient information to support an investigation into the activity, in the event the authorisation is found to be fraudulently provided.

End of Sharing and Facilitation Category.

Privacy and Confidentiality Rules

Category Scope

Users need to have confidence that providers are using their information appropriately and incorporating privacy-protecting measures across the entire information lifecycle, from collection through to use, sharing and disposal within the ecosystem.

The Trust Framework Privacy Rules supplement the requirements under the Privacy Act and do not replace any existing obligations. Participants are expected to familiarise themselves and must comply with all their legal requirements.

Category Outcomes

- Users have confidence that Trust Framework providers are taking a proactive and preventative approach to embed privacy across their organisation.
- Trust Framework providers embed user-centric design principles to ensure that users can exercise control over their information and maintain visibility over its use.

Category Rules

PV.1: Minimising privacy risks

Objective: All Trust Framework providers have undertaken assessments of privacy risks. Processes are developed and implemented to ensure that the risk of privacy incidents are minimised.

Rule no.	Rule
PV.1.1	All Trust Framework providers MUST comply with their obligations under the Privacy Act, including the Information Privacy Principles.
PV.1.2	All Trust Framework providers MUST complete a privacy impact assessment for the digital identity service(s) they provide as part of accreditation.
PV.1.3	The privacy impact assessment MUST include all of the following: • detailed service description. • information already held and new information to be collected. • the purpose for which the information is collected. • a map of the information flows. • how information will be stored, accessed, and disposed of by the accredited provider. • an analysis of mitigations for all risks identified. • consultation with relevant stakeholders.

Rule no.	Rule
PV.1.4	All Trust Framework providers MUST review the privacy impact assessment at the earlier of the following: • two years from the previous review, or • when there is a change to the digital identity service(s).
PV.1.5	All Trust Framework providers MUST have a designated individual(s) who is responsible for: • overseeing the privacy impact assessment process and review. • ensuring compliance with all applicable laws, regulations, and codes. • managing privacy policies. • monitoring privacy risks and compliance.
PV.1.6	All Trust Framework providers MUST ensure personnel receive regular training on privacy policies including: • lawful purposes and uses for personal and organisational information collected and held by the accredited provider. • processes to amend or update user's information when requested by a user. • processes regarding storage and disclosure of information. • awareness of privacy complaints and incidents procedures.
PV.1.7	All Trust Framework providers MUST ensure personnel receive communications regarding any changes to privacy policies and processes.
PV.1.8	All Trust Framework providers MUST maintain a documented privacy incident response plan.
PV.1.9	The privacy incident response plan MUST: • clearly assign roles and responsibilities. • set out escalation and notification processes. • processes to contain and assess the incident.
PV.1.10	All Trust Framework providers MUST establish an incident register and provide instructions for personnel to record privacy incidents.
PV.1.11	All Trust Framework providers MUST review their incident register on a regular basis and ensure applicable processes and policies are updated accordingly.
PV.1.12	All Trust Framework providers MUST have privacy statement.
PV.1.13	If a Trust Framework provider is collecting information for the purpose of undertaking a digital identity service transaction, then the provider MUST NOT use the information for any other purpose unless they are provided explicit authorisation of the user.

End of Privacy and Confidentiality Category.

Security and Risk Management Rules

Category Scope

Strong security and risk management ensure that personal and organisational information is stored, shared, and used in a secure manner.

By ensuring that there is clear accountability for security across a whole organisation, users can be assured that Trust Framework providers will maintain the confidentiality, integrity, and availability of the information that they process, store and share.

Category Outcomes

- Trust Framework providers embed strong governance practices to identify, manage and respond to security risks.
- Trust Framework providers embed information security practices to reduce the risks of information being lost, damaged, or compromised.
- Trust Framework providers can demonstrate that they have embedded practices to protect physical assets from damage or loss that would compromise the integrity of their digital identity services.
- Trust Framework providers embed practices to reduce the risk of harm to personnel, users and partners that would compromise the integrity of their digital identity services.

Table of risks

A table of risks is included at the end of this category. The application of these Rules and other measures applied by Trust Framework providers are expected to mitigate these risks.

Category Rules

SR.1: Security Governance

Objective: Trust Framework providers have embedded strong governance practices to identify, manage and respond to security risks. This includes:

- established clear procedures and plans to identify and manage risks.
- established clear processes to deal with security incidents.

