Te Tari Taiwhenua
Internal Affairs

Digital Identity Services Trust Framework Act 2023 Regulations

Summary of submissions
February 2024

Te Kāwanatanga o Aotearoa
New Zealand Government

Contents

Introduction

Purpose

This document summarises key stakeholder submissions that are informing the development of Digital Identity Services Trust Framework regulations. These regulations will be considered for approval by Cabinet in early 2024.

Background

Parliament passed the Digital Identity Services Trust Framework Act 2023[1] (the Act) in April 2023 with the aim to provide New Zealanders with more confidence in using online identity services and to have control over their personal identity data. The Act comes into force on 1 July 2024 and enables the introduction of a Digital Identity Services Trust Framework (Trust Framework), which will establish rules and regulations for the provision of secure and trusted digital identity services.

The rules will establish the technical service requirements that Trust Framework providers will need to meet when designing and delivering accredited services.

The regulations will establish broader legal and administrative process requirements that need to be met by regulated parties or will clarify how statutory functions being established under the Act (the Trust Framework Board and the Trust Framework Authority) will govern and implement the proposed regulatory system. The scope of the consultation covered the regulations only and not the proposed rules.

A glossary of key terms about digital identity and the Trust Framework can be found at **Appendix A**. Further information on the Trust Framework can be found at **Appendix B**.

Consultation

The Department of Internal Affairs (the Department) ran a consultation process to inform the development of the regulations. A discussion paper outlining the proposed policy for the regulations supported a four-week targeted consultation process that ran from 24 August 2023 to 20 September 2023. The consultation process included two online meetings. The meeting with government agencies was attended by 22 people including people from Crown entities and government-adjacent[2] entities. The meeting with non-government agencies was also attended by 22 people and was attended by private businesses and non-profit organisations.

The submissions' feedback received by the Department during the consultation process has been grouped into key themes based on proposed regulations. The Department received 15 submissions.

---

[1] Digital Identity Services Trust Framework Act 2023 No 13, Public Act Contents – New Zealand Legislation

[2] Public agency with statutory independence.

Personal information and quotes from submitters have been withheld from this report to protect personal privacy under the Privacy Act 2020 (Privacy Act).

Some submitters commented on topics that were outside the scope of this consultation on regulations, including topics related to the rules which are the technical components of requirements under the Act, and the implementation of the Trust Framework. Feedback on the rules and the Trust Framework's implementation issues will be considered in further development of the rules and as the regulator is established. The Department is aiming to have a separate round of consultation on the Trust Framework rules during the first quarter of 2024.

Use and release of information

Stakeholder's submissions will inform the development of the Trust Framework regulations and advice to Ministers on the policy intent supporting the regulations.

It is usual practice for all submissions made to the Department to be published on our websites. The submissions together with the rest of consultation materials can be found in the *Digital Identity Programme* section of the Digital Government website.[3]

The Privacy Act governs how the Department collects, holds, uses, and discloses personal information about submitters and the information they have provided. Submitters have the right to access and correct the information provided.

[3] About the Digital Identity Programme | NZ Digital government

Overview of submissions

Consultation covered key regulation requirements

Regulations are required for accredited providers and services under section 28 of the Act to give effect to key provisions establishing legal and administrative process requirements. The regulations will be developed in two or more phases. The first set of regulations are required to initially stand up the regulatory system.

The Department consulted on the following primary set of regulations necessary to establish the regulator and support the intent of the Act:

- Accreditation services;
- Accreditation process;
- Service levels;
- Complaints and dispute resolution ;
- Recordkeeping; and
- Reporting.

We anticipate that a second set of regulations will be developed as the Trust Framework evolves. These regulations will include any necessary cost recovery arrangements and other operational matters required for the Trust Framework Authority's administration of the scheme. Considering the potential impact cost recovery arrangements could have on participation in the Trust Framework, we invited submitters to provide their initial comments to help inform our future thinking on this core element.

We received feedback from government agencies and non-government organisations

We received 15 submissions through the targeted engagement. Some of the stakeholder submissions represent the views of several member groups.

