

2 December 2021

Committee Secretariat
Economic Development, Science and Innovation Committee
Parliament Buildings
Wellington

Dear Madam/Sir,

ICNZ submission on Digital Identity Services Trust Framework Bill

Thank you for the opportunity to submit on the Digital Identity Services Trust Framework Bill (**Bill**).

By way of background, the Insurance Council of New Zealand - Te Kāhui Inihua o Aotearoa (**ICNZ's**) members are general insurers and reinsurers that insure about 95 percent of the Aotearoa New Zealand general insurance market, including about a trillion dollars' worth of Aotearoa New Zealand assets and liabilities. ICNZ members provide insurance products ranging from those usually purchased by individuals (such as home and contents, travel and motor vehicle insurance) to those purchased by small businesses and larger organisations (such as product and public liability, business interruption, professional indemnity, commercial property and directors and officers' insurance).

Please contact Nick Whalley (nickw@icnz.org.nz) if you have any questions on our submission or require further information.

This submission has two parts:

- submission on the Bill, and
- other comments regarding the broader Digital Identity Services Trust Framework.

1. Submission

A. We support the framework underlying the Bill

We support the Bill's proposal to establish a formal Digital Identity Services Trust Framework (**framework**), noting that the intention underlying this is to:

- address gaps in regulation and assist with the development of trusted, people-centred digital identity services
- promote the provision of digital identity services within a consistent, structured and efficient trust framework that includes minimum requirements for security, privacy, identification management and interoperability, and
- support community resilience and realise the wider benefits of having such a framework in place.

In due course we expect that this framework will enable general insurers, in conjunction with accreditation providers and distribution partners, to verify the identity of their customers and transact with them more effectively. We also expect this will assist customers to switch between providers more easily, which is helpful from a competition and customer choice perspective.

We support the intention for this framework to align with equivalent frameworks in Canada, the United Kingdom and support mutual recognition of digital identity services with Australia. International equivalency is particularly important to the general insurance industry in Aotearoa New Zealand from a cost and complexity perspective because some insurers operate here as branches of overseas insurers or are part of a wider group of companies that also includes entities operating abroad.

We also support the incremental approach to implementation, with the initial 2020 to 2022 period focussing on development and a testing phase with a small number of participants, and the formal implementation of the legal trust framework, which entities can elect to join, coming later in 2022 to 2025, and a review occurring two years afterwards.¹ A campaign promoting the relevant trust marks in the lead up to, and following, the regime initially going live, together with an on-going public education campaign highlighting the benefits of this framework could be used to support the incremental roll out. The Accreditation Authority (**Authority**) should also actively monitor the use of the trust marks to ensure they are only used where appropriate.

B. Need for greater clarity on what is 'personal' and 'organisational' information

Greater clarity is required in the Bill about what constitutes 'personal' and 'organisation' information and how these terms interact. As currently drafted, we are concerned that the Bill could lead to unhelpful uncertainty about, and inconsistencies with, how framework participants (including accredited providers and parties relying upon the verification the framework provides) handle information. Specifically:

- The Bill defines a digital identity service in clause 9 as "*a service or product that, either alone or together with one or more other digital identity services, enables a user to share personal or organisation information in digital form in a transaction with a relying party*".
- While 'personal information' is well defined,² the definition of 'organisational information' is vaguely defined as "*information relating to a particular organisation*".
- While the definition of 'personal or organisational information' somewhat assists, in that it refers to information that describes the identity of an individual or organisation, the second limb of this definition, which refers to "*other information about that individual or organisation*", is open ended and unhelpful.
- Having definitions for 'personal information' as well as 'personal or organisational information' suggests that personal information, when used collectively with 'organisational information', takes on a different definition to the well-known definition afforded under the Privacy Act 2020.