Rule no.	Rule
SR.1.1	All Trust Framework providers MUST develop and implement a security management plan which: • identifies your people, information, and assets in relation to digital identity services provided, and their associated risks. • assesses the likelihood and impact of risks occurring. • assesses adequacy of existing safeguards. • determines which measures are likely to reduce or eliminate risks; and • implements security measures to reduce risks to acceptable level.
SR.1.2	All Trust Framework providers MUST complete a security risk assessment for the digital identity service(s) provided to inform the security management plan.
SR.1.3	The security risk assessments MUST, at a minimum, include assessments and mitigations for all the following risks as applicable to the service being provided: • weak human resource security. • insufficient incident response. • insecure facilitation mechanism. • credential loss due to device or facilitation mechanism failure. • insecure API endpoints. • service provider outage. • compromise of trust framework provider infrastructure. • security of hosting services. • weak service provider access controls. • credentials unable to be verified. • unauthorised usage of valid credentials.
SR.1.4	All trust framework providers MUST undertake an independent assessment to validate security risks are maintained appropriately.
SR.1.5	All trust framework providers MUST have a designated individual(s) who is responsible for identifying and managing security risks.
SR.1.6	All trust framework providers MUST review their security management plan at the earlier of the following: • two years from the previous review. • when there is a change in their structure, function, or activities.

Rule no.	Rule
SR.1.7	The security management plan review MUST: • determine the adequacy of existing policies, procedures, and mitigations. • be updated to respond to any changes regarding risks, threats, and operating environment.
SR.1.8	All Trust Framework providers MUST develop and implement a business continuity plan which covers: • functions in relation to digital identity service(s). • recovery requirements for systems. • identify and backup vital records. • testing requirements and restoration procedures.
SR.1.9	All Trust Framework providers MUST have documented instructions and procedures to assist personnel to identify, report and respond to security incidents.
SR.1.10	All Trust Framework providers MUST have documented policies and procedures for investigating security incidents.
SR.1.11	All Trust Framework providers MUST establish an incident register and provide instructions for personnel to security incidents.
SR.1.12	All Trust Framework providers MUST record at least the following information regarding security incidents: • time, date, and country of origin. • description of the circumstances. • whether the incident was deliberate or accidental. • an assessment of the degree of compromise or harm. • a summary of actions taken to resolve the incident.
SR.1.13	All Trust Framework providers MUST report significant cyber security incidents related to accredited digital identity services to the Trust Framework Authority.

SR.2: Information security processes

Objective: Trust Framework providers have established information security processes to reduce the risks of information being lost, damaged, or compromised. Providers have:

- identified relevant information and implemented appropriate security measures, and
- established processes to record and investigate internal security incidents.

Rule no.	Rule
SR.2.1	All Trust Framework providers MUST assess the identified information and systems with regards to their value, importance, and sensitivity.
SR.2.2	All Trust Framework providers MUST have processes in place to assess that their information security measures have been correctly implemented.
SR.2.3	All Trust Framework providers MUST have processes to ensure their security measures are fit for purpose by: • monitoring systems, networks, and processes for vulnerabilities. • keeping up to date with evolving threats.
SR.2.3	If information is no longer required, Trust Framework providers MUST ensure information is archived, destroyed, or disposed of securely and appropriately.
SR.2.4	All Trust Framework providers MUST have procedures to: • identify changes to normal behaviour. • determine the extent and impact of anomalous behaviour on data confidentiality, integrity or privacy breaches.
SR.2.5	All Trust Framework providers MUST collect and keep sufficient information security events to support audits, investigations and incident management, including: • external breaches. • insider threats. • longer-term persistent threats.
SR.2.6	All Trust Framework providers MUST separate, protect and store event logs and analysis capabilities to ensure the availability, accuracy and integrity of the information captured and held.
SR.2.7	All Trust Framework providers SHOULD protect digital information and systems using cryptographic products, algorithms and protocols that are approved by the GCSB as set out in Chapter 17 of the NZISM.
SR.2.8	All Trust Framework providers MUST securely manage cryptographic keys used in their digital identity services following a documented Key Management Plan.
SR.2.9	The Key Management plan MUST cover: • key management lifecycle. • system description. • records maintenance and audits.

SR.3: Physical security

Objective: All Trust Framework providers can demonstrate the steps taken to protect physical assets from damage or loss that would compromise the integrity of their digital identity services.

Rule no.	Rule
SR.3.1	All Trust Framework providers MUST minimise or eliminate, so far as is reasonably practicable, the risk of plant and structures being maintained, accessed, used, or removed without appropriate authority.
SR.3.2	All Trust Framework providers MUST implement physical security measures in line with identified threats, vulnerabilities and risk appetite.
SR.3.3	All Trust Framework providers MUST have processes in place to assess that their physical security measures have been correctly implemented.
SR.3.4	All Trust Framework providers MUST have processes to assess and respond to evolving threats or vulnerabilities, and ensure physical security measures remain fit for purpose.

