Updated Proposal for DINZ Council Consideration

Solving the Red X Problem:
Coordinating Credential Namespaces in Aotearoa

Further to the Executive Council meeting on Friday 6 March, Council guidance is sought on whether **Digital Identity NZ should support ecosystem coordination of credential namespaces** to accelerate trusted digital identity adoption across regulated and market use cases.

This proposal aligns with **the DINZ Strategic Plan**, which seeks to:

- accelerate adoption of trusted digital identity infrastructure
- strengthen New Zealand's digital trust ecosystem
- convene industry and government to unlock interoperability
- identify **commercially sustainable infrastructure opportunities for the ecosystem and for Tech New Zealand / DINZ.**

Credential namespace coordination represents a potential **high-leverage coordination opportunity** consistent with these strategic objectives.

The Red X Problem

Digital identity technology is largely solved.

The global ecosystem now has:

- Decentralized Identifiers (DIDs)
- Verifiable Credentials
- Digital wallets
- Trust registries
- Open interoperability standards

Yet large-scale adoption remains slow.

A key reason is **lack of namespace coordination.**

Technically, any human, non human (agent) or organisation can issue a credential.

However, relying parties often cannot easily determine:

- who issued the credential
- what the credential represents
- whether the issuer is trustworthy

This creates what can be described as the **“Red X Problem.”**

When a verifier encounters a credential they do not recognise, they effectively mark it with a **red X** and reject or ignore it.

Not because the technology failed but because the **meaning of the credential cannot be easily resolved.**

Until credentials can be **recognised, resolved, and trusted across ecosystems**, adoption will remain fragmented.

Why Namespace Coordination Matters

The internet scaled because shared naming infrastructure emerged early.

Examples include:

System	Coordination Layer
Websites	DNS domain names
Email	global addressing conventions
Telecommunications	telephone numbering plans
Payments	routing and settlement identifiers

These systems ensure participants can **recognise and resolve identifiers across networks.**

Digital credential ecosystems require a similar coordination layer so that:

- issuers are uniquely identifiable
- credential types are discoverable
- relying parties can recognise trusted credentials
- wallets can interoperate across ecosystems

Without this layer, credential ecosystems risk becoming fragmented silos.

Alignment with the DINZ Strategic Plan

Credential namespace coordination directly supports several pillars of the **DINZ strategy.**

Accelerating Trusted Credential Adoption

Namespaces allow credentials to be **recognised across sectors**, lowering barriers for relying parties and enabling scalable credential ecosystems.

Enabling Interoperability

Namespace coordination supports **cross-platform discovery and verification of credentials**, strengthening the interoperable ecosystem DINZ promotes.

Strengthening Trust Infrastructure

New Zealand currently has strong foundations through:

- the **Digital Identity Services Trust Framework (DISTF)**
- emerging wallet ecosystems
- global verifiable credential standards.

Namespace governance represents a **missing infrastructure layer** required for these components to operate coherently.

Delivering Commercial Value for the Ecosystem

The DINZ strategic plan also highlights the importance of identifying **sustainable commercial infrastructure opportunities** that support the broader ecosystem.

Namespace governance has the potential to evolve into such an opportunity.

Identifier systems such as **domain names, barcodes, and numbering systems** have historically become **economically valuable coordination infrastructure.**

This presents an opportunity for **DINZ and Tech New Zealand to incubate a commercially sustainable namespace governance model that supports the digital identity ecosystem.**

Regulated and Market Credentials

Credential ecosystems will likely emerge from two parallel forces.

Regulated credentials

Examples include:

- government identity credentials
- financial KYC attestations
- professional licences
- age assurance credentials.

These may operate under frameworks such as the **Digital Identity Services Trust Framework (DISTF).**

Market credentials

Examples include:

- retail loyalty credentials
- employment credentials
- education credentials
- memberships
- iwi or community attestations.

