Departmental Disclosure Statement

Digital Identity Services Trust Framework Bill

The departmental disclosure statement for a government Bill seeks to bring together in one place a range of information to support and enhance the Parliamentary and public scrutiny of that Bill.

It identifies:

- the general policy intent of the Bill and other background policy material;
- some of the key quality assurance products and processes used to develop and test the content of the Bill;
- the presence of certain significant powers or features in the Bill that might be of particular Parliamentary or public interest and warrant an explanation.

This disclosure statement was prepared by the Department of Internal Affairs.

The Department of Internal Affairs certifies that, to the best of its knowledge and understanding, the information provided is complete and accurate at the date of finalisation below.

31 August 2021.

Contents

Part One: General Policy Statement

The Digital Identity Services Trust Framework Bill (the Bill) establishes a legal framework for the provision of secure and trusted digital identity services for individuals and organisations.

The policy objectives of the Bill are to—

- help drive consistency, trust, and efficiency in the provision of digital identity services;
- support the development of interoperable digital identity services;
- provide people with more control over their personal information and how it is used; and
- enable the user-authorised sharing of personal and organisation information digitally to access public and private sector services.

How the Bill will achieve the policy objectives

To achieve these objectives, the Bill will establish a trust framework (consisting of primary legislation, and a set of rules (the **TF rules**), and regulations) for the provision of user-authorised digital identity services in New Zealand (the **trust framework**). It also establishes requirements for accrediting digital identity service providers against those rules. Specific provisions in the Bill will ensure that te ao Māori approaches to identity are considered in trust framework governance and decision-making.

Why this approach is needed

Currently New Zealand lacks consistency in the way personal and organisational information is shared, stored, and used in a digital identity environment. This has led to inconsistencies and inefficiencies in how this information is handled, undermining trust and confidence in the digital identity system for individuals, government agencies and the private sector.

This impedes people's ability to access services online, undermines their expectations regarding privacy and security, stifles innovation in service provision, and hinders the realisation of the significant social and economic benefits digital identity services could provide.

Specific measures to achieve the policy objectives

Opt-in accreditation scheme for digital identity service providers

The Bill establishes an opt-in accreditation scheme which will have a set of requirements for handling personal and organisational information which accredited digital identity service providers (**TF providers**) must comply with. Users or consumers of digital identity services will not have to be accredited to use accredited digital identity services.

Opt-in accreditation will allow digital identity service providers time to upgrade their systems to comply with the TF rules at their own pace, before applying for accreditation. The Bill allows accredited providers to use approved trust marks to show their compliance with the TF rules.

These service providers are likely to be organisations such as government departments, existing identity providers and other private sector organisations that verify identity. The Bill does not override any obligations under the Privacy Act 2020.

Trust Framework Board

The Bill creates a governance board (the **TF board**) which will undertake education, publish guidance, and monitor the performance and effectiveness of the trust framework. The TF board will also have responsibility for advising and recommending the TF rules to the Minister and undertaking consultation on the rules before it does so. The TF board members must include people with expert knowledge of te ao Māori approaches to identity, technology, and identity data management.

The rules, set by the Minister or by regulation, will support the sustainability of the trust framework by allowing it to be flexible to adapt to changes in the approach to how digital identity services are delivered. To enable transparency on what requirements providers are being accredited against, the rules for the trust framework will be published and accessible to the public.

Before recommending changes to the rules, the TF board must consult:

- the Office of the Privacy Commissioner;
- people or groups outside the board with expert knowledge of te ao Māori approaches to identity;
- TF providers;
- people or groups that are likely to have an interest in the TF rules; and
- any other individual or organisation that the board considers should be consulted.

In addition, committees of advisors may be established, and a Māori Advisory Group will be established to advise the TF board on Māori interests and knowledge as these relate to the trust framework. This will ensure that a wide range of views is considered in the development of the rules.

Trust Framework Authority

To ensure the TF rules are enforced and to protect the security and privacy of trust framework users, the Bill allows for the establishment of an (the **TF Authority**) that will be responsible for: making decisions on applications for accreditation and renewal of accreditation, conducting investigations following complaints, or on their own initiative, and granting remedies for breaches. The authority will also be responsible for maintaining a register of accredited providers.

