



Trust
Alliance
New Zealand

Report on Digital Identity

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

Version 0.2- June 2023

Chris Claridge

Klaeri Schelhowe

Table of Contents

- 1. Executive Summary 2
- 2. Background and Key Findings..... 4
- 3. Business Problem 6
- 4. Purpose of Digital Identity Workstream..... 7
- 5. Scenario 7
- 6. Technical Approach and Feasibility 7
 - 6.1. Overview of different Identity Models 7
 - 6.2. Risk Overview 8
 - 6.3. Key infrastructure 9
 - 6.4. Definition of a Decentralised Identifier (DID) 10
 - 6.5. Example of a DID 10
 - 6.6. Features and Benefits of a Decentralised Identifier (DID) 10
 - 6.7. Terminology for the Triangle of Trust 11
 - 6.8. Triangle of Trust 12
 - 6.9. Key Management 12
 - 6.10. Evaluation of Specifications and Standards 13
 - 6.11. Concept Development and Engagement 13
- 7. Example of a Use case/application – Non-Technical..... 13
- 8. Demonstration of Proof of Concept – Technical 14
 - 8.1. Key content of the technical demonstration PoC video 15
- 9. Overview of the technical roadmap 17
- 10. Subsequent next step delivered (out of scope) 18
- 11. Next building blocks for phase II 19
- 12. Outlook at Phase II Digital Identity MVP – 20
 - 12.1. Next steps 20
 - 12.2. Deliverables – Scope 20
- Appendix 1..... 22
- Disclaimer 22
- Extract of Glossary of Terms by DIA 22

1. 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.

2. Background and Key Findings

The Digital Identity Project was accomplished based on the key findings of Phase 0 – “Scoping Project of Inter-operable data modelling within the Potato Industry”. Please find the details below.

Generally, the primary sector lacks digitalisation, which causes challenges in data interoperability, the capture, sharing, utilisation of data. The value chain of the potato industry, from imported germplasm to final consumer goods, e.g. potato crisps, involves multiple information systems that operate in isolation or in silos. Complexity of data handling and traceability starts at imported germplasm for tissue culture multiplication and ends at the shelf for consumers. Due to regulatory compliance, financial management and other management requirements the same data elements need to be generated, managed and processed multiple times. This leads to inefficiency and data redundancy, which can create a higher failure rate due to data inaccuracy.

There exists a clear and strong demand for a data interoperability framework between value chain participants and stakeholders and process steps without losing control of the data ownership and security.

There are three defined areas across the value chain which are critical to data transparency and traceability:

1. **Proof of identity. Examples: grower or IVA, the buyer or intermediary**
2. Proof of location. Examples: geospatial data of a paddock or where the goods are currently located
3. Critical control points & transactions. Examples: seed registration form, e-phytosanitary certificate

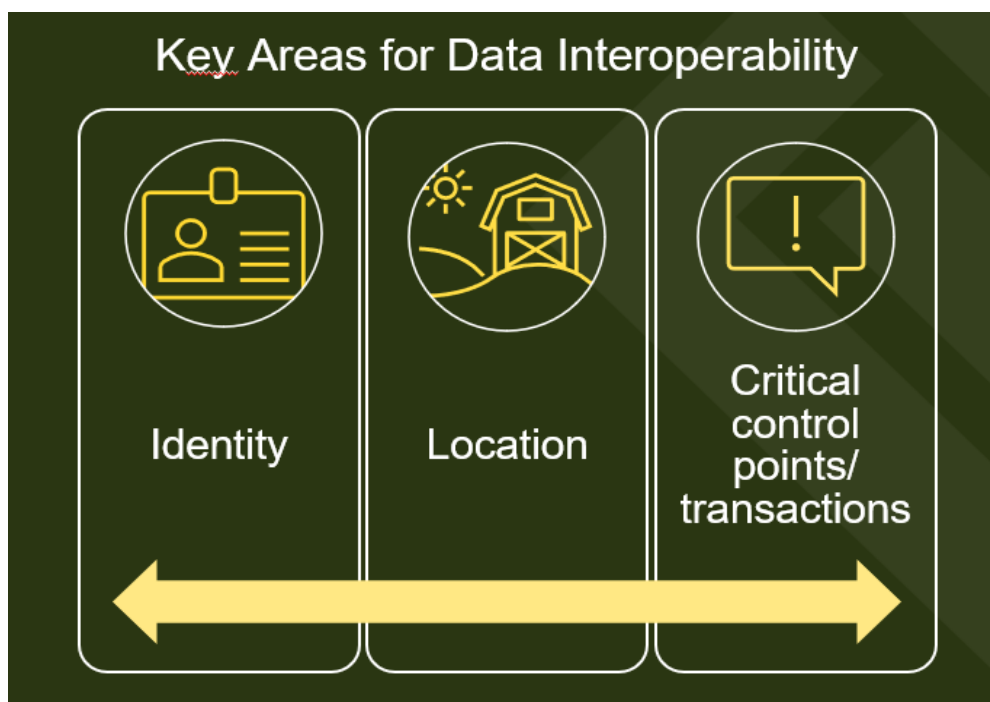


Figure 1: Findings of scoping Data Interoperability within the Potato Value Chain

If these data elements are not captured and shared accurately and in a timely manner it can lead to business and environmental risk. It is important that data is provided accurately and in a timely manner to the subsequent process steps otherwise the next events cannot be executed properly. In general, traceability and efficiency through the global value chain are lacking. Therefore, it is recommended as a starting point to establish a system **to prove identity**, location, and critical control points and

transactions through the value chain i.e. a digital identity legitimization per person, a unique location registry, and a secure & trustworthy system for traceability.

The primary sector lacks co-ordinated data systems which causes challenges when trying to use data to improve productivity and sustainability. Data interoperability - the capture, sharing, and utilisation of data - is a critical step in improving co-ordination of data systems to drive productivity and sustainability. There exists a strong demand from value chain participants and stakeholders for a data interoperability framework that clearly addresses data ownership and security. There are three defined areas across the value chain which are key to a successful data interoperability framework - see Fig1.

This problem is not unique to New Zealand. Multiple projects worldwide are trying to address this. The Trust Alliance (TANZ) has established formal links with RMIT Innovation hub in Australia and ILVO / Just Connect in Belgium to benchmark and peer review work undertaken. No offshore project investigated had a universal, easy to implement solution that could be applied across the New Zealand primary sector.

