paymentsnz®

Digital Identity Services Trust Framework Bill

Payments NZ submission to the Economic Development, Science and Innovation Committee

December 2021

Introduction

Payments NZ Limited (Payments NZ) welcomes the opportunity to make a submission to the Economic Development, Science, and Innovation Committee on the Digital Identity Services Trust Framework Bill (the Bill).

Payments NZ is a governance organisation at the heart of Aotearoa New Zealand's domestic payments system. Our company's constitutional objectives include promoting interoperable, innovative, safe, open, and efficient payments systems. We manage payment clearing system rules and standards and the systems we manage transact over $6 trillion annually.

Payments NZ works with industry to ensure payments are simple and secure for Kiwis and to lead the future direction of payments for all New Zealanders. We have a particular focus on the network non-competitive elements of the payment ecosystem and have a high level of expertise in shaping the rules, standards, governance models and strategic roadmaps for payments and payments related activities, including open banking.

In our submission, we make seven recommendations for the Committee's consideration.

Digital identity and payments

Digital identity, and trust in payments, sit at the heart of a safe, secure, and efficient payments system. Generally, for a payment instruction to be authorised, the payer must first authenticate themselves. Authentication is the process of confirming a customer's identity and/or credentials before they authorise a payment.

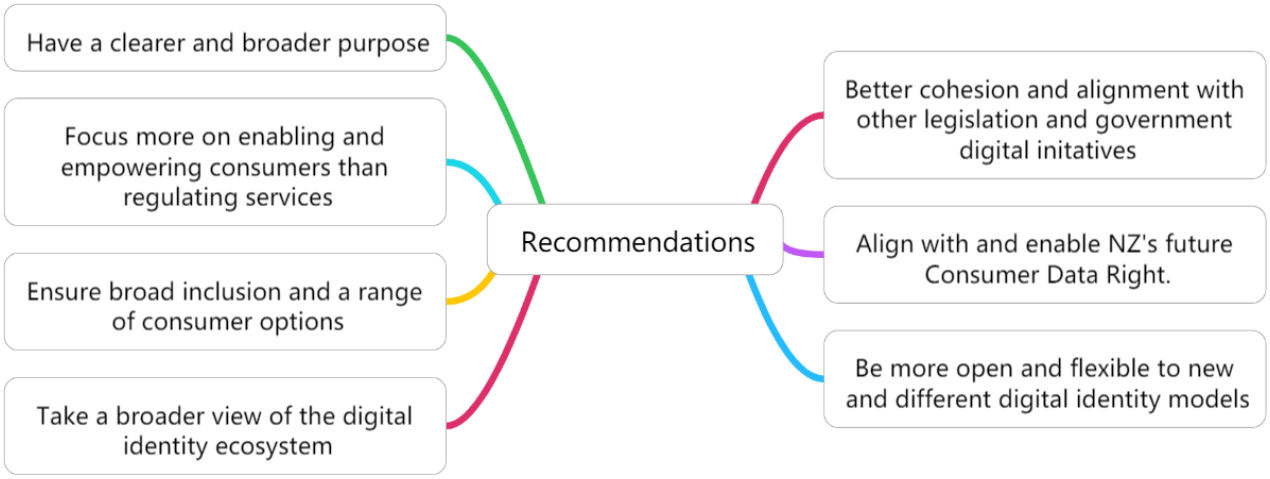
There has been significant growth in the 'business of payments', with shifts in consumer preferences and enabling technologies allowing new payment providers and business models to emerge. We are no longer dealing with a payments system, but with a diverse payments ecosystem. Increasingly complex and interconnected, the payments ecosystem exists in a world where the boundary between our physical and digital lives are blurred. All payment ecosystems operate, and are fundamentally dependent on, trusted and secure digital interactions. Digital identity, trusted digital data, and secure digital interactions are critical to the evolution of both the digital and payments ecosystems.

A highly relevant example of the link between digital identity and payments can be found in the future Consumer Data Right (CDR) framework. In an open banking arrangement under a CDR, the authentication of the customer (i.e. identity and credentials) is a critical part of setting up a data sharing arrangement where the bank shares the customer's account and transaction information with other parties. Digital identity legislation has the potential to enable more versatile, convenient, secure, and safe authentication processes and, in doing so, to underpin an innovative digital economy for Aotearoa New Zealand.

Executive summary and key recommendations

Payments NZ fully supports the establishment of a digital identity trust framework (the trust framework) through enabling legislation, as this has the potential to become one of the pillars of our future digital economy. However, in its current form, we believe the Bill does not yet make the most of its potential. We propose seven areas of recommended improvements, which are summarised below. Our submission provides the context and rationale supporting these recommendations.

Recommended areas of improvement



Seven recommendations

Recommendation #1: The scope and intent of the Bill should be more clearly defined, including by:

- Being consumer centric ('people centred'), and not digital identity service provider centric.
- Reflecting the context of the broader New Zealand digital economy and consumer experience in that economy.
- Reflecting and including all the principles approved by Cabinet.

Recommendation #2: The Bill should:

- Be focused on enabling consumers to have multi-faceted, privacy enhancing and personally controlled digital interactions.
- Provide a framework for consumers sharing and reusing their trusted verified data across services, sectors, and geographies.
- Specifically reference interoperability between services, sectors and geographies.

Recommendation #3: The Bill needs to focus on the consumer and the mechanisms that support a flexible and inclusive trust framework by:

- Covering the alignment and interoperability of physical and digital interactions.
- Including mechanisms to support inclusion of all New Zealanders, such as through delegations, guardianship, and temporary or permanent representation.

Recommendation #4: The Bill should aim beyond just governing digital identity service providers and establish a broader trust framework that guides national digital ecosystem evolution by:

- Adding a definition of 'digital identity'.
- Recognising the key components that make up a digital identity ecosystem.

Recommendation #5: The alignment and inter-relationship between the Bill and various other domestic governmental initiatives must be better understood before legislation is finalised.

Recommendation #6: That there should be as much alignment and consistency as possible between the applicable elements of the legislative and regulatory frameworks for the trust framework covered by the Bill and the upcoming Consumer Data Right (CDR) legislation.

- That the Bill includes the basis for digital identity to be used in the context of New Zealand's future CDR.
- That the future CDR reflects and enables the potential for the trust framework to be used in open banking.
- That the Bill clarify whether it is permissible for a consumer's digital identity credentials to be on-shared from within the trust framework to outside the framework.

Recommendation #7: The Bill needs to be more neutral so there is the potential, over time, to support new models of digital interaction and to promote the controlled enhancement of existing infrastructures (including payments). This includes:

- Being technology neutral.
- Being neutral as to the digital identity model used.
- Being neutral as to the terminology that is used and the definitions that apply (for example, "Identity Service Provider" and "Relying Party").
- Being clear as to how the digital identity of 'things' will be addressed, along with its underpinning ownership and delegation capabilities.

Recommendations explored

1. **The purpose and scope of digital identity systems should be expanded and further defined**

   The Bill looks to establish the rules and governance framework for systems that manage digital identity, but without an underlying definition, intent, or context for these systems. The scope and purpose of the Bill is narrow and as a result, the opportunity to define the needs and controls of the broader digital identity ecosystem risk being lost.

   As signalled by including the word 'services' in the title of the Bill, the focus is on digital identity *services*, and not on New Zealanders and businesses safely and conveniently using their digital identity.

   The principles approved by Cabinet in May 2021, (e.g. 'people centred') are not discernible anywhere in the Bill. The Bill should be consumer centric first rather than digital identity service provider centric.

   Recommendation #1: The scope and intent of the Bill should be more clearly defined, including by:
   - Being consumer centric ('people centred'), and not digital identity service provider centric.
   - Reflecting the context of the broader New Zealand digital economy and consumer experience in that economy.
   - Reflecting and including all the principles approved by Cabinet.

2. **Consumer empowerment needs to be at the centre of the Bill**

   The purpose of the Bill appears to focus on the service definitions and management of these services, and not on the consumer having trusted digital interactions.

   Service providers have evolved to 'fill a hole' in the authentication of individuals by building digital identity services on top of other primary services, such as those offered through social media platforms (e.g. emails, 'log in with...'). The increasing use of these digital identity service providers, partly due to a lack of alternatives, has resulted in consumer "lock-in" and control over parts of a consumer's digital life.

   The Bill should empower consumers by giving them options with respect to digital identity, so they do not have to worry about being locked-in to an existing provider. Being able to 'take with me' and reuse or share trusted identity as verifiable 'data about me' must be possible if we are going to have a flexible and vibrant digital economy. Service providers that can rely on direct and secure consumer interactions that use the sharing of verifiable data will find it easier to engage consumers, enabling them to move to alternative solutions and service providers. The Bill does not adequately provide a framework for how consumers can share and reuse their trusted verified identity data. Notably, the principle in the Cabinet-approved paper with respect to 'interoperability' refers to personal and organisational information being 'reused' across services, sectors and geographies. This principle is not reflected anywhere in the Bill.

Recommendation #2: The Bill should:

- Be focused on enabling consumers to have multi-faceted, privacy enhancing and personally controlled digital interactions.
- Provide a framework for consumers *sharing and reusing* their trusted verified data across services, sectors, and geographies.
- Specifically reference interoperability between services, sectors and geographies.

3. The Bill must promote and enable inclusivity by supporting more consumer options

The Bill could be more inclusive by ensuring the systems that support the identification of people have the flexibility and ability to cover a range of different identification services (e.g., governmental, commercial, social, iwi and consumer scenarios). The Bill is not clear on how it supports inclusion across a range of trusted relationship scenarios and contexts.

An end user should be able to select what verified digital identity information they wish to present, which may be single points of verified digital identity information, or a combined group of verified information collated from different services or issuers. The Bill does not directly enable this, leaving this matter open to interpretation.

A fully inclusive digital ecosystem means those that cannot, for any reason, act independently are enabled to act with visible and verifiable support. The identities of those supporting people who cannot act independently should be obvious, specific, and trusted. The Bill would be more inclusive if it explicitly catered for a broad range of trusted relationship scenarios which apply to both physical and digital interactions, both in the online and offline worlds. These trusted relationship scenarios include:

a. joint ownership;
b. guardianship;
c. delegations (which are critical for organisations to participate in the trust framework, i.e., the trust framework should support the verification of an individual's delegation); and
d. temporary or permanent representation.

In summary, as the Bill is services centric and not consumer centric, it does not yet adequately cater for the nuances of digital inclusion, or the breadth of possible digital identity interaction scenarios.

Recommendation #3: The Bill needs to focus on the consumer and the mechanisms that support a flexible and inclusive trust framework by:

- Covering the alignment and interoperability of physical and digital interactions.
- Including mechanisms to support inclusion of all New Zealanders, such as through delegations, guardianship, and temporary or permanent representation.

4. The Bill should be broader, focusing more on the wider identity ecosystem

The purpose (as defined in clause 3) of the Bill appears to be unduly narrow. "Digital Identity Services'' cannot be addressed in isolation, and other critical building blocks should be better aligned. The Bill should do more to capture these digital identity building blocks, rather than solely concerning itself with the governance process of digital identity service providers.

While primary information about an individual, e.g., a birth certificate, is often what is considered to identify an individual, many other identifiers and information provided could also be considered 'digital identity information'. The Bill is unclear as to what constitutes identity information and therefore what systems providers are expected to cover. This lack of clarity is further compounded by 'digital identity' itself not being defined or described in any way in the Bill.

While very important, 'digital identity' is only part of the architecture needed to support our digital life. As the Bill is service centric, it does not adequately incorporate other key parts of the digital identity ecosystem, in particular:

- *Identifiers*: ensuring there is sufficient identification of all the actors involved in the digital interaction.
- *Credentials*: ensuring identity information is issued, retained and shared whilst providing trusted provenance.
- *Verifying*: providing the ability to verify the identity credentials or data that is being presented digitally.
- *Access*: ensuring appropriate controls on accessing available identity credentials.
- *Trusted data sharing features*: covering privacy, controls, and trusted secure communication and messaging protocols.
- *Re-use and sharing*: safely managing the onward sharing and re-use of digital identity credentials.
- *Relationships and representation*: establishing the relationship between people, organisations or things and the rights and duties in the context of that relationship.

The Bill as currently drafted does not recognise the nuance associated with different contexts and, as a result, risks over-regulating solutions that need to be simpler to implement. By way of illustration, the identification of a person, a thing (as set out in section seven of this submission), or an organisation needs to be possible within the context of what each identification interaction requires (i.e. not just using the same identity mechanism for every interaction). Digital interactions could be governmental, commercial, societal, or informal. There may be some digital interactions where less robust forms of digital identity might be acceptable and preferred by the parties involved. In summary, versatility needs to be provided for.

The key concepts described in this section should be recognised in the Bill, and not left to regulation.

Recommendation #4: The Bill should aim beyond just governing digital identity service providers and establish a broader trust framework that guides national digital ecosystem evolution by:

- Adding a definition of 'digital identity'.
- Recognising the key components that make up a digital identity ecosystem.

5. The Bill needs to be closely connected with other legislative and governmental digital initiatives

A trusted ecosystem should align with a number of legal and operational jurisdictions. There are several digital initiatives, often supported by legislative proposals, under consideration in New Zealand at this time, for example:

- The statutory review of the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act.
- Work on a CDR and enabling legislation.
- The evolution of digital currencies and the potential for a Central Bank Digital Currency.
- Consultations on a Digital Strategy for Aotearoa.

From a Payments NZ perspective, the underlying governance, operational and technical trust models for these digital initiatives are all intrinsically linked. We expand on this point below, focusing on the review of the AML/CFT Act and the enabling CDR legalisation.

AML/CFT implications

The Ministry of Justice is currently reviewing the AML/CFT Act. One issue of concern in the AML/CFT area relates to the ability of one AML/CFT reporting entity relying on AML/CFT checks on a customer that have been completed by another entity.

While reliance is possible under certain circumstances, there are a range of risk and liability management reasons which mean many organisations will each perform their own checks on the same customer. This ensures each entity meets their AML/CFT obligations, but results in customer inconvenience and the need to duplicate effort, which may constrain the development of new business models.

The Bill currently does not adequately cover the sharing and re-use of verified digital identity credentials and, in the context of AML/CFT obligations, it is not clear whether digital identity credentials verified by one trusted party can be relied upon by another party as a part of their customer due diligence for AML/CFT purposes. The trust framework needs to closely align with the future framework for AML/CFT. A failure to do so would severely limit the benefit and usefulness of the trust framework.

Consumer Data Right Implications

The Bill's relationship with the upcoming legislation to introduce a CDR (expected in 2022) needs to be well defined and broadly understood. The trust framework and the CDR will each establish an accreditation framework and regulations so that trusted parties can offer services based on customers sharing confidential information securely. While the specific digital functions between the trust framework and the upcoming CDR differ, there is significant overlap which needs to be carefully managed. Our submission elaborates on the importance of aligning with the CDR below.

In summary, a trust framework that guards and guides the development of digital interaction capabilities is central to these and other initiatives. The Bill is currently narrow in its focus and does not consider the wider digital lives of New Zealanders, and the relationship with other initiatives, some of which involve current legislative change such as the introduction of a CDR and the AML/CFT statutory review.

Recommendation #5: The alignment and inter-relationship between the Bill and various other domestic governmental initiatives must be better understood before legislation is finalised.

6. The Bill's inter-relationship with the upcoming CDR is critical and should be defined

A CDR framework describes mechanisms for consumers to securely share data held about them with trusted third parties. The third party could be another product or service provider, or a separate entity such as a fintech. Payments NZ's API Centre works with industry to support the adoption and implementation of open banking.

Open banking is a broad term for a category of services that includes digital interactions and processes where a customer consents to share their financial data held by their bank with other third parties. The API Centre's standards and technical specifications set out the basis for how this sharing can occur efficiently and safely. As indicated earlier, one critical step in the customer consenting to share their financial data is the bank authenticating (identifying) the customer.

CDR legislation could support the sharing of financial data by designating the banking sector (i.e. bringing open banking within the ambit of the CDR framework).

Legislation to support a CDR framework is expected to be introduced in 2022.

A CDR and the trust framework enabled by the Bill support different digital interactions. A CDR supports data sharing arrangements, while the trust framework supports digital identity and digital identity services. However, there are significant overlaps between the two, and it is highly probable digital identity services will be used in digital interactions occurring in a CDR framework.

We are concerned the legislative and policy processes for the CDR and the trust framework may be disconnected. In saying that, we acknowledge the trust framework is voluntary while the CDR will be a designation framework. Nonetheless, we believe it is important to clarify whether a CDR and open banking services are anticipated to fall within the ambit of the trust framework under the Bill.

The bullet points below list the areas of overlap and potential synergies that could exist between the two initiatives:

- Both establish a framework to legislate and govern the introduction of new digital services in Aotearoa New Zealand.
- Both provide accreditation/certifying frameworks, criteria, and processes.
- Both will require customers to authenticate their identity.
- Both will require customer consent processes and safeguards, including over the whole consent lifecycle (i.e., customer consent creation, amendment, expiry/revocation/ cancellation).
- Both seek to support customers sharing confidential information about themselves.
- Both rely on the identification of every party in the digital interaction.
- Both will need to cater for bi-party and multi-party arrangements that rely on trusted sharing of data.
- Both will likely feature some form of trust register and 'trust mark'.
- Both will likely set regulations and technical standards.
- Both should cater to natural persons, companies, trusts and other entities.

- Both will require careful consideration and management of privacy, confidentiality, security, risk, and data management issues.
- Both should feature a complaint and dispute resolution mechanism.
- Both need to be able to evolve to support different interaction options, and new models and services.

We understand officials from the Department of Internal Affairs and the Ministry of Innovation, Business and Employment have worked together on these potential overlaps and synergies. However, we have significant concerns the two frameworks remain disconnected. While we acknowledge the trust framework is further advanced than the CDR legislative programme, we would like to impress on the Committee the importance of a cohesive inter-relationship between these frameworks.

There is a strong likelihood that any organisation that can operate under the CDR framework will also want to benefit from the trust framework. However, unless carefully managed this requires the same organisation to be accredited twice, separately, and to operate concurrently under both frameworks bearing the ongoing development and compliance costs that goes with that. At a technical level, there is a risk that the technical protocols used under each framework will differ, adding cost and reducing interoperability. While we want to avoid creating dependencies between a CDR and the trust framework, there is a compelling case for stronger alignment and reconciliation of the synergies between the two.

In an open banking context, a further point of concern relates to the ability to retain control over the onward sharing of a customer's data, outside the initial ecosystem of trust defined by the CDR laws and regulations. In these cases, shared data could be considered identity information covered by the trust framework enabled by the Bill.

An equivalent digital identity onward sharing scenario could be an accredited digital identity service provider's onward sharing of the consumer's digital identity credentials to a party outside of the trust framework. The Bill does not cover a consumer's digital identity credentials 'leaking' outside the trust framework (even if the consumer's consent is granted). Understanding whether this is possible or not should be clarified in the Bill.

Recommendation #6:

- That there should be as much alignment and consistency as possible between the applicable elements of the legislative and regulatory frameworks for the trust framework covered by the Bill and the upcoming CDR.
- That the Bill includes the basis for digital identity to be used in the context of New Zealand's future CDR.
- That the future CDR reflects and enables the potential for the trust framework to be used in open banking.
- That the Bill clarify whether it is permissible for a consumer's digital identity credentials to be on-shared from within the trust framework to outside the framework.

7. **The Bill needs to be more open to, and anticipate the evolution of new digital identity models**

Models of digital identity are evolving and new models are emerging. The Bill appears to govern the use of existing current-world approaches to digital identity service providers, rather than being flexible enough to allow better approaches and models to develop and be used in the future. Emerging models include:

- Social models where trust in an individual's identity is authenticated by a social group or many other individuals within the trusted ecosystem.
- Models based on decentralised interaction patterns (see below).
- The ability for an individual to be recognised in different environments and to be able to bring together these identification attributes (as trusted credentials) in a combined presentation.
- Use of digital identity credentials in new digital contexts, such as in the metaverse.
- Payment validation models which reference identity that can be cryptographically verified (potentially using verifiable credentials).

Two particular models or scenarios are that worth exploring further are, decentralised identity models, and the identity of 'things' because these illustrate the important benefits of the trust framework being able to evolve over time.

Decentralised identity

In general terms, there are three current digital identity models:

- The traditional digital identity model is *centralised* (verified credentials are stored and controlled by a single central authority or a single database).
- *Distributed* models support the "login with" option (you distribute your identification to a service provider that you and others trust).
- Emerging technologies increasingly look to use *decentralised* (or self-sovereign) models.

The framing of the Bill is based on current-world terminology and solution concepts. For example, the Bill uses terms coined specifically for use in traditional models of identity verification which are not used in decentralised models (e.g. an "Identity Service Provider" are "issuer" in decentralised models, and "Relying Party" is referred to as "Issuer" in decentralised models). The Bill should be neutral to specific technology and models and should promote interoperation of solutions and models. Otherwise, it risks hindering the adoption and use of evolving technologies like *decentralised* interactions that are increasingly gaining acceptance across the world.

The Bill needs to ensure adopting emerging digital technologies can be encouraged without eroding trust in the community. This means the trust framework will need to be flexible enough to support new interaction models while also coexisting with more traditional models of digital identity. The Bill does not appear to promote the necessary capabilities to allow digital identity models to evolve.

Identity of things

It is not clear whether the trust framework will be capable of supporting the identification of 'things' (as well as people and organisations). Each requires an identity that can be linked back to the personal identification of owners or responsible officers. Cryptographically verifiable identities of new asset types, arrangements, smart contracts, currency tokens and wallets also all

require identification. These 'things' should also be covered by the Bill (or explicitly excluded by focusing on natural or legal persons only).

To illustrate more fully, the ownership of things needs to be able to be reflected in digital interactions, such as in the often-mentioned Internet of Things scenario of a fridge ordering milk automatically. In this fridge scenario, you can't support the identification of the fridge without also supporting the ownership and delegation of the fridge in the digital identity framework. This will be key in ensuring that the appropriate arrangements and authorities are in place for that 'thing' to act.

Recommendation #7: The Bill needs to be more neutral so there is the potential, over time, to support new models of digital interaction and to promote the controlled enhancement of existing infrastructures (including payments). This includes:

- Being technology neutral.
- Being neutral as to the digital identity model used.
- Being neutral as to the terminology that is used and the definitions that apply (for example, "Identity Service Provider" and "Relying Party").
- Being clear as to how the digital identity of 'things' will be addressed, along with its underpinning ownership and delegation capabilities.

Payments NZ is grateful for the opportunity to make this submission to the Economic Development, Science and Innovation Committee on the Digital Identity Services Trust Framework Bill.

Steve Wiggins
Chief Executive
Payments NZ Limited