Trust Alliance New Zealand

Executive Summary of Digital Identity Report

Scoping Project within the Value Chain in the Primary Sector - Phase I
Version 0.1

Chris Claridge | Chairman
Klaeri Schelhowe | Executive Director
Trust Alliance NZ Inc. |
www.trustalliance.co.nz

Executive Summary

Following on from Phase 0 – "*Scoping Project of Inter-operable Data Modelling Within the Potato Industry*" - this report sets out the process and findings gained in scoping the requirements for an effective cross-sector data sharing and management solution.

Having analysed market drivers and technical options we have determined that a key foundational requirement for enabling truly secure data sharing and interoperability is the establishment of a secure digital identity mechanism.

Principle activities undertaken for this report were:

- Analysed the market for options.
- Proposed DID RFC (mid last year) to key stakeholders for feedback.
- Held several technical working groups, peer reviews, benchmarks etc.
- Embedded the feedback and finalised the technical concept/approach.
- Built a proof-of-concept toolset to allow anyone to integrate the digital identity framework into their services.
- Identified the limitations
- Developed the technical roadmap for the next phase.

We have identified the new W3C standard for DID's (Digital Identifiers) based on the Self-Sovereign Identity framework as a rapidly developing set of global, open standards that enable a robust, secure and completely decentralised approach to establishing digital identity. W3C DID standard eliminates the need for trusted 3rd-parties and promises to put individuals in control of their own data. It sets a benchmark to ensure scalability, portability, flexibility, and security. These aspects are critical to enable effective and trusted data sharing to support the upcoming initiatives such as N-cap, Fresh Water Farm Planning, INFDP, LINK2025, Keti Pamu, He waka eke noa, and Sustainable Agriculture Financial Initiative (SAFI).

The W3C DID standards provide enhanced trust and authenticity of digital identity while ensuring data sovereignty and control of the data by the holder. It delivers a standardised approach to ensure interoperability between different ecosystems and is open source, with no commercial conflict of interest and no gate-keepers controlling access. W3C DID standards are fully in line with the DIA Trust Framework and are GDPR considered and compliant.

We have identified that commercial players with vested interests in maintaining centralised, monopolistic control over data and its access, with rent-seeking business models, are likely to resist and see it as a disruption to their business. However, the rapid development and uptake of W3C DID technology across many sectors coupled with the ever-growing public awareness of the importance of controlling data means that centralised monopolistic control of data for commercial exploitation is now being firmly challenged. For farmers and growers this will mean they have the ability to easily share data with whichever party they like, in a controlled and permissioned manner, without the involvement of any 3rd party.

Key Deliverables and Outcomes

We developed a proof-of-concept set of tools and protocols to create decentralised Identifiers (DID's) and Verifiable Credentials (VCs) as a prerequisite for Digital Identity for individuals. We have now:

a) Developed a clear technology roadmap and governance stack, backed with an international benchmark input and standards.
b) Produced a white paper of the decentralised identity approach for feedback.
c) Performed a technical demonstration of the decentralised technology to show how to create a decentralised identifier, a verifiable credential and demonstrate the successful verification process.
d) Developed and created a video for the non-technical audience to demonstrate how the technology can be deployed, how DID's and verifiable credentials can be utilised, and discuss how the primary sector can benefit from it.

Next Stages

From here we intend to:

- Gather feedback and additional requirements for consideration and engage, communicate and support users/members accordingly.
- Define requirements for users/members of the deliverables.
- Develop the required tools and technical environment of the PoC phase for internal deployment and testing. This includes a reference W3C DID "digital wallet" that allows users to store and share verifiable credentials.
- Finalise tools and protocols for release.

We aim to deliver a toolkit of workable SDK's for early adopters to verify credentials within the defined PoC. Functioning protocols and reference implementations will be delivered for implementing digital identity at an individual level for data interoperability within the value chain. This will show the scalability and flexibility across sectors for data owners to manage & protect their data.

- Within the MVP stage we aim for insight and learning how a potential solution could be deployed to enable data interoperability between different parties in an easy, trustworthy, controllable and efficient way across the primary sector.
- Established awareness and build knowledge by the collective and inclusive approach of a co-design and co-developed process. Key stakeholders and early adopters will understand the DID methodology and be able to deploy DIDs to be prepared for the next phase of the data sharing framework.
- Further develop the governance of the technology to be commercially independent and neutral, and provide the requisite governance framework to ensure on-going interoperability.

Conclusion

We have demonstrated the need and market interest in a robust, open data sharing and digital identity management solution for the New Zealand primary sector. We have developed and demonstrated PoC application of a technology stack based on globally accepted open standards (W3C DID) and worked with sector participants to get feedback and guidance, and confirmation that we are on the right track. We now need to progress to minimal commercially viable implementation on a larger scale.

