Digital Identity Services
Trust Framework Authority

Trust Framework Authority application guidance

V2.0 September 2025

Internal Affairs
Te Tari Taiwhenua

Te Kāwanatanga o Aotearoa
New Zealand Government

Contents

About this guidance

The Trust Framework Authority is the regulator for accredited digital identity services in Aotearoa New Zealand. The Trust Framework Authority is responsible for accrediting providers and their services, and for monitoring compliance with the Digital Identity Services Trust Framework legislation, and relevant parts of the Privacy Act 2020.

This guidance is for providers of digital identity services seeking accreditation as a Trust Framework provider and/or for digital identity service(s) under the Digital Identity Services Trust Framework.

If you have any questions about the application process or need assistance, please contact TFA@dia.govt.nz.

Disclaimer

The information in this document is intended as a guide only. This document is not a substitute for and does not alter the provisions of the Digital Identity Services Trust Framework Act 2023 (the Act), or any Regulations, Rules, or terms of use that are made pursuant to, or that relate to, the Act.

This document is not a substitute for independent professional advice, including legal advice.

The Trust Framework Authority and Department of Internal Affairs do not warrant or represent (expressly or otherwise) that the information is current, accurate or complete. The Trust Framework Authority and Department of Internal Affairs excludes all liability and/or responsibility to you and any other person for any loss or damage directly or indirectly resulting from the use of, or reliance on, any of the information, including (without limit) resulting from any error, deficiency, flaw in, or omission from, the information.

The Trust Framework Authority may add, remove, or otherwise alter the information in this document without notice. The Trust Framework Authority is not responsible for the content of any third party information, content, website or document referenced in this document.

Glossary

Term	Definition
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
Digital identity service	A service provided by a digital identity service provider that, either alone or together with one 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
Trust Framework Authority	Trust Framework Authority. An administering body established under section 58 of the Digital Identity Services Trust Framework Act 2023
Trust Framework Provider	An accredited provider of any digital identity service, as defined in section 5 of the Digital Identity Services Trust Framework Act 2023
Trust Framework Register	A published register of Trust Framework Providers and accredited digital identity services. The Trust Framework Register is available on the Department of Internal Affairs' Website.

Overview

The Trust Framework Authority accreditation process requires assessment of an application for accreditation against the Digital Identity Services Trust Framework legislation, and relevant parts of the Privacy Act 2020. Assessment determines if the provider's digital identity service and the provider meet the Trust Framework Authority's accreditation requirements.

Accreditation is optional.

The Trust Framework accreditation mark enables everyone (including relying parties and potential users) to identify which services have been accredited. Users can be confident that accredited services are trustworthy and will protect their personal information.

Accreditable services

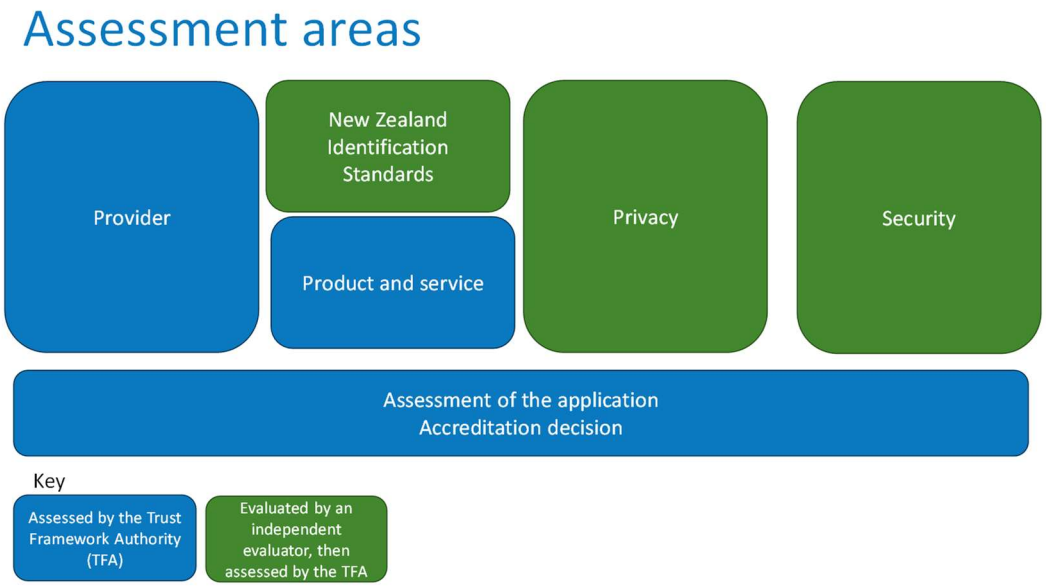
There are five digital identity service types which may be accredited:

- **Information service** - A service that provides:
    - Personal or organisational information; and
    - A level of assurance as to the accuracy of that information.
- **Binding service** - A service that binds personal or organisational data.
- **Credential service** - A service that creates a reusable credential.
- **Authentication service** – A service that enables a person to use an authenticator to access another service, for example a log-in service or a 2–factor authentication service.
- **Facilitation service** - A service that enables a person to present a credential to a relying party.

You can apply for accreditation of more than one digital identity service type in the same application, if all the service types in the application relate to the same service/product offered by the provider.

If you are applying for accreditation of a credential service, all service types in the application must relate to the same credential. You can only apply for one credential per application.

An organisation that applies to become an accredited provider, but is not yet accredited, is referred to as a 'provider', or 'the applicant'. Providers that have been accredited by the Trust Framework Authority are referred to as a 'Trust Framework provider'.



Applications for accreditation are assessed across the following areas:

- **Provider** – The provider of the digital identity service(s) and its key people, with a focus on compliance with requirements set out in the Trust Framework legislation. This requires completion of the application form and provision of supporting documents and information as indicated in the application form.
- **New Zealand Identification Standards** – Applicants must obtain and provide either:
  - An assessment of conformance with the New Zealand Identification Standards from the Department of Internal Affairs, and supporting documents and information, OR
  - An identification management evaluation from an independent identification management evaluator, and supporting documents and information.
- **Privacy** – Focuses on compliance with the Privacy Rules and relevant parts of the Privacy Act 2020. Applicants must obtain and provide a privacy evaluation from an independent privacy evaluator.
- **Security –** Focuses on compliance with the Security and Risk Management Rules. Applicants must obtain and provide a security evaluation from an independent security evaluator.
- **Product and service –** This will be assessed per the information and documentation provided in support of the other areas, and through a demonstration of the service to the Trust Framework Authority.

Accreditation process

Step 1: Preparation

The provider should meet with a Trust Framework Group representative to scope and define the service and confirm that this is consistent with the service types that may be accredited.

The provider gathers evidence to illustrate that they meet the accreditation requirements for each of the five assessment areas.

This includes obtaining independent evaluations of identification management (or a conformance assessment against the New Zealand Identification Standards), privacy and security.

Step 2: Application

The provider submits their accreditation application to the Trust Framework Authority.

Step 3: Assessment

The Trust Framework Authority assesses the provider's application, working with the provider to clarify information and requesting more information if required.

The Trust Framework Authority determines the accreditation outcome.

Step 1: Preparing to apply

Define the service

The provider should meet with a Trust Framework Group representative to scope and define the service and confirm that this is consistent with the service types that may be accredited.

The representative will also answer any questions about the accreditation process. To start this process, contact TFA@dia.govt.nz.

The definition or scope of the service is needed for each of the independent evaluations.

Identification management evaluation / conformance assessment

Providers need to demonstrate sufficient competence in identity management. Applicants must obtain and provide either:

- An identification management evaluation from an independent identification management evaluator

  OR

- An evaluation of conformance with the New Zealand Identification Standards.

The evaluator will provide their evaluation to the provider, who then submits the evaluation to the Trust Framework Authority as part of their application for accreditation.

Engage an evaluator

Independent evaluators considered by the Trust Framework Authority to have the appropriate skills, knowledge and experience to conduct identification management evaluations can be found at https://www.dia.govt.nz/Trust-Framework-for-Digital-Identity-Independent-evaluators. The provider engages and pays for the independent identification management evaluator.

Alternatively, the evaluator for conformance with the Identification Standards is the Department of Internal Affairs (DIA). The relevant DIA team can be contacted at identity@dia.govt.nz. There is no charge for the conformance evaluation.

Evaluation

The provider sends the required documents and information to the evaluator (DIA or an independent evaluator listed on the TFA website). The documents required will depend on the Identification Standards being evaluated. The evaluator will be able to assist with identifying these.