We consider that the definition of 'personal information' and 'organisational information' should be specifically reworked to:

- Exclusively focus on the central purpose of the framework and the relevant information in this context (i.e. to verify or share information regarding a user's digital identity).
- Reflect the specific use cases under the framework and ensure parameters are sufficiently clear and distinct in each respect. This includes:
 - establishing or digitally identifying an individual/organisation
 - sharing identification details for that individual/organisation
 - sharing other personal information for an individual
 - sharing sensitive information about an individual/organisation, and
 - sharing organisational details an entity holds for, or about, an individual/organisation.

¹ This approach enables the regime to be efficiently tested and refined based upon practical experience and manageable progress, with industries and entities able to join when doing so makes sense. This will also ensure that the framework is workable for participants and durable in the longer-term.

² See clause 5 of the Bill referring to the definition under the Privacy Act 2020.

- Clarify either that ‘personal information’ cannot be ‘organisational information’ or detail the specific areas where these definitions overlap.
- Have regard to relevant ‘organisation’/business structures (e.g. companies, partnerships and trusts) and applicable organisational authorities that sit under them (e.g. directors for companies, partners for partnerships and trustees for trusts, and those with appropriate delegated authorities) and how these relate to the verification services the framework provides.

Additionally, a clearer distinction should be drawn between an end user’s ‘organisational information’ for digital identity purposes that falls within the framework, and the commercially owned ‘organisational information’ of the other party/service provider relying upon the verification that falls outside of it.³

If these matters are not addressed in the Bill (which would not be our preference, given their centrality to the operations of the framework), they will need to be the subject of detailed regulations, rules and/or guidance at some later point.

C. A transition period for penalties should be provided for

Consideration should be given to introducing a transition period (i.e. 2 years) before strict liability penalties under the Bill apply. In our view, time should be allowed for accreditation providers to become completely familiar with requirements and overcome the risk of inadvertent error during the initial implementation phase without penalty, with a more co-operative and education-focussed approach to compliance being more appropriate at this stage. We expand upon this in the section 3 below (under the heading ‘The appropriate approach to enforcement’).

D. The potential impact of additional penalties on insurance should be considered

Clauses 94 to 99 of the Bill introduces new penalties for individuals and body corporates. Directors and Officers’ insurance (**D&O**) is experiencing a period of low capacity and high premiums.⁴ D&O provides protection for the directors, officers and employees of a company against personal liability arising from legal claims against them in the course of undertaking their duties on behalf of the company. Introducing offences with financial penalties, such as those under the Bill, increases the level of risk presented and creates uncertainty, particularly until more is known about what these obligations mean in practice and how they will be practically monitored and enforced. These factors can result in premium adjustments for insurance customers at a time when some are already facing less availability and affordability.⁵ There could be a similar effect on Statutory Liability insurance, which provides cover for certain unintentional breaches of legislation, albeit not to the same extent as D&O. We raise this issue simply so that the potential impacts of these penalties on insurance availability and affordability, which may otherwise have been unknown, are considered.

E. Appropriate controls are required for information sharing

In so far as information collected by the Authority from framework participants for compliance purposes is to be shared with other government agencies, we strongly believe that the source party should be notified about the nature of the information shared and who it is being shared with, so that they have a fair opportunity to proactively engage with this exchange.

³ This reflects our understanding that the intention is to refer to the information of the end user of the framework (see definition of ‘user’ in clause 5). This could either be a consumer (e.g. personal) or business (e.g. organisation) using the framework, via an accreditation provider (see definition of ‘TF Provider’), to verify or share information about their digital identity with another trust framework participant, such as a service provider (see the definition of ‘relying party’), who then relies upon that relevant verification.

⁴ For further information on this point, see the Institute of Directors, Marsh, and MinterEllisonRuddWatts report [D&O insurance in a hard market](#).

⁵ For further information on the hardening D&O market, see MinterEllisonRuddWatts’ [2021 Litigation Forecast – D&O Insurance: Increasingly costly and uncertainty](#).