Extract of Glossary of Terms by DIA[1]

Term		Meaning
Accreditation		An act to give approval to a Digital Identity Service Provider who has demonstrated they meet the applicable requirements of the trust framework.
Accredited digital identity service		A digital identity service that is accredited by the trust framework authority to be provided by a particular trust framework provider.
Attribute		A piece of information that describes something about an Entity (for example, an individual's name, address and whether they are resident in a particular place are all attributes about the individual).
Authentication		A process for establishing an Authenticator is genuine or as represented.
Authentication assurance		The degree of certainty that the current request is being made by the original entity; expressed as AAn, where n represents a level of assurance.
Authenticator		One or more things known and/or possessed and controlled by a User (such as a password, a code, a piece or software or a device), that the User can use to access a service or other thing online.
Binding		A process carried out to validate the connection between an Entity and information about that Entity to a level of assurance or confidence.
Binding assurance		The degree of certainty that the Entity information relates to the Entity claiming it; expressed as BAn, where n represents a level of assurance.
Credential		A record kept in digital form that: (a) is issued to an Entity and held by a holder; (b) describes a set of identity or other attributes or properties of the Entity or another Entity the holder represents; and (c) is bound to an Authenticator.
Data minimisation		The act of: (a) limiting the collection and holding of personally identifiable information; (b) minimising identifiability, observability, and linkability of personal information when it is shared.
Digital Identity Authentication Service, or authentication service		A digital identity service that: ● ensures the connection of a user to an authenticator, AND ● secures the sharing of personal or organisational information between trust framework participants by ensuring the authenticator(s) are possessed and controlled by an authorised holder.
Digital Identity Binding Service, or binding service		A digital identity service that ensures the connection (binding) of personal or organisational information to an individual or organisation.

[1] Digital Identity Services -Trust Framework DIA Jan 22 - NOT GOVERNMENT POLICY – WORKING DRAFT – IN CONFIDENCE

Digital Identity Credential Service(s), or credential service(s)		A digital identity service that: ● combines bound information and an authenticator to establish a trusted reusable credential, AND ● maintains a trusted reusable credential.
Digital Identity Facilitation Service(s), or facilitation service(s)		A digital identity service that assists Users to share credentials with Relying Parties.
Digital Identity Information Service, or information service		A digital identity service that provides an assessment of the accuracy of personal or organisational information.
Digital Identity Service		A service or product provided by a digital identity service provider and that, either alone or together with 1 or more other digital identity services, enables the sharing of personal or organisational information in digital form by a user in a transaction with a relying party.
Digital Identity Service provider		An individual or organisation who or that provides a digital identity service, whether the provider or service is accredited under this Act or not.
Digital Identity Services Trust Framework, or trust framework		The legal framework to be established to regulate the provision of digital identity services for use in transactions between individuals and organisations.
Digital Identity System		An interconnected system for the exchange and verification of Entities' digital identities and related attributes, involving: (a) Trust framework providers; (b) Users; and (c) Relying Parties.

Entity		Something that has separate and distinct existence and that can be identified in a particular context, such as:
		(a) an individual;
		(b) an Organisation;
		(c) a device;
		(d) a software application; or
		(e) a product or service.

Facilitation		Processes that support users to claim, hold and manage their credentials, and to share their credentials with relying parties.
Facilitation mechanism		A service or tool that can facilitate the presentation of 1 or more Credentials (fully or partially) in response to a request from a Relying Party. Examples include digital wallets or an exchange.
Identification management		Determining the accuracy of information, binding that information to the correct individual or organisation, and enabling the secure reuse of the information.
Information and data		For record keeping and format of personal and organisational information, to ensure a common understanding of what is shared.

management		
Information assurance		The degree of certainty attached to the reliability of the quality and accuracy of the Entity information; expressed as IAn, where n represents a level of assurance.
Information; or data		Facts about an individual or organisation, from which conclusions can be inferred.
Metadata		A type of data describing context, content and structure of data and its management through time.
Organisation		Any organisation, whether public or private, and whether incorporated or not.
Organisational information		Information relating to a particular organisation.
Participants		For the purposes of the Trust Framework, means (a) Users (b) Trust Framework providers (c) Relying parties.
Personal information		has the meaning given in section 7(1) of the Privacy Act 2020: (a) means information about an identifiable individual (b) includes information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages, and Relationships Registration Act 1995 or any former Act.
Personal or organisational information		Personal information or organisational information that describes- (a) the identity of an individual or organisation (b) other information about that individual organisation.
Portability		The capability to move credentials from one facilitation mechanism to another.
Privacy requirements		Ensuring the privacy and confidentiality of the information of individuals or organisations is maintained.
Relying party		An individual who or an organisation that relies on personal or organisational information shared in a transaction with a user through 1 or more accredited digital identity services.
Security and risk management		Ensuring information is secure and protected from unauthorised modification, use, or loss.
Security management plan		A plan of action that an organisation uses to address its security risk, based on the context in which the organisation operates and through threat and risk review.
Security risk		Any event that could result in the compromise, loss of integrity or unavailability of information or resources, or the deliberate harm to people measured in terms of its probability and consequences.

Securit y risk assess ment		An activity undertaken to assess the security controls for a system and its environment to determine if they have been implemented correctly and are operating as intended.
Sharing and facilitation		Facilitating the sharing of information with relying parties including authorisation processes.
Subject		An Entity that is the focus of a Transaction.
Trust framework provider		A digital identity service provider who or that is accredited by the trust framework authority to provide 1 or more accredited digital identity services.
User		An individual- (a) who shares personal or organisational information in a transaction with a relying party through 1 or more accredited digital identity services; and (b) does so for themselves or on behalf of another individual or an organisation.