DIGITAL IDENTITY .NZ

Te Tari Taiwhenua
Internal Affairs

Submission Form

Digital Identity Services Trust Framework Regulations

How to submit this form

The Department of Internal Affairs would like your feedback on the proposals contained in the discussion paper, *Digital Identity Services Trust Framework Regulations.*

Please complete this submission form and send it to us by email to Digital.Identity@dia.govt.nz

We need to receive your submission by **5pm, Wednesday 20 September 2023.**

When completing this form, please provide comments and supporting explanations for your reasoning where relevant. Your feedback will provide us with valuable information and inform decisions about the regulatory proposals.

We appreciate the time and effort you are taking to provide your views on the regulatory proposals outlined in the discussion paper. If you would like to add to your submission or to discuss anything, please reach out us at Digital.Identity@dia.govt.nz

Submitter information

Could you please provide some information about yourself. It will be used to help us understand how different sectors view the proposed regulations.

Your name, email address, phone number and organisation

Name:	**Colin Wallis**
Email Address:	**colin.wallis@digitalidentity.nz**
Phone Number:	**021 961 955**
Organisation (if applicable):	**Digital Identity**

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 Service Trust Framework

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

☑ User X Relying party ☑ Digital identity service provider / potential Trust Framework (TF) provider

☑ Other (please specify): Platform Provider

About DINZ

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 & agency) and Ōritetanga (equity & partnerships).

Privacy and Official Information

Privacy Act 2020

The Privacy Act 2020 establishes principles about the collection, use and disclosure of personal information. The Department of Internal Affairs adheres to these principles, so any personal information you provide to us will only be used for the purpose of assisting in the development of policy advice in relation to the issues canvassed in the discussion paper.

☐ Please tick this box if you do not wish to have your name or other personal information included in any information about submissions we may publish.

Publication and Official Information Act 1982

It is usual practice for submissions made to the Department to be published on our website. We may also publish our submissions analysis and submissions may also be subject to a request made under the Official Information Act 1982. 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

Regulations

The following sets out the key areas as well as a proposed cost recovery section that we are seeking initial feedback on.

1. Accredited Services

The Digital Identity Services Trust Framework Act requires that the regulations prescribe the types of digital identity service that may be accredited under the Act. We propose that the regulations specify that the following five services can be delivered as accredited services by TF providers:

1. Information Services;
2. Binding Services;
3. Authorisation Services;
4. Credential Services; and
5. Facilitation Services.

Descriptions of these services are contained on page nine of the accompanying Discussion Document.

1. **Do you agree or disagree that the five identified services should be subject to accreditation under the Act?**

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

Please explain why / comment

We agree and we also disagree with the proposition, as detailed below:

1. *Agree*: The legal framework being proposed for an opt-in accreditation uses these service definitions, and it is appropriate that these digital identity services form the core of what falls in-scope for accreditation. However, we note that the services enumerated above are not accurately listed: "Authorisation Service" is incorrect, and should of course be "Authentication Service". Our responses are predicated on the assumption that this service in the submission form was an error, and that the in-scope service is "Authentication Service", as communicated elsewhere. If this is the structure of the trust framework that the Government wants to offer an accreditation service for, then these are the correct services at a minimum.

2. *Disagree*: Use of the term “should be subject to” infers a default authority and is not accurate. The Act does not give the authority to the regulatory regime to impose accreditation as inferred here. A better description for what is being considered here is “can be accredited by the TF Authority".

3. *Disagree*: The definition of Facilitation Service is not a typical term in industry practice and is too abstract as defined. The name "Facilitation Service" is understood to mean essentially Devices or User Agents. We strongly advise reuse of well-understood and widely-accepted definitions relevant to the digital identity ecosystem, not the creation of new abstractions that have the potential to overloaded. We appreciate that the term has probably been drawn from here: https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-terminology/ which is a noble effort to instigate consensus on the use of certain terms across Aotearoa in the context of digital identity but at the end of the day it is the job of the TF Board to review the terms and decide if they will accept the proposed meaning and descriptor for the purposes of the Regulation given the capacity for misinterpretation.

2. Are the definitions of the services adequate?

☑Yes ☑No ☐ I don't know ☐ Unsure

Please explain why / comment

1. *Yes*: For the purpose of a discussion document to provide a conceptual introduction, these definitions serve an adequate purpose.
2. *No*: These definitions are not adequate for any other use beyond a conceptual introduction. Service definitions that are testable and actionable are required to support operation of the Digital Identity Services Trust Framework.

3. Are there any other services which you think should or could be accredited?

There are no other services defined in the Trust Framework. It describes a complete system, so there are no other services necessary to complete the system.

We imagine that, in the fullness of time, there could be value in establishing strong guidance and ultimately accreditation for an *Authorisation Service* and for *Consent*. Other components, not necessarily services, should also be considered in future, such as user experience.

2. Accreditation Requirements

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 to the TF Authority and demonstrate they can meet the accreditation requirements specified in the Act, rules and regulations. You can find the information about the proposed accreditation requirements and related matters on pages 10 to 14 of the discussion document.

