Submission to the
Economic Development, Science and Innovation Committee

on the
Digital Identity Services Trust Framework Bill
2 December 2021

Colin Wallis
Executive Director
Digital Identity NZ
M | +64 21 961955

SUMMARY:

1. Digital Identity New Zealand (DINZ) appreciates the opportunity to make a submission to the Economic Development, Science and Innovation Committee on the Digital Identity Services Trust Framework Bill (the Bill). This submission is the result of a collaborative working-group effort between DINZ members and the subject matter expertise of DINZ's Executive Council Members. We appreciate the invitation to speak to the Committee about our submission.

2. Digital identification is a subject that every New Zealander should be concerned about. This Bill is a critical component of the digital identity ecosystem that will operate in Aotearoa New Zealand over the next few decades. We are at a critical juncture in the evolution of digital identity around the world, and we can learn from and leverage those developments, while also ensuring our framework delivers for New Zealanders now and in the future.

3. DINZ supports the Bill's intent if it is to accomplish the objectives that are outlined in the Bill's Digest: [1]

   A legal framework for the provision of secure and trusted digital identity services for individuals and organisations.

   The primary objectives of the Bill are to—
   a. *help drive consistency, trust, and efficiency in the provision of digital identity services:*
   b. *support the development of interoperable digital identity services:*
   c. *provide people with more control over their personal information and how it is used:*
   d. *enable the user-authorised sharing of personal and organisational information digitally to access public and private sector services.*

4. DINZ has supported, and will continue to support, the intent of the Bill. DINZ specifically supports:
   a. an opt-in certification (accreditation) scheme for service providers who can demonstrate they can meet the Trust Framework rules, which are currently under development;
   b. a governance board responsible for reviewing and recommending changes to the Trust Framework's rules, including taking into account the views of stakeholders (including groups with expertise in te ao Māori);
   c. a Māori Advisory Group to provide advice to the governance board on Māori digital identity interests;
   d. the ability of the governance board to form advisory committees (from both the public and private sectors) to provide advice and report to the board; and
   e. an independent accreditation authority that certifies (accredits) organisations while monitoring and enforcing compliance.

5. However, DINZ considers that the Bill's intent could be more clearly reflected in the draft Bill as currently written. DINZ considers the Bill must provide equitable opportunities to encourage greater participation and adoption, be aligned with existing

[1] https://www.parliament.nz/en/pb/bills-and-laws/bills-digests/document/53PLLaw26591/digital-identity-services-trust-framework-bill-2021-bills

national and international standards, and reduce friction while remaining true to the Bill's objectives as stated in the Bill's Digest. Below, DINZ makes a number of recommendations to amend the Bill, and suggestions on specific issues and clauses (attached in appendices) to help the Government develop an adaptive and extensible Digital Identity Services Trust Framework for Aotearoa New Zealand.

OUR SPECIFIC RECOMMENDATIONS

6. DINZ recommends the Bill be amended to:

6.1. **Allow flexibility to account for unanticipated challenges during the formative years.** DINZ understands that unlike other common law jurisdictions adopting digital identity trust frameworks (e.g. Australia, United Kingdom and Canada), Aotearoa New Zealand will not be undertaking multi-year pilots of the proposed Digital Identity Services Trust Framework before passing legislation as is being done in Australia and Canada and widely expected in the UK. This means that rules will be developed concurrently with passing legislation, which in turn will necessitate a significant collaborative and coordinated effort across public and private sectors, leveraging scarce domain knowledge, experience and expertise located within DINZ and overseas. Even with all of this knowledge, experience and effort, the legislation should allow for changes to the rules and regulations during the first few years of operation to ensure extensibility and adaptation; The same approach applies to technology. While not covered by the Bill, it is worth noting that as technology advances, matures, and gains mass consumer acceptance, Te Tiriti o Waitangi principles can be reflected in technology options.

6.2. **There needs to be greater recognition that we operate in a global context.** Assurance frameworks and associated conformity assessment and certification regimes already exist, for example, International Accreditation Forum utilises the ISO/IEC 17000 series of standards and DEPA's approach to accreditation. While acknowledging that there will be instances where a uniquely Aotearoa New Zealand requirement is needed for the operation of the Trust Framework, drafting legislation and rules that reflect existing established practise and standards will provide a variety of benefits to participants, ranging from consistent use of terminology across different jurisdictions to processes and methods to ensure impartiality.

6.3. **Encourage interoperability under the Trust Framework by optimising alignment.** One of the policy objectives of the Bill is to 'support the development of interoperable digital identity services'. However, the draft legislation does not fully exploit the potential benefits that interoperability can offer NZ derived services conformant under the Trust Framework seeking to become conformant under Trust Frameworks overseas to expand their services, or vice versa. As mentioned in 6.2 above, using the correct terminology and reflecting existing international standards and practice certainly helps interoperability by reducing cost and friction caused by services having to make wholesale changes to their products for each jurisdiction. It is known that mutual recognition with the Australian Government Digital

Transformation Agency's (DTA) Trusted Digital Identity Framework (TDIF) is an objective, but there needs to be greater appreciation that that too will change as Australian legislation approaches, so great care needs to be taken not to too closely replicate Phase 1 developments in Australia as they too will change in operation and practice over time.

6.4. **Māori seats in governance structures must be included in the Bill**. Māori will be consulted, and various instruments will be proposed to enable their participation, but the draft legislation does not include a seat at the governance table with voting rights for Māori. Given the importance of identity to Māori, personal and community data sovereignty can be baselined in the Bill using Te Tiriti o Waitangi principles of equitable partnerships (Ōritetanga), self-determination (Rangatiratanga) and governance (Kāwantanga), by giving Māori voting rights.

6.5. **Governance clauses in the Bill should be changed to create more equitable representation and governance.** Beyond Māori seats referred to in 6.4 above, DINZ notes the absence of any actor representing the interests of individuals, whose interests at the end of the day, are those that this Bill seeks to foster. From the development of the rules through to the governance, there should be a societal representative cross section of industry and individuals. Furthermore, the draft legislation indicates a one-sided approach to governance, with only public sector agencies having voting rights. This has the potential to disincentivise participation by the private sector. The governance board should have a minimum representation of independent and non-vendor members with relevant domain expertise. Clause 47 of the Bill should be changed to ensure that all members of the governance board are treated equally and have equal voting rights, regardless of their employer.

6.6. **Add a new definitive clause in the Bill to prevent the possibility of a single Government department from regulating its own activities**. The Government department that will be the "responsible department" administering the Act is not identified in the draft Bill, although it is widely assumed it will be the Department of Internal Affairs (DIA). The DIA operates the dominant market digital identity solution RealMe and we believe it will be important for the DIA to make RealMe's strategic intentions clear well in advance of legislation. This is so that potential conflicts of interest can be fully understood, action taken either by the DIA or through this legislation to mitigate the risks exposed, and to allow the private sector time to evaluate the risk. Of course, RealMe's strategic intentions could change over time. To prevent this conflict of interest, be it with DIA and RealMe or any other agency with an operational digital identity service, inserting such a new clause would improve transparency.

6.7. **Potential to create a new statutory organisation to administer the legislation.** The responsible agency for this should ideally be the creation of a new fit for purpose statutory organisation as is envisaged in the Australian Digital Identity Legislation Discussion Paper (see page 34) to promote transparency and impartiality, ensuring that there are no conflicts of interest with existing services or other public sector

owned and operated digital identity services for example RealMe, MyIR, MyMSD, My Health Account. If the "responsible department" simply has to be an existing agency, then the perhaps Privacy Commissioner and MBIE might be more appropriate than the DIA, as this would more closely follow the model proposed in Australia's legislation discussion document.

6.8. **Review business modelling and lean into 'fair cost allocation' to improve adoption and reflective of overseas operational experience.** To ensure that the Trust Framework is viable and equitable to all parties, a broader business modelling discussion of the authorities' financing and charging should be conducted. According to the DIA's Proactive release paper, the $1.5 million estimated costs of operating the Trust Framework should be paid by participating private sector service providers only. The cost to public sector entities is borne by the Crown. All stakeholders want the legislation to have a high level of participation and adoption but requiring the private sector to cover the costs adds to the disincentives and creates a potential barrier to entry for the private sector to seek certification under the Framework in sufficient numbers. Because public sector service providers are most likely to be able to afford the costs and reap the benefits of certification, costs should be allocated fairly. The costs of audit and product changes can quickly outweigh the benefits derived from certification thereby making the effort unviable, as experienced anecdotally by international digital identity trust frameworks, such as Kantara and the historic experience of the Gov.UK Verify service.

6.9. **Review the draft legislation in light of other existing legislation to ensure compatibility.** While DINZ supports this legislation, it is vital that other associated legislation is amended to ensure it is compatible and removes any ambiguities for consumers or those providing services in this sector.

6.9.1. For example, Clause 15 of the Bill relates to the Electronic Identity Verification Act (EIVA) 2012 but it is not clear if the impact of parts of this Bill on the Trust Framework have been thought through.

6.9.2. A further example is the Anti Money Laundering and Countering Finance of Terrorism act 2009 (AML-CFT Act 2009), which coincidentally is currently under review. The two pieces of legislation need to be aligned and compatible.

6.9.3. Both the Privacy Act 2020 and the Identity Information Act 2012 may also require consequential adjustments. We are supportive of the precedence the Privacy Act will have over the Trust Framework. However, there should be greater clarity on understanding how the Trust Framework authority will work with other regulators such as the Privacy Commissioner. For example, Part 6 of the Bill makes it clear that if there is a complaint, the Trust Framework authority may refer the complaint (in full or in part) to the Privacy Commissioner if it considers the complaint may be more appropriately dealt with by the Privacy Commissioner. However, it is not clear if it is intended that both the Trust Framework authority and the Privacy Commissioner could both

independently investigate and rule on a privacy complaint in cases where the relevant action breaches both the Trust Framework rules and the Privacy Act.

6.9.4. The Government recently announced that it would introduce Consumer Data Rights (CDR) in 2022. Again, it is important to ensure that there is alignment between CDR and the Trust Framework to avoid confusion and implementation challenges, compliance cost and general barriers to innovation and adaption and implementation.

BACKGROUND:

7. DINZ was formed to help Aotearoa New Zealand's transformation as a digital nation, where everyone can prove who they are digitally in a secure and trusted way. Our vision is to be a country where people can express their identity using validated and trusted digital means in order to fully participate in a digital economy and society. Our mission is to create a digital identity ecosystem that enhances privacy, trust and improves access for all people in Aotearoa New Zealand.

8. DINZ is a purpose driven, inclusive, membership-funded organisation, whose members have a shared passion for the opportunities that digital identity brings. DINZ supports a sustainable, inclusive and trustworthy digital future for all New Zealanders.

9. DINZ members include Aotearoa New Zealand tech exporters, local and multinational IT firms, start-ups, universities, Government agencies, financial service providers and large corporate users of digital identity.

10. Now that the new framework is progressing, and there has been some progress on potential rules, DINZ seeks to play a valuable role in the rules development as they are crucial to the framework's successful implementation. As the Bill is structured, DINZ has concern that private sector views and input may not be sought

EMPHASIS ON SPECIFIC ISSUES THAT NEED TO BE ADDRESSED IN THE BILL:

11. **Service provider accreditation**: DINZ would like to see references to 'certifying' services (the term used in ISO/IEC 17065:2012 Conformity assessment — Requirements for bodies certifying products, processes, and services) rather than 'accrediting', although it is acknowledged that the Bill may be referencing some other international standard for its terminology, and if that is the case, it should be explicitly referenced. Furthermore, a service provider that has one or more certified 'accredited' services alongside non-certified 'accredited' services should be removed from the legislation. DINZ is concerned that this will cause confusion and misunderstanding among consumers of digital identity services, leading them to believe that an uncertified 'unaccredited' service is certified 'accredited,' when it is not. The focus of certification 'accreditation' should be on the service, not the provider.

12. **Independent voting rights for the Trust Framework Board:** The Bill anticipates "The CEO" will appoint members to the Trust Framework Board, who may or may not be from the public service (Clause 46). However, Clause 47 specifically states:
"*Voting rights: Only members of the TF board who are public service employees have voting rights on the board*."

13. Clause 47 will likely disenfranchise any member of the board who is not a public servant, would not be consistent with international standards nor existing practice, nor Australia's intended Governance principles of Independence, Transparency and Accountability (Australian Digital Identity Legislation Discussion Paper - page 33) and may serve to be a significant deterrent to any individual to participate on the board.

14. Clause 47 also negates the benefit of ensuring that members of the Trust Framework board have expertise in all the areas identified, as not all will have voting rights. This wording is particularly concerning as the functions of the board (as set out in Clause 44) include, among others:
    - recommending draft Trust Framework rules to the Minister, reviewing the rules at reasonable intervals, and recommending updates to them;
    - recommending regulations to the Minister;
    - undertaking awareness and education programmes for Trust Framework providers and the public; and
    - monitoring the effectiveness of the Trust Framework.

15. As these functions in paragraph 14 are critical to the success of the framework on an ongoing basis and this is the only source of input prescribed in the Bill for input to the Minister, it is not credible to have a governance structure where not all board members are treated equally.

16. The minutes of the Cabinet Economic Development Committee of 17 February 2021 state:[2]

[2] https://www.dia.govt.nz/diawebsite.nsf/Files/Proactive-releases/$file/proactive-release-digital-identity-trust-framework.pdf

However, there is a risk that a Board where only public-sector representatives have decision-making rights regarding the Trust Framework may be perceived as non-inclusive particularly by Treaty partners. Therefore, the Bill will establish that the Chief Executive must also ensure that the Board has appropriate knowledge and expertise in technology, identity and data management (particularly the ethical use of data), privacy, security and Te Ao Māori interests

17. **Recommendation**: That Clause 47 is adjusted to ensure all members of the Governance Board are treated equally and all have equal voting rights.

18. **Recommendation:** That members of the Board are appointed with equal voting rights from both the public and private sectors including the digital identity services industry communities and independents.

19. **Sparse recognition of the role of the private sector in providing solutions.** The minutes of the Cabinet Economic Development Committee of 17 February 2021 state[3]: *"agreed that the Board must have appropriate knowledge and expertise in technology, identity management, privacy, security and Te Ao Māori interests and participation".*

    However, the Bill does not specifically require representative members on the board who are able to provide input from their perspective as a provider of Digital Identity services. The draft Bill is written from the perspective of the public sector and its services (e.g. RealMe, MyIR, MyMSD, My Health Account) - a clear and obvious example being in the area of governance where the Trust Framework Board does not allow individuals from the private sector nor independents voting rights.

20. **Recommendation:** The Bill should state that there should be a minimum representation of private sector members or independents on the Trust Framework board.

21. **The potential for conflict of interest of the Department of Internal Affairs (DIA) in operating the Trust Framework.** The Government agency responsible for regulation is not expressly stipulated in the Bill. However, there is a widely held expectation that it is the DIA. While DINZ is confident that genuine efforts would be made to maintain a separation between DIA's Service Delivery and Operations branch (where RealMe is located) and DIA's Policy Regulation and Communities branch, the potential for conflict of interest would dominate perceptions of the Bill both in Aotearoa New Zealand and abroad, and would undermine the private sector's confidence in the Trust Framework Authority's impartiality in its operation of the Trust Framework, having the obvious knock-on effect of disincentivising private sector participation.

22. **Recommendation**: In the interests of full transparency, the DIA should be required to lay out the future strategy and roadmap for RealMe before the draft legislation is enacted. If the future strategy and roadmap envisions RealMe's continued development as a competitive market player while maintaining its current market dominance, the DIA should not be the responsible agency. Instead, ideally, a new statutory body, or at the

very least a public body with no vested interest in the operation of digital identity services, would be established. This will promote objectivity and eliminate any potential conflicts of interest with the DIA's RealMe service or other Government-owned and operated digital identity services.

23. **Seek out and advance opportunities for improved interoperability and portability.** While we raised the topic of interoperability in 6.3 in the context of international harmonisation in keeping with the Bill's intent, opportunities for interoperability and portability exist domestically also, for example in reducing the complexity in porting verified identification credentials curated by one certified 'accredited' digital identity service to another at the individual's direction and explicit consent - just as number portability in similar critical infrastructure sectors such as Telecoms has been made easier following legislation.

24. **Estimates of costs and numbers of Accreditations not reflective of experience internationally:** The establishment of this framework will incur costs and the Government has agreed to allow the authority to recover costs through variable charging for accreditation:

    The total cost of the Trust Framework in the near term (under a model where accreditation to the Trust Framework is opt-in) has been estimated at $1.5 million[4], with the Accreditation Authority having the capability to undertake up to 100 'simple' accreditations or up to 25 complex accreditations (with the relative cost of simple and complex accreditations estimated at $10,000 and $40,000 respectively).

25. The figures referenced in this estimate do not reflect current experience internationally. While these figures differ from the $10,000 to $250,000 stated on page 46 of the paper referred to in paragraph 25 above, they are closer to overseas experience reflecting that the business and financial viability of proceeding with certification/accreditation drops off once 6 figures is surpassed. Annualised, Kantara approves (certifies) around 3-6 digital identity services for the US Federal Government using the 3 US based assessors of its cohort of 5, Australia around 3 through its Trusted Digital Identity Framework (TDIF), and the UK Government's 2 UKAS assessors managed around 8 in 18 months (including those that withdrew during the process) when Gov.UK Verify was fully operational.

26. It is understood that cost recovery from the private sector will be sought. If this is the case, it is critical that only the variable costs associated with private sector applications be passed on to the private sector, rather than the Trust Framework's total cost/cost recovery of $1.5 million per year.

27. **Recommendation:** Only those cost attributable to non-government sectors should be charged to non-government sectors.

28. **Recommendation:** To encourage private sector applicants to apply to the Trust Framework, the fee charged should be kept to a minimum.

---

[4] https://www.dia.govt.nz/diawebsite.nsf/Files/Proactive-releases/$file/proactive-release-digital-identity-trust-framework.pdf

CONCLUSION

Thank you for the opportunity to provide feedback on the Digital Identity Services Trust Framework Bill.

We are happy to engage further to discuss our submission and provide any further assistance. We welcome the invitation to appear before the Committee to speak to our submission.

If you have any further queries do not hesitate to contact me.

Yours sincerely,

Colin Wallis
Executive Director, Digital Identity NZ
M +64 21 961955

APPENDIX:

DINZ'S COMMENTS ON SPECIFIC CLAUSES IN THE BILL:

29. **Clauses 10/18/22-31:** iterates accrediting a service provider that has one or more accredited services alongside other services that are not accredited, DINZ has concerns that this will lead to confusion and misunderstanding for the public as consumers of digital identity services. It is the service, not the provider, that should be the target of accreditation. That this is articulated in ISO/IEC 17065:2012(en) Conformity assessment — Requirements for bodies certifying products, processes and services. The US Government's National Institute for Standards and Technology (NIST) that specifies the standard that federal agencies should follow, references the 17000 series. And while the UK specifies a range of standards in its draft Digital Identity and Attributes Trust Framework, it is understood that the ISO 17000 series will also be referenced once the draft section giving details on certification is made public.

30. **Clause 11**: prohibits Trust Framework providers from collecting, using, sharing, or otherwise dealing with personal or organisational information. We suggest adding 'selling' of personal information is prohibited i.e. 'prohibits Trust Framework providers from collecting, using, sharing, selling or otherwise dealing.'

31. **Clause 12**: trust marks and misuse of trust marks, the legislation makes no mention of steps to take to preserve the integrity of the trust mark. Again, there are developed standards for this, for example ETSI TS 119-612 v1.1. The terms of use is not the same thing as preserving the integrity of the trust mark.

32. **Clause 19**: suggest adding 'storage and disposal' bullet point

33. **Clause 31**: obligation of Trust Framework provider to tell Trust Framework of any changes to key information or specified information. Suggest obligation stipulates that immediate notification is required.

34. **Clauses 32-37** regarding the Trust Framework register is another example where drafters need not develop from a zero base. The aforementioned ETSI standard stipulates the requirements, drawn from experience of operating such registries in Europe.

35. **Clauses 38-39** regarding third party assessors, is another example where the term used is inconsistent with the ISO/IEC 17000 series where the term auditor is used, not assessor.

36. **Part 4,** regarding the Trust Framework Board clauses, clause 47 (that only Trust Framework board members who are public service employees have voting rights) is the most unjust towards the private sector, and fails the otherwise good intent of the Bill. This part of the draft Bill also misses the opportunity for Māori voting representation from iwi, the more progressive of which are potential service providers. DINZ's believes that the Bill should go further than merely adopting the principles of te Tiriti o Waitangi,

having identity related experts and undertaking engagement. Expertise in operating conformity assessment and certification schemes is missing from Part 4.

37. **Parts 5, 6 and 7:** Trust Framework Authority. While the responsible agency is not named, if it were to be DIA, then this creates a significant potential conflict of interest with its operation of RealMe. While DINZ is confident that genuine efforts would be made to maintain a 'Chinese wall' between DIA's Service Delivery and Operations branch where RealMe is located, and DIA's Policy Regulation and Communities branch, the optics will not assist in building the consumers' nor the private sector's confidence in the Trust Framework Authority's impartiality in the operation of the Trust Framework.

38. **Clause 103; Immunity for Trust Framework providers for actions of users.** This is supported by DINZ, as no doubt Government departments strongly support it too, but it is not seen as a significant motivator for non-government entities to get certified, in part because it can be insurable.

39. **Clause 105: Regular reviews:** DINZ suggests three yearly rather than five yearly, which is more closely aligned with international information security management system audit practice.

ANNEXURE ONE:

REFERENCES:

There are a number of initiatives and actions that are relevant to this Framework mentioned in this submission. Below are some references to assist the committee.

DINZ Working Group and Terms-of-Reference
https://digitalidentity.nz/dinz-distf-working-group/

Australian Government Digital Transformation Agency - Digital Identity Legislation
Australian Digital Identity Legislation Discussion Paper
https://www.digitalidentity.gov.au/sites/default/files/2021-01/Digital-Identity-Legislation-Consultation-Paper_Accessible_131120.pdf

Australian Trusted Digital Identity Framework
https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework

Digital Economy Partnership Agreement (DEPA)
https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/

United Kingdom Accreditation Service
https://www.ukas.com/

United Kingdom Digital Identity Attributes Trust Framework (in development)
https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/uk-digital-identity-and-attributes-trust-framework-alpha-version-2

The Global Trust Framework & Spec Commons - Kantara Initiative
https://kantarainitiative.org/home/
https://kantarainitiative.org/trustoperations/
https://kantarainitiative.org/download-category/service-assessment-criteria-sets/

ISO/IEC 17065:2012
https://www.iso.org/standard/46568.html

NIST references to ISO/IEC 1700 re US Federal
https://csrc.nist.gov/CSRC/media/Events/ISPAB-MAY-JUNE-2012-MEETING/documents/may30_conformity_ggillerman.pdf
https://csrc.nist.gov/CSRC/media/Presentations/usg-testing-assessment-and-conformance-models/images-media/3-Carnahan-ISPAB-FINAL.pdf