Digital identity service type	New Zealand identification standards to be assessed against
Information service	Information Assurance Standard
Authentication service	Authentication Assurance Standard

Digital identity service type	New Zealand identification standards to be assessed against
Credential service	Federation Assurance Standard - Requirements for Credential Providers establishing Credentials
	Information Assurance Standard
	Authentication Assurance Standard
	Binding Assurance Standard
Facilitation service	Federation Assurance Standard - Requirements for Facilitation Providers establishing facilitation mechanisms
	Federation Assurance Standard - Requirements for the presentation of Credentials by Facilitation Providers
	Authentication Assurance Standard
Binding service	Binding Assurance Standard Information Assurance Standard

The evaluation will determine any remedial actions required to demonstrate sufficient competence in identification management. The provider may be asked to provide additional evidence and to give a demonstration of the service to the evaluator.

Prior to applying for accreditation, providers will need to address remedial actions identified in the evaluation and submit any additional evidence of compliance to the independent evaluator.

Finalise evaluation

The independent evaluator will complete the evaluation using the Independent Identification Management Evaluation template.

The provider will include the conformance statement or completed evaluation template in their application for accreditation, along with the information that was provided to the independent evaluator.

Independent privacy evaluation

Providers need to have a privacy evaluation conducted by an independent evaluator.

The independent privacy evaluation includes evaluation of compliance with:

- Part 4: Privacy Rules of the Trust Framework Rules
- Relevant parts of the Privacy Act 2020.

The privacy evaluation consists of a privacy impact assessment and evaluation of the effectiveness of key privacy requirements and expectations.

Independent evaluators considered by the Trust Framework Authority to have the appropriate skills, knowledge and experience to conduct privacy evaluations can be found on the independent evaluators webpage.

The provider engages the evaluator and pays for the evaluation.

The cost of the evaluation must be agreed with the evaluator and may depend on the readiness of the material for evaluation and complexity of the information.

The evaluator will provide their evaluation to the provider, who then submits the evaluation to the Trust Framework Authority with the remainder of their application.

Engage an evaluator

The provider must engage an independent evaluator from the list of evaluators considered by the Trust Framework Authority to have the appropriate skills, knowledge and experience to conduct privacy evaluations. The provider will negotiate fees and payment terms directly with the evaluator.

The independent privacy evaluator can support the provider to develop suitable privacy documentation that helps to ensure good delivery of privacy practices, if this is agreed between the evaluator and the provider as part of the engagement.

The provider may want the independent evaluator to develop their Privacy Impact Assessment for them. If so, they should let the independent evaluator know at the point they engage services as it will affect the scope of work.

Conduct privacy impact assessment

The privacy impact assessment may be conducted by the provider or by the independent evaluator.

The provider does not need to have their Privacy Impact Assessment independently evaluated if:

- it has been developed by one of the independent privacy evaluators considered by the Trust Framework Authority to have the appropriate skills, knowledge and experience to conduct privacy evaluations, and
- it relates specifically to the digital identity service for which accreditation is sought, and
- it has been completed in the last 12 months, and
- the independent privacy evaluator confirms it meets the requirements of the Trust Framework Authority as set out in the Trust Framework Authority privacy evaluation template and guidance.

Complete evaluation

The evaluation consists of:

- Evaluation of compliance with privacy expectations and requirements relevant to the digital identity service.

- Documentation of information used to inform the evaluation including documents, interviews, and additional evidence such as screen shots or notes from discussions.

The independent evaluator performs the evaluation based on material provided by the provider, along with any additional verification or information required (including, for instance, walk-throughs of processes or testing).

The independent evaluator completes their evaluation using the Trust Framework Authority independent privacy evaluation template.

Independent security evaluation

Providers need to have a security evaluation undertaken by an independent evaluator. The independent security evaluation includes evaluation of compliance with Part 5: Security and risk management of the TF Rules.

Independent evaluators considered by the Trust Framework Authority to have the appropriate skills, knowledge and experience to conduct security evaluations can be found on the independent evaluators webpage.

The provider engages the evaluator and pays for the evaluation.

The cost of the evaluation must be agreed with the evaluator and may depend on the readiness of the material for evaluation and complexity of the information.

The evaluator will provide their evaluation to the provider, who then submits the evaluation to the Trust Framework Authority.

