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

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.

By establishing a trust framework, the Bill responds to industry demands for a set of enforceable rules that enable the provision of trusted digital identity services. The Trust Framework is designed to address findings that people are concerned with how their data is stored and used, that their information is over-shared, and that government needs to do more to protect personal information.

Accrediting trusted digital identity services

The Bill establishes the legal framework to support the Trust Framework by enabling the setting of rules that must be met to become an accredited digital identity service and outlining how the Trust Framework will be governed and enforced. These rules will be primarily outcome-based but may also include technical rules. Therefore, depending on their nature, rules may be set by Order-in-Council or by the Minister. They will at least 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 a trust 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 or rule changes.

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. Board members must include people with knowledge and expertise of te ao Māori approaches to identity, 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. The Authority will be 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.

Enforcement mechanisms made available to the Authority in instances where accredited digital identity service providers breach the rules include: issuing a private or public warning; placing additional record keeping or reporting requirements on the provider; issuing a compliance order; or suspending or cancelling accreditation.

The Bill also establishes criminal offences for activities that threaten the integrity of the Trust Framework. These offences include knowingly or recklessly representing oneself as being an accredited participant or accredited service when they are not; knowingly or recklessly supplying false or misleading information to the Authority; or obstructing the Authority.

Accreditation through the Trust Framework 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;
- setting the Trust Framework rules and requirements for accreditation;
- 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.