27 March 2026

Practice Note: Scoping of Services

In an application to the Trust Framework Authority for accreditation, a provider must define the scope of the service(s) for which accreditation is sought.

Definition of the scope of the service(s) is integral to accreditation. Anything outside of the defined scope cannot be claimed to be accredited.

Scope definition is also key to the independent evaluations required for an application to be assessed.

The Trust Framework Authority will only assess applications for accreditation where the scope of the service is consistent with the contents of the application for accreditation, including the independent evaluations.

Defining the Scope of the Service

Service scope: A written description of the service (product). The scope outlines the specific digital identity-related functions an accredited provider delivers and for which accreditation is sought.

When determining and defining the scope of the service, the provider must consider and define:

1. The product/service (or services) that the provider wishes to be accredited.
2. The service types[1] that make up the product/service.
3. The parameters of the service, including where the service begins and ends, systems and platforms included in accreditation, API endpoints and third-party sub processors (if applicable).
4. Out-of-scope parts of the end-to-end information or process flow (ie. a provider will not apply for accreditation for all five service types if the service/product(s) for which accreditation is sought does not contain all of these).

Accreditation can only be granted to services within the ownership and control of the provider.

[1] Information services, binding services, authentication services, credential services, facilitation services (per the Digital Identity Services Trust Framework Regulations 2024)

Where third party providers are involved in the delivery of the service and/or they have access to the personal information in the service, they are to be considered within scope when defining the service(s) for the purposes of accreditation. These third parties and their roles and responsibilities for service delivery and access to the information must be identified.

The scope of the service must be included in the application for Trust Framework accreditation.

Defining the Scope of the Independent Evaluations

Evaluation scope: A written description of the specific activities and evidence an evaluator will assess to determine whether a provider meets the requirements. The written scope sets the boundaries and depth of the assessment, ensuring clarity on what will and will not be evaluated. This agreed scope forms the foundation for the contract with the evaluator and for the evaluator's work programme.

When determining the scope of the independent evaluations, the provider must consider:

1. The defined scope of the service (as above)
2. Relevant inputs and dependencies that may influence the delivery or risk profile of the service or the information in the service. This includes systems, processes and environments in scope, and interfaces with relying parties, third party providers and data sources.

The provider must ensure that all independent evaluations reflect the same service scope (i.e. they are all evaluating the same service/product).

When undertaking independent evaluations, the evaluator must:

1. Undertake evaluation within the constraints of the defined scope of the service and of the evaluation.
2. Follow the guidance and requirements provided by the Trust Framework Authority in the evaluation templates (available at https://www.dia.govt.nz/Trust-Framework-for-Digital-Identity-templates-and-guidance). These templates reflect the requirements of the legislation (especially the Digital Identity Services Trust Framework Rules) for which evaluation is required.

When undertaking an evaluation for the purpose of an application for Trust Framework accreditation, the evaluator should not do the following:

1. Do work additional to that defined in the templates (for example, where the template requires sighting a document the evaluator is not required to fully audit the contents of that document)
2. Evaluate the privacy or security of information not within the scope of the defined service, unless this is explicitly identified in the contract between the parties.

Examples

Example 1

A provider wishes to apply for accreditation of a wallet that includes Facilitation and Authentication service types. Information, binding and credential issuing are undertaken by another provider (whether accredited or not). The credential is available to the wallet via an authorisation flow.

1. The scope of the service must include definition of the product (the wallet) and the service types that the wallet is based on (facilitation and authentication). The processes and information flows within and between the service types in the product are in scope.
2. As all processes and information in the application for accreditation of the Facilitation and Authentication service types are owned/controlled by the provider, no third parties are in scope.
3. The scope of the independent security evaluation must include the security considerations related to the scope of the service and anything that may also impact on the security of the wallet, information and the credentials within it (including, for instance, the authentication flows).

Example 2

A provider applies for accreditation of an online identity verification service that includes the Information and Binding service types. The service is used by multiple businesses for one-time identity proofing of new customers. The provider hosts the service in a cloud tenancy with an external provider. The provider also uses a third-party status page service to publish uptime and incident notices, and a separate email marketing platform to send newsletters and product updates to its business customers. Neither the status page nor the email marketing platform integrates with the identity verification service, and neither can access personal information or transaction logs.

1. The service scope is the identity verification service delivering Information and Binding. It includes all related processes and information flows, plus the supporting systems and platforms such as the provider's API gateway, authentication servers and the cloud environment where personal information and verification logs are processed and stored.
2. The cloud infrastructure provider that hosts the service is in scope. The provider relies on this third party for delivery of the service, and the third party can access or influence the protection of personal information stored or processed in the service. The third party and its role must be identified.
3. The external status page service is out of scope. It publishes availability information only, does not participate in the Information or Binding flows, is not involved in delivery of the identity service, and has no access to personal information within the service. The email marketing platform for newsletters is also out of scope. It is a business support tool, not part of the defined identity service, and has no access to personal information processed by the service. It therefore does not fall within the service scope for accreditation.