Of the 15 submissions analysed in this report, seven were from government agencies, one was from a government-adjacent agency, two from Crown entities and five were from non-government organisations. See table below for the list of submitters.

Stakeholder name	Type of organisation
Accident Compensation Corporation	Crown entity
Digital Identity New Zealand	Non-government organisation
Inland Revenue Department	Government Agency
Ministry for Ethnic Communities	Government Agency
Ministry of Social Development	Government Agency
New Zealand Customs Service	Government Agency
Office of the Private Commissioner	Crown entity
Reputationaire	Non-government organisation

Reserve Bank of New Zealand	Government-adjacent agency
Statistics New Zealand	Government Agency
Te Kāhui Raraunga	Non-government organisation
Te Whatu Ora – Health New Zealand and Te Aka Whai Ora – Māori Health Authority	Government Agencies
Trust Alliance New Zealand	Non-government organisation
Waka Kotahi New Zealand Transport Association	Government Agency
Yoti	Non-government organisation

The following table summarises the submissions by organisation category. Definitions for the categories are in **Appendix A: Glossary of key terms**.

Submitter category	Number
User plus other category (Iwi)	1
Other category (specified as N/A)	1
Digital identity service provider / potential Trust Framework provider	1
Combination of relying party and Trust Framework provider	3
Combination of all the categories above	3
Not given	6
TOTAL	15

High-level summary of feedback

Regulation	High-level summary of feedback received
Accredited services	• Submitters requested more clarity on the accredited services descriptions.
Accreditation requirements	• Further clarity on the 'fit and proper person requirements'. • A two-year accreditation period was seen as not long enough to imbed compliance requirements. • Questions were raised about the implementation of accreditation marks. • Some submitters did not support the financial viability requirement. • Some submitters found the provisional accreditation description needed further explanation. • The accreditation requirements need to acknowledge Māori needs in the digital identity space.
Service levels	• Better understanding of the difference between service levels and assurance levels. • Service level compliance costs were seen as a potential barrier.

Complaints and dispute resolution	• Further information was requested on what constitutes a complaint. • The Department should ensure the complaints process is accessible and provide guidance to Trust Framework providers when requiring due regard to tikanga Māori.
Recordkeeping	• Feedback included further need for clarification on recordkeeping requirements. • Mixed reactions to the seven-year proposed period for recordkeeping. • One submission suggested that regulations should include provisions on data accessibility and disposal.
Reporting	• Some submitters commented that unnecessary reporting could increase resourcing requirements. • Feedback recommended that the Trust Framework Authority provides guidance on the requirements for reporting.
Cost Recovery	• Large cost recovery fees may bring challenges to uptake. • Development of cost recovery regulations need to consider any equity or representation issues.
Comments considered out of scope	• The Department needs to engage with Māori over te ao Māori perspectives on Digital Identity when implementing the Trust Framework. • Other issues related to the implementation of the Trust Framework.

Key themes from submissions

Overall, submitters supported the establishment of the Trust Framework regulations for the provision of secure and trusted digital identity services. There were requests for clarification of the scope of some of our regulatory proposals, simplification of some of the proposed regulatory requirements and strengthening acknowledgement of te ao Māori views on digital identity when proposing regulations.

Accredited services

The Act requires that the regulations prescribe the types of digital identity services that may be accredited

In the discussion paper, we proposed that regulations specify that the following five services can be delivered as accredited services by Trust Framework providers:

1. *Digital Identity Information service*: provides an assessment of the accuracy of personal or organisational information.
2. *Digital Identity Binding service*: assures the connection of personal or organisational information to an individual or organisation.
3. *Digital Identity Authentication service*: assures 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 held and controlled by an authorised holder.
4. *Digital Identity Credential service*: combines bound (connected) information and an authenticator to establish and maintain a reusable credential.
5. *Digital Identity Facilitation service*: assists users to share credentials or parts of credentials with relying parties.

Several submitters requested more clarity on the accredited services descriptions

A majority agreed with the accredited services we proposed for Trust Framework regulations. At the same time, we received significant feedback about the definitions, description, rationale and scope of the proposed services, seeking more clarity on these services. Some submitters noted that Binding Services cannot be delivered as standalone services as they could be part of some or all the other services.