Complaints and Remedies

To protect the integrity of the trust framework and to enforce compliance with the TF rules, the Bill allows for people to submit complaints to the authority if they believe a TF provider has breached 1 or more of the TF rules, the regulations, terms of use of trade marks, or the Act. If the authority finds that a breach has occurred, it can grant remedies, such as publishing a public warning, suspending a TF provider's accreditation or cancelling their accreditation. The Bill also contains offences for activities that threaten the integrity of the trust framework, such as falsifying accreditation.

Part Two: Background Material and Policy Information

Published reviews or evaluations

2.1. Are there any publicly available inquiry, review or evaluation reports that have informed, or are relevant to, the policy to be given effect by this Bill?	**YES**
Australian Post, A frictionless future for identity management, 2016, available at: https://auspostenterprise.com.au/content/dam/corp/ent-gov/documents/digital-identity-white-paper.pdf Digital Identity NZ: Nine out of 10 Kiwis want more control of their digital strategy, 2019, available at: https://digitalidentity.nz/2019/06/05/nine-out-of-10-kiwis-want-more-control-of-their-digital-identity/	

Relevant international treaties

2.2. Does this Bill seek to give effect to New Zealand action in relation to an international treaty?	**NO**

Regulatory impact analysis

2.3. Were any regulatory impact statements provided to inform the policy decisions that led to this Bill?	**YES**
Progressing Digital Identity: Establishing a Trust Framework, Department of Internal Affairs, 2 July 2020. The report can be accessed on the Department of Internal Affairs website at: https://www.dia.govt.nz/diawebsite.nsf/Files/Proactive-releases/$file/Combined-Digital-Identity-Proactive-Release.pdf **Detailed policy for a Digital Identity Trust Framework, Department of Internal Affairs, 10 February 2021.** The report can be accessed on the Department of Internal Affairs website at: https://www.dia.govt.nz/Resource-material-Regulatory-Impact-Statements-Index#digital. Some parts of this Regulatory Impact Statement have been withheld in accordance with the Official Information Act 1982 sections: • 6(b)(i) - to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a Government • 9(2)(f)(iv) - maintain the constitutional conventions for the time being which protect the confidentiality of advice tendered by Ministers of the Crown and officials **Additional policy decisions for the Digital Identity Services Trust Framework Bill, Department of Internal Affairs, 11 August 2021.** The report can be accessed on the Department of Internal Affairs website at: https://www.dia.govt.nz/Resource-material-Regulatory-Impact-Statements-Index#digital	

2.3.1. If so, did the RIA Team in the Treasury provide an independent opinion on the quality of any of these regulatory impact statements?	**NO**

Progressing Digital Identity: Establishing a Trust Framework, Department of Internal Affairs, 2 July 2020 – No independent opinion was provided by Treasury. However, a Treasury representative was present on the panel for this Regulatory Impact Statement. **Detailed policy for a Digital Identity Trust Framework, Department of Internal Affairs, 10 February 2021** - Treasury did not provide an independent opinion. High level policy was already agreed in the July Regulatory Impact Statement and Treasury were comfortable with an internal-only panel for the review of this RIS. **Additional policy decisions for the Digital Identity Services Trust Framework Bill, Department of Internal Affairs, 11 August 2021** – Treasury did not provide an independent opinion and were comfortable with only an internal panel for the review of this RIS.