Digital Identity has been identified as a prerequisite for data interoperability. It enables the establishment of a data interoperability framework through creating authenticated users who can then share data in a permissioned, secure and trusted way. Earlier projects carried out by TANZ (see Fig2) have established that decentralized identifiers (DIDs), a novel set of identifiers created to W3C standards, could be a simple, open solution easily implemented through TANZ. Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity without reliance on any central authority or controller.

A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID. In contrast to typical federated identifiers, DIDs have been designed so that they may be decoupled from centralised registries, identity providers, and certificate authorities. Specifically, while other parties might be used to help enable the discovery of information related to a DID, the design enables the controller of a DID to prove control over it without requiring permission from any other party. DIDs are URIs that associate a DID subject with a DID document allowing trustable interactions associated with that subject. A DID is a globally unique, highly available, and cryptographically verifiable identifier.

“A globally unique persistent identifier that does not require a centralized registration authority and is often generated and/or registered cryptographically. The generic format of a DID is defined in § 3.1 DID Syntax. A specific DID scheme is defined in a DID method specification. Many—but not all—DID methods make use of distributed ledger technology (DLT) or some other form of decentralized network.”¹

DIDs are not governed by a centralised entity and can be deployed across a network such as TANZ, or across multiple networks with easy interoperability. TANZ with its current membership of 32 industry members are able to deploy DIDs across the entire primary sector. The current membership represents the majority of farms in New Zealand.

¹ [Decentralized Identifiers \(DIDs\) v1.0 \(w3.org\)](https://w3.org/TR/did-core/)

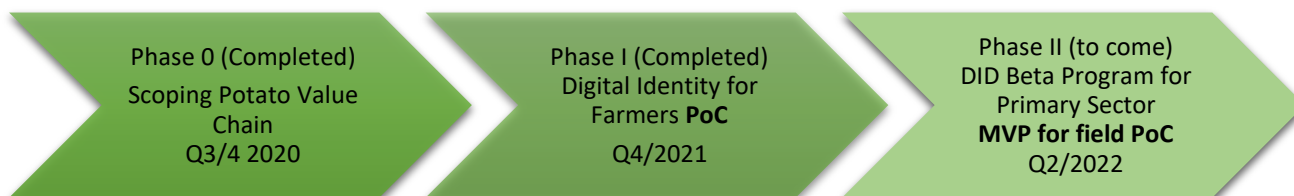


Figure 2: Project Phases

The value chain of the potato industry has been a useful exemplar to formulate concepts. The value chain from imported germplasm to final packaged consumer goods involves multiple information systems operating in isolation.

At Phase 0 we investigated and identified the data elements in a value chain. The concept of three key issues: identity, location and critical control points (see – Fig 1) was developed.

For Phase 1 we have now developed digital identity as a proof of concept (PoC) through the use of DIDs. The focus of this phase was on a working technology demonstration to enable proof of identity as a prerequisite for data sharing. This then allows a data interoperability framework to be established.

For the next Phase 2 we will expand on the proof-of-concept technology implementation to deliver a minimum viable product (MVP) for digital identity using decentralised identifiers to enable data sharing mechanisms to be deployed.

3. Business Problem

There is no centralised database of farmers or farms to provide a unique identification system. Farmers are using multiple information systems and are creating multiple digital identities. Creating a single centralised dataset with one system of identification is virtually impossible. There is not a digital identity system operating utilised by the primary sector participants that could enable farmers to prove their digital identity to allow the sharing of data and for interoperability to occur between stakeholders. Currently growers & farmers cannot prove their digital identity in a trustful, efficient way with other parties. Differentiation between operating/company level and personal level identities does not exist. Furthermore the roles & responsibilities by individual and operating entity at a farm are not transparent e.g. land owner vs land user vs land operator etc. There is insufficient transparency at the individual level for traceability processes, especially regarding compliance requirements.

“The OECD report also highlights the fact that NZ would not reach its stated climate change goals on current policy settings and that better use of digital technology in agriculture would be part of the solution.” The digital platforms for managing irrigation, fertilisers and tracking animals are not necessarily inter-operational, nor do they produce data that can be easily combined,” the report said.

Policy work should “ensure interoperability across digital tool platforms by requiring agritech players to adopt common standards, while letting them choose the most suitable common standards to converge to.”

Source: Business Desk; OECD fears 'large, sudden' house price fall in NZ 01.02.22

4. Purpose of Digital Identity Workstream

To prove & verify digital identity for farmers & growers including the relationships between different digital identities. The digital identity on an individual level will enable the farmer & grower to share data in a trustworthy way with other value chain members.

A farmer or grower needs to prove their identity before they are able to share data e.g. for compliance purposes, such as licence to operate, biosecurity, export regulations, levy payments, level of water quality, GHG, nitrogen level etc. This needs to be done in an efficient and trustful way. The verified data elements by individual parties will be used downstream in the value chain for demonstrating provenance and data integrity with a view to helping create easier, more robust compliance and assist in areas such as market access.

5. Scenario

- As a farmer I should be able to prove my digital identity for sharing critical data elements with parties along the value chain e.g. land use purpose, compliance requirements, growing procedures, and environmental metrics
- As an example that follows from the above. every farmer should have a [NZBN](#)², which could be used as a base identifier in the first instance. The NZBN could be incorporated into a verifiable credential which is used to prove identity for a grower, business or other entity.

6. Technical Approach and Feasibility

6.1. Overview of different Identity Models

The evolution from centralised approach to decentralised model. The graph below shows the technology and the characteristics for all three models. For the time being all three models will be used depending on requirements and feasibility. The decentralised model is being more and more applied for different applications where self-sovereignty identity, security or trust is important.

The benefit of a decentralised digital identity model includes:

- a) Full user control of their transactions without any authorisation from a central authority. This means the verification process is independent of any third party.
- b) Data is tamper-resistant and can't be altered due to use of consensus algorithms enforcing network integrity.
- c) The infrastructure and the network is exceptionally secure through cryptography and distributed approach.
- d) The open-source development of the base technologies is ensuring easy adoption by solution providers.

The decentralised approach is the preferred architecture for the identity model at this stage. The prognosis by the experts stated that the decentralised approach has a good chance to be implemented and rolled out rapidly. This is based on the general international acceptance, volume of activity, and rapid development in this area. This said, there is no indication of a hard switchover to the distributed model; commercial players with vested interests in maintaining centralised, monopolistic control over data and its access, with rent-seeking business models, are likely to resist. The centralised and federated models will likely remain in parallel and transition to a decentralised model in the future. The way in which decentralised digital identity has been developed means that it can “plug in” to existing centralised/federated systems easily, facilitating easy transition.