We also received feedback suggesting that providing examples of each of the services could assist with descriptions and how the services connect to each other in the Trust Framework. One submission noted that future consideration and flexibility must be retained to incorporate additions to the accredited services list as the digital identity environment evolves.

Accreditation requirements

Digital identity service providers need to demonstrate to the Trust Framework Authority that they can meet the accreditation requirements

The Act requires that any digital identity service provider that wants to deliver one or more of the services prescribed in the regulations as an accredited service will need to apply and demonstrate to the Trust Framework Authority that they can meet the accreditation requirements specified in section 25(1) of the Act.[4]

In the discussion paper, we proposed that the regulations incorporate the following requirements that Trust Framework providers would need to meet when applying for accreditation of services:

- *Incorporation in New Zealand*: Companies that wish to provide accredited services will need to be incorporated in New Zealand to apply for accreditation. If an international company wants to apply for accreditation, it must have a New Zealand subsidiary.
- *Organisational capability*: Applicants will need to provide the information specified by the Trust Framework Authority to demonstrate that the organisation seeking accreditation:
    - has the organisational capability to deliver Trust Framework accredited services;
    - is financially sustainable;
    - can meet the standards prescribed in rules to deliver services to one of the service levels provided for in regulations; and
    - has arrangements in place to provide a complaints and dispute resolution process that meets the requirements specified in regulations.
- *Fit and proper person requirements*: Applicants will be required to grant permission for the Trust Framework Authority to validate information provided by the applicant to support a fit and proper person assessment of the applicant and any officers responsible for the governance and management of the Trust Framework provider.

  The applicant would also need to provide information demonstrating the Trust Framework provider has appropriate policies and procedures that ensure employees entrusted with the delivery of accredited services meet fit and proper person requirements prescribed by the Trust Framework Authority.

---

[4] Information required by section 25(1), includes whether the applicant has:

- been convicted of a criminal offence in New Zealand or overseas;
- been, or is, the subject of a formal Privacy Commission investigation or proceeding;
- previously had an application for accreditation for themselves or a service they provided declined;
- had their accreditation as a Trust Framework provider or of a service they provided suspended or cancelled; or
- not complied with additional record-keeping or reporting requirements, or a compliance order imposed or issued under section 83 of the Act.

There was wide-ranging feedback on our accreditation requirements proposal, including comments on implementation and scope

There was a call for more clarity on the 'fit and proper person requirements'

Submitters shared views about how to check the fit and proper person requirements and who that would apply to, including larger organisations such as government agencies.

A two-year accreditation period was seen as not long enough to imbed compliance requirements

The suggested two-year accreditation period was seen as too much of a compliance burden. Some submitters noted that accommodating to the speed of change in technology and regulatory requirements takes time. Accreditation requirements would add resourcing pressure. A more flexible set of re-accreditation requirements was suggested.

Questions were raised about the implementation of accreditation marks

Implementation issues and risks were raised by some submitters, especially about the misuse, renewal and education on the use of accreditation marks. It was suggested that the Trust Framework Regulations should simply state that any promotion of Trust Framework-accredited services must comply with Trustmark terms of use and publish those terms of use separately.

Some submitters questioned the financial viability requirement

One submission noted that the financial viability requirement could have unintended outcomes, like favouring existing businesses and organisations over start-ups with smaller financial capacity.

The submission also noted that the cost recovery mechanism has not been developed yet and this could impact the way business models operate and therefore the financial sustainability of organisations. The submission also suggested that an application cost, both in time and financial outlay, could become a deterrent to applying.

Some submitters found the provisional accreditation description needed further explanation

Submitters wanted to know if provisional accreditations would enable providers to trade as accredited providers or let them offer accredited services.

The accreditation requirements should acknowledge Māori needs in the digital identity space

Some submitters reflected concerns regarding the involvement of Māori stakeholders to ensure the accreditation process is equitable and reflective of Te Tiriti o Waitangi principles.