We are also concerned by the broad drafting of clause 101(2)(a) of the Bill, which allows members of the statutory Governance Board (**Board**), Authority or Māori Advisory Group to disclose any matters that in their opinion ought to be disclosed for the purpose of giving effect to the Bill. In our view, clause 101(3) should be amended to make it clear that disclosure of commercially sensitive and personal information is prohibited. While clause 101(1) refers to maintaining secrecy, as currently structured, this clause is subject to clause 101(2). Also, while clause 101(4) records that nothing in this clause limits any obligations under the Privacy Act 2020, this statement is general in nature. See clauses 61(5) and (6) of the Bill for an example of language that we believe would be more appropriate.

F. Other comments

In the appendix we set out our more technical feedback on provisions of the Bill.

2. Other comments about the framework

We also take this opportunity to provide feedback on other aspects of the proposed framework, noting that we have not had the opportunity to do so previously.

A. Appropriate safeguards are required when users intend to share others' information

Robust guidance, standards and/or rules will be required to support the operation of clause 11((1)(a) of the Bill and ensure a 'user' of the framework is only sharing personal or organisational information on behalf of someone else within appropriate parameters.⁶ Amongst other things, this include ensuring appropriately specific authority and informed consent is obtained from the party that is having their information shared in advance of this occurring - with a clear record of what specific information is to be shared, for what purpose and over what duration, with protections and controls in place to ensure these parameters are strictly complied with, potentially with reference to a consent renewal or lapse mechanism triggering a pre-arranged retention or destruction scheme.

Appropriately addressing these matters will be particularly important when the party who is having their data shared is an organisation, is vulnerable and/or lacks digital literacy or ready access to technology themselves. We expanded on the importance of ensuring vulnerable customers and those who lack digital literacy are adequately protected in our earlier submission to the Ministry of Business, Innovation and Employment (**MBIE**) on the proposed Consumer Data Right (**CDR**).⁷

In broader terms:

- Under this framework it appears to be assumed that all individuals have ready access to digital commerce, which may not be the case.⁸ This regime should enable accessibility of services, and ensure personal information rights are appropriately protected, in all circumstances.
- In developing the guidance, standards and/or rules underlining the regime, consideration should also be given to specifying minimum customer experience requirements, standardised information/data points and information retention, transfer and destruction requirements. These will provide certainty, assist with efficiency, maximise interoperability and ensure sufficient user control and protections are in place. Ideally these should be part of the standard implementation requirements, providing the settings required to successfully deliver the framework and uphold the integrity of, and maintain trust and confidence in, in it going-forward.

B. Need to ensure the framework and Board are sufficiently flexible and responsive

⁶ See definition of 'user' in clause 5 of the Bill.

⁷ https://www.icnz.org.nz/fileadmin/user_upload/ICNZ_submission_on_Consumer_Data_Right_071020.pdf, see comments specifically on pages 2, 3-4 and 14-15 in this regard.

⁸ See the Citizen Advice Bureau's report Face to Face with Digital Exclusion, https://www.cab.org.nz/assets/Documents/Face-to-Face-with-Digital-Exclusion-/FINAL_CABNZ-report_Face-to-face-with-Digital-Exclusion.pdf.

The regulations, rules and standards underlying the framework need to be sufficiently flexible that they can respond and evolve as new technology, accepted standards and trends emerge and/or to meet any changing needs and expectations of framework participants.

It will also be critical that the representatives appointed to the Board, and charged with monitoring and ensuring the effectiveness of the regime and developing the relevant secondary legislation, have the appropriate level of knowledge and expertise regarding technology, identity and data management (including with respect to the ethical use of data, privacy and security),⁹ and are sufficiently 'dialled in' to industry developments and trends, including as these relate to new technology, standards and cyber security and breaches. Doing so will also be important for those who support the Board and those involved in operating the accreditation regime (including in respect of applications for new or renewing accreditation). Failing to do so runs the risk of significantly undermining the integrity of, and trust and confidence in, the framework.

It is particularly important to reflect upon the significant pace of change from a cyber security and breach perspective in this context. For example, in their most recently quarterly report (Q2 2021), the national Computer Emergency Response Team (CERTNZ) records a 37% increase in unauthorised access and a 150% increase in ransomware since their last Q1 2021 report.¹⁰ This latest report also highlighted the particularly significant volume of phishing and credential harvesting being reported on.