2.3.2. Are there aspects of the policy to be given effect by this Bill that were not addressed by, or that now vary materially from, the policy options analysed in these regulatory impact statements?	**NO**

Extent of impact analysis available

2.4. Has further impact analysis become available for any aspects of the policy to be given effect by this Bill?	**NO**

2.5. For the policy to be given effect by this Bill, is there analysis available on:	
(a) the size of the potential costs and benefits?	**YES**
(b) the potential for any group of persons to suffer a substantial unavoidable loss of income or wealth?	**NO**
Limited information on the size of the costs and benefits is available in the 10 February 2021 Regulatory Impact Statement: https://www.dia.govt.nz/Resource-material-Regulatory-Impact-Statements-Index#digital	

2.6. For the policy to be given effect by this Bill, are the potential costs or benefits likely to be impacted by:	
(a) the level of effective compliance or non-compliance with applicable obligations or standards?	**YES**
(b) the nature and level of regulator effort put into encouraging or securing compliance?	**YES**

The February RIS states that the benefits of the policy are dependent on the uptake of the accreditation scheme. It also stated that early engagement as part of the Digital Identity and Rules Development Programme indicated strong demand for accreditation.

However, as stated in the RIS, there is limited quantitative evidence to support the analysis, including for the costs and potential benefits.

The TF board will have functions under the Bill to provide education and guidance for the public and will have funding for this function. However, it is not currently known to what level the TF board will encourage providers to become accredited.

Limited information is available in the 10 February 2021 Regulatory Impact Statement: https://www.dia.govt.nz/Resource-material-Regulatory-Impact-Statements-Index#digital

Part Three: Testing of Legislative Content

Consistency with New Zealand's international obligations

3.1. What steps have been taken to determine whether the policy to be given effect by this Bill is consistent with New Zealand's international obligations?
Throughout the development of the policy and Bill, officials have engaged with the Office of the Privacy Commissioner to ensure the Bill upholds people's right to privacy as stated in the: • Universal Declaration of Human Rights; • Cross-Border Privacy Enforcement Agreement; and • International Covenant on Civil and Political Rights. Digital identity can also enable digital trade and other cross-border transactions. Mutual recognition of digital identity services with Australia has been signalled as a priority for the Single Economic Market agenda by the New Zealand and Australian Prime Ministers (in their annual Leaders' Meetings in 2019 and 2020).

Consistency with the government's Treaty of Waitangi obligations

3.2. What steps have been taken to determine whether the policy to be given effect by this Bill is consistent with the principles of the Treaty of Waitangi?
This Bill allows for the creation of a trust framework for digital identity services which will set rules and regulations for how personal and organisational information is handled when delivering these services. As the Bill impacts approaches to identity, it has implications for the rights and interests of Māori protected by the Te Tiriti O Waitangi. The Bill also establishes a Māori Advisory Group (the Group) to advise the TF board on Māori interests and knowledge. The TF board is required to seek the advice of the Group on matters of tikanga Māori and Māori cultural perspective. The TF board must also give effect to the Group's advice to the extent that it considers is reasonable and practicable after taking into account other relevant considerations. The policy positions for the Bill were informed by engagement and research involved Māori during 2019. The Department has engaged with Māori and iwi on the Bill through the Data Iwi Leaders Group and a Māori technical working group. However, short timeframes for consultation on the Bill has meant that the Department has not been able to have a more detailed consultation process with Māori stakeholders. The Bill makes it a requirement for the TF board membership to have knowledge of te ao Māori approaches to identity. It also requires the TF board to consult with persons or groups with expertise in Māori approaches to identity before recommending rule changes to the Minister. The Department also undertook a series of focus group research sessions to better understand Māori views towards the use and sharing of data in both the public and private sectors. The Department has engaged with Te Arawhiti and Te Puni Kōkiri in the development of the Bill.

Consistency with the New Zealand Bill of Rights Act 1990

3.3. Has advice been provided to the Attorney-General on whether any provisions of this Bill appear to limit any of the rights and freedoms affirmed in the New Zealand Bill of Rights Act 1990?	**YES**
Advice has been provided to the Attorney-General by the Ministry of Justice which is expected to be available on the Ministry of Justice website upon introduction of the Bill. Such advice, or reports, will be accessible at: http://www.justice.govt.nz/policy/constitutional-law-and-human-rights/human-rights/bill-of-rights	

Offences, penalties and court jurisdictions

3.4. Does this Bill create, amend, or remove:	
(a) offences or penalties (including infringement offences or penalties and civil pecuniary penalty regimes)?	**YES**
(b) the jurisdiction of a court or tribunal (including rights to judicial review or rights of appeal)?	**NO**
Sections 94 to 99 details the offences and associated fines in the Bill. This is detailed further in **Appendix One**.	