Concerns about key aspects of Māori data sovereignty, control and management were shared as well. One submission suggested that the accreditation process should embed a cultural competency framework to ensure services are culturally appropriate for Māori.

Service levels

We proposed regulations to enable providers' systems and processes to be assessed by the Trust Framework Authority to determine what level of service they can provide

As part of the accreditation process, the regulations will enable providers' systems and processes to be assessed by the Trust Framework Authority to determine what level of service they can provide when delivering information, binding, and/or authentication services.

We proposed regulations to provide four service levels that will apply to the delivery of information, binding, and authentication services.

The requirements and standards Trust Framework providers will need to meet to achieve a given service level will be set out in the rules. The rules will require compliance with the New Zealand Identification Management Standards (NZIMS), which will be incorporated by reference. The level of assurance set out in the NZIMS will form part of the requirements prescribed for each service level.

Feedback received was sceptical of the need to set out service levels

Submitters wanted a better understanding of the difference between service levels and assurance levels

Several submitters found it difficult to differentiate the proposed service levels to determine what level of *service* Trust Framework providers can supply when delivering information, binding and/or authentication services, from the level of *assurance* those services may achieve.

Service level compliance costs were seen as a potential barrier by some submitters

Some feedback received suggested that even the minimum requirements of the lowest service level, including investment or system change, could represent a substantially high financial requirement that potential service providers could struggle to meet.

Complaints and dispute resolution

The Act establishes processes for dealing with complaints and disputes

Part 6 of the Act establishes processes for dealing with complaints and disputes. It enables any person to complain to the Trust Framework Authority if they believe a Trust Framework provider has breached the Trust Framework rules, regulations, terms of use of accreditation marks, or provisions of the Act.

The Act also enables regulations to set out requirements for Trust Framework providers to provide and operate their own internal complaints and dispute resolution processes.

These processes can be used by complainants to address and resolve issues directly with the Trust Framework provider. Any complaints not resolved using this internal system can then be referred to the Trust Framework Authority for consideration.

We proposed that the regulations require that every Trust Framework provider must:

- receive and consider complaints about any service provided by it, including complaints that the provider has failed to comply with the Trust Framework rules, regulations, terms of use of accreditation marks, or other requirements arising from provisions in the Act;
- establish and maintain policies and procedures for dealing with such complaints fairly, promptly and without undue formality;
- publicise its complaints policies and procedures to users, prospective users, relying parties and other stakeholders with an interest in its services; and
- ensure that complainants are aware that in the event they are dissatisfied with the outcome of the internal complaints process they may lodge a formal complaint with the Trust Framework Authority.

The ability of an applicant to comply with these requirements will be assessed when they apply for accreditation.

Submitters suggested improved guidance to comply with the requirements

Further information was requested on what constitutes a complaint

Some submitters considered that the discussion paper did not provide enough information about the scenarios this complaint process would be applied to. Those submitters also wondered if it would be separate to the referral of complaints to officeholders covered by section 72 of the Act. Other submitters encouraged the creation of alternative dispute resolution processes to be more cost-efficient.

The Department should ensure the complaints process is accessible and provide guidance to Trust Framework providers when requiring due regard to tikanga Māori

Feedback highlighted the need to make the resolution process accessible, particularly to people who experience barriers to accessing digital platforms or those who do not want to use digital channels to access services.

Some submitters would appreciate more clarity and practical guidance on how the Trust Framework Authority would expect Trust Framework providers to have due regard to tikanga Māori. One of the submissions highlighted the risk that, without the acknowledgment of Māori values, traditions and principles, the complaint resolution system could alienate Māori users or stakeholders.

Recordkeeping

The Act requires the Trust Framework providers to collect information about its activities and hold that information for a set period

In accordance with section 42 of the Act, we proposed that the regulations require Trust Framework providers to collect and retain information about their activities, store it in a secure database, and provide the Trust Framework Authority with access to those records in reasonable time upon request.

We proposed that the regulations require the Trust Framework provider to retain the information necessary to assure that it has delivered accredited services in accordance with the requirements specified in the rules and regulations. Where information received by the Trust Framework provider is of a personal nature and subject to the Privacy Act, the regulations will allow the provider to keep a record of the source of information used in the provision of digital identity services rather than the personal information itself.