² NZBN= New Zealand Business Number is a globally unique identifier available for every Kiwi business.

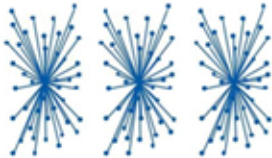

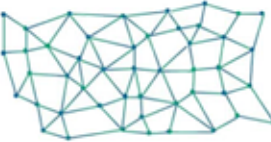
IDENTITY MODELS	Centralized	Federated	Decentralized
			
TECHNOLOGY	<ul style="list-style-type: none"> • ID/Password • Multifactor Authentication • Single Sign On 	<ul style="list-style-type: none"> • OAuth • OpenID • SAML 	<ul style="list-style-type: none"> • DLT • Cryptography
CHARACTERISTICS	<ul style="list-style-type: none"> • Identity fragmented across many enterprises • Enterprises control user data • Centralized data is a honeypot for cyber attacks 	<ul style="list-style-type: none"> • Less fragmentation of login credentials • User information fragmented across many enterprises • Enterprises control user data • Centralized data is a honeypot for cyber attacks 	<ul style="list-style-type: none"> • Identity can be portable across enterprises • User information in user's wallet or a secure cloud • Decentralized data limits data exposure on cyber attacks • Users control their data

Figure 3: Identity Model, Citibank

6.2. Risk Overview

The below graph visualises the risk and cost aggregation between a centralised and decentralised identity model. For certain application a centralised model is mandatory, but with a decentralised model productivity, enhanced willingness to share data and self-control will be the advantages.

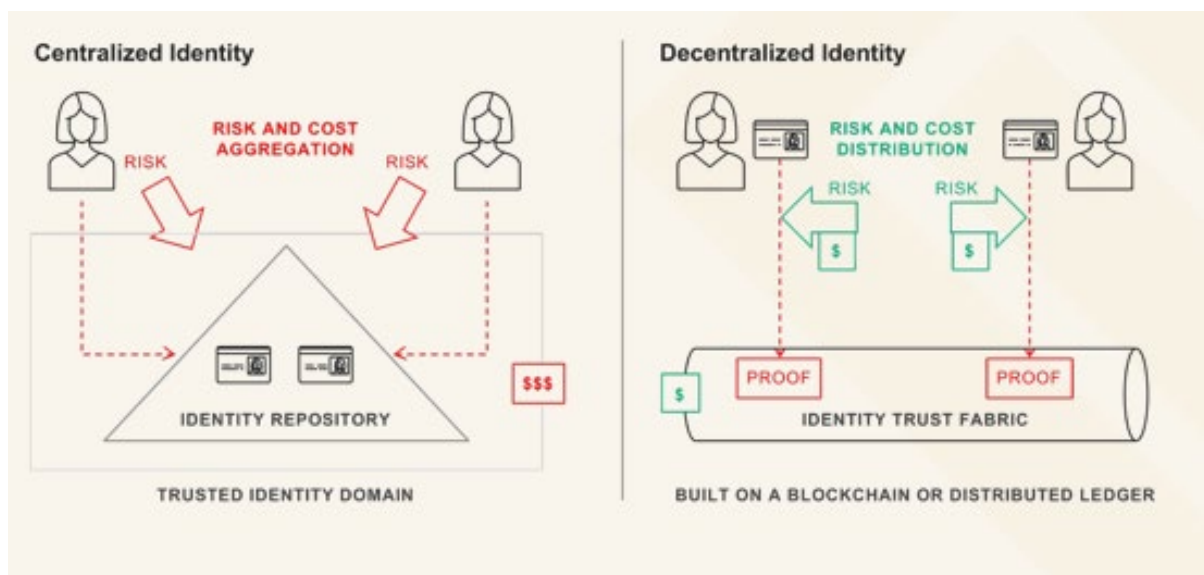


Figure 4: Risk overview, Citibank

6.3. Key infrastructure

According to the international research and benchmark analysis the key components of the ecosystem will be based on the Trust over IP model.³

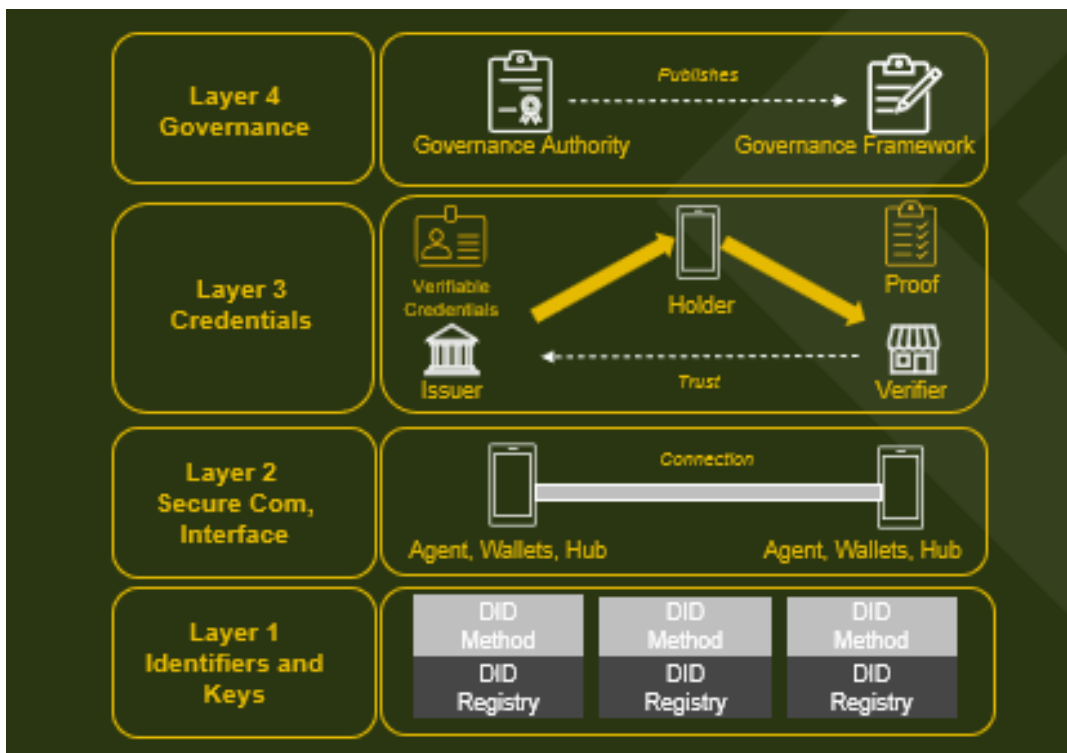


Figure 5: Source: SSI A. Preukschat, D Reed

The purpose of Layer One is providing the technical components to establish trust. Basically, one machine can securely connect with another on a cryptographic basis. The prerequisite for this is to have a very strong public key verification mechanism in place. Ideally this is being done without using a centralised authority. A decentralised infrastructure or other utilities can be implemented to provide the required trust level. Decentralised systems e.g. distributed ledger or blockchains, are one approach to this.