4. **Do you agree or disagree with the proposed accreditation requirements and the TF Authority's assessment criteria?**

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

Please explain why / comment

The discussion document only provides a high-level overview of the regulations, and the rules are only defined with basic definition statements. There is not enough information to determine if the accreditation requirements are appropriate for the TF Authority goals (we think not; for example with organisation identity and relating that to 'the fit and proper person' representative and to the documentation and other objects), nor whether these requirements are a justifiable investment for TF Providers to receive the benefit of accreditation.

Some requirements in the bulleted list are largely administrative while others disguise the potentially significant investment and incremental effort needed to achieve accreditation;

For example 'has the capability to meet the service standards specified in the rules to an appropriate level of assurance' is at a completely different level of difficulty than ' has demonstrated that it is financially sustainable' which can be drawn from annual accounts. The TF Provider can't determine the capability of its own services/products to meet a level acceptable for accreditation without seeing the assessment criteria that the auditor will use to assess a service's fitness for purpose.

5. **Do you think anything is missing or needs to be removed?**

The regulations are still at the conceptual design stage, so there is a lot that we expect will be changed, added, or removed as the TF Board develops up the initial accreditation offering.

A major concern we have is that the design process DIA is undertaking is investing a lot of time and effort on designing the entire accreditation requirements for the final target state, rather than what makes the most sense for Day 1 which might be something simpler and less burdensome. Any part could be removed, and there are a multitude of things that could be added.

This is why other jurisdictions piloted the operational system for 2-3 years before legislating, and to continue with pre-assessment so as to iron out issues and give the Identity Service Providers confidence that the return is worth the investment.

DIA needs to complete its conceptual design and prioritisation work before we can provide useful input into specific elements to implement.

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?**

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

Please explain why / comment

For accreditation to build value in the market it will take many years. Consequently, we do not believe TF Providers will be considering only being accredited for 2 years in business cases. If renewal is streamlined and the cost is justifiable, then 2 years might be appropriate.

The suitability of a 2 year period is entirely dependent on the accreditation requirements (particularly the rigour of the audit against the rules) provided by the TF Authority. If it is a significant burden every two years, then the period is too short.

Many TF providers may find a two-year accreditation cycle much too short, especially if there has been no technical change or functionality change to their systems in that period. We suggest a more-flexible set of re-accreditation triggers are considered that are a combination of:

- *Time-Based Trigger*: A starting default window of two years.
- *Reporting-Based Tigger*: After the time based trigger elapses, if the TF participant provides regular annual reporting on usage and system changes, then they are eligible for re-accreditation processes to adopt Change-Based triggers.
- *Change-Based Trigger*: If no significant functional or technical change has been reported to occur in a TF provider's service then the re-accreditation window can be extended for another year, to a maximum of five years since the last re-accreditation.

Other schemes, such as Kantara (which was based upon ISO and national standards) use a three-year accreditation cycle: full audit in Year 1, random sampling in Year 2, random sampling in Year 3, and full audit in the Year 4. Alongside this, any change in the service or any change in the standards, requires the impacted parts of the service to be audited. That might be less burdensome and more predictable, particularly for services that don't change much over time.

7. **Are there any implementation issues or risks associated with the accreditation process that should be addressed?**

There are no accreditation processes and audit specifics described, only a conceptual outline of regulations. The provisional accreditation describes something more like a qualifying assessment process or a report. A qualifying assessment would be useful, whereas a provisional accreditation that cannot be used in the market has no obvious value.

It would be helpful to have an accreditation journey mapped out. This question is probably best asked by the TF Authority when it is seated and has confirmed the process. The TF Authority itself will be highly reliant on the auditors, so without auditors to help co-create the accreditation process, the answer is open-ended. Clearly, time and cost are the key concerns for applicants and a good sense of both is needed before being able to answer this question sensibly.

Another risk is for services whose components don't naturally fall in the service categories laid out in the DISTF standards, rules, and regulations. Via a Statement of Practice or Applicability or similar, these differences will have to be exposed and enumerated.

Lastly, is the issue of pre-assessment. DINZ has previously discussed with DIA the notion of offering pre-assessment on a cost recovery basis but there was no outcome. DINZ still believes pre-assessment would assist all stakeholders.

8. **Do you agree or disagree that the accreditation mark should be displayed against services only?**

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

Please explain why / comment

- *Agree*: We agree with the base proposition that the Accreditation Mark must be used only in relation to services that have been accredited. Afterall it was DINZ that raised this mis-drafting in its submission on the DISTF bill and saw changes in the revision as a result The intent is understood: that the integrity of the Accreditation Trustmarks must be established, communicated, and protected.
- *Disagree*: Given the substantial existing body of commercial law addressing misrepresentation, we wonder if the TF Regulations should simply state that any promotion of TF-accredited services must comply with Trustmark terms of use, and publish those terms of use separately. This is a level of detail that does not need to be specified within and solved for by the TF Rules and the TF Regulations.
- *Caution*: There are ways to display the Trustmarks in relation to accredited services that might fall foul of a regulated requirement to be "displayed against services only". This is a term that is legally ambiguous, and confusing from a marketing perspective. We note that the visual and operational design of the Trustmark has to be very thoughtful of how to represent the Service inside the brand so that consumers and relying parties and verifiers alike are not confused into assuming a brand is accredited rather than one component service out of many that the brand may offer.

