SUBMISSION BY

DIGITAL IDENTITY.NZ

to

Payments NZ Limited

on its

CONSULTATION ON PAYMENTS FOR THE NEXT GENERATION

April 2025

Prepared by the cross-industry Digital Identity Services Trust Framework Working Group of Digital Identity NZ (DINZ) with input from individual subject matter experts as well as DINZ member organisation representatives from a mix of large / medium corporates, public service agencies and academia.

Digital Identity New Zealand (DINZ) thanks the Payments NZ Limited (PNZ) for the opportunity to provide a submission, particularly for the one-week time extension.

Please note this submission only relates to Q26 and Q27 and more general comments on the consultation's scope, approach and the additional potential that could emanate from looking at the space through a slightly different lens.

DINZ authorises PNZ to release its submission. Please also note that DINZ will also be publishing its submission on the DINZ website.

As always, we are happy to provide any clarifications in writing, on a call, or in a physical meeting.

DocuSigned by:
Colin Wallis
F84DA1755B8C410...

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

About DINZ

DINZ is a not for profit, membership funded association and a member of the New Zealand Tech Alliance. DINZ is an inclusive organisation bringing together members with a shared passion for the opportunities that digital identity can offer. It supports a sustainable, inclusive, and trustworthy digital future for all New Zealanders through its vision — that every New Zealander can easily use their Digital Identity in its mission to empower a unified, trusted, inclusive Digital Identity ecosystem for Aotearoa New Zealand that enhances Kāwanatanga (honourable governance), Rangatiratanga (self-determination and agency) and Ōritetanga (equity and partnerships).

General Comments

Digital identity advances and regulatory changes have the potential to deliver tangible benefits to real time payment processing. The order of the terms and ideas is deliberate. This is a conceptual starting point that needs deeper exploration than was reflected in the document. Could the focus be on extending the reach of payment systems to serve the unbanked community so banks can meet a regulatory requirement to serve the public, or reducing fraud through better security, or a mission to offer a future-proofed, user-attractive, financially competitive alternative to credit cards and alternative payment systems? We believe starting out on this next generation payments conceptualisation with a better understanding of the data and the problems and opportunities that digital identity in particular can address could dramatically help with prioritization and configuration of a conceptual architecture design.

The connections between digital identity technologies, strategic goals, and the architecture design were not obvious to us in the document. With regard to digital identity at least (but applies to more generally to the structure of the document and approach) we think that ‘problem domain’ (rather than ‘problem definition’) might have helped start the document on a more logical path that more clearly differentiates problems in the multiple process and would better surface solution components. You’ll see this reflected in our comments on Q26.

As the world of digital identity continues to undergo significant changes into the foreseeable future, we encourage the solutioning to aim for a “starting line” that can adopt and adapt digital identity advances in the future. Designing an architecture for the finish line (that we felt was implicit in the document) when there is so much uncertainty can lead to analysis paralysis and a very high risk business case. We appreciate that it’s not easy to look beyond the current state globally and to design for a future-proof state that doesn’t exist today, but incorporates mix and match, plug and play components that can be adapted to avoid wholesale replacement further down the line.

DINZ welcomes any future opportunities to work with Payments NZ on designing the nextgen payments platform to take advantage of innovation in the digital identity world. We see potential for many indirect benefits to taking a wider perspective on trade or servicing society, and are excited to see where this can go!

Question 26 (Page 61) Digital Identity - Problem Definition

To what extent do you agree/disagree with the benefits of the verifiable credentials service? What changes, if any, should be made to further develop the benefit statements? What impacts do you foresee for the people and businesses of Aotearoa as a result?

Response to Question 26

DINZ strongly agrees that digital identity services have tremendous potential to improve the way businesses and consumers interact, and that digital identity is a key part of the rapid evolution we are seeing in the digital world today. We also agree that there is not a clear view on how recent regulatory and technical advances could be utilised by payment systems.

However we also see how digital identity related advances (particularly continuous/dynamic/point in time advances) are being used in some ecosystems overseas to address identity assurance and build trust in commercial activity, before payments are transacted. The wide array of approaches we see today are the result of the variety of commercial activities and competitive differentiation free market economies encourage.

This is not a problem to solve, as suggested in the problem definition. It is the environment in which payment systems enhanced with digital identity features could address specific problem domains. We believe the problem definition needs to be pivoted to problem domains before architecture designs (data flows included) are developed further. For example, Verifiable Credentials can be used to establish trust between two parties, no argument there. But the request to pay and digital identity mechanisms needed to facilitate payment may use derived artifacts such as transaction tokens, digests, or private exchange of payment info. Some of these may be mandated by industry bodies or regulators. Our complex world is not the problem, it's our reality.

A case in point. Payments are typically made in relation to some form of agreement or contract. There is an important separation of concerns to be aware of. Payment processing is concerned with the movement of funds, whereas a contractual transaction is concerned with fulfilment of obligations. How tightly or loosely these concerns are coupled varies considerably by use case, sector, jurisdiction and so on. Special care needs to be taken when extending the real-time digital interaction information scope as it may conflict/overlap with digital identity verification performed as part of the existing trust relationship between the parties. We suggest using a problem domain, rather than a problem definition, so boundaries can be articulated with an applicable desired outcome and reflected in the conceptual architecture design.

Where payments require AML/KYC rigour, then we agree it is crucial to verify the identities of all parties. An end-to-end identity verified payment processing system would add considerable value to doing business.

Where payments do not require AML or KYC, it is highly beneficial to identify that the payment recipient party is the one required by the entitled party. In the parlance of Zero Knowledge Proofs, knowing who is making the payment in many cases is not necessary, and requiring it may breach confidentiality or privacy rights. Examples; a company may sometimes pay for purchases by staff, families and partners with joint accounts may share payment methods, and there are numerous examples. Knowing where a payment came from is different to knowing who made the payment. The problem definition should be refined to reflect the use of digital identity for an individual or organisation, or the identity of the payment source which brings us back to our suggestion of pivoting to a 'problem domain' lens, rather than a 'problem definition' lens.

We see challenges with the approach that Next Gen takes with sharing identity claims, if the problem domain is not articulated. Conversely, we see enormous potential if the problem domain is well articulated.

Question 27 (Page 62) Potential Benefits of a Verifiable Credentials Service

To what extent do you agree/disagree with the benefits of the verifiable credentials service? What changes, if any, should be made to further develop the benefit statements? What impacts do you foresee for the people and businesses of Aotearoa as a result?

Response to Question 27

Conceptually, verifiable credentials have huge potential to add value to payment systems. DINZ is very supportive of developing services and features in payment systems that can take advantage of the real-time identity claim verification. However, adoption of VCs can be highly disruptive and there is a lot of uncertainty to overcome. There is both complexity and overlaps with non-transactional aspects of trade which should be considered at this stage. We suggest this part of the project needs to develop beyond conceptual benefits and work on an impact or value assessment to articulate benefits with greater clarity.

The introduction of verifiable credential features into the payments network will have an impact. Whether this is beneficial or not will depend on perspectives - so "it depends". Do the benefits outweigh the risks? Can the risks be avoided or mitigated, making the benefits more valuable? These are important questions when determining safety and security benefits.

For example VC's can provide a level of assurance, they do not automatically assure/assert identity. They are a claim, which has its trust anchored to the issuer, the binding to the data subject, and the verifiability of the presentation. If that is well matched to the risk profile of the use case then the benefits can be realised. If the assurance level is mismatched, then the use of VC's could be harmful rather than beneficial. From a high level conceptual view, the VC's are potentially an essential part of assuring identity, but they are not the whole solution as inferred.

VCs, like any identity asset, have their own uses, potential misuses, and exposure to abuse. Their adoption will change the payment network's exposure to fraudulent activity. That may be better than today but may not be as beneficial as alternatives such as tokens generated from earlier exchanges of VCs, or APIs in some more established traditional payments ecosystems.

Topics such as dispute resolution are in the realm of contractual relationships rather than payment processing. By extending payment processing to end-to-end identity management, it may complicate dispute resolution, or enhance it.

Protection of privacy is another area of impact that may be beneficial or harmful. By extending the payment network to process sensitive personal information, that info is now being shared, stored, and collected. Yes, a case can be made for the benefits as it may provide a more secure and less intrusive mechanism than current systems, but it may introduce new privacy concerns as well. It may also duplicate effort if existing systems address non-payment aspects of the relationship and need to continue.

Embracing VC's and other digital identity features also has the potential to expand payment systems into new areas. For example servicing unbanked citizens, or situations where privacy preserving anonymity is important. By enabling unbanked individuals to access payment sources in real-time, support services can be transacted in real-time. There are benefits relating to new opportunities as well as solving problems.

The foregoing discussion serves to reinforce our sense that the more logical approach to the conceptual architecture might have been to start with the data and the problem domains there (digital identity included) and then extend it to payments.