These everyday use cases may drive **early wallet adoption and ecosystem growth.**

A coordinated namespace approach allows regulated and market ecosystems to evolve **while maintaining interoperability.**

The Commercial Infrastructure Opportunity

Namespace coordination could evolve into **a sustainable ecosystem infrastructure service.**

A useful analogue is **GS1**, the global not-for-profit membership organisation responsible for product barcodes and business identifiers.

GS1 provides:

- globally unique identifiers
- governance of identifier standards
- membership-based services enabling interoperability.

GS1 New Zealand alone generates **high seven-figure annual revenues** through identifier registration and membership services. This includes pre allocation of numbers to MBIE for the NZBN to ensure global interoperability.

This demonstrates that **identifier governance can support a commercially sustainable ecosystem model.**

Credential namespaces could evolve in a similar way as trusted identifier infrastructure for the **digital credential economy.**

If coordinated early, this could represent a **commercial value proposition aligned with the DINZ and Tech NZ strategic mandate to incubate ecosystem infrastructure.**

Why This Could Become the GS1 of Digital Identity

Many of the world's most successful digital infrastructures began as simple coordination mechanisms. The global barcode system, governed by GS1, is a well-known example. What began as a way to uniquely identify products evolved into essential global infrastructure underpinning retail, logistics, and supply chains.

Today, organisations pay membership and licensing fees because the value of globally interoperable identifiers far exceeds the cost of coordination. GS1 New Zealand alone generates high seven-figure annual revenues while operating as a neutral not-for-profit steward of this infrastructure.

Credential namespaces could follow a similar trajectory. As verifiable credentials scale across sectors such as finance, retail, education, and government services, the ability to uniquely identify issuers, credential types, and trust frameworks becomes foundational infrastructure. If coordinated early, New Zealand has the opportunity to incubate a neutral governance model that supports interoperability while creating a sustainable commercial ecosystem service.

In this sense, credential namespace governance could become the GS1 of digital identity, i.e. under the radar but critical infrastructure that enables trusted digital interactions across the economy.

Possible Role for DINZ and Tech New Zealand

DINZ does not need to operate namespace infrastructure directly.

However, it can play a valuable role in **ecosystem coordination and incubation.**

Potential actions include:

Convene

Use the **Trusted Credential Adoption (TCA) Working Group** to bring together:

- credential issuers
- relying parties
- wallet providers
- regulators
- ecosystem participants.

Coordinate

Develop voluntary guidance on:

- issuer identification models
- credential naming conventions
- namespace governance principles.

Align

Ensure emerging approaches align with:

- DISTF
- trust registries / VICALs
- international standards.

Incubate

If ecosystem demand emerges, **DINZ / Tech New Zealand could incubate a neutral credential namespace governance model.**

Over time this could evolve into an **independent governance entity providing identifier services for credential ecosystems.**

Such an entity could operate on a **membership and identifier registration model similar to GS1**, providing sustainable funding for infrastructure stewardship.

Why This Matters Now

Verifiable credentials are moving from experimentation to **global deployment.**

If namespace coordination is not addressed early:

- ecosystems may fragment
- interoperability costs will increase
- Verifier / relying party adoption will slow.

Conversely, early coordination could position **New Zealand as a global reference model for trusted credential ecosystems.**

Council Decisions

Council may wish to consider:

1. Should **DINZ support ecosystem coordination of credential namespaces?**

2. Should this work be **incubated through the Trusted Credential Adoption (TCA) Working Group?**

3. If so should the TCA Group develop an **initial discussion paper on credential namespace governance for New Zealand, by end May 2026?**

4. Should DINZ explore, with Tech New Zealand, whether a **commercially sustainable namespace governance model could be incubated if ecosystem demand emerges?**

In Summary

Digital identity is often framed as a **technology challenge.** Increasingly it is becoming a **coordination challenge.**

Credential namespaces may appear small, but they determine whether credentials are:

- recognised
- interoperable
- trusted.

If coordinated effectively, namespace governance could become **one of the quiet but critical infrastructure layers enabling New Zealand's trusted digital economy, while also delivering long-term commercial value aligned with the DINZ strategic mandate.**