9. **Are there any implementation issues or risks associated with the introduction of the accreditation marks that should be addressed?**

This discussion document talks about regulations at a high level, and does not go into implementation in detail with a draft Terms of Use agreement for the Mark, so it's not possible to comment meaningfully. Or perhaps the question is aimed at responses around market traction issues and risks?. As the value proposition only goes as far as being a government assurance, it isn't developed sufficiently to comment on risks or issues.

Related to implementation risks more broadly, are the issues of revocation if or when the service falls out of compliance, misuse by misrepresenting its scope, etc, on its website. This will require legal contracts and likely a cryptographically-protected digital Trustmark that can be managed digitally/remotely.
https://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.02.01_60/ts_119612v020201p.pdf
— think of Open Badges (basic) but with added very high levels of protection.

10. **Do you have any concerns about the proposed approach to considering applications for provisional accreditation?**

The provisional accreditation describes something more like a qualifying assessment process/report. A qualifying assessment would be useful, whereas a provisional accreditation that cannot be used in the market has no obvious value.

As currently outlined in the TF Regulations, the "provisional accreditation" seems pointless from the TF Provider's perspective: the provisionally-accredited service is not accredited, the provisionally-accredited service cannot display the accreditation marks, the provisionally-accredited service has no guarantee that it will earn accreditation, and TF participation is opt-in.

If a provisional accreditation scheme is implemented, we recommend that the digital.govt.nz or a specific DISTF website would display accredited, provisionally-accredited services and applications for accreditation, clearly distinguishing them! Doing this would allow consumers, relying parties, and verifiers to gain an indication of a possible future accreditation coming down the line.

12 Months may be too short to allow for changes to be made to the service and to get it re-audited. 18 months might be more reasonable.

3. Service Levels

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. Further details are contained in the discussion document on pages 15 and 16.

11. **Do you agree or disagree that assessing an organisation's ability to provide a service up to a prescribed level is appropriate?**

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

Please explain why / comment

Academic point: For something to be appropriate it needs context. Service Levels as described here have no context, so it's difficult to understand how service levels could be prescribed.

Terminology Point: 'Service Levels' have different meanings in different contexts though they can be associated. The term Service Levels in this context is confusing since the same term can be used in a quality of service 'SLA' context, but we do not think that is the intention. TF Providers also offer products and services that might have a 'service level' applicable to them. Why is the term Assurance Level not used, or at least a derivative of that, to indicate that the meaning has its roots in that realm, rather than Quality of Service SLAs?

That said, if Service Levels for all intents and purposes Assurance levels, then yes, we Agree in principle. But much more clarification is needed as to why there should be four when most of the rest of the world operating digital identification TFs use three.

Also, Service Levels are thresholds rather than limits — they should describe an assured minimum others should expect through criteria transparently communicated and assessed by the auditor and confirmed as achieved or not achieved, rather than that assessment and decision made by the TF Authority. The establishment and operation of the DISTF Regulations must first and foremost be seen and pursued as an exercise in strengthening and supporting the market to build trust, not an industry-oversight exercise

To extend this point further, a TF Provider's Quality of Service could in theory be enhanced by an applicable Level of Assurance applied to it.

12. Are service levels useful for commercial purposes?

Yes, commercial agreements to provide services will set service level expectations. They are at the heart of customer experience and competitive positioning. In this context they can theoretically serve two main purposes; (a) a TF Provider's Level of Assurance for a service to be made available for relying parties' for transactions whose risk profile demands an evidential level of identity-related assurance; and (b) a TF Provider's Level of Assurance for a service associated with a service level in a Quality of Service context as introduced in the response to Q11. However, care would be needed to ensure the TF Board did not overreach the scope of the Act if it were to exploit the opportunity in (b) to any extent in pursuit of offering more value and incentive to potential TF Service Providers.

We are also concerned that even the minimum requirements of the lowest Service Level represent a substantially high bar that either many potential service providers will struggle to meet or will find that it requires too much investment and system change to enable participation with innovative use-cases that require lower-level trust and assurance, yet should be able to participate visibility in the wider TF ecosystem.

Under the impression we have - that the TF Authority will determine what Service Level a particular provider's service has achieved, but acknowledging the wider expectation that higher Service Levels will be viewed in the marketplace as being "more trustworthy", and noting the uncertainty that remains around costs, processes, and contracts - there is a real risk here Identity Service Providers will be disincentivised to apply.