We proposed the regulations require Trust Framework providers to retain their records for seven years following their last use. This period should ensure the Trust Framework Authority can access records necessary for regulatory system monitoring and compliance management activities without imposing unnecessary recordkeeping compliance costs to providers.

Overall submitters agreed with the need to keep accurate and accessible records

Feedback included further need for clarification on recordkeeping requirements

There was a request for a more clarity on recordkeeping requirements and the type of records to be retained. One submission suggested that providers should retain information that is pertinent to the integrity and transparency of their operations including transaction logs, audit logs, compliance documentation, security incident reports and user complaint and resolution records. Other submitters shared their ideas on keeping records of software updates, contractual agreements, and system forensics to facilitate investigations following any security breach.

Feedback received showed mixed reactions to the seven-year proposed period for recordkeeping

Stakeholders' views on recordkeeping duration were generally split between two positions. Some submitters considered the seven-year period to be too long, raising concerns that this could create risks to cyber-security. Those submitters believed that service providers storing large amounts of personal information could become very appealing targets to hackers. Other submitters were concerned about data storage costs that such a long time necessitates.

Other submitters suggested a flexible approach for the duration of recordkeeping. One of the submissions highlighted that some documents could have a lifetime longer than seven years (for example, a passport can last for 10 years), meaning that users could be unable to prove their identity for three years.

One submission suggested that regulations should include provisions on data accessibility and disposal

The submitter stated that beyond the regulations requiring Trust Framework providers to collect and store data, regulations should ensure that data can be accessed, retrieved and disposed of efficiently when needed.

Reporting

The Act enables the regulations to establish Trust Framework provider reporting requirements

We proposed that the regulations require every Trust Framework provider to deliver an annual report to the Trust Framework Authority that contributes to their ability to monitor and assess the performance of each Trust Framework provider and overall regulatory system. Annual reports will need to include information in a form specified by the Trust Framework Authority on:

- Organisational governance and management;
- Services use;
- Service delivery;
- Complaints and disputes resolution;
- Fraud; and
- Financial performance.

Overall, stakeholders agreed with the proposed reporting regulations but suggested amendments

Some submitters commented that unnecessary reporting could increase resourcing requirements

Some submitters believed that unnecessary reporting could divert resources without adding significant value, having a disproportionate impact on smaller entities. More clarity on the requirements was also suggested to avoid misinterpretations, ambiguities and inconsistent reporting formats. Some submitters thought that the proposal to provide reports annually would be burdensome and expressed a preference for periodic reporting instead. Submitters generally supported the fraud reporting requirement but saw the requirement for detailed financial performance information as unnecessary.

Feedback recommended that the Trust Framework Authority provides guidance on the requirements for reporting

Some submitters suggested that the Trust Framework Authority could provide operational guidance to Trust Framework providers on periodic and incident reporting, which aligns with guidance on similar reporting requirements from other government agencies.

Some of the feedback proposed that, rather than include the notification of fraud events in "other reporting" as proposed, it should be specified as "incident notification" to highlight that incidents represent a risk of serious harm.

Other feedback suggested that reporting requirements should include cyber-security incidents. There was also a suggestion that the inclusion of a definition of serious harm and the inclusion of incident notification expectations and processes would align the requirements with security requirements established under the Privacy Act. This submitter noted that if an incident is raised with the Trust Framework Authority, then the Trust Framework Authority should respond to it, for example, by opening an investigation.

Other submissions did not agree with the suggested 20-working day reporting period and suggested that a shorter period to notify the issue and a longer period to report would provide more flexibility and better align with provisions in the Privacy Act.

Cost recovery

The Act includes a provision for establishing regulations to recover some operational costs through fees

While cost recovery arrangements will be developed as and when required after the regulations are finalised, the discussion document sought initial feedback to help inform advice on cost recovery regulations.

