Scope for independent security evaluation for [Provider name] and [Service name]

[Date]

V1.0 July 2025

# About this guidance

As regulator, the Digital Identity Services Trust Framework Authority (the Trust Framework Authority) assesses and accredits providers, and their services, against the Trust Framework rules and regulations.

Independent security evaluators play a role in the evaluation of providers seeking accreditation under the Digital Identity Services Trust Framework (the Trust Framework).

Independent security evaluators provide an evaluation on whether the provider meets the requirements of the Trust Framework Authority as set out in the [Digital Identity Services Trust Framework Rules 2024.](https://www.dia.govt.nz/diawebsite.nsf/Files/Trust-Framework/$file/DISTF-Rules-2024.pdf)

This template is for the provider and independent security evaluator to agree the scope for the evaluation.

The final assessment and accreditation decision will be made by the Trust Framework Authority.

If you have questions about the evaluation process or this guidance, or need assistance, please contact the Trust Framework Authority at [TFA@dia.govt.nz](mailto:TFA@dia.govt.nz).

# Scope details

This document records the security evaluation for [Provider name] for [Service name].

| Scope details | |
| --- | --- |
| Provider |  |
| Date submitted |  |
| Service name |  |
| Digital identity services applied for |  |
| Evaluator |  |
| Evaluator Organisation |  |
| Reviewer (if relevant) |  |
| Date evaluation completed |  |
| Template version | V1.0 |

# About this template

The purpose of this Security independent evaluation scoping template is to provide a tool to be completed by the provider and agreed with the independent evaluator to define and agree the scope of the security evaluation. It was developed to support the evaluation of providers who intend to undertake accreditation under the Trust Framework as a provider of digital identity services.

The content of this scope will be signed by both the provider and independent evaluator. This document is one of two documents to support the security evaluation. The document is shown in context in the diagram below.

The scope will be input to the **Security independent evaluation** and must be done prior to the start of the evaluation. Any changes to the scope identified during the evaluation should subsequently be updated into this scope document.

## Purpose

The purpose of this document is to define and agree the scope of the security evaluation between the provider and the independent evaluator. This is to support the evaluation of providers who intend to undertake accreditation under the Trust Framework as a provider of digital identity services.

## Service overview

Provide an overview of the service in scope including a high-level diagram of the service and the key components considered in scope.

## Scope

The following digital identity services are in scope for this evaluation: Remove any services not in scope

* Information service
* Binding service
* Credential service
* Authentication service
* Facilitation service

The following technical components are in scope of the evaluation:

* [list]

The following supporting services are in scope:

* [list]

The service is hosted in the following location(s):

* [list]

The following portals are in scope:

* [list]

## Out of scope

The following are out of scope of the evaluation. Where a component is out of scope, a justification has been provided.

| **Component** | **Justification** |
| --- | --- |
|  |  |
|  |  |
|  |  |

## Previously conducted independent evaluations

The following list highlights any previously conducted independent evaluations that have been conducted on the service that may be relied upon during this evaluation, when that was conducted, and the scope of that evaluation. This may include, for example, ISO27001 audit or penetration testing.

The following should be noted regarding the use of previously conducted independent evaluations:

* The evaluation must have taken place in the last 12 months.
* The scope of 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.
* If the applicant identifies other evaluations they want to be included later, this requires an update to the scope (and may require additional cost).

| **Previously conducted evaluation** | **When conducted** | **Scope** |
| --- | --- | --- |
|  |  |  |
|  |  |  |