13. Are there any implementation issues or risks that should be addressed?

Yes, if we understand Service Levels broadly as levels of assurance then they should be established in the standards and rules, and the claimed level should be proposed by the TF Providers for their products which reflect what is needed by the market segments they serve to be confirmed (or not) by the auditor. Service level determination should not be a post-audit determination handed down by the TF Authority.

The regulatory regime aims to build trust through valued accreditation — so the assessment criteria should be aimed at whether the TF Provider's product can meet the Service Levels set by the standards reflected in the rules.

4. Complaints and dispute resolution

The discussion document outlines the key elements of the complaints and disputes resolution process, including the proposed requirements TF providers will need to meet when providing an internal complaint and disputes resolution process, on pages 17 to 20.

14. Do you agree or disagree with the proposed internal complaints and dispute resolution requirements TF providers will need to meet?

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

Please explain why / comment

While most of the internal requirements are in line with standard business practices, only complaints relevant to the DISTF Act should be directed to the TF Authority.

If the complaint is in relation to privacy or security or some other office holder, then it is outside the scope of the Act and should be dealt with directly with the appropriate crown agency. These communication channels already exist and policies and processes are already established to meet these legal obligations. The TF Authority should have no role or value-add in these existing flows.

For the avoidance of doubt, the types of roles of a person or entity that is eligible to raise a complaint should be clarified. For example NZ citizens, other TF providers, consumer advocates, government agencies, NZ technology body advocates are anticipated to be eligible. Are organisations not incorporated in NZ able to raise complaints?

15. Are there any implementation issues or risks that need to be addressed?

Yes, including those outlined below:

1. *Tikanga Māori*: There is a requirement to have particular regard for tikanga Māori. It's a worthy sentiment, but lacks the detail needed to be meaningful as part of accreditation. The Act, section 53(2) states: "The board must seek advice from the Māori Advisory Group if a matter the board is dealing with raises matters of tikanga Māori". Approving these regulations is a matter for the TF Board to deal with and to raise matters of tikanga Māori. Some practical guidance for all TF Providers on all rules and regulations regarding tikanga Māori will make the job of accreditation and dispute resolution much easier for the TF Authority.

2. *Investigation Pathway*: For the investigation pathway, the TF Authority investigates, makes the determination, and prescribes the remedies. The artefacts from an investigation can be used in a civil court case. There are no checks and balances, meaning the TF Authority has to be perfect all the time. If it fails to meet that standard, there is no appeal or redress option baked into this regulation.
   We note that some Trust Frameworks overseas use unconnected independent contractors having no potential conflict of interest to investigate complaints to determine their veracity, actual, and potential harm, and report findings to the TF Authority equivalent (be they from third parties or from accredited or provisionally-accredited Identity Service Providers). This approach has benefits including that it avoids the risk of perceived bias by the TF Authority.

16. **Does the overall complaints and dispute resolution process offer sufficient avenues for complainants to seek redress?**

Yes, provided that our suggestions are accepted - at least to start with until there is more operational evidence to evaluate the efficacy of the process.

No, because there is seemingly no avenue to handle complaints about the TF Authority or Board. It is not addressed in the discussion paper.

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?**

No (see above). Any complaints that actually need to be dealt with by the TF Authority will actually need to be dealt with by the TF Authority.

5. Recordkeeping

The proposed 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. You can find more information about the proposed requirements on page 21 of the discussion document.

18. **What type of information should be retained by TF providers?**

We recommend DIA explore the logging, recordkeeping, and reporting requirements of CERT NZ (https://www.cert.govt.nz/) and those adopted overseas as a starting point. The proposed regulations are suboptimally worded when describing how a TF Provider keeps records. Providing services often requires multiple systems, and so keeping all relevant records in one database is highly impractical. Not all recordkeeping takes the form of structured data. The regulations should focus on what records should be kept, and not how they should be kept.

We note the following sentence from the discussion paper; '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'. We assume the idea is to log the fact that an event occurred, with the metadata involved but without including the PII itself. e.g "Provider X received Person Y's DoB on Date Z". Since a person's DoB doesn't change it doesn't need to be logged just as long as the TF Provider knows who they were. In essence it is a way to include privacy-by-design in logging and we support this.

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?

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

Please explain why / comment

It will depend on the records the TF Authority requires and other legal requirements. The statute of limitations varies by legislation, so the time frame is whatever is appropriate for that law. Consumer Guarantees is relevant to the life of the product, fair trading is relevant to the terms in the contract. 1-3 years seems to be reasonable for most product and service delivery related record keeping. Most technical logs are wiped after 30 days, etc. It all depends on which record and for what purpose. Any records relating to Accreditation or engagement with the TF Board or Authority might be kept for one year more than the full audit cycle for reference, whatever the audit cycle timeframe is agreed.