Engage an evaluator

The provider will need to engage an independent evaluator to conduct the security evaluation. Providers will negotiate fees and payment terms directly with the evaluator.

One independent security evaluator should perform all aspects of the evaluation including reviewing and evaluating all documentation provided.

Agree scope

The provider and the evaluator will need to agree the scope of the independent evaluation. This must be consistent with the scope of service(s) for which accreditation is sought.

Scoping considerations include:

- the services that are in scope for the evaluation
- technical components in scope for the review
- geographic locations where the service is hosted
- anything that is out of scope of the evaluation and why
- any previously-conducted independent evaluations that have been conducted on the service and may be relied upon during this evaluation, when they were conducted, and the scope of these reviews.

In addition to including internal systems and networks in scope, connections from third-party entities need to be identified to determine inclusion in scope.

Similarly, if a provider outsources in-scope functions or facilities to a third party, or utilises a third-party service that impacts how it meets security requirements, the provider will need to work with the third party to ensure the applicable aspects of the service are included in scope.

For a previous evaluation to be used as an input to the security evaluation:

- The evaluation must have taken place in the last 12 months.
- The previous evaluation must be made available to the evaluator.
- The scope of the previous evaluation must be consistent with the scope of this evaluation.
- The independent evaluator makes the decision on whether the previous evaluation can contribute towards this evaluation.
- The evaluator may still wish to ask questions relating to a previous evaluation e.g. for an audit of compliance with ISO27001, the evaluator may want to see the policies evaluated.

The provider is required to list any other evaluations they want to use as evidence in the evaluation.

Conduct evaluation

The independent evaluator will perform the evaluation based on the material provided by the provider, along with any additional verification or information required (including, for instance, walk-throughs of processes or testing of controls).

The independent evaluator will complete their evaluation using the Trust Framework Authority independent security evaluation template.

Evaluation involves the following steps:

- Evaluation of compliance with the Security Rules. This is done through:
  - Interviews.
  - Walkthroughs.
  - Observations.
  - A review of technical evidence.
  - Detailed testing if needed.
- Confirming findings and remediations - Confirmation of the findings and their planned or actioned remediations that have been identified in the evaluation of the controls and risks.
- Documenting the information used and additional evidence - Documentation of information used to inform the evaluation including documents, interviews, and additional evidence such as screen shots or notes from discussions.

Address any significant remedial actions identified in the evaluation

The provider must address any significant remedial actions identified in the evaluation and submit any additional evidence of remediation to the independent evaluator**.**

Finalise evaluation

The independent evaluator will finalise the evaluation and issue the completed independent security evaluation.

Product and service assessment

For the product and service assessment, the provider will need to:

- prepare a detailed description of each of the services for which accreditation is sought
- supply their Data management plan
- complete the relevant Credential format questionnaire if the application is for a credential or facilitation service.

After receipt of an application by the Trust Framework Authority, the provider may also be invited to:

- provide a demonstration of the service
- a 'question and answer' session to answer questions in relation to the application.

Information and Data Management Plan

The requirements for an Information and data management plan are set out in Rule 17 of the Digital Identity Standards Trust Framework Rules.

Rule 18 sets out practices for managing information ethically. Under Rule 18(1) the information and data management plan must reflect Māori cultural perspectives and specific kaitiakitanga responsibilities working with Māori data.

Under Rule 18(2) all Trust Framework Providers must inform users if personal or organisational information and related data is to be stored and/or processed outside of New Zealand.

Detailed service description and demonstration

For both the detailed description of the service and the demonstration (if any), the Trust Framework Authority requires the provider to include:

- **Summary** – A brief overview of the service.
- **Service features** – A description of the service's features covering the end-to-end processes.

- **User experience** – How a user onboards to the service, and a description and screenshots of any user interfaces, how a user controls and manages their information, how to access user support and any additional user-related features.
- **User consent** – Processes and detail of how an individual is informed of the use of their personal information and provides informed consent for this use.
- **Interfaces** – All the connection points from the service to other service providers, users and relying parties. How the service preserves security, prevents unauthorised access to data, and privacy at these connection points.
- **Functionality** – How the service meets the specific functionality outlined below for informed authorisation by the user and the revocation of services.