C. Need to avoid inconsistencies and ensure clarity across government agencies and regimes

We acknowledge that the Bill and arrangements under it are not intended to override obligations under other legislation including the Official Information Act 1982 and Privacy Act 2020,¹¹ or limit or otherwise affect the Electronic Identity Verification Act 2012 or the Identity Information Confirmation Act 2012, which we endorse.

Inconsistencies between requirements and approaches are particularly unhelpful from a regulatory burden and cost perspective, and in terms of wider trust and confidence in the framework. Ensuring there is consistency and alignment in practical terms, as the framework develops, will require the Board and those who support it to be vigilant and well connected with other agencies operating in this space (including the Office of the Privacy Commissioner, MBIE regarding the development of the CDR and any separate team working within the Department of Internal Affairs on the RealMe platform).¹² Effective collaboration and planning between agencies will also enable previous work and experience to be efficiently leveraged. From a broader customer protection perspective, it will also be important for the Board to be well connected with the approaches and work the Financial Markets Authority and Commerce Commission are undertaking and ensure alignment in these respects. We suggest that formal protocols and policies be developed to ensure appropriate coordination and planning with these other agencies is occurring.

It would be useful to get a clearer picture of how the Bill will interact with the other regimes once it is implemented including what additional obligations will be imposed on an entity that elects to participate in this framework over and above their existing obligations. These matters will also impact upon what role an entity may decide to take on under the framework (e.g. as a provider rather than a relying party).

⁹ We endorse the references in clauses 46(2)(c) and (d) of the Bill in this regard.

¹⁰ <https://www.cert.govt.nz/about/quarterly-report/quarter-two-report-2021/>.

¹¹ See, for example, references in clauses 11, 16, 19, 61, 75 and 101 of the Bill.

¹² To that end, we are supportive of the intention to accredit the RealMe platform under this framework rather than develop an entirely new accredited public verification platform. This allows the Government to appropriately utilise, refine and build upon what already exists and draw upon insights from this previous work.

We expect that specific and detailed guidance will need to be developed to clarify what breaches, complaints and other matters fall within this framework, as opposed to being matters that fall under the Privacy Act 2020 and/or for the Office of the Privacy Commissioner to otherwise engage with, and to the extent overlaps exist, which regime takes precedence and the capability for joint investigations or action to be undertaken (if appropriate). Within the parameters of the Bill, consideration should also be given to developing a specific information sharing protocol between those operating this framework and the Office of the Privacy Commissioner and explaining this and the extent to which previous privacy breaches are relevant to accreditation in guidance. Care should also be taken to ensure that privacy and digital identity trust marks are clearly distinguishable to the public, with the different purposes of these being clearly spelled out.

D. An appropriate approach to enforcement

In terms of enforcement action undertaken by the Authority,¹³ in our view, there should be a focus on early intervention and proactive engagement should any issues arise. The dispute resolution process could be utilised as a potential point of escalation, where required, with formal enforcement action reserved for situations where issues cannot be mutually worked through. Consistent with this, we are supportive of references under some enforcement provisions of the Bill to the Authority taking reasonable steps to give notice to providers, giving them a reasonable opportunity to comment and considering their feedback.¹⁴

A regulatory approach based on cooperation and open dialogue would be particularly appropriate in the initial years of the framework's operation given it will be new and both the Authority and the industry will be learning and developing and refining arrangements as they go. We would also support the Authority working closely with the digital identity services industry to develop detailed guidance on requirements, including specific expectations and examples of best practice.

E. Funding and equal treatment of private and government participants under the framework

While we acknowledge that the framework is likely to result in commercial benefits for participants, it is also important to have regard to the significant public good aspects associated with this development, as confirmed by the World Bank.¹⁵ In our view, this warrants some contribution from Government in addition to cost recovery from participants.

We also consider that it is appropriate that government accreditation providers contribute from a cost recovery perspective. These providers are deriving benefit from this regime, otherwise private providers would be effectively subsidising them and this would ensure there is a more level playing field – which is important given government providers may potentially compete with private providers for business. This would also allow costs to be spread over a larger pool of providers, lowering barriers of entry and further incentivise private providers to opt-in to the framework.