Layer Two represents the next layer of the application. Digital wallets and agents are being implemented to ensure privacy of the users, security of personal data, data portability and user control: “self-sovereignty”. The big advantage of this layer is the peer-to-peer communications which ensures privacy and security once identity has been confirmed, without reliance on any 3rd parties.

At Layer Three data exchange protocols and methods will create the verifiable credential trust triangle. Here holders, issuers and verifier are using exchange protocols that run on top of DID communication methods to share and verify credentials. Additional functionality such as secure messaging or workflow modelling protocols can be implemented in Layer Three as well.

The human interactions with a wide range of applications are covered in Layer Four. It is designed to establish and enable a digital trust ecosystem. Especially for this layer the governance framework is very important and critical to ensure a frictionless data exchange between different tools, apps, sites and businesses. The better defined the governance model the greater the trust users can have in the integrity of the application and the more consistent the user experience in terms of security, privacy and data protection across the ecosystem.

³ Detail see appendix four - White paper ToIP

6.4. Definition of a Decentralised Identifier (DID)

“A globally unique persistent identifier that does not require a centralised registration authority and is often generated and/or registered cryptographically. The generic format of a DID is defined in § 3.1 DID Syntax. A specific DID scheme is defined in a DID method specification. Many—but not all—DID methods make use of distributed ledger technology (DLT) or some other form of decentralised network.”⁴

6.5. Example of a DID

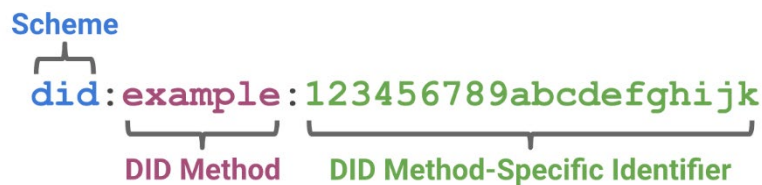


Figure 6: DID example by W3C

6.6. Features and Benefits of a Decentralised Identifier (DID)

A DID is a globally unique, highly available and cryptographically verifiable identifier. It is a novel set of identifiers that facilitate the verification of decentralised identity. Digital proofs with public key cryptography is a proven technology in widespread use. However, existing solutions and standards involve the use of centralised authorities for issuing digital identity, and centralised repositories for the handling of public key information. This leads to the issue of how to trust the ultimate root source of digital identity, and creates points of inherent weakness i.e. centralised servers which can be attacked and compromised, and the managers of the servers must be trusted arbitrarily.

DIDs used in conjunction with decentralised infrastructure can overcome these issues and provide the following benefits:

- a) Never changing, permanently existing
- b) Easily resolvable for other parties to read the public key or reach a specific address of the required agent.
- c) Cryptographically verifiable: the user/holder should be able to prove control over their private key and the link to the DID
- d) Decentralised: the registry of DIDs cannot be held and managed by a single authority, the single points of failure through a cyber-attack or tampering need to be avoided, therefore the use of distributed ledgers or file services, peer-to-peer networks or blockchain infrastructure is fit for purpose.⁵

⁴ [Decentralized Identifiers \(DIDs\) v1.0 \(w3.org\)](https://w3c.github.io/did-core/)

⁵ Source: Self Sovereignty Identity, A. Preukschat

The difference to the existing cryptographic approach is the involvement of the verifiable data register (DLT, blockchain, or any other decentralised register). By using a distributed decentralised technology the public keys are not a single point of risk anymore due to the triple play of:

1. Recording of transactions
2. Grouping of transactions into blocks linked to the previous groups
3. Cryptographic replication across all peers in the network. This is what provides the strong foundation needed for the ubiquitous adoption of the verifiable digital credentials.⁴

For rapid adoption of DIDs, the registries can be managed in conventional databases, however the trust level is dependent on the administration of this database. Privacy is not the same level compared to the DLT solution and the core element of eliminating the single point of control and failure is not covered. However, the fact that this is easily implemented means there is limited barriers in transitioning from the partially decentralised model to a fully decentralised model.

6.7. Terminology for the Triangle of Trust

- DID** – Decentralised Identifier
 - Holder** - Entity holding the VCs and presents it to the Verifier. Credentials are presented as Verifiable Presentations.
 - Issuer** - Entity which issues credentials. Credentials are issued as Verifiable Credentials (VC)
 - Verifier** - Entity which receives VCs from Holder and provides benefits from them.
- Verifier verifies that
- Verifiable Credentials and Presentations have valid digital signatures
 - Verifiable Credentials are not expired
 - Holder entitled to hold them
- VC** – Verifiable Credential
 - Verifiable Data Registry** - Holds all the essential data and meta-data.
 - Public keys of the issuer
 - Schemas and properties that contain VC