SR.4: Personnel security

Objective: All Trust Framework providers have established processes to reduce the risk of harm to personnel, users and partners that would compromise the integrity of their digital identity services.

Rule no.	Rule
SR.4.1	All Trust Framework providers MUST ensure the eligibility and suitability of personnel who have access to information and systems that support operations relevant to digital identity service(s).
SR.4.2	All Trust Framework providers MUST have processes to manage and assess the ongoing suitability of its personnel.
SR.4.3	All Trust Framework providers MUST have processes to manage changes in roles or the departure of personnel, including: • removal of access rights to physical and electronic resources. • return of assets.
SR.4.4	All Trust Framework providers MUST set up Trust Framework role-based access management protocols.
SR.4.5	All Trust Framework providers MUST ensure personnel receive communications regarding security policies, including: • responsibilities. • issues and concerns.

SR.4.6	All Trust Framework providers MUST ensure personnel receive appropriate and up-to-date security training.

Security Risks

The table below presents key risk associated with digital identity services. Trust Framework providers are expected to apply mitigations to these risks, and supply evidence of these mitigations when seeking accreditation.

Risk no.	Risk and Description
DIS.R01	**Weak Human Resource Security** A digital identity service providers' environment is intentionally or unintentionally compromised by a malicious staff member. This is due to weak security awareness training and security vetting, and may lead to information disclosure, modification, loss, or system outages.
DIS.R02	**Insufficient Incident Response** A security incident occurs at a digital identity service provider that is not responded to in a timely and effective manner. This is due to weak incident response processes, and may lead to information disclosure, modification, loss, or system outages.
DIS.R03	**Insecure Facilitation Mechanism** A digital identity facilitation mechanism is compromised due to vulnerabilities being present within its source code. This is due to insecure development practices, and may lead to information disclosure, modification, or loss.
DIS.R04	**Credential Loss due to Device or Facilitation Mechanism Failure** A digital identity facilitation mechanism is no longer accessible due to the device it was held on being lost or destroyed. Therefore, the credentials within the facilitation mechanism are no longer usable. If credentials are unable to be securely regenerated or migrated within a reasonable time, a user may be left with no digital credentials and not be able to access services they require.
DIS.R05	**Insecure API Endpoints** An API endpoint that is used by a digital identity service is compromised due to an insecure authentication or authorisation mechanism being implemented. This may lead to unauthorised access to or modification of personal information.
DIS.R06	**Service Provider Outage** A disaster or large duration outage occurs, causing disruptions at a Trust Framework provider. The provider is not able to maintain or restore its services in a reasonable amount of time. This may lead to prolonged service outages.

Risk no.	Risk and Description
DIS.R07	**Compromise of Provider Infrastructure** A Trust Framework provider's infrastructure is compromised due to inadequate host maintenance, patching, updating, and hardening. This may lead to information disclosure, modification, loss, or system outages.
DIS.R08	**Security of Hosting Services** A Trust Framework provider is compromised due to a datacentre breach, or compromise of their cloud service provider. This may lead to information disclosure, modification, loss, or system outages.
DIS.R09	**Weak Service Provider Access Controls** Technology components that deliver a digital identity service and protect its data are compromised due to weak access controls. This may lead to information disclosure, modification, loss, or system outages.
DIS.R10	**Credentials Unable to be Verified** The mechanism used to sign credentials for authenticity expires or becomes unavailable due to inappropriate management. This leads to user credentials expiring and unable to be used for verification.
DIS.R11	**Unauthorised usage of Valid Credentials** A facilitation mechanism holding digital identity credentials is maliciously used by an unauthorised person. This is due to insecure access controls being in place to secure the facilitation mechanism and it may lead to the misuse of digital credentials and theft of identity.

End of Security and Risk Management Category.

Information and Data Management Rules

Category Scope

Personal and organisational information being collected, held and shared within the Trust Framework can be managed in commonly accepted ways that meet industry good practice standards.

There are commonly accepted requirements for information management practices. Trust Framework providers should implement these practices, including appropriate governance, information lifecycle management, and recordkeeping and reporting for information and data. Consideration should also be given for ethical handling of information and data.

Having robust, commonly accepted data and information management practices in place supports mutual trust among providers and users, as well as interoperability of the digital identity services.