Similarly, to ensure a more level playing field and reinforce the integrity of the framework, it is appropriate for government providers to also be subject to enforcement action. It should not be assumed that government participants are likely to be more compliant under this framework, noting that several government agencies have recently been the subject of serious data breaches.¹⁶

We also query the appropriateness of clause 47 of the Bill, which provides that only members of the Board who are public service employees have voting rights. In addition to promoting private sector

¹³ Which includes potentially suspending or revoking accreditation or issuing pecuniary penalties in the event of non-compliance.

¹⁴ See, for example, clauses 83, 84, 91, 92 and 93 of the Bill.

¹⁵ Pages 50 of the relevant Regulatory Impact Statement dated 10 February 2021, [https://www.dia.govt.nz/diawebsite.nsf/Files/Proactive-releases/\\$file/proactive-release-digital-identity-trust-framework.pdf](https://www.dia.govt.nz/diawebsite.nsf/Files/Proactive-releases/$file/proactive-release-digital-identity-trust-framework.pdf).

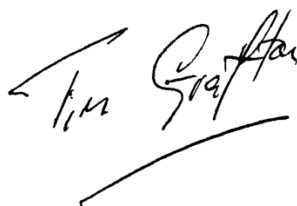
¹⁶ See, for example, the recent Reserve Bank of New Zealand data breach in January 2021, <https://www.rbnz.govt.nz/our-response-to-data-breach>, the Waikato District Health Board's breach in May 2021, <https://www.waikatodhb.health.nz/information-system-update-service-and-clinic-latest/> and the Accident Claims Compensation breach in October 2021, <https://www.rnz.co.nz/news/in-depth/454320/acc-staff-posted-clients-details-to-snapchat-group>.

engagement with the framework and a more level playing field, ensuring equal voting rights will support the Board to be appropriately flexible and responsive to change (as outlined under B. above).

3. Conclusion

Thank you again for the opportunity to submit on this matter. If you have any questions, please contact our Regulatory Affairs Manager by emailing nickw@icnz.org.nz.

Yours sincerely,

A handwritten signature in black ink that reads "Tim Grafton". The signature is written in a cursive style with a long horizontal stroke underneath.

Tim Grafton
Chief Executive

A handwritten signature in black ink that reads "Nick Whalley". The signature is written in a cursive style and is placed on a light-colored rectangular background.

Nick Whalley
Regulatory Affairs Manager

Clause reference	Comment
3(a) (Purpose)	<p>What it means “to establish governance and accreditation functions that are transparent and incorporate te ao Māori approaches to identity” needs to be expanded upon in the specific context of this Bill and framework. Similarly, clause 20(1)(b) of the Bill refers to consultation with people or groups outside the Board with expert knowledge of te ao Māori approaches to identity before rules are made.</p> <p>We acknowledge that these matters may be clarified via secondary legislation and/or guidance.</p>
11(1)(a) (Requirements for providers dealing with personal or organisational information when providing accredited digital identity services)	<p>Unless a provider has obtained information directly from an individual/organisation themselves, the framework will involve them collecting information through another organisation or government entity and accordingly, being a third party for information collection purposes.</p> <p>How this and other third-party information sharing arrangements would practically operate need to be carefully worked through, particularly in so far as the information in question is ‘personal information’ under the Privacy Act 2020, which can generally only be used for the primary purpose it was collected for,¹⁷ and/or where the intention is to share information across different sectors or uses.</p> <p>At a minimum the framework should provide for consent management and authorised uses to be clear and transparent to end users. Also see more comments under heading 2. A. above.</p>
12 (Trust marks)	<p>We suggest that only one set of template trust marks be approved for use. We are concerned that having a wide array of different trust marks that look different may be confusing for end users, add to participants costs and undermine the integrity of, and trust and confidence in, the framework. For the same reasons and to increase certainty, consideration should also be given to the trust marks having an upfront expiration date.</p> <p>We acknowledge that these matters may be addressed via secondary legislation and/or guidance.</p>
26 (Accreditation – notice of decision)	<p>From a certainty and efficacy perspective, it would assist if this clause included a timeframe for the Authority to determine an application for accreditation. This could include an option for an extension by the provision of a notice in advance of the original deadline expiring within defined parameters (e.g. where the application is particularly complex and/or resource intensive to work through).</p>
41 (Record keeping and reporting by accreditation providers)	<p>The minimum period that records must be held for should be prescribed, ideally in line with other regimes (e.g. 7 years).</p> <p>We acknowledge that this issue may be addressed via secondary legislation and/or guidance.</p>

¹⁷ See s 22 of the Privacy Act 2020, Privacy Principle 10 (Limits on use of personal information).

Clause reference	Comment
61(2) (Power to require information or documents)	The timeframe that an individual or organisation must provide information within should be aligned with the equivalent periods under the Privacy Act 2020 (e.g. up to 20 working days with an option for an extension). ¹⁸
68(1) (Who may make complaint)	While we acknowledge this may be inferred with reference to the Interpretation Act 1999, for clarity, ideally this provision should be amended to make it explicit that, in addition to an individual/natural person, 'any person' includes a 'corporate sole', 'body corporate' or 'unincorporated body'.
82(b) (Remedies following finding of breach)	The potential for the Authority to require an accreditation provider to comply with additional recordkeeping or reporting requirements indefinitely is inappropriate and arbitrary. A timeframe within which additional requirements must be satisfied should always be prescribed, with reference to the specific conditions that if met, would mean it no longer applies.
83 to 85 (Public warning and compliance orders)	Given the possible subjectivity in interpretation, further detail is required about what constitutes 'reasonable grounds', 'reasonable steps' and 'reasonable opportunity'. It would also assist if appropriate minimum timeframes for the provision of notice were specified before public warnings and compliance orders were issued, and once a compliance order is issued, to remedy a breach and/or report. We acknowledge that these issues may be addressed via secondary legislation and/or guidance.
93(2) (Suspension or cancellation of accreditation following finding of a breach)	We are concerned that this sub-clause, which enables the Authority to suspend or cancel accreditation, whether or not they have found a breach, is too broad. This power should be limited to circumstances when a breach has been found, as otherwise it could be used without sufficiently legitimate grounds for doing so. An appropriate minimum notice period should also be provided for before any suspension or cancellation occurs, with an explicit right for this decision to be reviewed after a certain period of time has elapsed after the suspension or cancellation occurs. We acknowledge that this issue may be dealt with via secondary legislation and/or guidance.
100(3) (Regulations)	The parties that must be consulted before regulations are made should be expanded to include impacted, or potentially impacted, stakeholders and those that will, or may, otherwise have an interest. See clause 20(1) of the Bill for an example of language that we believe would be more appropriate.
Various	Consideration should be given to reflecting upon the use of blockchain technology (or other similar technology improvements) to future-proof the Bill.

¹⁸ Sections 44 and 48 of the Privacy Act 2020.

Further detail is required about the following matters referred to under the Bill, although we expect these will be addressed in either secondary legislation and/or guidance:

Clause reference	Further detail required
9(2)(c) (Meaning of digital identity service)	What appropriate 'secure sharing' will involve.
19 (Content of rules)	What specific requirements related to identification management, privacy and confidentiality, security and risk, information and data management, sharing and facilitation, reporting and the particular format of information/data under the rules will involve.
92(1) (Suspension or cancellation of accreditation if breach on 3 or more occasions)	<p>What specific breaches of the Bill, rules, regulations or terms of use for the trust mark on at least three separate occasions within a 12-month period would result in this power being used. We expect that there would be a de minimis threshold. Consideration should be given to the appropriate treatment when circumstances are ongoing (as opposed to being a discrete one-off event) and/or where multiple end user individuals/organisations are affected.</p> <p>Also see comments about notice and review periods regarding clause 93 above, which are also relevant to this provision.</p>