Informed authorisation

Providers need to show or explain where the service asks for and receives valid user authorisation before undertaking the service, including recording the details of the authorisation and ensuring the user is:

- permitted to authorise the service
- informed of what they are authorising, including the specific information used to inform the user.

The Trust Framework Rules have several requirements relating to informed authorisation; in particular:

- Rule 11(1) Information, binding or authentication.
- Rule 11(2) Credentials.
- Rule 11(3) Facilitation.

Revocation

Providers will need to show or explain how a user can revoke a credential that has been issued to them.

The Trust Framework Rules have several requirements relating to revocation of credentials; in particular rule 8(3).

Credential format questionnaire

The Credential format questionnaire outlines how the provider complies with ISO 18013-5, 18013-7 and 23220 series and/or the W3C Verifiable Credentials Data Model. It is to be completed by providers of credential and facilitation services.

There are separate questionnaires available for credential and facilitation services. Providers complete a general section followed by sections relevant to the standard(s) that they comply with. All questions in the relevant section must be answered.

The Trust Framework Authority will provide the questionnaires to providers applying for accreditation if applicable for their application.

Step 2: Applying for accreditation

Once all the preparation outlined above has been carried out, an application for accreditation can be made. The Trust Framework Authority accreditation application form can be found on the Forms and guidance page of the Trust Framework Authority website.

This form must be completed by providers as part of the application process for:

- applications to be accredited as a Trust Framework provider and for a digital identity service to be accredited
- applications once a provider has already been accredited as a provider and for a digital identity service, for Trust Framework providers who want to apply for an additional digital identity service.

An application consists of the following completed documentation (each of these is available at https://www.dia.govt.nz/Trust-Framework-for-Digital-Identity-templates-and-guidance):

- Application form
- Delegations form (required to confirm that the person who completes the application to the Trust Framework Authority is authorised to act on behalf of the applicant)
- Independent identification management evaluation (or conformance assessment against the New Zealand Identification Standards), and supporting information and documentation provided to the evaluator to enable the evaluation
- Independent security evaluation, and supporting information and documentation provided to the evaluator to enable the evaluation
- Independent privacy evaluation, and supporting information and documentation provided to the evaluator to enable the evaluation
- Credential format questionnaire (if applicable; the Trust Framework Authority will confirm)
- Applicant's complaints and dispute resolution process(es) (per regulations 14-17 of the Digital Identity Services Trust Framework Regulations 2024)
- Detail on applicant's ownership structure, including ultimate beneficial ownership interests including jurisdictions and an organisational chart.
- Applicant's Information and data management plan.

Contact the Trust Framework Authority at TFA@dia.govt.nz who will provide a secure link to submit the application.

For New Zealand public agencies, upload documents with a security classification up to and including SENSITIVE. For documents with a higher security classification, contact the Trust Framework Authority to discuss access to these documents.

Step 3: Assessment

The Trust Framework Authority assesses the provider's application, working with the provider to clarify information and requesting more information if required.

The Trust Framework Authority determines the accreditation outcome.

Following accreditation

If accreditation is granted, the provider and service(s) will then be listed on the Trust Framework Register, and the provider will be able to use the accreditation mark in relation to accredited services in accordance with the Trust Framework Accreditation Mark Terms of Use.

Where accreditation of more than one digital identity service is applied for, the outcomes may be different for different services. A provider must be accredited for at least one digital identity service to be accredited.

Regular reporting will be required from accredited providers (for detail see https://www.dia.govt.nz/Trust-Framework-Authority-Maintaining-accreditation). Compliance and monitoring may also be undertaken by the Trust Framework Authority.

Declining accreditation

If the Trust Framework Authority declines an application or any part of an application, the provider can apply for a reconsideration of this decision. The provider must make the reconsideration application within 20 working days after receipt of the notice of the original decision. The Trust Framework Authority must consider any new, additional, or relevant information supplied by the provider and any decision made on the reconsideration will be final. However, an applicant can apply to a court for judicial review of the decision. An application form for a reconsideration is available on the Trust Framework Authority website.

Renewal of accreditation

Providers need to renew their accreditation every three years. Under section 31(2) of the Digital Identity Services Trust Framework Act 2023, if a renewal application is made before expiry of the current accreditation, then accreditation will continue until the renewal application is decided. Under section 31(3) of the Act, if the renewal application is not made prior to the expiry of the current accreditation, then a fresh application must be made for accreditation to continue.