Te Tari Taiwhenua
Internal Affairs

Digital Identity Services Trust Framework Regulations

Discussion paper
August 2023

Te Kāwanatanga o Aotearoa
New Zealand Government

Contents

1. Introduction

Purpose

The Department of Internal Affairs (the Department) seeks your views on the proposals outlined in this discussion paper for the development of regulations required to enable the establishment of the Digital Identity Services Trust Framework.

Overview

In a world where digital services are increasingly prevalent, it is important people can prove who they are online in a trusted, safe and consistent way. Digital identity services give people the ability to securely share information about themselves (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.

New Zealand's digital identity environment currently lacks effective regulatory arrangements that ensure consistent application of digital identity service standards. This makes it difficult to ensure the delivery of secure services people feel they can trust.

To provide New Zealanders with more confidence in using online identity services, Parliament has passed the Digital Identity Services Trust Framework Act 2023 (the Act). The Act comes into force on 1 July 2024 and enables the introduction of a new regulatory Trust Framework, which will establish rules and regulations for the provision of secure digital identity services.

The Act provides for 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 provide advice to the TF Board on issues that raise matters of tikanga Māori, and to 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.

The Trust Framework will give people more control over their own data, including what they choose to share about themselves and who they share it with. We anticipate this will increase consumer confidence in digital identity services, as well as encourage innovation in the technology industry more broadly.

The rules will establish the technical service requirements that providers will need to meet when designing and delivering accredited services. The rules have already been the subject of early consultation with key stakeholders and will be the subject of a further final round of consultation, likely in the first quarter of 2024. They cover—identification management; privacy and confidentiality; security and risk; information and data management; and information sharing and facilitating arrangements.

The regulations will complement the rules by establishing 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.

The regulations will be developed in two phases. The first set of regulations (covered in this discussion paper) outline the necessary legal and procedural requirements to initially stand up the regulatory system. They will cover:

- *Accreditation Services:* Definition of the types of services that will be subject to accreditation under the Act.
- *Accreditation Process*: Accreditation requirements, application assessment criteria, and accreditation duration.
- *Service Levels:* Establishment of different service levels that providers can meet when delivering accredited services.
- *Complaints and Dispute Resolution:* The internal complaints and dispute resolution process requirements TF providers need to meet.
- *Recordkeeping*: The information to be retained by TF providers and the period they are required to retain that information.
- *Reporting*: The reporting requirements that will apply to TF providers.

We anticipate a second set of regulations will be developed and recommended to the Minister for the Digital Economy and Communications by the TF Board in 2024. These regulations will address any necessary cost recovery arrangements and other operational matters required to frame the TF Authority's administration of the scheme. The regulations may include:

- *Cost Recovery:* The establishment of fees for the partial recovery of the TF Authority's ongoing costs for administering the Trust Framework, including consideration of accreditation applications or renewals. It is anticipated that the TF Authority's initial establishment and first two years of operating costs will be met from Crown funding without a contribution from fees.
- *Dispute Resolution Scheme:* The establishment of any requirements and criteria that the TF Authority must meet should it want to recommend a dispute resolution scheme, together with any proposed fees to recover costs associated with the provision of complaints and dispute resolution services. The establishment of a fees regime will be considered in conjunction with the development of the TF Authority's complaints and dispute resolution operating model, which will consider the role, if any, of an external dispute resolution service provider.
- *Third Party Assessors*: Arrangements for the certification of third-party assessors to carry out functions relating to the accreditation of TF providers, including appointment criteria, recordkeeping, and reporting requirements.
- *Other Operational Matters:* Any other operational matters that the TF Board considers should be established in regulations to provide greater certainty to both the TF Authority and regulated parties on compliance requirements and ensure the cost-effective management of the regulatory system by the TF Authority. The regulations, for example, will cover any changes to accreditation renewal requirements and compliance order forms.

How to have your say

Written submissions on the proposals outlined in this discussion paper are due **by 5pm, Wednesday, 20 September 2023.**

Please refer to the key questions throughout the discussion document to help guide your feedback on the proposed Trust Framework regulations. You may use our submission form that will be issued in conjunction with this discussion paper to provide your feedback.

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

Please send your submission to Digital.Identity@dia.govt.nz

Use of Information

The information provided in your submission will be used to inform the development of the regulations, including advice provided to the Minister. We may contact you directly if we need to clarify any matters raised in your submission.

Release of Information

It is usual practice for all submissions made to the Department to be published on our website. We may also publish our submissions analysis, which will include a summary of submitters' views and the names of individuals or organisations that have made submissions. Submissions may also be subject to a request made under the Official Information Act 1982.

The Privacy Act 2020 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 personal information.

Any personal information you supply to us in your submission will only be used for the purpose of assisting in the development of policy advice associated with the issues and proposals canvassed in this discussion paper. Please state in your submission or covering email, if you **do not** wish to have your name, or other personal information published.

In addition, if there is information in your submission you do not want released, please make this clear in your submission or associated covering letter or email and explain why. For example, some information may be confidential because it is commercially sensitive or personal. You may also ask for your details to be withheld if your submission is requested under the Official Information Act 1982. We will take your statement into account and will consult with submitters when responding to requests under the Official Information Act.

Next Steps

When the submissions period closes on 20 September 2023, we will analyse the submissions and use the findings to inform the development of final advice on the regulations for consideration by the TF Board and the Minister for the Digital Economy and Communications. We anticipate the regulations will be developed and gazetted in 2024.

2. Context

Digital identity and online service delivery

Many government and private sector services are now online. In keeping with this digital environment, New Zealanders expect to be able to access services and complete transactions remotely, rapidly, and with minimal paperwork. However, many online transactions that require the provision of digital identity information—such as online banking, claiming a welfare payment, or opening a utilities account online—need high levels of security to ensure users' personal information is safe and their privacy is protected.

While the use of digital identity services is generally seen as being efficient and provides more opportunities for individuals than paper-based identity systems, it also comes with risks. Unlike written or spoken information, digital information can be more easily accessed, copied and shared from anywhere in the world. Unfortunately, we are now facing increasing fraud and security risks because of the rapid evolution of global digital sharing.

It is important for people to feel secure and confident in using digital identity services, including being in control of their information and who has access to it. A 2019 survey by Digital Identity New Zealand found 79% of New Zealanders are concerned about the protection of their identity and use of personal data by organisations. Moreover, nine out of ten New Zealanders stated the idea of being more in control of their digital identity is appealing.[1] This suggests there is a low level of confidence in the current state of the digital identity system.

Trust Framework – Purpose and benefits

The Trust Framework will help ensure the provision of more secure and trusted digital identity services for New Zealanders

The Digital Identity Services Trust Framework Act will establish:

- a legal framework for the provision of secure and trusted digital identity services for individuals and organisations; and
- transparent governance and accreditation functions that incorporate te ao Māori approaches to identity.

The Trust Framework will make it easier for individuals (users) to securely access and share information about themselves with relying parties through regulated TF providers.[2] It will also reduce transaction costs for relying parties that need verified identity and other personal information to provide their services.

---

[1] Nine out of 10 Kiwis want more control of their digital identity - Digital Identity New Zealand

[2] A relying party is an individual or an organisation that relies on personal or organisational information shared with them before being able to provide the products or services they offer.

The Trust Framework will enable users and relying parties to reduce the time and cost associated with a multitude of online and face-to-face transactions that require verification of identity and other personal information. Examples include opening new bank accounts; accessing and providing health services; completing property transactions; accessing New Zealand superannuation or other government services; completing an employee recruitment and appointment process; or verifying proof of age to enable access to age restricted products and services such as alcohol or entry to adult establishments such as, for example, a night club.

The introduction of the Trust Framework aims to bring a stronger sense of security and increase trust and confidence in the use of digital identity services within New Zealand. In summary, the anticipated benefits of the Trust Framework include:

- enabling user-controlled access to, and sharing of, personal information;
- minimising identity theft and privacy breaches;
- improving information sharing efficiency;
- reducing unnecessary sharing of information; and
- improving access to online and face-to-face services that require the provision of identity and other personal information.

Having more secure and trusted digital identity services will also:

- build New Zealand's resilience to unexpected events by enabling secure digital access to essential identity documents and personal information;
- support New Zealand's long-term economic growth and development; and
- enable digital trade and other cross-border transactions.

Uptake strategy

Realising the benefits from the Trust Framework enables requires buy-in and uptake from users, TF providers, and relying parties, as it is an opt-in regulatory system. This will be a key challenge and focus for the TF Board and TF Authority who are responsible for promoting use of the system and ensuring effective regulatory management of it.

Trust Framework parameters

Use of the Trust Framework is opt-in; personal information will not be held in a centralised database

Public consultation during Parliament's consideration of the Digital Identify Services Trust Framework Bill in late 2021 highlighted some concern that the Trust Framework may be seeking to establish a mandatory and centralised identity regime.

The proposed system will be decentralised with no new powers for the Government to collect or share people's information without their consent. One of the key objectives of the Trust Framework is to support and enable users to choose what information about themselves is being shared with third parties.

Also, it will not be compulsory for people to use Trust Framework accredited digital identity services, or even to use any digital identity services at all. To ensure access, people will still be able to apply for government services in-person and provide physical credentials to show who they are.

Operation of the Trust Framework will involve user-controlled data sharing

The current lack of regulation in the provision of New Zealand's digital identity services means individual services are often provided directly to an individual with varying levels of security depending on the strength of the service provider's systems and processes. Access to, and sharing of, information is primarily controlled by the service, rather than the user.

However, under the Trust Framework individuals will be able to access, claim, and share their own information through accredited digital identity services (identified by accreditation marks). This will occur as part of a standardised process to ensure personal identity data is handled securely and according to the users' requests, as outlined in **Figure 1** on page 8.

Government services

The Trust Framework will apply to Crown entities and government departments as well as iwi, private sector, and other non-government organisations that seek accreditation

The Act and its associated rules and regulations will apply to Crown entities and government departments that choose to opt-in and deliver services under the Trust Framework, alongside iwi, private sector, and other non-government organisations.

As **Figure 1** shows, in addition to being relying parties, some Crown entities and government departments may also seek accreditation to provide accredited services. For some, this may be limited to being an accredited information provider. For others, it could include choosing to provide other accredited services as ''infrastructure providers."

Crown entities and government departments that wish to provide accredited services will need to meet the requirements specified in the Act, associated rules and regulations. For example, the identity verification service RealMe will continue to be provided by the Department of Internal Affairs. To be offered as an accredited service, however, the Department will need to meet the accreditation requirements.

International Alignment

In 2018, the Government committed to a programme led by the Department to develop options for a new approach to digital identity. That programme investigated how the Government could set up the right rules and environment to take advantage of new technologies, offering a modern approach to meet the evolving needs and expectations of New Zealanders in the digital identity landscape.

Throughout 2019 and 2020, the Department undertook extensive research and engaged with key stakeholders, including equivalent agencies internationally. New Zealand is not the only country implementing legislation to modernise its digital identity system. The Trust Framework will align with similar trust frameworks being developed in Australia, Canada and the United Kingdom, and will be a key foundation in the Government's commitment to achieving mutual recognition of digital identity services with Australia under the Single Economic Market agenda.[3]

Enabling Regulations

The regulations will complement the technical and operational service-related requirements established in the Trust Framework rules that apply to TF providers and their delivery of accredited services. It is our intention that the regulations will provide a flexible way for Trust Framework processes to evolve over time as the digital identity system matures and technology develops.

The development of the rules and regulations will be informed by eight principles to ensure they are—people-centred; privacy enabling; security enhancing; enabling of Te Ao Māori approaches to identity; sustainable; interoperable; and open and transparent.[4]

Further Information

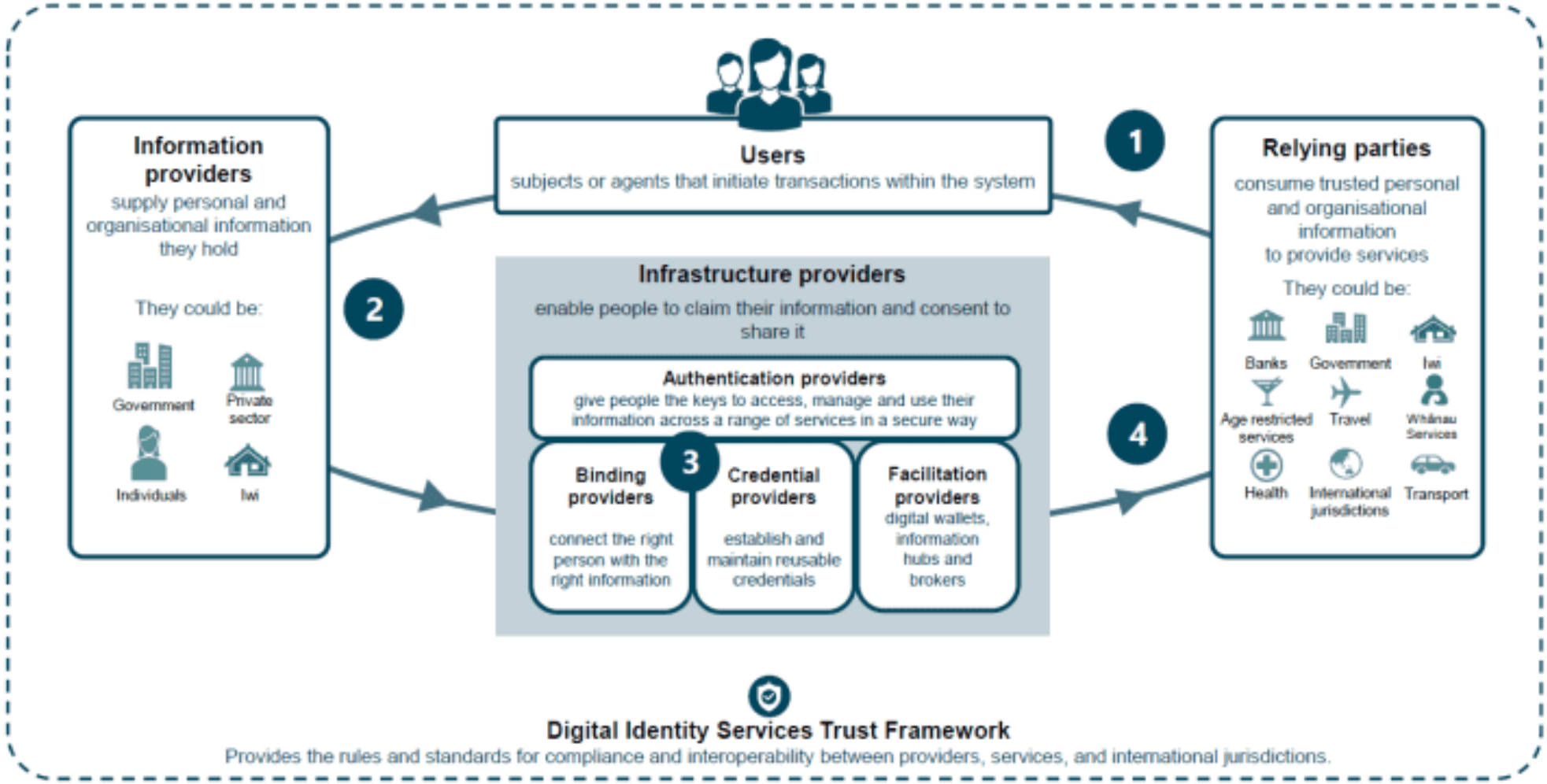
Appendix A provides a glossary of key terms used in this paper. **Appendix B** contains links to further information on the Trust Framework.

[3] For further information see - https://www.mfat.govt.nz/en/countries-and-regions/australia-and-pacific/australia/new-zealand-high-commission-to-australia/single-economic-market/

[4] For further information see - Trust Framework principles | NZ Digital government

Figure 1: Digital Identity Services Trust Framework

This Framework outlines the relationship between users, information providers, infrastructure providers, and relying parties.



3. Accredited Services

Overview

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

Proposed Regulations

We propose that the regulations specify that the following services can be delivered as accredited services by TF providers under the Act:

- *Digital Identity Information Service:* provides an assessment of the accuracy of personal or organisational information.
- *Digital Identity Binding Service:* assures the connection of personal or organisational information to an individual or organisation.
- *Digital Identity Authentication Service:* assures the connection of a user to an authenticator and secures the sharing of personal or organisational information between TF participants by ensuring the authenticator(s) are held and controlled by an authorised holder.
- *Digital Identity Credential Service:* combines bound (connected) information and an authenticator to establish and maintain a reusable credential.
- *Digital Identity Facilitation Service:* assists users to share credentials or parts of credentials with relying parties.

We are seeking comments on the services that may be accredited under the Act, in particular:

1. Do you agree or disagree that the five identified services should be subject to accreditation under the Act? Please explain why/comment
2. Are the definitions of the services adequate?
3. Are there any other services which you think should or could be accredited?

4. Accreditation Requirements

Overview

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 TF Authority that they can meet the accreditation requirements specified in the Act, rules and regulations.

The Act establishes certain requirements that applications for accreditation must meet. These include:

- being in a form, and made in a manner, approved by the TF Authority;
- containing information prescribed in regulations; and
- providing the information required by section 25(1), which 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 TF 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.

Proposed regulations

General requirements

In addition to meeting the requirements specified in section 25(1) of the Act, we propose that the regulations incorporate the following requirements that TF providers would need to meet when applying for accreditation of a service or services.

Incorporation in New Zealand

We want to ensure the enforceability and integrity of the Trust Framework. Therefore, TF providers need to be subject to New Zealand law. 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, they must have a New Zealand subsidiary.

Organisations that are registered as Incorporated Societies in New Zealand will also be eligible to apply for accreditation as will New Zealand Crown agencies and government departments.

Organisational Capability

Applicants will need to provide information specified by the TF Authority to demonstrate that the organisation seeking accreditation:

- has the organisational capability including the people, policies, processes and systems required to deliver TF accredited services;
- is financially sustainable;
- can meet the standards prescribed in rules to deliver the service or services to one of the service levels provided for in regulations (refer to the following section for further information on service levels and the associated levels of assurance they provide); and
- has arrangements in place to provide a complaints and dispute resolution process that meets the requirements specified in regulation (further information on these requirements are outlined in the complaints and dispute resolution section of this paper).

Fit and Proper Person Requirements

Applicants will be required to grant permission for the TF 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 TF provider. This will include permission for the Authority to request a Police vetting check.[5]

The applicant would also need to provide information demonstrating the TF 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 TF Authority.

Assessment criteria

The Act enables the TF Authority to accredit a provider if it is satisfied that they meet the requirements in sections 23 to 25 of the Act, any criteria for the assessment of applications, and any other requirements set by regulations.

---

[5] The New Zealand Police may release any information they hold if relevant to the purpose of the vetting request. This may include:

- Conviction History Report.
- Infringement/demerit reports.
- Active charges and warrants to arrest.
- Charges that did not result in a conviction including those that were acquitted, discharged without conviction, diverted, or withdrawn.
- Any interaction had with New Zealand Police considered relevant to the role being vetted, including investigations that did not result in prosecution.
- Information regarding family harm where the applicant was the victim, offender or witness to an incident or offence, primarily in cases where the role being vetted for takes place in the applicant's home environment where exposure to physical or verbal violence could place vulnerable persons at emotional or physical risk.
- Information subject to name suppression where that information is necessary to the purpose of the vet.

We propose that that the regulations provide for the TF Authority to use the following criteria to assess applications for accreditation. There is sufficient evidence to satisfy the TF Authority that the applicant:

- is a company that is incorporated in New Zealand, an incorporated society registered in New Zealand, or a New Zealand Crown entity or government department;
- will deliver one or more of the digital identity services specified in regulations established under the Act;
- has the capability to meet the service standards specified in the rules to an appropriate level of assurance;
- has demonstrated it will provide an internal complaints and dispute resolution process that meets regulatory requirements;
- has officers responsible for the governance and management of the TF provider that are fit and proper persons that can be entrusted with the delivery of digital identity services;
- has policies and processes in place to ensure its employees entrusted with the delivery of accredited services meet fit and proper person standards prescribed by the Authority;
- has demonstrated that it is financially sustainable; and
- has provided all the information specified in section 25 and addressed to the TF Authority's satisfaction any issues of concern arising from any past practises as an identity services provider that have been the subject of an investigation by the Privacy Commission or the TF Authority, or resulted in a decision to previously decline, suspend or cancel an accreditation.

Duration

Accreditation will be for a two-year period

The Act provides that the accreditation of a TF provider or service expires at the end of the period set by regulations (section 30(2)). We propose the regulations specify that a service accreditation ends two years (24 months) after the date it is granted by the TF Authority.

We have considered options ranging from annual through to five yearly and indefinite accreditation. In proposing a two-year accreditation period, we have sought to balance the need to provide the TF Authority, users and relying parties with appropriate assurance that TF providers are meeting accreditation service standards against the compliance costs associated with renewal requirements.

We consider a two-year accreditation period is appropriate given we are introducing a new regulatory system and there are likely to be changes in service standards in a rapidly evolving industry. We anticipate the rules will be updated in response to technology advances and changes in commercial practice. Providers will need to demonstrate they are able to meet changes in service standards.

The Act allows for regulations to establish different expiry periods for different types of TF provider, different types of service and different levels of service. During the Trust Framework's establishment phase, we consider a standard two-year period should apply to everyone. We anticipate that this is a matter the TF Authority may wish to review based on its experience administering the regulatory system two to three years after commencement.

Renewal

TF providers will be able to renew their service accreditations

The Act includes provisions covering the accreditation renewal process (section 31). When TF providers apply for renewal, they will need to demonstrate that they continue to meet the accreditation requirements and standards specified in the Act, rules and regulations, unless different requirements for renewal applications are established in regulations.

We propose that the TF Board consider introducing regulations that refine the renewal application requirements when developing the next tranche of regulations. The aim will be to establish a renewal application process that provides the TF Authority with assurance that TF providers can continue to meet accreditation requirements, in particular any changes that have been introduced since an applicant's original accreditation, while minimising renewal application compliance costs.

Accreditation mark

Users and relying parties will be able to identify an accredited service through an accreditation mark

If approved, a TF provider will be able to deliver the accredited service or services under the Trust Framework and display an accreditation mark that would apply to each accredited service. The accreditation mark that would be applied to each specific accredited service is an important distinguishing factor, as some organisations with accredited services could also provide non-accredited services, which do not display the accreditation mark.

Display of the accreditation mark will help users decide who they want to share their personal information with. If they chose to use a TF provider's accredited service, they will know that the:

- service meets the technical standards set out in the rules that apply to that service;
- service is delivered to a prescribed service level (as specified in the rules and regulations and discussed further in the next section of this paper); and
- TF provider has undergone an assessment for security and privacy and will give the user control over the identity information they choose to share.

To reduce the risk of a user or relying party misunderstanding whether a TF provider is delivering an accredited service, we propose that the regulations specify that the TF Authority will only allow accreditation marks to be displayed against specific services, rather than being displayed as a 'generic' accreditation by the organisation.

Provisional accreditation

Under the Act, the TF Authority may grant provisional accreditation for a 12-month period or a longer period as agreed. Provisional accreditation is intended to enable potential TF providers to test their proposed products/services for development and investment purposes, and obtain assurance that if they proceed with development as proposed they will meet the requirements for full accreditation.

A provider or service with provisional accreditation is not a TF provider or an accredited service for the purposes of the Act. When they are ready to do so, the applicant will still need to demonstrate to the TF Authority that they meet the necessary requirements to receive full accreditation.

We are not proposing to develop additional regulations for provisional accreditation. Under section 32(5) of the Act, applications for provisional accreditation will need to be made in the manner established by the TF Authority. In doing so the applicant will need to demonstrate to the TF Authority that the organisation and their proposed services—when fully developed—will meet the requirements in the Act and the proposed regulations, and rules that apply to full accreditation.

International participation

There is a long-term plan for digital identity credentials to be used internationally, which will be enabled through mutual recognition agreements with other countries. This will enable credentials to be used overseas with accreditation, assurance, and enforcement functions able to be applied within the country of origin.

Australia will be the first country we achieve mutual recognition with, following the New Zealand Government's commitment to mutual recognition of digital identity services with Australia under the Single Economic Market agenda.

We are seeking comments on the accreditation scheme, in particular:

4. Do you agree or disagree with the proposed accreditation requirements, and the TF Authority's assessment criteria? Please explain why/comment.
5. Do you think anything is missing or needs to be removed?
6. Do you agree or disagree with the proposed two year accreditation period? If you disagree, what do you think is a more appropriate period, and why?
7. Are there any implementation issues or risks associated with the accreditation process that should be addressed?
8. Do you agree or disagree that the accreditation mark should be displayed against services only? Please explain why/comment
9. Are there any implementation issues or risks associated with the introduction of the accreditation marks that should be addressed?
10. Do you have any concerns about the proposed approach to considering applications for provisional accreditation?

5. Service Levels

Overview

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

Each of the services will have four service levels. The service level indicates the capability that a TF provider can deliver their associated service to.

Service levels will indicate to prospective users and relying parties what level of assurance a given service may achieve. Levels of assurance are specific to attributes (or pieces of information about a person), not the service or organisation. Therefore, the service level will indicate to other people the capability of an accredited service and the expected level of assurance that service can provide.

Proposed regulations

The regulations will provide for the service levels that will apply to the delivery of information, binding, and authentication services.

The requirements and standards TF 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 levels of assurance set out in the NZIMS will form part of the requirements prescribed for each service level.

Further details on the service levels contained in the *New Zealand Identification Management Standards* are available via this link: https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/applying-the-standards/

Benefits

In practice, service levels will help relying parties understand the outcome of TF Authority assessment processes without having to know what the process was. They will give relying parties and other digital service providers an understanding of how robust the TF provider's processes are.

Establishing the service level through the accreditation process will also allow TF providers who rely on other providers for information, binding, or authentication services to understand what level of assurance that provider can deliver. This increases the level of trust that relying parties and other TF providers have in the Trust Framework.

Assurance information adds a layer of detail which enables TF providers to understand the capability, systems and processes other providers have in place, allowing them to work together more easily. It also allows them to identify possible partners and reduces the need for TF providers to spend a significant amount of time assessing other parties' processes.

We are seeking comments on the inclusion of service levels as part of the accreditation scheme, in particular:

11. Do you agree or disagree that assessing an organisation's ability to provide a service up to a prescribed level is appropriate? Please explain why/comment
12. Are service levels useful for commercial purposes?
13. Are there any implementation issues or risks that should be addressed?

6. Complaints and dispute resolution

Overview

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

Section 28 of the Act also provides for regulations that set out requirements for TF providers to operate their own internal complaints and disputes resolution processes. These processes can be used as a first port of call by complainants to address and resolve issues directly with the TF provider. Any complaints not resolved using this internal system can then be referred to the TF Authority for consideration.

This approach is consistent with the principles established in the Act that guide the TF Authority's approach to complaints management, which are that:

- processes for complaints should be fair, accessible and have particular regard to tikanga Māori;
- complaints should be resolved in a timely and efficient manner; and
- complaints should be resolved at a level appropriate to the seriousness and nature of the complaint.

Proposed regulations – TF Provider internal complaints process

We propose that the regulations require that every TF provider must:

- receive and consider complaints about any service provided by it, including complaints that the provider has failed to comply with the TF 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, without undue formality and with due regard to tikanga Māori;
- incorporate the use of any disputes resolution scheme or process the TF provider is a party to through their membership of a particular industry;
- 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 TF Authority.

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

Potential future regulations for a dispute resolution scheme

The Act also allows for the development of regulations to establish requirements and criteria that would enable the TF Authority to recommend a dispute resolution scheme for the Minister's approval. Any scheme would need to complement and operate alongside the TF Authority's complaints process which can lead to the TF Authority applying a range of remedies where it finds a TF provider has breached legislative requirements.

Further work is required on the development of the TF Authority's complaints and dispute resolution operating model, before we can determine whether regulations are required to support the establishment and implementation of accessible, fair, timely, and cost-effective complaints and dispute resolution arrangements. This will include considering what role, if any, an external alternative dispute resolution provider could play to support or complement the TF Authority's complaints investigation and compliance management functions.

Complaints and dispute resolution process

Figure 2 highlights key elements of the complaints and dispute resolution process provided for in the Act.

Complaints must be about breaches: Under the Act the TF Authority is charged with addressing complaints received from any person that believes a TF provider has breached the provisions of the Act, the rules, the regulations, or the terms of use for the accreditation mark.

The Complainant must try and resolve a complaint directly with the TF Provider before involving the TF Authority: Complainants are expected to make reasonable efforts to resolve a complaint directly with the TF provider concerned before involving the TF Authority. This should involve using a TF provider's internal complaints resolution process and utilise any disputes resolution scheme or process that the TF provider is a party to through their membership of a particular industry.

Preliminary Assessment: When the TF Authority receives a complaint it will complete a preliminary assessment. The assessment process will include providing the TF provider with the opportunity to comment on the complaint. The preliminary assessment can result in the TF Authority:

- referring the complaint (in full or in part) to the Ombudsman, the Privacy Commissioner, the Inspector-General of Intelligence and Security[6] or another officeholder when, following consultation with those officeholders, the TF Authority determines the complaint falls within their jurisdiction and would be more appropriately dealt with by them;
- informing the parties to the complaint that it will not consider the complaint further and explaining its reasons (the reasons for not further considering a complaint are outlined in section 73 of the Act); or

[6] The Inspector-General of Intelligence and Security provides independent oversight of the New Zealand Security Intelligence Service and the Government Communications Security Bureau. The Inspector-General can investigate complaints against the intelligence agencies.

- deciding that a breach appears to have occurred.

The TF Authority will advise the complainant and the TF provider or providers of its preliminary assessment and its reasons for it. Where its assessment is that it a breach may have occurred, the TF Authority will inform the parties about its powers of investigation and the remedies it may grant, and also provide information on any dispute resolution scheme run by the Authority.

Investigation: Following the preliminary assessment process the TF Authority may commence an investigation after notifying the TF provider of its intention to do so. The requirements the TF Authority must meet for conducting an investigation are established in section 80 of the Act.

Findings: If the TF Authority is satisfied that a breach has occurred, it will provide the TF provider and the complainant with written notice of its decision and the reasons for it.

Remedies: The TF Authority may also apply one or more of the following remedies after first giving the TF provider a reasonable opportunity to make submissions on the remedies:

- issuing a private or public warning;
- requiring the TF provider to meet additional record-keeping or reporting requirements;
- issuing a compliance order requiring the TF provider to remedy the breach;
- suspending the TF providers accreditation or the accreditation or the relevant service; and
- cancelling the TF provider's accreditation or the accreditation of the relevant service.

Redress through the courts

The Act enables the provision of accessible, fair, efficient, and effective complaints and dispute resolution processes that have particular regard to tikanga Māori.

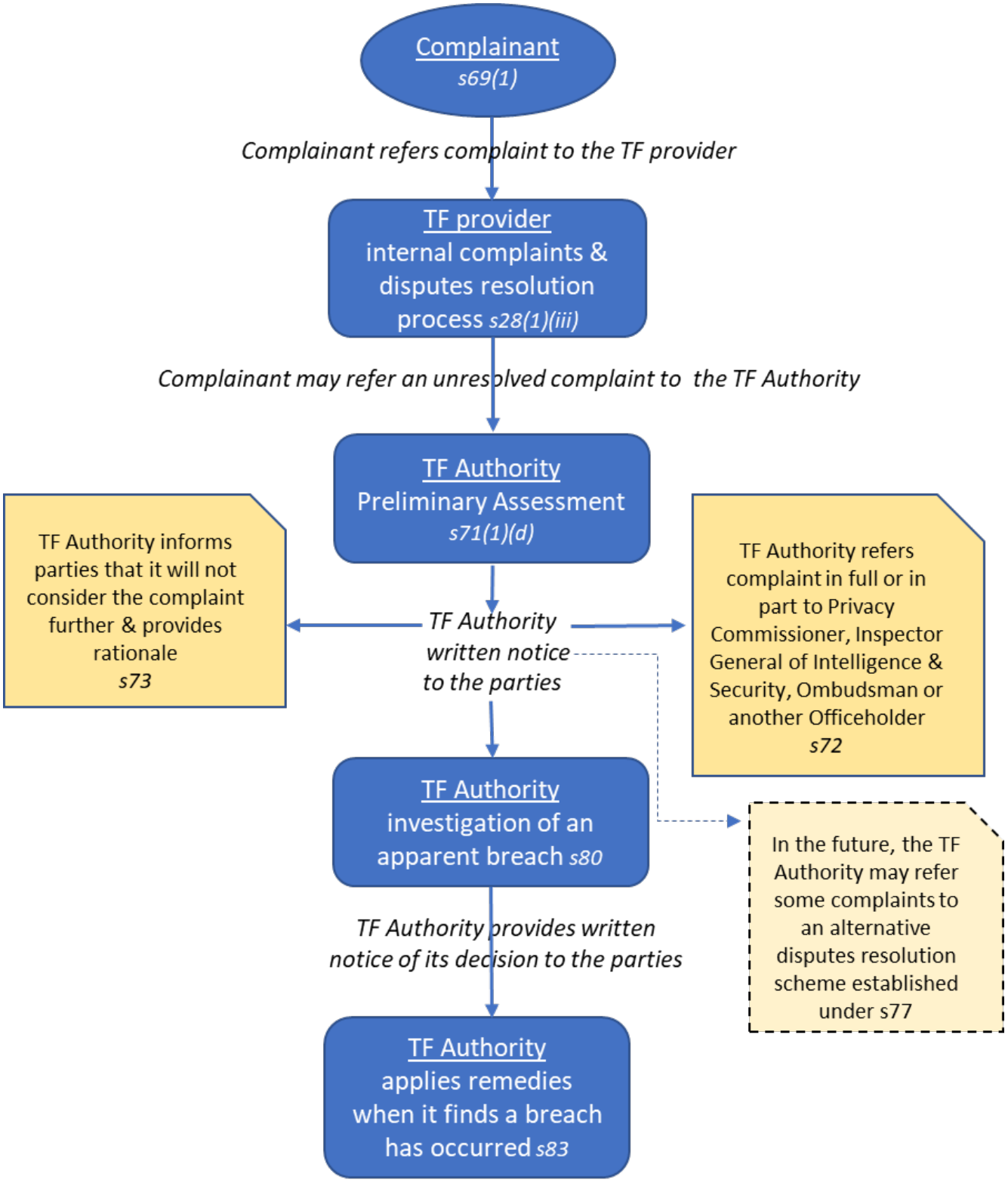
Participants in the Trust Framework system are also able to pursue civil claims under the general law in the usual way (for example, any private contractual disputes or negligence claims, subject to the limited immunity in section 104 of the Act for TF providers).

Decisions made by the TF Authority, including those relating to the complaints and dispute resolution process, may be subject to judicial review by the High Court.

We are seeking comments on the complaints and dispute resolution process, in particular:

14. Do you agree or disagree with the proposed internal complaints and dispute resolution requirements TF providers will need to meet? Please explain why/comment
15. Are there any implementation issues or risks that need to be addressed?
16. Does the overall complaints and dispute resolution process offer sufficient avenues for complainants to seek redress?
17. Do you consider there is a need for an alternative dispute resolution process to complement the complaints investigation and compliance management functions that will be undertaken by the TF Authority? If so, in what circumstances could it add value?

Figure 2: Trust Framework Complaints and Dispute Resolution process



7. Recordkeeping

Overview

The Act enables the establishment of regulations requiring TF providers to collect required information about its activities and hold that information for a set period.

Retaining records on the information gathered to deliver accredited services to users and relying parties is necessary to demonstrate the integrity of providers' service delivery processes, and support the TF Authority's monitoring and compliance management activities. For example, when investigating a security breach, the TF Authority may ask the TF provider about what information may have been compromised and how.

Proposed regulations

In accordance with section 42 of the Act, the regulations will require TF providers to collect and retain information about their activities, store it in a secure database, and provide the TF Authority with access to those records at all reasonable times upon request.

The regulations will require the TF provider to retain information necessary to provide assurance that it has delivered accredited services in accordance with the requirements specified in the Act, rules and regulations. Where information received by the TF 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 the information used in the provision of digital identity services rather than the personal information itself.

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

The seven-year time frame is aligned with requirements for the retention of records in the Companies Act 1993, as well as financial record keeping requirements in the Goods and Services Tax Act 1985, Securities Act 1978 and Tax Administration Act 1994.

We are seeking comments on record keeping requirements, in particular:

18. What type of information should be retained by TF providers?
19. Do you agree or disagree with the proposed seven-year time frame for record keeping? If not, what time frame do you think is more appropriate and why?
20. Are there any implementation issues or risks that should be addressed?

8. Reporting

Overview

The Act enables the regulations to establish TF provider reporting requirements.

Proposed regulations

Annual Reports: The regulations will require every TF provider to deliver an annual report to the TF Authority. This will contribute to the TF Authority's ability to monitor and assess the performance of each TF provider and the overall regulatory system. Annual reports will need to include information in a form specified by the TF Authority on:

- *Organisational Governance and Management:* Organisational governance and management arrangements, and the personnel responsible for them.
- *Service use:* Service transaction volumes, and the types of parties accessing each accredited service.
- *Service Delivery:* Steps taken to ensure accredited services are delivered in accordance with required service standards; any breaches of service standards, and actions taken to remedy them; and steps taken to improve service delivery.
- *Complaints and Disputes Resolution:* Number and type of complaints made to the provider; and the outcomes achieved by internal complaints and disputes resolution processes, including instances where the TF provider has upheld the complaint and implemented remedies to ensure its service meets compliance requirements.
- *Fraud:* Any attempted fraud events, and the actions taken to address them.
- *Financial Performance:* The TF provider's financial position and performance.

This is a form of self-assessment and reporting, which enables the TF Authority to provide oversight of TF providers without going through a full reaccreditation process each year.

Other Reporting: We also propose that the regulations will require every TF provider to submit separate reports within 20 working days covering any actual or suspected fraud events, or any other events that adversely affect confidentiality, the integrity or availability of the digital identity service, and has caused or presents a risk of serious harm.

For the avoidance of doubt, the regulations will also refer to TF providers' obligations under the Privacy Act 2020 to report privacy breaches that have caused serious harm to the Privacy Commission and require the provider to also inform the TF Authority. These reporting requirements are designed to ensure the TF Authority is aware of significant events, and is able to intervene or assist to resolve issues where appropriate.

The regulations will also require TF providers to report to the TF Authority on any changes to the organisation's people, operating policies, processes, or systems that have a material impact on their ability to meet accreditation requirements as specified in the Act, rules, or regulations.

We are seeking comments on reporting requirements, in particular:

21. Do you agree or disagree with the proposed reporting requirements? Please explain why/comment
22. Do you agree or disagree with the time limit for reporting actual or suspected fraud or other events that have caused or present a risk of serious harm? Please explain why/comment
23. Are there any implementation issues or risks that should be addressed?

9. Cost Recovery

Context

The Act includes provision for the establishment of regulations to recover certain costs through fees, including the cost of administering the accreditation process and more generally the costs of operating the Trust Framework.

It is anticipated that the TF Authority's initial establishment and first two years of operating costs will be met from Crown funding without a contribution from fees. Therefore, early entrants will not need to pay an initial accreditation fee. Later entrants and providers seeking to renew accreditations would, however, incur a fee if cost recovery regulations are introduced.

We anticipate consultation on cost recovery regulations relating to the TF Authority's administration of the accreditation process and the Trust Framework more generally will take place during the second round of regulations development.

Participation from users, TF providers, and relying parties in the digital identity system enabled by the Trust Framework is essential to giving people greater control of information about themselves, and to access services more easily. We will, therefore, consider what impact cost recovery arrangements have on participation. In setting fair and equitable fees, we will distinguish between the TF Authority's services that deliver a significant private good and those that are more generally considered to deliver a public good.[7]

We are seeking initial comments on cost recovery arrangements, in particular:

24. To what extent do you think accreditation fees should be used to cover the costs of accreditation and the administration of the Trust Framework?
25. If you are a potential TF provider, to what extent would accreditation fees impact on your participation in the Trust Framework and why?
26. Are there any implementation issues and risks that need to be addressed?

[7] According to NZ Treasury Guidelines, a private good is one where people can be excluded from its benefits at a lower cost and use by one person conflicts with use by another. Examples of private goods include passports, birth certificates and licenses. In our case the provision of an accreditation can be considered a private good.

A merit good is one that is likely to be produced at a lower level than the community desires in a free market situation. This may be because the public benefit of the good is greater than the private benefit, and consumers only take into account the private benefit when making decisions.

A public good is one where excluding people from its benefits is either difficult or costly and its use by one person does not detract from its use by another. There is a good case for recovering the cost of a public good through general taxation or, if the benefits are localised, from local government revenue. Examples include national security and street lighting. Many services provided by Government share the characteristics of public goods to some extent. Although such services might have some elements of public good, there still might be justification for recovering costs.

Appendix A – Glossary of key terms

Term	Definition
Accreditation	An act to give approval 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 TF Authority to be provided by a particular TF provider.
Digital identity	A digital representation of a person's identity information and other attributes about them 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
TF Authority	The Authority established under section 58 to oversee the running of the Trust Framework.
TF Board	The board established under section 42 of the Act to oversee the TF Authority.
TF provider	A digital identity service provider accredited by the TF 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/