Legislative statement: Digital Identity Services Trust Framework Bill – Second Reading

Presented to the House of Representatives in accordance with Standard Order 272

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

Digital identity services support digital transactions by enabling secure user-authorised sharing of personal or organisational information with third parties to prove identity and attribute information. These include services that check the accuracy of information and its connection to a user, and those that facilitate secure sharing.

The Bill establishes the Digital Identity Services Trust Framework (the Trust Framework) – an opt-in accreditation scheme for digital identity services that can demonstrate they meet requirements for handling information. The Trust Framework is designed to put the user in control of their own information, deciding what information they want to share and how they want to share it. The Bill does not demand that any person has a digital identity credential, uses any digital identity services, or that any personal or organisational information be shared, collected or used.

The Bill is now ready for the second reading stage. The Economic Development, Science and Innovation Committee (the Committee) provided its report on 19 April 2022 and recommended that the Bill is passed with amendments.

Accrediting trusted digital identity services

The Bill enables the setting of rules that must be met to become an accredited digital identity service and outlines how the Trust Framework will be governed and enforced. These rules are made up of technical standards and requirements made by the Minister. They will cover identification management; privacy and confidentiality; security and risk; information and data management; and sharing and facilitation.

Digital identity service providers who opt-in and become accredited under the Trust Framework will be able to demonstrate their compliance using an accreditation mark, giving consumers confidence in knowing which services are compliant with the Trust Framework rules.

Governing the Trust Framework

The Bill creates the Trust Framework Board (the Board) which will:

- undertake education and publish guidance;
- monitor the performance and effectiveness of the Trust Framework; and
- have responsibility for recommending Trust Framework rules to the Minister.

The Bill places requirements on the Board to undertake consultation with the Office of the Privacy Commissioner, Māori and others as directed by the Minister prior to recommending rules.

The Bill also establishes a Māori Advisory Group to advise the Board on Māori interests and knowledge as these relate to the Trust Framework. The Board will be required to give effect to the advice of the Māori Advisory Group unless not reasonably practicable. The Board members must include people with knowledge and expertise of te ao Māori approaches to identity and engaging with Māori, technology, and identity and data management.

The Trust Framework's governance arrangements will be reviewed two years after the Bill is enacted, and subsequently every five years.

Maintaining the integrity of the Trust Framework

To ensure the Trust Framework rules are enforced and to protect the security and privacy of Trust Framework users, the Bill establishes the Trust Framework Authority, responsible for:

- making decisions on applications for accreditation and renewal of accreditation;
- maintaining a register of accredited providers;
- conducting investigations following complaints, or on their own initiative; and
- ordering remedies for breaches.

The Authority may also certify third party assessors to carry out some of its assessment functions.

Where accredited digital identity service providers breach the rules, the Authority may: issue a private or public warning; place additional record keeping or reporting requirements on the provider; issue a compliance order; or suspend or cancel accreditation. The Bill also establishes criminal offences for activities that threaten the integrity of the Trust Framework.

The Bill will not override obligations under other Acts, such as the Privacy Act 2020. However, it does provide accredited digital identity service providers with immunity from civil liability when they are acting in good faith and where their actions do not amount to gross negligence.

The Bill establishes other regulation-making powers

Regulation-making powers enabled under this Bill include:

- defining the types of providers and services that may be accredited;
- establishing a fees framework;
- setting requirements for complaints and dispute resolution processes;
- setting requirements for the provision of information as part of an application for accreditation;
- setting criteria for assessing applications and the length of accreditation;
- setting requirements for certifying third party assessors; and
- setting requirements for record-keeping and reporting by Trust Framework providers.

Amendments have been made to the Bill

A number of changes were recommended by the Committee. The substantive recommended changes to the Bill are outlined in below and are largely clarificatory in purpose:

Clause	**Amendment made**
8A, 42(2)	Replaces cl 42(2) and lists all the ways in which the Bill gives effect to the principles of te Tiriti o Waitangi/the Treaty of Waitangi in order to align with the approach taken with other legislative programmes such as the Data and Statistics Bill.
12	Trust marks changed to "accreditation" marks and will apply to services only (not Trust Framework (TF) providers) in order to make it clearer to potential users which services are and are not accredited.

9(3), 17 & 19*, 26A	In the Bill's first reading, the TF rules could be established either by the Minister as statutory rules or by Order-in-Council in the form of regulations. Amendments have been made to clarify responsibilities for the rule-making process. Clauses 17 and 19 have been restructured to limit the Minister's power to make TF rules to subject-matter that was in cl 19(1)(b) (the technical requirements). The more procedural requirements (e.g. reporting requirements, self-assessment, fees etc) that were in cl 19(1)(a) and (c) have been moved elsewhere (to 9(3) and 26A) to be made by regulations. This split is in recognition of the fact that the technical requirements may need to adapt more rapidly to changes in technology and business models. In the event of any potential conflict, clause 19(3) clarifies that regulations prevail over the rules. Clause 19(4) has also been inserted to clarify the relationship between the TF rules and the Privacy Act. Amendments to clause 26A also allow fees to be set by regulations to recover costs of operating the trust framework and fees may vary to reflect the different costs associated with administering different types of TF providers
18	Clarifies that TF rules must not apply to digital identity services that are not accredited services.
20(1)(b), 44(3), 52(4A)	In response to concerns from Māori, a requirement has been added to consult and invite submissions from tikanga experts who have knowledge of te ao Māori approaches to identity. Additionally, cl 44(3) adds an obligation for the Board to engage with Māori – as provided in the requirements for consultation with iwi and hapū agreed in their engagement policy (cl 52(4A)) – to recognise and provide for Māori interests in the operation of the trust framework
44(1)(e)	Adds words in order to clarify that the Minister can impose other functions on the Board "to achieve the purposes of the Act"
59(da)	Clarifies the Authority's responsibilities by adding a function for the Board to undertake compliance monitoring of TF providers
61(3)(ba)	Adds a circumstance for use of the Board's power to require information or documents: when assessing whether to lift additional record-keeping or reporting requirements imposed under section 82.
61(5)(aa)	Clarifies that the Board's power to require information or documents does not extend to circumstances where another Act specifically deals with access to the information or document.
75(3)	Because it is likely that dispute resolution services will be performed by third parties, clause 75 has been amended to allow the chief executive to employ or engage individuals or organisations to provide dispute resolution services to resolve complaints.
82(2)	Clarifies that in the event that a TF provider or service fails to comply with a compliance order issued under clause 87 that the Authority can then suspend or cancel their accreditation.
83A	Allows the Authority to impose additional record-keeping or reporting requirements for any period the Authority considers appropriate and to lift those requirements if satisfied they are no longer needed
93(6)	Adds a definition of TF provider to include officers, managers, employees, and contractors – the accreditation of a TF provider or service may be suspended or cancelled if any of the circumstances listed in cl 93(1) applies to any of these persons

101	It is unlikely that the members of the Board, the Authority and the advisory groups will have access to much sensitive information given their largely governance and regulatory functions. The secrecy clause has therefore been removed.
102	The Public Service Act 2020 provides public service officials with immunity from civil proceedings. Therefore, the immunity clause has been amended to apply only to persons who are not public service employees.
103(2)	Clause 103 has been amended to clarify that the immunity provisions will not apply for proceedings under the Privacy Act.
104	The clause has been amended to clarify that the scope of the review include: • ensuring the privacy and security of user information (including Crown-held data) and protect it from unauthorised use; and • providing opportunities for Māori engagement in the trust framework.