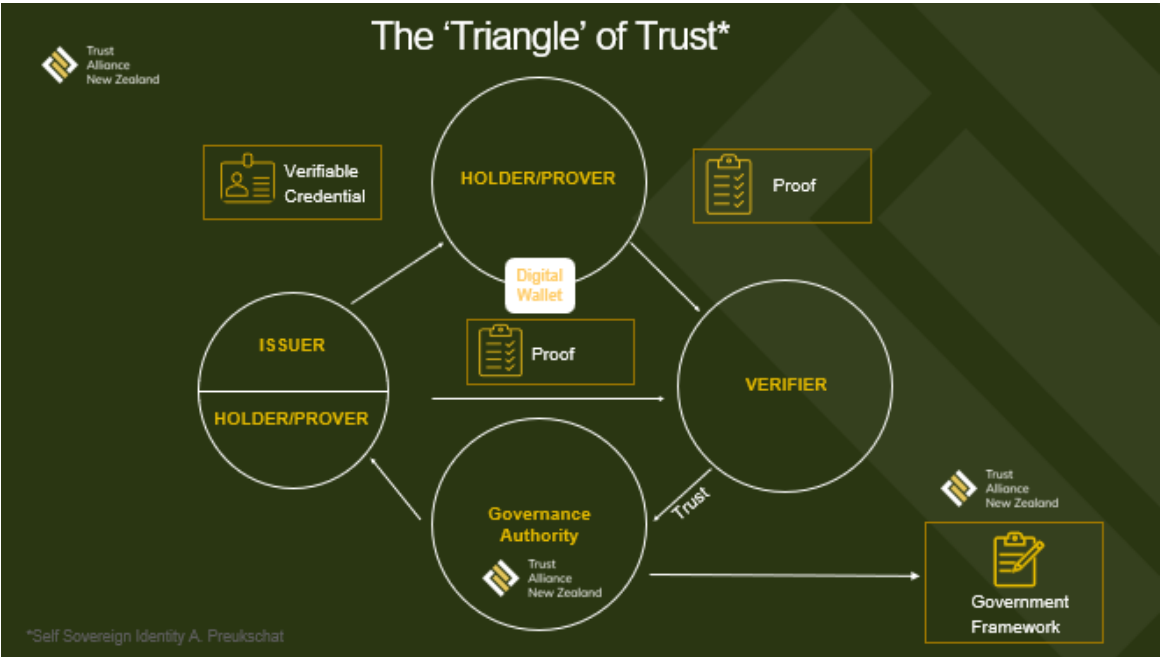


Figure 7: Source: SSI A. Preukschat, D Reed

6.8. Triangle of Trust

The above diagram of the trust triangle shows how verifiable credentials will be issued, verified, and how the holder can prove a certain claim without exposing the actual data. The holder of the verifiable credential can decide if and up to which level of detail he wants to give access to the individual data attributes (or claims). The governance authority - in this example the Trust Alliance NZ - defines the rules and policies for the trust framework within this ecosystem, which the issuers must follow. The main reason for a secondary governance trust triangle is to determine common understanding, procedures and policies to ensure consistency in the digital trust ecosystem.

6.9. Key Management

One of the core parts of the tech stack is the key pair creation, management, and associated cryptographic mechanism. The below diagram shows how the asymmetric key cryptography is set up and works behind the scenes.

- “Bob sends a message (e.g. a DID document for a verified NZBN or FEP) encrypted with Alice’s public key (recorded on a distributed ledger to ensure tamper-resistance), which only she can decrypt using her own private key; therefore only Alice can read the message.
- If Bob sends a message (e.g. a DID document for a verified NZBN or FEP) encrypted with his own private key, it can be decrypted by Alice (or anybody else) using Bob’s public key confirming to her that Bob has in fact sent it. Similarly, if Bob sends a message along with a hash of the message (a.k.a. a digital signature) encrypted with his own private key then Alice can check the message integrity i.e. whether the message contents , has been tampered with, or not.”⁶

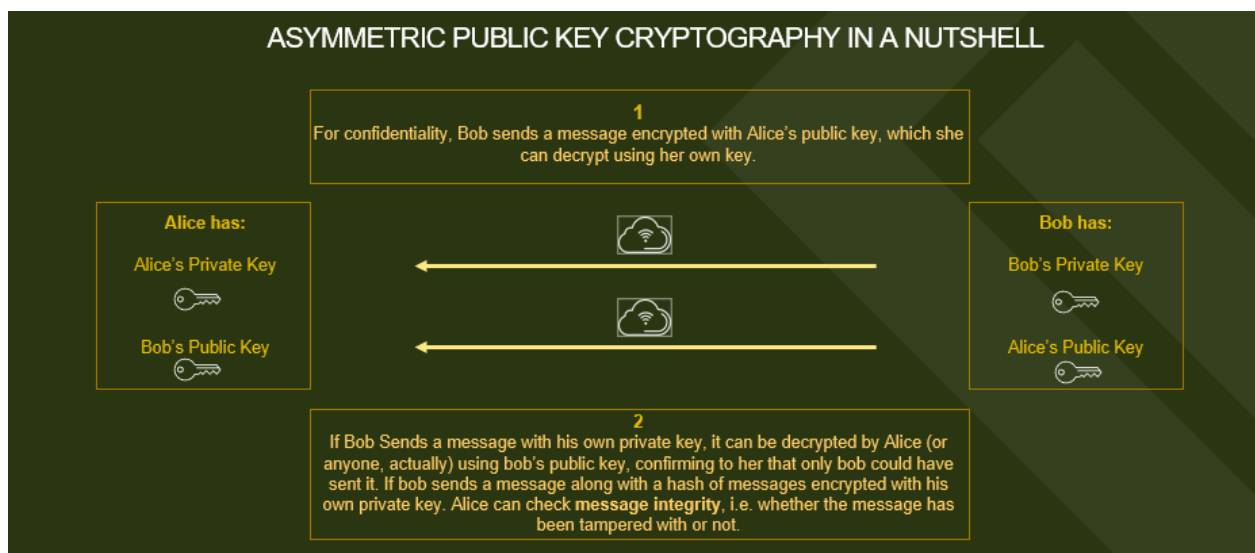


Figure 8: Blockchain and the Supply Chain, N. Vyas, A. Beije, B. Krishnamachari

⁶ Blockchain and the Supply Chain, N. Vyas, A. Beije, B. Krishnamachari

6.10. Evaluation of Specifications and Standards

The result of the proper analysis for the international benchmark study is clear: The tools, protocols and infrastructure development have to be in line with the W3C standards. This ensures scalability, portability, independency of a single vendor approach and international acceptance.

*“W3C standards define an **Open Web Platform** for application development that has the unprecedented potential to enable developers to build rich interactive experiences, powered by vast data stores, that are available on any device. Although the boundaries of the platform continue to evolve, industry leaders speak nearly in unison about how HTML5 will be the cornerstone for this platform. But the full strength of the platform relies on many more technologies that W3C and its partners are creating, including CSS, SVG, WOFF, the Semantic Web stack, XML, and a variety of APIs.*

W3C develops these technical specifications and guidelines through a process designed to maximize consensus about the content of a technical report, to ensure high technical and editorial quality, and to earn endorsement by W3C and the broader community.”