A more practical approach is to include a retention clause in the awarding of accreditation which may follow on into the TF Providers Terms of Use to its customers. For example the right to make a privacy claim expires after six months, so while people may have the right to be forgotten, there is a legitimate reason to retain their personal details for six months in order to respond to a complaint. The retention requirements should be settled when the design of the regulations has developed further**.**

20. Are there any implementation issues or risks that should be addressed?

There is Insufficient detail given so far to implement, so issues and risks can't really be identified yet. This is, of course, a significant risk in and of itself.

6. Reporting

The Act enables the regulations to establish TF provider reporting requirements. Details on the proposed annual and other reporting requirements are outlined on page 22 of the discussion document.

21. Do you agree or disagree with the proposed reporting requirements?

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

Please explain why / comment

There is insufficient detail to agree with the reporting requirements. As a fundamental approach, the test of necessity should be applied. What purpose does the reporting detail serve? There are no explanations why theTF Authority wants the reporting detail. If a detail is going to be used to assess the performance of a TF Provider, it's important to understand how it is used to determine that.

Rather than "Other" reporting consider "incident" reporting. If an incident should be raised to the TF Authority, then the TF Authority should do something with it. That may mean providing support to the TF Provider, starting an investigation, etc. The regulations should be oriented to helping TF Providers handle incidents as the regulatory regime is here to support the adoption of the trust framework.

Given the requirement that all TF participants must be incorporated in New Zealand (or be a Crown Agency), we wonder about the requirement to duplicate financial-performance reporting to the TF Authority when this information is already being furnished elsewhere. We also wonder what the financial-performance-and-sustainability reporting might look like for a Crown Agency (further underscoring the questions above about the purpose of this reporting and how it will be used).

22. Do you agree or disagree with the time limit for reporting actual or suspected fraud or events that have caused or present a risk of serious harm?

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

Please explain why / comment

We can't really comment without knowing the supporting role the TF Authority might play in responding to incidents with serious harm. There is a difference between notification and reporting when it comes to incidents - this hasn't been fully developed in the discussion document.

Crucially, any incident that presents a risk of serious harm must be notified as soon as possible after being discovered. We recommend that the DISTF Regulations avoid novel timeframes for incident notification, but instead start with the existing expectations detailed by the Privacy Act or other relevant legislation or existing accepted practice such as CERT NZ as a minimum-viable approach.

23. Are there any implementation issues or risks that should be addressed?

The reporting requirements have not been developed to the point where implementation can be evaluated. Consequently we're unable to target the issues and risks and comment meaningfully.

7. Cost Recovery

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. While the discussion document is not proposing specific cost recovery arrangements, it seeks initial feedback on the intent to recover costs and the likely impact of cost recovery on participation in the Trust Framework. Further context is provided on page 24 of the discussion document.

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?

Setting fees and the extent to which they should be recovered should be influenced by where the line is drawn between the TF being a public or a private good (our perspective being that it is part of the digital infrastructure of the nation so more a public good even if delivered by some organisations that are not wholly public) as well the TF's perceived market value, the tangible benefits to the TF Provider, and the overall cost of accreditation/compliance to the TF Provider. When the regime has more cost and benefit detail arising from early years operations, the appropriate value of accreditation can be determined. This is a better basis for determining the extent that accreditation fees can cover the administration costs of the regulatory regime.

From a market adoption perspective, the paper already states that the first two years will be free of fees to encourage adoption. While accepting that fees are just one cost component, clearly the government expects to use accreditation fees as a lever to influence adoption rates: how elastic or not fee costs are is a marketing decision for the Government.

25. If you are a potential TF provider, to what extent would accreditation fees impact on your participation in the Trust Framework and why?

As described above, the fees and overall cost of accreditation and compliance needs to be justified by the business benefits. If the accreditation has low value, then any fees would be a significant deterrent. If accreditation has clear benefits, then the TF Board will need to build a price elasticity model to match their uptake goals. The way to answer this question is through a market validation exercise.

Even in the first two years where the costs are free of fees, notional costs should be captured and communicated to help TF Providers understand the longer term financial investment.

26. Are there any implementation issues and risks that need to be addressed?

As pointed out above, if there is no clear value proposition for both the end user market and the TF Providers, any fees will become a significant deterrent.

As things stand, the absence of information about potential accreditation fees and compliance costs beyond the initial two-year period will likely cause many potential TF participants to defer their involvement until at least indicative information is available. While the May 2021 proactive release and RIS provide a range on page 12 of between $10,00 and $250,000, it is too broad and unsubstantiated to be meaningful.

Additionally, fees and cost recovery seem to be approached in the discussion paper without regard for the TF Provider's existing certifications. As DIA will find during its operation of the 2 years of no fees, the likely cost in auditing a prospective TF Provider service that has not seen any audit before will be substantially higher than a TF Provider service that can attest to existing certifications. So this point alone demonstrates that one size will not fit all. The DIA could also incentivise the good behaviour TF Providers demonstrate through having an existing certification by offering a discount.

Other comments

Do you have any further comments you would like to provide to us on the proposed regulations?

We offer a set of comments relating to the Digital Identity Services Trust Framework Discussion Paper dated August 2023 from which the template and requisite responses have been drawn. The paper contained sections not directly applicable to the response template in order to provide context but we have commented on these also.