3.4.1. Was the Ministry of Justice consulted about these provisions?	**YES**
Prior to the lodgement of the February 2021 Cabinet paper, the Department engaged with the Ministry of Justice on the penalties in the draft Bill. The Ministry of Justice raised the following to discuss further: • the dollar amount of the penalty fines that were proposed; • whether the proposed pecuniary penalties are appropriate for an opt-in framework; • the analysis underlying some of the proposals for penalties; and • if some penalties had accounted for legitimate mistakes where a provider had not intended to commit an offence. The Department worked with the Ministry of Justice to discuss these issues and make changes to the Bill including removing pecuniary penalties from the Bill.	

Privacy issues

3.5. Does this Bill create, amend or remove any provisions relating to the collection, storage, access to, correction of, use or disclosure of personal information?	**YES**
Section 19 sets out the content of the TF rules that set requirements for accredited providers. These include rules that will relate to how personal information and organisation information is collected, stored, accessed and shared. These rules will not override the Privacy Act 2020 and accredited providers will still have to meet their obligations under the Privacy Act 2020.	

3.5.1. Was the Privacy Commissioner consulted about these provisions?	YES
The Office of the Privacy Commissioner has been engaged in the development of the trust framework policy and the Bill. This has included the Privacy Commissioner being on the Governance Group for the Digital Identity programme.	

External consultation

3.6. Has there been any external consultation on the policy to be given effect by this Bill, or on a draft of this Bill?	YES
The Department engaged with a working group that included a wide variety of key public and private sector stakeholders in the development of the policy. As well as public agencies, the working group included representatives from: ANZ, ASB, Auckland University, MATTR, Payments NZ, Planit, Sphere Identity, SSS IT Security Experts, Two Black Labs, Westpac and Xero. Between 1 June and 20 July 2021, we presented the Bill's policy proposals to targeted stakeholders for discussion. Stakeholders consulted over this period included: • representatives from the digital identity sector, including Digital Identity NZ members, MATTR, and private consultants; • private sector representatives with an interest in the trust framework, including ANZ, BNZ, ASB, Consumer NZ, Internet NZ and Payments NZ; and • a Māori technical working group with subject matter expertise, including leaders from Māori digital identity initiatives and public service members with relevant Māori expertise. The Department received feedback from these stakeholders that they were generally supportive of the legislation and the opt-in accreditation scheme. They also provided some feedback on the governance structure and liability framework. The Department has made changes to these in the Bill in response to this feedback. No public consultation on the Bill has been undertaken.	

Other testing of proposals

3.7. Have the policy details to be given effect by this Bill been otherwise tested or assessed in any way to ensure the Bill's provisions are workable and complete?	YES
The Department has worked closely with external stakeholders who may be part of the trust framework to develop the rules that will be given effect by this Bill. These stakeholders have provided feedback on the rules, including workability of them. As part of this work the Department have also engaged with the Data Iwi Leaders Group who have expertise in Māori approaches to identity to ensure the TF rules also consider te ao Māori approaches to identity.	

Part Four: Significant Legislative Features

Compulsory acquisition of private property

4.1. Does this Bill contain any provisions that could result in the compulsory acquisition of private property?	**NO**

Charges in the nature of a tax

4.2. Does this Bill create or amend a power to impose a fee, levy or charge in the nature of a tax?	**NO**

Retrospective effect

4.3. Does this Bill affect rights, freedoms, or impose obligations, retrospectively?	**NO**

Strict liability or reversal of the usual burden of proof for offences

4.4. Does this Bill:	
(a) create or amend a strict or absolute liability offence?	**YES**
(b) reverse or modify the usual burden of proof for an offence or a civil pecuniary penalty proceeding?	**NO**
Sections 97 to 99 create strict liability offences as the prosecution does not need to prove intent. Further detail on these offences and associated fines are outlined in **Appendix One**.	