For more read: [Standards - W3C](#)

6.11. Concept Development and Engagement

A preliminary white paper outlining the technical approach of decentralised identifiers (see below RFC for DIDs/VC) was developed and shared between the key stakeholders. It was evaluated, discussed and further developed together with the technical working group and the wider international ecosystem such as RMIT. For details see the RFC DID white paper in the appendix.

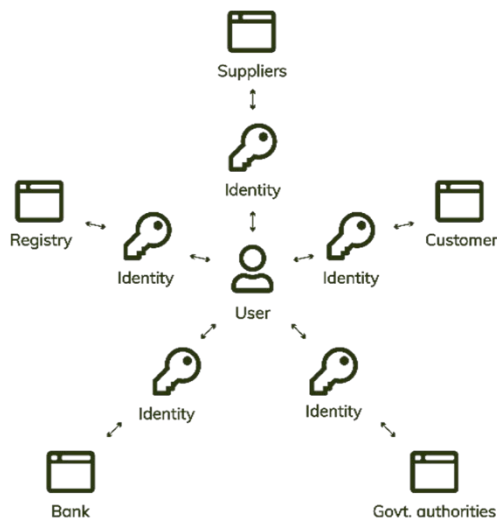
7. Example of a Use case/application – Non-Technical

This TANZ Identity Solution Demonstration video shows the benefit of how a decentralised model could be used by farmers and growers to manage and control their own digital identity e.g. for login credentials, via a trustworthy digital fingerprint through DID's and VC.

On the left side, the centralised model, the farmer has to manage and hold numerous different credentials to identify himself, typically with username and password, to enter different portals, software tools, etc. The “keys” and login details are held by numerous different providers. Possibly a number of different two-factor authentication layers are also placed on top, in an attempt to compensate for the inherent weaknesses of the centralised username/password security model.

On the right side, the decentralised model, the user has one digital identity with which the user can sign into numerous different providers portals or software applications, without any of the service providers being federated in any way i.e. they are all independent on not sharing user identity data in any way. In a well-established decentralised identity ecosystem the user and providers do not even need to be part of the same identity “network”, since the methods for resolving identity across different networks is a core part of DID design. For more details see the demonstration video: [TANZ Identity Solution demonstration - YouTube](#)

Centralised model driven by suppliers



Decentralised model driven by user

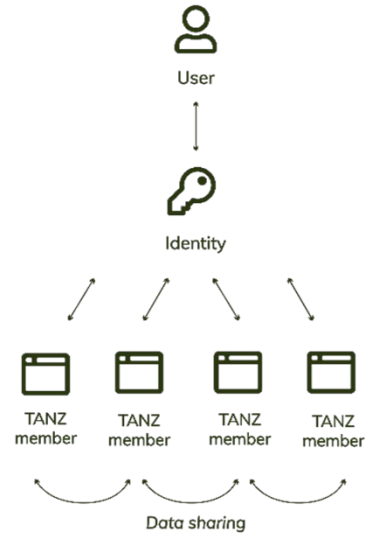


Figure 8: TANZ Registry Example

8. Demonstration of Proof of Concept – Technical

A working proof of concept was implemented. The below process flow is shown in the live [demonstration video](#) to the key stakeholder as a proof of concept for the technology. As per the feasibility study, the technical approach of using decentralised identity for proving the authenticity of individuals is a recommended way forward.

Based on the concept of the trust triangle the TANZ Proof of Concept deployed the following DID and VC process:

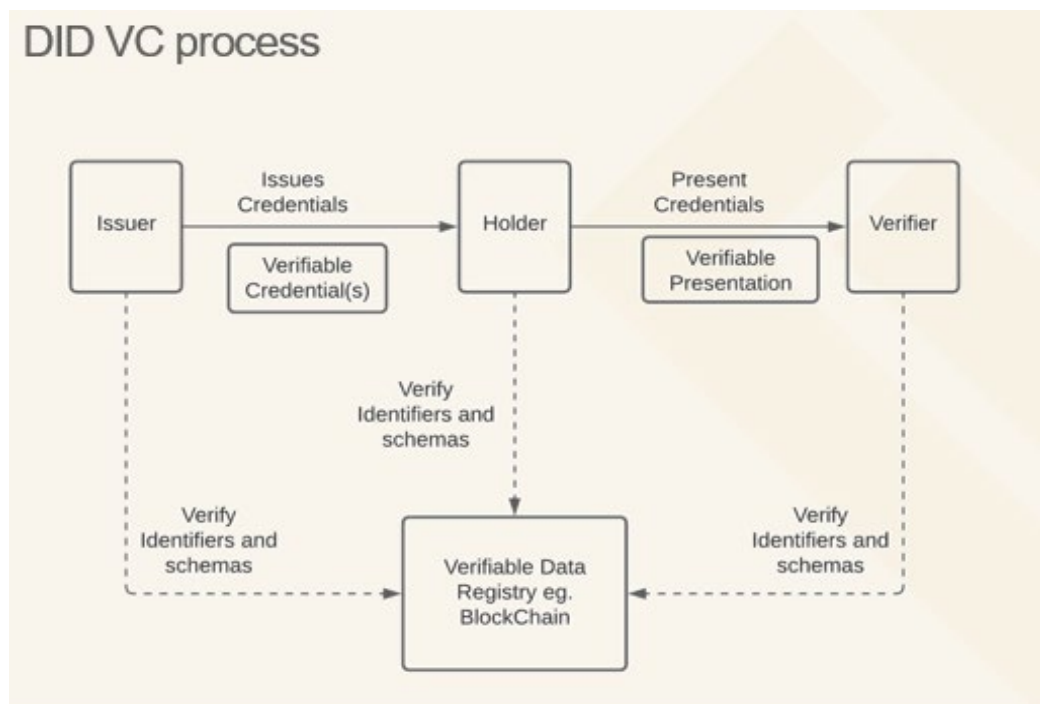


Figure 9: Source: TANZ tech stack documentation

8.1. Key content of the technical demonstration PoC video

This video covers the technical presentation and explanation of how to create, verify and revoke technically decentralised identifiers and verifiable credentials to prove digital identity. It is an exemplar with deployed real-world tools to show the decentralised approach.