Category Outcomes

- Trust Framework providers can access and re-use personal and organisational information using common approaches, frameworks and good practice guidelines that support interoperability.
- Users have confidence that trust framework providers have prioritised users' rights to access, control and manage their information according to their personal, cultural, and organisational choices.
- Trust Framework providers demonstrate they understand and support information and data management good practices.

Category Rules

IF.1: Information and Data Governance

Objective: Trust Framework providers have good practices for managing digital identity information and data safely and securely.

Rule no.	Rule
IF.1.1	All Trust Framework providers MUST develop and implement an information and data management plan that covers requirements for handling information and data used in the digital identity service(s) they provide.

Rule no.	Rule
IF.1.2	The information and data management plan MUST: • define risks around the information and data that is stored and shared. • detail practices for managing information and data, including managing information and data ethically. • detail practices for recordkeeping, including details records, methods of retention and period of retention. • include retention and disposal schedules for personal and organisational information intended to be shared within the Trust Framework.
IF.1.3	All Trust Framework providers MUST have a designated individual(s) responsible for maintaining the information and data management plan and overseeing its implementation and operation.
IF.1.4	All Trust Framework providers MUST review their information and data management plan at the earlier of the following: • two years from the previous review. • when there is a change to the digital identity service(s).

IF.2: Managing information ethically

Objective: All Trust Framework providers have practices in place to manage culturally sensitive personal and organisational information to minimise the potential to cause harm to individuals, or organisations.

Rule no.	Rule
IF.2.1	The practices for managing information ethically in the information and data management plan MUST include: • considerations of Māori cultural perspectives. • specific kaitiakitanga requirements when handling Māori information.
IF.2.2	All Trust Framework providers MUST inform users of where personal or organisational information and related data is stored and processed.

IF.3: Recordkeeping

Objective: All Trust Framework providers have established good practice recordkeeping processes that provide consistency, transparency and trust in their information management processes at each stage of the information's life cycle.

Rule no.	Rule
IF.3.1	The practices for recordkeeping outlined in the information and data management plan MUST include details to support investigations or analysis of compliance of their digital identity service.
IF.3.2	Information about a digital identity service transaction MUST be retained for the retention period set by the Digital Identity Services Trust Framework Regulations unless there is a legislative requirement to retain for a different period.
IF.3.3	All Trust Framework Providers MUST inform the Trust Framework Authority if a retention period different to the one set by Digital Identity Services Trust Framework Regulations applies to their service.

End of Information and Data Management Category.

End of Digital Identity Services Trust Framework Rules.

Glossary

This glossary provides a list of terms and descriptions that appear in the Digital Identity Services Trust Framework documentation. The meanings reflect the current use of the terms within the Trust Framework's context only. Terms that are used with their standard English dictionary meaning may not have been included.

Glossary of terms

Term	Description
Accreditation	The approval of a digital identity service that has demonstrated that it meets the applicable requirements of the Trust Framework.
Accredited digital identity service	A digital identity service that is accredited by the Trust Framework Authority to be provided by a particular Trust Framework provider.
Attribute	A piece of information that describes something about an Entity (for example, an individual's name, address and whether they are resident in a particular place are all attributes about the individual).
Agent	An individual who initiates a transaction on behalf of another subject through an established delegation.
Authentication	A process for establishing that an Authenticator is genuine or as represented.
Authentication assurance	The degree of certainty that the current request is being made by the original entity.
Authenticator	One or more things known and/or possessed and controlled by a User (such as a password, a code, a piece or software or a device) that the User can use to access a service or other thing online.
Authenticity	In relation to a credential, means the credential confirmation of active or revocation status.
Binding	A process carried out to validate the connection between an Entity and information about that Entity or an authenticator to a level of assurance or confidence.
Binding assurance	The degree of certainty that the Entity information relates to the Entity claiming it.
Credential	A record kept in digital form that: (a) is issued to an Entity and held by a holder; (b) describes a set of attributes or properties of the Entity or another Entity the holder represents; and (c) is bound to an Authenticator.