Further, we offer a summary of high level concerns relating to the implementation of the DISTF in general and a recommendation given the current state of the project where there is minimal ability for introducing changes.

For the avoidance of any doubt, we reiterate here that DINZ supports the establishment of a sovereign regulated trust framework. However, we do have concerns about the approach, scope, achievability, and commercial desirability of the TF as it is currently expressed.

Our concerns are founded in consideration of the milestones to be achieved through what is by any measure a demanding set of activities over the difficult period between now and 1 July 2024 and in the extent of uncertainty about costs, benefits, and accreditation processes.

Our concerns are also founded in the fact that DINZ fundamentally deeply cares about the DISTF, wants to provide advocacy and find ways to best support DIA in its difficult mahi. Where we contribute with critique we aim to do so in the context to positively support DIA and to obtain best outcome for digital identity services in New Zealand.

A: Comments on the Digital Identity Services Trust Framework Discussion Paper dated August 2023:

1. Purpose

a. Conversation summary: This discussion paper was produced by DIA, rather than the TF Board itself. If DIA were not to be the Crown Entity responsible for rules and regulations, what is the outcome of this? The original expectation was that the TF Board would be formed and resourced by now, and should be directing this activity. Since it isn't we have assumed this paper will form the basis of a briefing document on regulations for the TF Board to consider.

2. Overview

a. The overview describes the current state of digital identity services as creating a problem for NZ society that is undermining trust. The lack of consistency by the current service providers is the issue, and we need this regulatory regime to address this. Much of this sentiment derives from the original problem statement in the Regulatory Impact Assessment. This is a misrepresentation of the issues facing NZ with digital identity and trust. It also misses the point of the trust framework concept. This regulation is not addressing an existing problem in the market; its goal is to add assurance to new forms of online trust relationships that will play an important part in supporting independent identity services. This overview steers the incoming TF Board down the wrong path.

b. The language in the overview is not consistent with the Act. It frequently uses language that infers a broader problem or regulatory reach than the Act describes. As a briefing document for the incoming TF Board, it is a concern that they may exceed their mandate and conflict with other regulatory bodies.

c. The term "Trust Framework" in the Act only refers to the legal framework the Act creates. The term "trust framework" used by industry refers to a digital ecosystem incorporating trust mechanisms to operate. The benefits attributed to the legal framework in Paragraph 5 are the result of the industry trust framework. These benefits will be realised whether there is a NZ regulatory regime or not. This overview does not clearly describe the value the regulatory regime will contribute to the industry trust framework. This is a shame, as it has an important role to play.

d. The overview does not adequately describe the separation of duties between the TF Board and TF Authority. For example, who is responsible for promoting the trust framework? which regulations will be maintained by the Board versus the Authority? raising disputes with the Board versus the Authority, etc. The overview does not describe regulatory topics that are *out of scope*, so should questions on those duties be addressed here, or some specified place elsewhere?

e. The rules within the regulatory regime have only been specified to a basic requirements definition level, based on the consultation to date. Should one of the regulations requirements be for the Board to establish and maintain the rules? That is what the Act requires, but there is no provision for the TF Providers to work with the Board on maintaining the rules. Where will the Board get its deep subject matter domain expertise and industry insight from to take on this task? There is genuine concern that the rules will not be sufficiently developed in time for prospective TF Providers to determine if their product/service could match them, make an application, have an auditor assess and provide a report, potentially make changes to the service design and software, re-audit, make the case to the Board for it to determine whether or not to grant accreditation within an acceptable timeframe that returns value to the TF Provider from the credibility of the TF regime.

f. Regardless of the timing for the second set of regulations, understanding how costs and disputes will be regulated is an early decision making requirement for anyone considering accreditation. The approach and uncertainty surrounding these aspects is a significant deterrent to accreditation.

g. There is no specific section or paragraph specifying the scope. Rather, it is left to the reader to infer it from the other sections. This makes it difficult to determine if there's a common understanding of scope. A major case in point is identity of organisations and things - not specific to TF Provider organisations which might potentially be addressed in the Section 4: Accreditation Requirements. Establishing and confirming Identity of organisations and their associated organisation information attributes and their relationship to an individual or to assets and other objects or to other organisations in a network to an appropriate level of assurance/confidence is critical in building trust relationships in a digital nation.

3. Next Steps

a. Based on overseas experience and the progress witnessed to date, there is concern that we will not see an operational regime issuing accreditations for a long time. The Pan Canadian Trust Framework's Viola Verified was launched approximately a year ago after two years of piloting. While several prospective TF applicants are going through the process, not one has emerged so far. It was a similar case in Australia with the TDIF, which we understand is the exemplar that the DISTF was set to follow. After three years of piloting the implementation 2016-19, the accreditation regime commenced. At the time writing just three Government services and four private sector and CE services have opted in to be accredited in the past four years. What volume might the DISTF expect in 1-2 years from July 1st 2024 with no implementation lead-in runway, limited resources and a smaller addressable market of providers than Australia has?

4. Context

a. "*Unfortunately, we are now facing increasing fraud and security risks because of the rapid evolution of global digital sharing*". This is a misrepresentation. If anything, the rapid growth in global digital sharing is the result of an improving threat landscape and identity security.

We can do more online today than before because we have the tools that keep us safer and minimise harm. Because we are doing more, there is a larger market for bad actors. Increasing fraud and security risks is not why a regulatory regime for a trust framework is needed. Emerging modern architectural approaches such as Verifiable Credentials and their developing trust based ecosystems have been developed precisely to improve the threat landscape and serve the public better than the current digital identity management services built on centralised or federated architectures. While the discussion paper calls out Verifiable Credentials specifically, in fact it is the existing centralised and federated architectures that present most risk.

This law provides public assurance that these new offerings are trustworthy. The legal framework is not addressing the fraud and security concerns - it's equipping the public with assurance mechanisms for new ways of doing things. The new trust frameworks will continue to improve the threat posture of identity services with or without the regulations.

b. We are disappointed that DIA is quoting from DINZ research from 2019, six months after the 2022 research report "*Digital Identity in Aotearoa: Identity and Trust in an Increasingly Digital New Zealand*" was released in February 2023[1].

c. "*This suggests there is a low level of confidence in the current state of the digital identity system*". Absolutely not, this is not what the research suggested. The concern is the low level of trust in organisations, not the systems they use. As systems get better, as they have, if the concerns are getting worse then it's trust in the organisations through mismanagement of the systems that needs to be addressed. The new trust frameworks industry is considering or developing will give NZers more control and transparency, and will create systemic protections from harmful actions and reduce risks to individuals. That's the goal. Then the story is how these new laws give some bite to go with the bark. If you want to talk to the concerns expressed by the public, then talk about how the new regime will help users hold information providers and relying parties to account.

d. In our comments on the Overview section above we note that there's no mention of organisational identity, nor the Identity of Things, and that equally applies in this Context section. Organisation information is as equally important as personal identity information in the context of developing trust relationships in a digital nation. The discussion paper does not make an explicit statement about scope. Organisational identity information could include attributes relevant to the organisation by the nature of its operation and trading. DINZ member Trust Alliance NZ makes a case in point for a farm enterprise. Individually these examples could be seen as unimportant but in the context of an operating farm enterprise they are critical for the farm enterprise to maintain a license to operate and meet financing and international market access and traceability requirements identity for objects such as farm equipment and organisational documents, reports, licenses, certifications etc are required.

[1] https://digitalidentity.nz/wp-content/uploads/sites/25/2023/02/Digital-Identity-in-Aotearoa-Report_final-1.pdf

5. Trust Framework – Purpose and Benefits

a. "*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. It will also reduce transaction costs for relying parties that need verified identity and other personal information to provide their services*". All these benefits are from the industry definition of trust frameworks. The regulatory regime only adds costs in this context. The legal trust framework does not ensure the provision of anything. It is designed to give assurance about those who are providing new identity services. These services will be established in the market whether there is a regulatory regime or not. The regime has an important purpose and material benefits but they're missing from this section.

6. Uptake Strategy

a. "*responsible for promoting use of the system*". Again, this is not what the Act says. It says "*undertake education and publish guidance*". The role of promotion is different from education. The Board is not in this alone. DINZ and the industry can complement the investment in education and guidance with outreach. It's an unusual situation for a regulatory regime to play an important part in establishing novel services into an existing market so care needs to be taken around the optics and perceptions with words like 'promoting'.

7. Trust Framework Parameters

a. "*Use of the Trust Framework is Opt-In*". The two main points here have issues:

i) Public concern by some sectors of society that this may be seeking to establish a mandatory and centrally controlled regime. The language changes in this discussion paper from what is in the Act to the use of broadening and absolute terms which is unhelpful to addressing this particular public perception. We recommend holding to the language of the Act when publishing to external audiences and authoring advice for the Board to avoid risking speculation and concern.

ii) *A decentralised system enabling users to choose what information is shared.* This is factually incorrect. The architecture doesn't address user choice on what is shared. It only looks at how information is shared.

b. "*Operation of the Trust Framework will involve user-controlled data sharing".* This is outside the scope of the Act:

i) Nothing in the Act, the rules, or regulations to date focuses on user control of data sharing by information providers or relying parties

ii) The whole regime is focused on the infrastructure and how it will operate, not on the data that Users, Information Providers, and Relying parties pump through it.

8. **Accreditation Requirements**

    a. *Incorporation in NZ*. NZ Crown Agencies and Government Departments can apply but this leaves out many Crown Entities that manage significant amounts of identity related activity, such as Universities. Consider changing Crown Agencies to Crown Entities.

    b. *Fit and Proper Person*. It is typical to only need the 'fit and proper' test of those with delegated authority for the TF Provider services. Applying 'fit and proper' prescriptions for staff, even through information on policy and procedures, is a liability minefield. If the design and wording is not fully thought through, there could be unintended consequences such as making the accredited services uninsurable.

9. **Accreditation Mark**

    a. This whole section raised lots of questions and issues both in the discussion paper and in the presentation that followed its release. The consensus in DINZ is that the Accreditation Mark elements have not been sufficiently developed to constructively comment on.

B: A brief summary of high Level concerns relating to the implementation of the Trust Framework

Just nine months out from the proposed implementation date of July 1st 2024 that takes in both the general election and the Christmas holiday period, DINZ has taken stock of where the project is at more broadly. We acknowledge that this is beyond the scope of the DISTF Regulations Discussion Paper but a brief helicopter view of the state of the overall project provides context for DINZ's comments on the paper and should be read in conjunction, which is why they are included here and not as supplementary feedback.

The Regulatory Impact Statement of May 2021 is a useful starting point. proactive-release-digital-identity-trust-framework.pdf - Internal Affairs which starts at Page 38. The Statement laid out the uncertainty around costs and take up. The panel's QA assessment then remains equally as valid more than two years later;

'The panel considers that the information and analysis summarised in the RIA partially meets the quality assurance criteria. There is uncertainty about the costs and benefits of the proposal and gaps in the evidence, including the likely uptake of the Trust Framework, some of which results from the lack of consultation on the specific proposals. However, the analysis shows a good understanding of these limitations, makes appropriate use of available evidence and includes suitable measures to rectify the issues. The RIS provides a balanced view of the advantages and disadvantages of the options and is a sound basis for further work to develop the detailed framework'.

And then with regard to costs we note this: "However overall demand for participation to the Trust Framework remains uncertain, particularly given the significant costs of becoming accredited (initially estimated at between $10,000 and $250,000 including the costs of obtaining independent pre-accreditation documents). This impact statement will therefore review whether accreditation to the Trust Framework should be optional or mandatory for some or all sector participants." Of course we know that the risk has been partially mitigated by taking the optional route and that the first 2 years of accreditation are free of fees - provided the incoming government carves out the funding so that it does not get caught up in public spending cuts. Nonetheless as per our response to Q25, TF Providers will want to understand the notional costs from the initial years of implementation to determine the overall value proposition.

There were two matters DINZ considers of a material nature that were not highlighted in the RIS beyond the obvious one - the impact of the pandemic on engagement and resource capacity.

The first was the impact of the decision to develop the trust framework legislation concurrently with the development of the Rules. No other common law jurisdiction that NZ is typically compared to that are ahead of us in digital identity trust frameworks, have taken this approach. All have developed the standards, the rules, the processes, the legal contracts and paraphernalia and then piloted the system with pre-assessment to learn, further develop and improve, prior to legislating. Had the NZ DISTF followed this 'lead-in runway' approach stakeholders would know so much more about the operational dynamics than we do today. There would have been an opportunity to test the assessment criteria with pre-assessment and test use cases to determine if they were in scope or not and provide guidance accordingly. For example, it's not clear how organisations and networks relate to the Trust Framework. Like people, they need to be digitally identified too. How would the Facilitation Service impact them? Or the other specified Services? We appreciate there were reasons why NZ departed from this approach but it comes with considerable risks that we don't believe were fully understood when the decision was taken.

The second was the impact of minimal domain expertise specifically in the development and operation of digital identity trust frameworks within DIA. While the PIS refers to research of similar initiatives overseas, there is a big difference between observing, gathering knowledge etc and actually operating within a digital identity trust framework with its requisite development of contracts and processes that some DINZ members and its staff have experienced. It's quite reasonable to have expected DIA to contract in resources with the appropriate level of expertise to assist the Policy and Regulations teams so there was no need to raise the matter in the RIS. What was unforeseen was Treasury's decision to not provide DIA with additional targeted funding in the 2022-23 year ending June 30th 2023, arguably the most critical year for development, leaving DIA to try and make progress from baseline funding and existing capability.

Understandably progress was slower than originally planned which we assume necessitated the extension of the implementation date by 6 months. Even so, the revised project plan and timescale is ambitious to say the least, as milestones tumble over into the first 6 months of 2024, with the final deliverable due in June 2024, one month before the July 1st implementation date. There's a real sense now that the project is driven by time at all costs.

It is the combination of all these factors above (admittedly some uncontrollable) that should be cause for concern because there's little that can be done in the way of mitigation.

What can be done is to set expectations accordingly. There will not be a long waiting list of TF Providers seeking accreditation on July 1st and it will be perhaps well into 2025 or 2026 before we will see accredited trust marked TF Providers emerging out the other end of the system. Nonetheless lessons have and will be learned and the implementation experience from the first couple of years will prove invaluable to getting to a successful outcome longer term, the goal that DINZ remains steadfastly committed to.

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 Framework*. If you would like to provide any supplementary feedback, you can email us at Digital.Identity@dia.govt.nz