The following components were built to demonstrate the technical proof of DIDs and VCs

- Demo wallet for a user/holder
- Three different verifiers a) DIA b) Transport Authority c) Licence Authority
- DID Records/Book on the TANZ infrastructure
- QR code as an enabler to requesting data and establish connection via web service

In the demonstrated proof of concept implementation, the following events and transactions occurred:

- 1) The user/holder logs into their digital wallet.
- 2) After login two verifiable credentials are created:⁷
 - a) a passport
 - b) a driving license⁸These VC's can be verified by the demonstration entities which have been created, the "DIA" and "Transport Authority".
- 3) The wallet creates two DIDs for these verifiable credentials and stores the metadata on the TANZ infrastructure (blockchain) and the content (DID Document) on IPFS distributed storage⁹.
- 4) IPFS is, in this case, the DID registry. The wallet calls to the IPFS connector service via a wallet agent.
- 5) The created verifiable credentials can be shared and verified with the demo verifiers app by presenting the VC QR code, which is held in the wallet. The use of a QR code to initiate and manage credential requests and provision is an example of a verifiable credential presentation; many other methods are possible, but the use of a QR code gives an example of a quick and simple approach using an everyday device – the mobile phone.
- 6) The demo issuer is issued a customised credential that attest to certain claims e.g. driving license classes or blood type, in our example, and a new DID is created.
- 7) The holder of the wallet can scan a QR code (a verifiable credential presentation) generated by the issuing authority, and after scanning the verifiable credential will be installed in the wallet.
- 8) When a verifying party requests a credential from the user, again a QR code is generated which can simply be scanned. This triggers a request for a specific credential, which the user through their digital wallet can then choose to provide or decline.
- 9) When providing the credential, the user also has the ability to select which data attributes are actually shared with the verifying party. For example, they could share their age and name, but not their blood type.

⁷ The actual process of the creation of VCs which would happen in the real world, was not in scope for this demonstration, therefore a set of VC's were self-generated on login to enable demonstration of an end-to-end use of the technology.

⁸ SDK="A software development kit (SDK) is a collection of software development tools in one installable package. They facilitate the creation of applications by having a compiler, debugger and perhaps a software framework. They are normally specific to a hardware platform and operating system combination To create applications with advanced functionalities such as advertisements,[4] push notifications etc; most application software developers use specific software development kits. see more: https://en.wikipedia.org/wiki/Software_development_kit

⁹ IPFS= InterPlanetary File System

Proof of Concept of DID's/Verifiable Credentials

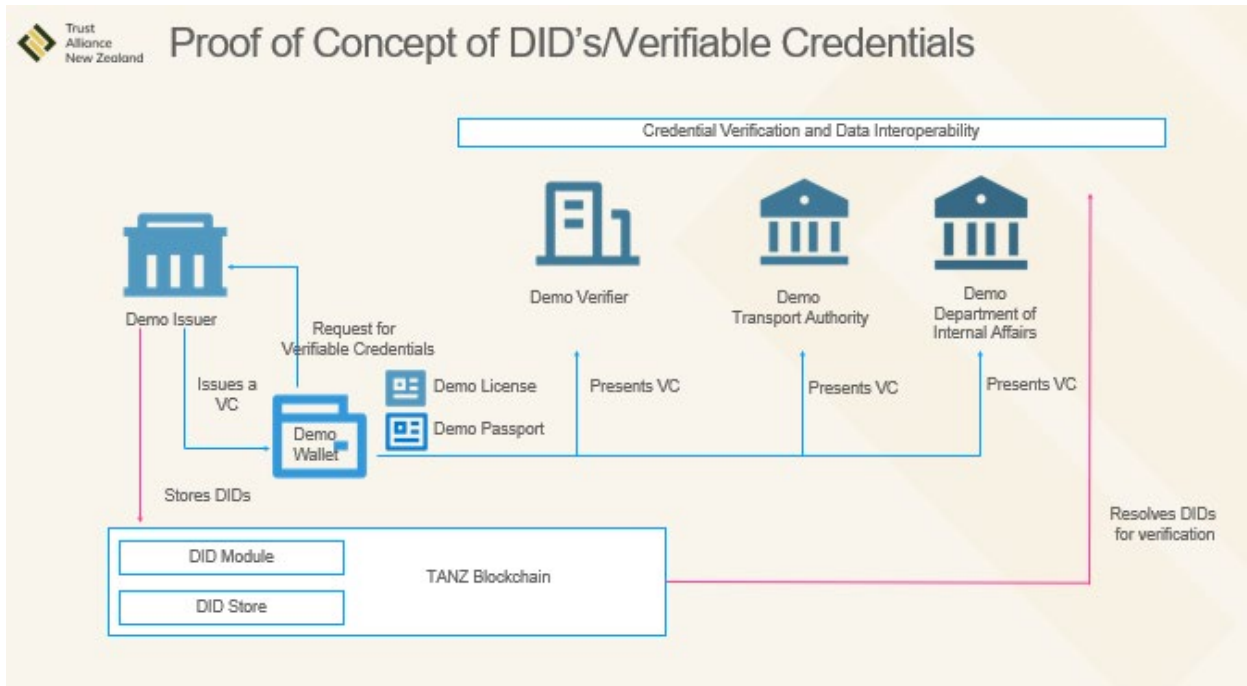


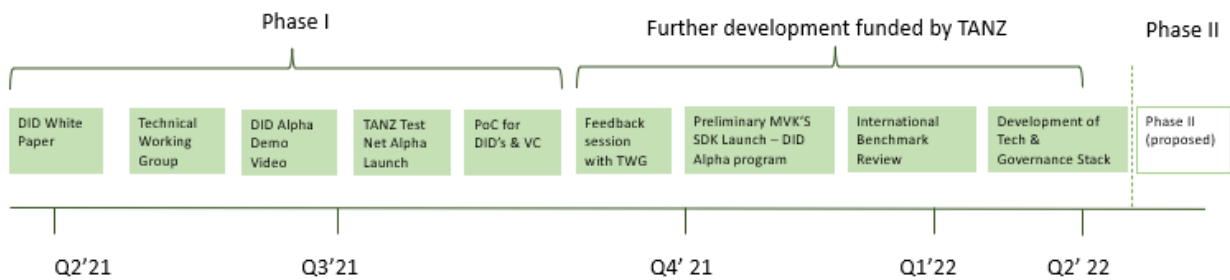
Figure 10: Source: TANZ tech stack documentation

The below listed tools were defined and developed in a demo stage to visualise how the technology will be utilised to address the business problems in the sector.