Stakeholders agreed on the need for an appropriate cost recovery model that was not onerous for providers

Some submitters think that large cost recovery fees may bring challenges to uptake of the Trust Framework

Several engagement participants raised concerns about cost recovery fees being used to fund the broader administration of the Trust Framework.

Some submitters were concerned that leaving the development of cost recovery and renewal arrangements until later in the Trust Framework's establishment phase created short-term uncertainty for potential entrants. Feedback suggested that uncertainty around costs and the benefits behind a cost recovery model could prevent providers from deciding to opt-in to the framework.

Development of cost recovery regulations need to consider any equity or representation issues

Stakeholders believe that fees could create potential equity issues between well-established firms that could afford them, and small start-ups that could not. One of the submissions noted the cost recovery fees could become a barrier to access for Māori leading to a lack of representation from iwi and Māori companies and organisations. This was seen as a potential system that does not fully serve or understand the needs of Māori in the digital identity space.

Comments that were out of scope

We received a wide range of comments about implementation

The Department needs to engage with Māori over te ao Māori perspectives on Digital Identity when implementing the Trust Framework

We received substantial feedback from stakeholders highlighting the importance of acknowledging specific Māori needs in the space of digital identity to make the Trust Framework accessible for potential Māori users and Māori providers.

Potential accessibility and equity issues for Māori were seen as a fundamental risk for the implementation of the Trust Framework. These issues will be considered by the Trust Framework Authority.

Other issues related to the implementation of the Trust Framework

We heard concerns about other issues related to the implementation of the Trust Framework itself, rather than the development of the Trust Framework regulations. These included:

- the ability of the Trust Framework Authority to develop the Trust Framework;
- the number of Crown entities and government agencies seeking accreditation;
- digital inclusion and accessibility to non-native English speakers and;
- the implementation of international digital trade commitments.

Feedback related to the implementation of the Trust Framework will be considered in the development of the Trust Framework rules and in establishing the Trust Framework Authority. The Department is aiming to have a separate round of consultation on the development of Trust Framework rules during the first quarter of 2024.

Appendix A – Glossary of key terms

Term	Definition
Accreditation	Approval given to a digital identity service provider who has demonstrated they meet the applicable requirements of the Trust Framework.
Accredited digital identity service or accredited service	A digital identity service accredited by the Trust Framework Authority to be provided by a particular Trust Framework provider.
Digital identity	A digital representation of a person's identity information and other attributes about them that they can use to prove who they are online and digitally to access services.
Digital identity service provider	An individual or organisation that provides a digital identity service, whether the provider or service is accredited under the Trust Framework or not.
Digital Identity Services Trust Framework; or Trust Framework	Has the meaning given in section 8 of the Act. The legal framework established to regulate the provision of digital identity services for transactions between individuals and organisations.
Relying party	An individual or an organisation that relies on personal or organisational information shared, in a transaction with a user, through one or more accredited digital identity services
Trust Framework Authority	The Authority established under section 58 of the Act to oversee the running of the Trust Framework.
Trust Framework Board	The board established under section 42 of the Act to oversee the Trust Framework Authority.
Trust Framework provider	A digital identity service provider accredited by the Trust Framework Authority to provide one or more accredited digital identity services.
User	An individual who- (a) shares personal or organisational information, in a transaction with a relying party, through one or more accredited digital identity services; and (b) does so for themselves or on behalf of another individual or an organisation.

Appendix B – Further information on the Trust Framework

To read more about the Digital Identity Services Trust Framework and digital identity in New Zealand, please visit the links below.

The Act

New Zealand Legislation: Digital Identity Services Trust Framework Act 2023 No 13, Public Act – New Zealand Legislation

What is digital identity?

Digital NZ: https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/what-is-digital-identity/

Digital Identity NZ: https://digitalidentity.nz/

Background on New Zealand's digital identity programme

Digital NZ: https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/about-the-digital-identity-programme/

New Zealand Foreign Affairs and Trade – the Single Economic Market agenda: https://www.mfat.govt.nz/en/countries-and-regions/australia-and-pacific/australia/new-zealand-high-commission-to-australia/single-economic-market/

The Trust Framework concepts and principles

Digital NZ: https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/trust-framework/