Term	Description
Conformance	The outcome of verifying that a standard or technical specification was applied to design and/or delivery of digital identity services.
Data minimisation	The act of: (a) limiting the collection and holding of personal information; (b) minimising identifiability, observability, and link-ability of personal information when it is shared.
Derived value, or derived assertion, or derived predicate.	A value deduced or inferred from information in a credential.
Digital Identity Authentication Service, or authentication service	A digital identity service that: • ensures the connection of a user to an authenticator, AND • secures the sharing of personal or organisational information between trust framework participants by ensuring the authenticator(s) are possessed and controlled by an authorised holder.
Digital Identity Binding Service, or binding service	A digital identity service that ensures the connection (binding) of personal or organisational information to an individual or organisation.
Digital Identity Credential Service(s), or credential service(s)	A digital identity service that: • combines bound information and an authenticator to establish a trusted reusable credential, AND • maintains a trusted reusable credential.
Digital Identity Facilitation Service(s), or facilitation service(s)	A digital identity service that assists Users to share or present credentials with Relying Parties.
Digital Identity Information Service, or information service	A digital identity service that provides an assessment of the accuracy of personal or organisational information.
Digital Identity Service	A service or product provided by a digital identity service provider and that, either alone or together with 1 or more other digital identity services, enables the sharing of personal or organisational information in digital form by a user in a transaction with a relying party.
Digital Identity Service Activity	A required action or process undertaken to complete part of, or all of, a digital identity service.
Digital Identity Service provider	An individual or organisation who or that provides a digital identity service, whether the provider or service is accredited under this Act or not.

Term	Description
Digital Identity Services Trust Framework, or the Trust Framework	The legal framework to be established to regulate the provision of digital identity services for use in transactions between individuals and organisations.
Digital Identity System	An interconnected system for the exchange and verification of Entities' attributes, involving: (a) Trust Framework providers; (b) Users; and (c) Relying Parties.
Entity	Something that has separate and distinct existence and that can be identified in a particular context, such as: (a) an individual; or (b) an organisation.
Facilitation	Processes that support users to claim, hold and manage their credentials, and to share or present their credentials with relying parties.
Facilitation mechanism	A service or tool that can facilitate the presentation of 1 or more Credentials (fully or partially) in response to a request from a Relying Party. Examples include digital wallets or an exchange.
Identification management	Determining the accuracy of information, binding that information to the correct individual or organisation, and enabling the secure reuse of the information.
Information and data management	For record keeping and format of personal and organisational information, to ensure a common understanding of what is shared.
Information assurance	The degree of certainty attached to the reliability of the quality and accuracy of the Entity information.
Level of assurance	An indicator of the robustness of the identification processes taken to establish an entity's information. See Identification Management Standards.
Metadata	A type of data describing context, content and structure of data and its management through time.
Organisation	Any organisation, whether public or private, and whether incorporated or not.
Organisational information	Information relating to a particular organisation.
Participants	For the purposes of the Trust Framework, means (a) Users (b) Trust Framework providers (c) Relying parties.

Term	Description
Personal information	Has the meaning given in section 7(1) of the Privacy Act 2020: (a) means information about an identifiable individual (b) includes information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages, and Relationships Registration Act 1995 or any former Act.
Personal or organisational information	Personal information or organisational information that describes: (a) the identity of an individual or organisation (b) other information about that individual organisation.
Portability	The capability to move credentials from one facilitation mechanism to another.
Privacy requirements	Ensuring the privacy and confidentiality of the information of individuals or organisations is maintained.
Relying party	An individual who or an organisation that relies on personal or organisational information shared in a transaction with a user through 1 or more digital identity services.
Revocation	The act of invalidating a credential before its expiration date.
Security and risk management	Ensuring information is secure and protected from unauthorised modification, use, or loss.
Security management plan	A plan of action that an organisation uses to address its security risk, based on the context in which the organisation operates and through threat and risk review.
Security risk	Any event that could result in the compromise, loss of integrity or unavailability of information or resources, or the deliberate harm to people measured in terms of its probability and consequences.
Security risk assessment	An activity undertaken to assess the security controls for a system and its environment to determine if they have been implemented correctly and are operating as intended.
Sharing and facilitation	Facilitating the sharing or presenting of credentials with relying parties including authorisation processes.
Subject	An Entity that is the focus of personal or organisational information.
Trust Framework Provider	A digital identity service provider who provides one (1) or more digital identity services that are accredited by the Trust Framework Authority.
TF Authority *or* Trust Framework Authority	The authority established under section 58 of the Digital Identity Services Trust Framework 2023.

Term	Description
TF Board *or* Trust Framework Board	The board established under section 43 of the Digital Identity Services Trust Framework 2023.
TF Register *or* Trust Framework Register	The register of Trust Framework providers and accredited services established under section 34 of the Digital Identity Services Trust Framework 2023.
Transaction	the action of conducting one or more digital identity services.
User	An individual who: (a) shares personal or organisational information in a transaction with a relying party through 1 or more accredited digital identity services; and (b) does so for themselves or on behalf of another individual or an organisation.
Verifiable credential	A tamper-evident credential that has authorship that can be cryptographically verified.
Verifiable presentation	A tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification.