DIGITAL IDENTITY.NZ

Te Tari Taiwhenua
Internal Affairs

Digital Identity Services Trust Framework Rules Consultation

Submission Form

APRIL 2024

About the consultation

The Digital Identity Services Trust Framework Act 2023 (the Act) comes into force on 1 July 2024. It enables the introduction of a new regulatory regime, which will establish Rules and regulations for the provision of trusted digital identity services.

The Trust Framework aims to create a digital identity ecosystem where people have more control over their own data, including what they choose to share about themselves and who they share it with. It sets out the legal framework for digital identity services, supporting New Zealanders to have more confidence in using online services.

The Trust Framework is governed by primary and secondary legislation:

- The Digital Identity Services Trust Framework Act was passed on 5 April 2023;
- The Digital Identity Services Trust Framework Regulations, which received policy approval through Cabinet earlier in March, are currently being drafted; and
- The Digital Identity Services Trust Framework Rules.

The Trust Framework Rules (TF Rules) will establish the technical and operational requirements that digital identity service providers will need to comply with to achieve and maintain accreditation by the Trust Framework Authority.

The development of the draft TF Rules has been supported by a range of stakeholders, which includes broad representation from the public and private sector.

The draft TF Rules cover five categories prescribed by the Act: Identification management, privacy and confidentiality, security and risk, information and data management, and sharing and facilitation. Each rule category includes an outcome that outlines what the rule aims to achieve.

Consultation on the Digital Identity Services Trust Framework was completed during the legislative process for the Act. This covered the structure of the Trust Framework, governance, te ao Māori provisions, and compliance and enforcement powers. DIA also conducted targeted consultation on the policy direction of Regulations in 2023. The consultation for the TF Rules is targeted given the operational and technical nature of the Rules.

Submitting your feedback

We are seeking your feedback on the proposed Digital Identity Services Trust Framework Rules. This submission form sets out key questions to guide your feedback on the draft Rules. Please enter your feedback in this submission form and send your completed form to distf@dia.govt.nz by **5pm, Friday, 3 May 2024.**

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

Timing and next steps

The team at DIA will collate and analyse all submissions once the consultation closes, and update the Rules accordingly. These will be reported to the Trust Framework Board for consideration. A summary of feedback and key themes will also be published on our website.

We anticipate the rules to be finalised and gazetted in September 2024. Questions and more information

If you have questions about this process, or need assistance, please contact distf@dia.govt.nz.

Trust Framework Rules Consultation

Submitter information

Please provide some information about yourself. It will be used to help us understand how different submitters view the proposed Trust Framework Rules. This section is separate to the actual submission form for easy removal to protect your personal information. Please refer to our Privacy Statement below for further information.

Name:	Colin Wallis
Email Address:	info@digitalidentity.nz
Phone Number:	021 961 955
Organisation:	Digital Identity New Zealand

Are you making this submission on behalf of an organisation? ☑ Yes ☐ No

If yes, please provide a brief description of your organisation and your interest in the Digital Identity Services Trust Framework.

DINZ is a not for profit, membership funded association and a member of the New Zealand Tech Alliance. DINZ is the voice of digital identity in Aotearoa- an inclusive organisation bringing together members with a shared passion for the opportunities that digital identity can offer. It supports a sustainable, inclusive and trustworthy digital future for all New Zealanders through its vision- that every New Zealander can easily use their Digital Identity in its mission to empower a unified, trusted and inclusive Digital Identity ecosystem for Aotearoa New Zealand that enhances Kāwanatanga (honourable governance), Rangatiratanga (self-determination and agency) and Ōritetanga (equity and partnerships).

Please confirm which of the following categories you or your organisation identifies with or represents (you may select multiple categories if necessary):

☑User ☑Relying party ☑Digital identity service provider / potential Trust Framework (TF) provider ☐Other (please specify):

To assist us with the publication process or release under the Official Information Act please respond to the following:

☑ I consent to my submission being published by the Department and released under the Official Information Act if requested.

☐ I consider my submission, or an identifiable part of my submission, should be withheld from release under the Official Information Act and have stated the grounds that apply under section 9 of the Act for consideration by the Department.

Reasons for withholding submission in whole or in part:

Privacy Statement

The information provided in your submissions will be used to inform the development of the TF Rules and help form our advice to Ministers for the approval of these rules. We may contact submitters directly if we require clarification of any matters in submissions, as such, we collect personal information from you in the submission form, including your name; your email address or phone number; and the name and brief information about your organisation.

The Privacy Act 2020 governs how we collect, store, use and disclose personal information about submitters and the information you have provided. You have the right to access and correct your personal information. Your personal information will be removed *2 years* after the conclusion of this consultation, at which point we will securely destroy the submission forms.

We will quote or publish some of the submissions on our website. Submitters' personal details are collected separately to the submission, therefore can be easily removed before publication.

Please specify clearly in the submission form if you do not wish to make your submission (or any specific part of your submission) public, or if you prefer to have your submissions published anonymously.

Submissions are subject to request under the Official Information Act 1982 (OIA). If you have any objection to the release of any information in your submission including which parts you consider should be withheld, together with the reasons for withholding the information, please note these in your submission form. We will take your objections into account and will consult with you when responding to requests under the OIA.

Trust Framework Rules Consultation

Submission form

This form sets out the key areas that we are seeking your feedback on the proposed Trust Framework Rules.

Accredited Services and activities

The Digital Identity Services Trust Framework regulations prescribe the types of digital identity services that may be accredited under the Act. The TF Rules set out what activities are required to be completed for each service.

Descriptions of these services and activities are contained on page 7 to 10 of the accompanying TF Rules document.

1. Are the definitions of the activities an accurate reflection of the functions and processes intended by the Digital Identity Services Trust Framework?

☐ Yes ☑No ☐ Not sure ☐ No position

Please explain why / comment

Activities should not be described as functions and processes. The references to the Identification Management Standards assumes Identity Service Providers have the same functions and processes as relying parties. This is not the case. The trust framework is intended to nurture an innovative eco-system, so rules should be based on defining accountability for deliverables and non-functional assurances for the targeted activities. The “how” focus of the activities definitions takes the rules down a road that doesn’t fit the market.

The W3C Verifiable Credential Specification states that VCs are not intended for user authentication of online services. The Identification Management Standards are designed around relying parties using Authenticators for access to online services.

2. Are the corresponding activities for each DISTF service an accurate reflection of the functions you expect that service to undertake? Please see pages 8-9 of the TF Rules document.

☐ Yes ☑No ☐ Not sure ☐ No position

Please explain why / comment

The activities are tasks that will be performed when offering services to relying parties and users, but the service definitions do not align with the range of services, solution providing, and systems integration roles that various vendors perform.

The language also changes when moving between identification management and identity services. Information Providers will issue verifiable credentials, which can be used for information sharing and identity assurance. For example an information service as described here is not an Identity Service, it's a personal information service. One of the defining characteristics of improved trust is that intermediaries should not know personal attributes (information).

More examples: the mDL evolved out of the need for in-person identity verification, Verifiable Credentials evolved out of decentralised/offline exchanges, while authenticators serve identification needs for online services. While these all share common identity activities, the service definitions, solution designs, and systems integration are all quite different. The services do not describe the services we expect to offer, and so the rules for accreditation do not line up elegantly with the services being offered or consumed.

3. Are there any other activities which you think should or could be included as part of one or more of the five DISTF services?

☐ Yes ☐No ☑Not sure ☐ No position

Please explain why / comment

We do not see the value in combining activities into service definitions. Why can't we simply accredit the activities, regardless of the service design? Packaging the activities into defined services adds complexity and reduces flexibility, with no obvious benefit.

Identification Management

All personal and organisation information transacted through the Digital Identity Services Trust Framework need to go through robust process to ensure its level of accuracy and quality.

This category sets out the requirements for verifying and binding personal information and establishing a credential, including providing levels of assurance for the information being presented.

You can find the information about the proposed rules on pages 14 to 17 of the accompanying TF Rules document.

4. Do you agree with the requirement to conform to the Identification Management standards?

☐Strongly agree ☐ Agree ☐ Not sure ☐ Disagree ☑Strongly disagree

Please explain why / comment

The identification management standards were designed for relying parties working with Authenticators of entity information. Identification management is not the same thing as identity management. Many of the responsibilities described fall on the Information Provider and the Relying Party. For example, the information assurance standard has very specific relying party objectives, which an infrastructure provider should never know or do. They should never examine or interfere with the information flow between the info provider, the subject, and the relying party.

Issuing a verifiable credential is not the same as authenticating entity information. The issuer of a credential has no way of knowing how a subject might use that credential, or the level of assurance required by a relying party. Credentials bind information to a subject and the issuer, which are verified by the relying party. The credential does not have to be bound to an "authenticator" to be useful in identity management – verification and validation methods can be decoupled from issuance in decentralised systems.

There are many issues at the detail level which reduce the value of getting accredited. Examples: (IM.5.10) credential verification methods must be encrypted. In decentralised solutions there is no transmission of information to be encrypted. Public Keys and DID documents are used for decryption and validation, so they can't be encrypted themselves – they are intentionally public. IM.5.4 – there are many scenarios where a credential must never be revoked, but they may be terminated/expired. Historic documents should be immutable rather than revocable, otherwise trust can be broken. IM.5.12 – why are the rules specifying formatting standards? There is a separate standards conformance assessment. IM.5.14 – why must standards and formats be published on a public website? These are technical interoperability details which can be surfaced in many ways.

5. Do you agree with the alignment between each activity to an equivalent section of the Identification Management Standards? For example, *Verifying Information* requires conformance with the Information Assurance Standard.

☐Strongly agree ☐ Agree ☑Not sure ☐ Disagree ☐ Strongly disagree

Please explain why / comment

In general, the combination of service definitions, activities, outcomes, Identification Management Standards, and IMS controls makes these rules incredibly complex to understand. There is also no tie back to principles. Can we please simplify this?

Perhaps just specify the activities that should be regulated and how the principles are being applied to those activities. Any identity service provider undertaking those activities as part of their service offering can sign up to be regulated and accredited.

6. Do you agree that all attributes on a credential be verified and bound? See Rules IM.5.1 & IM.5.2.

☐ Yes ☐No ☑Unsure ☐ No position

Please explain why / comment

What does "established" mean in this context? Credentials can be issued or presented as documents, as well as available as a service. Not all attributes in a credential are about the subject, some of them may be about the issuer, or supporting details. These do not need to be bound to the subject, but are bound to the credential. Verification of documents by relying parties can happen any time, and more than once. The language seems to assume a real-time connection between the credential provider and relying party - that's a very narrow use case.

7. Are requirements in IM.5.12 appropriate for the format of credentials? If not, please suggest alternatives or additions.

☐ Yes ☐No ☑Unsure ☐ No position

We do not believe the rules should specify the format of credentials. The rules should require providers to declare the standards they have adopted, and conformance to those declared standards. Requiring the Minister to sign-off updated rules every time standards change is not a good use of rules or Minister's time.

8. Should standards for any other processes be included in the TF Rules? For example, these could be standards for unique identifiers or semantic data. In your answer, consider if *guidance* may be more appropriate for some standards.

☐ Yes ☑No ☐ Unsure ☐ No position

Please explain why / comment

These rules effectively become law, which is not the appropriate place to schedule something as dynamic as industry standards, processes or formats. Rules are for governing activity, not specifying systems or processes. The focus is far too operational rather than management and governance.

9. Do you consider there to be any implementation issues or risks associated with the proposed rules relating to Identification Management?

Please comment below

If someone is implementing identification services such as authentication of users for online services, then the identification management standards are relevant and practical to assess. After a broad discussion across several Identity Service Providers, there was complete consensus that the proposed rules are far too complex and unclear to be adopted. As a result, we have a grave concern that these rules will prevent Identity Service Providers from considering accreditation.

10. Do you have any recommendations for removing, modifying, or adding to any of the Identification Management rules?

Please comment below

Perhaps just specify the activities that should be regulated and how the principles are being applied to those activities. Any identity service provider undertaking those activities as part of their service offering can sign up to be regulated and accredited.

Focus the rules on management and governance of Identity Service provision, rather than standards, process, formatting, etc. These rules are trying to do too much.

Tie the rules back to principles. That way, when a rule proves to be unhelpful we have a principle to direct how it can be improved in the future.

11. Do you have any other comments for the Identification Management rules, or the corresponding objectives?

Please comment below

The approach to specifying the endorsed versions of in-scope category standards is open-ended (i.e., in the form "Version 1 or later") rather than specific and actionable (e.g., in the form "use the most-recent published version or the version immediately prior if that is not deprecated"). The importance of adherence to compatible and contemporary standards is crucial for digital identity, and mayhem is likely to result if this approach is not tightened.

Sharing and Facilitation

All digital identity service transactions need to be authorised by an individual that has the necessary authority to do so. Users need to be appropriately informed of what they are authorising, and authorisations should be recorded by trust framework providers.

You can find the information about the proposed rules on pages 18 to 22 of the accompanying TF Rules document.

12. Do you agree with the requirement to conform to the Federation Assurance Standard of the Identification Management Standards?

☐ Strongly agree ☐ Agree ☐ Not sure ☑ Disagree ☐ Strongly disagree

Please explain why / comment

"This standard applies whenever an individual, organisation or group wants to establish a Credential that can be reused by Entities in identification processes with multiple Relying Parties (RP)". Identification processes are undertaken by the relying parties, not the credential provider or facilitation provider.

The only time this would be relevant is when a credential or facilitation provider is presenting a credential(s) for use in identification by a relying party.

Objective 3 – FA3.01 is problematic. A credential provider must not include unique identifier information in the credential to mitigate risks of tracking and profiling. However some unique identifiers are so extensively used that they are unlikely to comply. These are the ones people would use for tracking and profiling. Adding to this, there are plenty of unique identifiers that are intentionally public – NZ Business Number, GST Number, Internet Domain Names, mobile phone numbers, etc.

13. Are there any other requirements that could be set as rules, including additional standards, to support the objectives for facilitation establishment and credential presentation?

Please comment below

As explained above, we believe the rules should focus on the management and governance of Identity Service Provision activities, rather than prescribing standards, processes or systems.

14. Do you agree with the requirement to obtain authorisations for the activities listed? See Rule AN.1.1 on page 20 of the draft rules document.

☐ Strongly agree ☐ Agree ☐ Not sure ☑Disagree ☐ Strongly disagree

Please explain why / comment

Users request services from service providers. Getting users to authorise the technical activities by which those services are provided is not appropriate. The whole point of providing services is to abstract away and take care of this complexity, so they don't have to think about it at a detailed technical level.

15. Do you have any comments on the rules for valid authorisation and permitted user? See Rules AN.2.1, AN.2.2, AN.3.1 and AN.3.2 on pages 20-21 of the draft rules document.

Please comment below

This language does not put the user at the centre. For example a relying party should obtain informed consent before engaging with Identity Service Providers about someone. TF Providers should only accept instructions from users, and if that instruction is received through a third party, they should verify its authenticity with the subject.

A TF Provider cannot inform a user about what they are authorising unless the TF Provider knows what the relying party is going to do. It shouldn't be the job of the TF provider to obtain authorization for activities requested by relying parties. This language leaves that open.

16. Are there any implementation issues or risks associated with the rules set out in *Informed authorisation* and *Authorisation record* on pages 21-22 of the draft rules document?

Please comment below

17. Do you have any recommendations for removing, modifying, or adding to any of the Sharing and Facilitation rules?

Please comment below

18. Do you have any other comments for the Sharing and Facilitation rules, or corresponding objectives?

Please comment below

Privacy and Confidentiality

Users need to have confidence that providers are using their information appropriately and incorporating privacy-protecting measures across the entire information lifecycle, from collection through to use, sharing and disposal within the ecosystem.

You can find the information about the proposed rules on pages 23 to 25 of the accompanying TF Rules document.

19. Do you have any comments on the rules in this category?

Please comment below

PV.1.4 digital identity services will be constantly changing, so reviewing the Privacy Impact Assessment (PIA) on each change is impractical. This would normally happen the other way round – each change would be assessed for their privacy consequences beforehand. Only if the consequences are significant enough to justify a review of the PIA would that review happen. We review the service changes for privacy, we don't review the PIA for service changes.

20. Are there any implementation issues or risks for the rules in this category that need to be addressed?

Please comment below

21. The privacy rules require Trust Framework Providers to implement certain privacy requirements, to minimise privacy risks. Do you agree that these requirements are sufficient?

☐ Strongly agree ☐ Agree ☐ Not sure ☐ Disagree ☐ Strongly disagree

Please explain why / comment

22. Do you have any recommendations for the Privacy or Confidentiality Rules to be removed, added, or modified?

Please explain why / comment

23. Do you have any other comments for the Privacy rules, or corresponding objectives?

Please comment below

Security and Risk Management

Strong security and risk management ensures that personal and organisational information is stored, shared, and used in a secure manner. By ensuring that there is clear accountability for security across a whole organisation, users can be assured that Trust Framework providers will maintain the confidentiality, integrity, and availability of the information that they process, store and share.

You can find the information about the proposed rules on pages 26 to 32 of the accompanying TF Rules document.

24. Do you have any comments on the rules in the security and risk management category?

Please comment below.

As this is a legal document, please change the references to security risks. The common practice is to maintain a security risk register, as part of the security management plan.

This section should reference a security risk register rather than “security risks”.

25. Providers must provide evidence that they are compliant with these rules. How do you think this evidence should be provided?

Please comment below.

Use a risk register, and a declaration from the designated individual regarding the independent assessment. The regulatory authority does not want to be accountable for approving the security management of a TF Provider.

26. Do you agree with the security risks identified in Rule SR.1.3? The risks are described further on pages 31-32 of the draft rules document.

☐ Strongly agree ☐ Agree ☐ Not sure ☑Disagree ☐ Strongly disagree

Please explain why / comment

Security Risks are normally described in terms of the vulnerability and potential harm, rather than what causes it. A service provider outage is not a security risk, it is an incident. What are the security consequences of the outage?

Use of the term "weak" is problematic. By definition, any incident that could have been avoided is the result of a weakness. However perfection is impossible, so everything is "weak" in hindsight.

27. Do you agree or disagree with the proposed cryptography requirements in Rule SR.2.7?

☐ Strongly agree ☐ Agree ☐ Not sure ☑Disagree ☐ Strongly disagree

Please explain why / comment

First, please use the full name of the security manual as the acronyms are so close (NZIMS and NZISM).

The cryptography specifications in the security manual were not selected for the data classifications such as public, commercial, etc. They are intended for use in more sensitive classifications such as restricted or secret.

28. The Security and Risk Management rules require Trust Framework Providers to implement certain practices, in order to minimise security risks. Do you agree that these requirements are sufficient?

☐ Strongly agree ☐ Agree ☑Not sure ☐ Disagree ☐ Strongly disagree

29. Do you have any recommendations for removing, modifying, or adding to any of the Security and Risk Management rules?

Please explain why / comment

SR.2.4. "identify changes to normal behaviour." The approach is normally to look for anomalous behaviour rather than model what is "normal" and assess changes. Profiling normal behaviour goes against privacy principles, and is unnecessarily complex to do.

30. Do you have any other comments for the Security and Risk Management rules, or corresponding objectives?

Please comment below

Information and Data Management

Personal and organisational information being collected, held, and shared within the proposed Trust Framework can be managed in commonly accepted ways, that meet industry good practice standards.

There are commonly accepted requirements for information management practices. Trust Framework providers should implement these practices including appropriate governance, information lifecycle management, and recordkeeping and reporting for information and data. Consideration should also be given for ethical handling of information and data.

You can find the information about the proposed rules on pages 33 to 35 of the accompanying draft rules document.

31. Do you have any comments on the rules in this category?

Please comment below.

From the perspective of a service provider, the regulatory burden and the retention costs are likely to be much too high (e.g., keeping records of all transactions for seven years, which is perhaps pegged against the financial-audit obligations; keeping records of other activities for twelve months; and keeping some for thirty days such as good practice for cybersecurity). Stronger clarity about "recordkeeping" means in this context is needed.

32. Do you have any recommendations for removing, modifying, or adding to any of the Information and Data Management rules? This may include recommendations and data (or other) standards that support interoperable and secure digital identity services.

Please explain why / comment

IF3.1 It would be very helpful if a standard was specified to help all stakeholders understand and meet the recordkeeping expectations.

IF3.2 Neither the rules nor regulations for that matter are specific on what "information" means in this context. For example, gigabytes of network traffic information is generated every day about identity services, but is usually only held for 30 days. Commercial

contract related information is held for 7 years for auditing purposes. Information is retained for a reason, and implementable direction is required here by way of retention requirements to serve specific purposes.

33. Do you have any other comments for the Information and Data Management rules, or corresponding objectives?

Please comment below

IF.3.2 – the rules (and indeed the regulations) have the potential to render uneconomic, the retention period requirements. These should be reasonable and will differ from one provider to the next. Rather than have the regulator specify the period, perhaps require the TF Provider to have a data retention plan that can be assessed for being reasonable?

General Questions

34. Are there any other requirements that should be set as rules? This may be additional standards, or requirements to improve security, privacy, interoperability, or user experience.

Please comment below

35. Do you have any further comments you would like to provide to us on the proposed Digital Identity Services Trust Framework Rules?

Please comment below

Overall, these rules are not fit for purpose — they are overly complex and in our opinion will be too expensive for the vast majority of NZ companies to comply with.

As we have pointed out a number of times above, we have serious concerns that the structure of the rules is incredibly complex, and the focus is too operational. The rules are trying to do too much at the system/process/operational level.

In their current form, the rules layer complexity with service definitions on top of simple activities, then map those service definitions onto bespoke standards maintained somewhere else. The rules comprise 4 standards, 5 services, 7 activities, and 10 roles. The DISTF documentation set offers low comprehensibility for non-identity specialists (and is tough-going for identity specialists too!). The documentation is not helping clarify the expectations and nature of the rules environment, and is still causing confusion in the digital identity community.

Our working group has over 30 members. Even the most experienced experts were

struggling with the complexity, and the business leaders were struggling to see how they would afford operating a compliant business.

The material made available for consultation is broadly impenetrable and we wonder what sort of artefacts will be made available in future to encourage participation and engagement from throughout NZ Inc., as the current artefacts fall short of what is required. What level of consumability will be set out around these rules? As they stand, these rules are "opaque" for a general audience.

The following bullet points summarise comments made by members in their review of the rules and may help inform future revisions:

- The regulatory burden should not be one-size-fits-all (e.g. proving a document should be different than proving an identity; validating a passport should be different than proving a student enrolment status) and it's currently quite heavy across the board. In thinking about how the rules work for different sizes of organisations is there a mismatch between the aspiration for the DISTF to enable an inclusive and innovative digital identity ecosystem for all Aotearoa and the nature and positioning of the DISTF rules (which feel "heavy" and better suited to citizens doing business with Government).
- While we acknowledge the intent to lean into and to some extent ‘future-proof’ the rules with decentralised architectures in mind, in their current form substantial parts of the rules are limited to decentralised identity scenarios. It’s unclear how the rules work in organisations with ‘hybrid identity architectures’ where a mix of status-quo centralised approaches are in place with adoption of emergent decentralised approaches over time.
- Risk management controls for data management are prescriptive and skewed too far towards the capabilities of large enterprises. For example behaviour anomaly detections. As risk management controls are always improving as a function of the technology (e.g. AI based anomaly or risky sign-in detections) prescribing specific controls into the rules which are then locked post gazetting, does not support future evolutions.
- There is too much coverage of general implementation in these rules that should be covered by other existing standards and referenced as such.
- In none of the documentation throughout this process has there been sufficient attention to versioning nor packaging/indicating specific aspects are intended for a specific audience/role.

Supplementary feedback

Thank you very much for participating in this consultation process. Your feedback will help us inform decisions about the regulations proposals on the *Digital Identity Services Trust Framework*. If you would like to provide any supplementary feedback, you can email us at distf@dia.govt.nz