Civil or criminal immunity

4.5. Does this Bill create or amend a civil or criminal immunity for any person?	**YES**
Section 102 provides that members of the TF board, members of the authority, and members of an advisory committee are immune from civil liability for good faith actions or omissions when carrying out or intending to carry out their functions. Section 103 provides that a trust framework provider is immune from civil liability if a user of their service causes harm or damage to any individual, organisation, or themselves if the provider was acting in good faith and was not grossly negligent.	

Significant decision-making powers

4.6. Does this Bill create or amend a decision-making power to make a determination about a person's rights, obligations, or interests protected or recognised by law, and that could have a significant impact on those rights, obligations, or interests?	**NO**

Powers to make delegated legislation

4.7. Does this Bill create or amend a power to make delegated legislation that could amend an Act, define the meaning of a term in an Act, or grant an exemption from an Act or delegated legislation?	**NO**

4.8. Does this Bill create or amend any other powers to make delegated legislation?	**YES**
Section 17 of the Bill allows the TF rules to be set by the Minister or by regulation. In both instances the TF board will make recommendations to the Minister and will be required to undergo consultation. Section 44(1)(b) of the Bill gives the TF board the function to recommend regulations to the Minister relating to matters that may be the subject of regulations under section 100. These powers allow the trust framework to be flexible and adapt to changes in the approach to how digital identity services are delivered. Further information on the content of the rules and regulations is provided in **Appendix Two**.	

Any other unusual provisions or features

4.9. Does this Bill contain any provisions (other than those noted above) that are unusual or call for special comment?	**YES**
This Bill creates an opt-in regulatory framework with offences and penalties. Digital identity service providers would still be able to provide their services without being accredited to the trust framework and therefore not subject to the penalties and offences in this Bill.	

Appendix One: Further Information Relating to Part Three

Offences – question 3.6

Table of offences in the Digital Identity Services Trust Framework Bill

Provision	Description of offence	Fine
s94	knowingly or recklessly represents themselves as a trust framework provider or service.	$50,000 for an individual $100,000 for a body corporate.
S95	Knowingly or recklessly uses a trust mark that is contrary to the terms and conditions set by the authority.	$50,000 for an individual $100,000 for a body corporate.
s96	knowingly or recklessly gives false information to the Authority in an application or renewal for accreditation.	$50,000 for an individual $100,000 for a body corporate.
s97	fails to give the authority key information or specified information in an accreditation application without a reasonable excuse.	$10,000 for an individual $20,000 for a body corporate.
s98	not telling the authority of a change in key information in an application for accreditation without reasonable excuse.	$10,000 for an individual $20,000 for a body corporate.
s99	obstructing the Authority without reasonable excuse when it is carrying out its functions.	$10,000 for an individual $20,000 for a body corporate.

Appendix Two: Further Information Relating to Part Four

Detail on rules and regulations – question 4.8

Regulations – created by Governor-General through Order in Council

Provision	Description
s23	setting fees for accreditation applications
s23	the required information to be contained in applications for accreditation
s25	Setting the criteria for the assessment of applications
s27	Requirements for the applications for reconsideration for accreditation
s28	setting the duration period for accredited providers and services
s29	Setting requirements for renewal applications
s30	setting requirements for applications for provision accreditation
s38	permitting the certification and suspension or cancelation of third-party assessors by the authority
s40, s41	prescribing requirements for record keeping and reporting by TF providers and third-party assessors
s69	Requirements for complaints
s75, s76	set the requirements for an alternative dispute resolution scheme
s85	information required in a compliance order

Rule categories – created by the Minister or by Governor-General through Order in Council

Category	Description
Identification management	requirements on determining the accuracy of information, binding that information to the correct person or organisation, and enabling the secure reuse of the information.
Privacy and confidentiality	requirements on how providers ensure the privacy of users is maintained.
Security and risk	requirements for providers, to ensure information is secure and protected from unauthorised modification or use, and loss.
Information and data management	requirements on record keeping, and on format of *attributes* ensuring a common understanding of what is shared.

Sharing and facilitation	requirements for facilitating sharing of information with relying parties, including authorisation processes and allowing a user to act on behalf of another individual or organisation.