Tools	Function
Demo Issuer	<ul style="list-style-type: none"> • A Holder (User) can request a verifiable credential (Digital Identity) • Holder needs to fill the form, upload and submit data • Then the holder should scan the QR Code from the wallet
Demo Verifier	<ul style="list-style-type: none"> • The Verifier demo app is able to validate and prove the authenticity
Demo Transport Authority and DIA	<ul style="list-style-type: none"> • A dummy representation of Transport Authority and DIA for showcasing purpose
DID Book	<ul style="list-style-type: none"> • A developer tool which shows what is happening “under the hood”. In the proof of concept demo: • Used to revoke a DID/credential • Explore events • Search a DID
Demo Wallet	<ul style="list-style-type: none"> • A simple working secure digital wallet that facilitates user interactions, creation of VC presentations, and exchange of data with issuers and verifying parties.

	<ul style="list-style-type: none"> • Two credentials are generated after login into the wallet • Two DID documents are stored on chain
--	--

9. Overview of the technical roadmap



The progress of the achievements and milestones so far is visualised in the graph above. Phase I was accomplished in the middle of Q4 last year. In the meantime, the development continued with the support of the society and members to ensure the continuity of progress and deliverables. The Minimal Viable Product SDK (MVK) was launched in an alpha status and made available as open source on Github and Npmjs.

Please find further details under below links:

[GitHub - TrustAllianceNZ/trust-sdk: SDK for data interoperability](https://github.com/TrustAllianceNZ/trust-sdk)
<https://www.npmjs.com/~trustalliance>

10. Subsequent next step delivered (out of scope)

Based on the successful proof of concept and positive feedback from the technical working group the preliminary tools and protocols were developed further, so that a set of MVK¹⁰/ SDKs were released as open source to the tech community (beyond TANZ members). The feedback and requirements are being collected and summarised for Phase II. Preliminary work to get the MVK's to the next stage is in progress.

Core Tools /MVK's	Description of functionality	Stage
1. SDK to create Verifiable credentials	The software development kit will enable the operator to create a verifiable credential.	Specification and features defined, Preliminary developed and for PoC executed, approved by key stakeholders
2. SDK to create Decentralized Identifiers	With this software development kit the user can generate and create a decentralized identifier.	Specification and features defined, Preliminary developed for PoC executed, approved by key stakeholders
3. SDK / Service to create Cryptographical Keys / Digital Signatures	This service will create and manage cryptographical key pairs for the issuer, the holder and verifier.	Specification and features defined, Preliminary developed for PoC executed, approved by key stakeholders
4. Service to store DID Documents in a distributed storage (IPFS)	Connector between issuer and DID Document storage	Specification and features defined, Preliminary developed for PoC executed, approved by key stakeholders
5. DID Agent	Create, Revoke, Resolve, Update DIDs - Connects with chain Store DID documents in a Decentralised file store	Specification and features defined, Preliminary developed for PoC executed, approved by key stakeholders
6. DID Book	DID Operations: this functionality enables the user on the development back end to revoke and search DIDs	Specification and features defined, Preliminary developed for PoC executed, approved by key stakeholders

¹⁰ MVK=Minimal viable development kit

7. TANZ Infrastructure architecture for a testing incl. Docker Hub	Set up of test environment is locally	Specification and features defined, Preliminary developed for PoC executed, approved by key stakeholders
--	---------------------------------------	--

11. Next building blocks for phase II

Due to the undertaken work and outcome of Phase I the building blocks for the next Phase II are clearly derived, defined and peer-reviewed. The below overview describes the next elements to be developed.

Future Tools	Description of Functionality	Next step
Digital Wallet	Stores the credentials, keys Protect them from theft Keep it handy easily available across devices	Define and draft specifications in line with governance stack and policies
Digital Wallet Agent	This is a software module, which is wrapped around the wallet to “speak” to other wallets and protect that only “you are responsible for your VC and your keys (Translation, Key creation, back up, exchange VC)	Develop and draft features, specifications
Webservices	A set of RESTful API endpoints with service management functionalities to create verifiable credentials and decentralised identifiers. This product utilises the TANZ SDKs to create Decentralised Identifiers and verifiable credentials.	Develop and draft features, specifications
DID Operations (admin/backend)	Issuance, verifying, revoke and binding DID’s for VC Authentication of using DID’s Node Management, Decentralised System Operation/Administration	Develop and draft features, specifications
Workflow processes	Mapping of business operations to DID Operations (Hierarchy, transaction, requirements, conditions)	Develop and draft features, specifications

	execution) Member Application (“User Interfacing”) DID Management (e.g. Issuance, Transparency)	
IPFS Connector	Connecting the DID Document to the distributed storage	Develop and draft features, specifications

12. Outlook at Phase II Digital Identity MVP – “Design, build and test DID’s in the Primary Sector Value Chain”

12.1. Next steps

The tools and protocols developed in the proposed project will enable the Trust Alliance members and solution providers to establish verifiable credentials and prove authenticity for permissioned data sharing. This will enable interoperability of data to occur where data sharing mechanisms have been established.

Based on a technical roadmap, the PoC for Digital Identity will be released into a Beta Program for DID’s. Within this program selected use cases for the PoC will be tested, applied, and verified by selected stakeholders across the different use cases.

High-level process:

2. Finalise building the required to tools and environment of the PoC phase.
3. Define requirements for users/members of the deliverables.
3. Engage, communicate and support users/members accordingly.
4. Gather feedback and additional requirements for consideration to apply.
5. Finalise tools and protocols for release.

12.2. Deliverables – Scope

A toolkit of workable SDK’s deployed by early adopters to verify credentials with the defined and approved PoC approach will be developed. Protocols for implementing digital identity at an individual level for data interoperability within the value chain will be specified, which demonstrate the scalability and flexibility across sectors and enablement for data owners to manage & protect their data as requested.

Within the MVP development stage we aim to receive comprehensive feedback of a workable solution. It will give insight, learning and illustrate how a potential solution could be deployed to enable data interoperability between different parties in an easy, trustworthy, controllable and efficient way.

Established awareness and built knowledge by the collective and inclusive approach of a co-designed and co-developed process. Key stakeholders and early adaptors will understand better the DID’s methodology and being able to deploy DID’s to be prepared for the next phase of the data sharing framework.

Tools and protocols which will be provided to key stakeholder group to evaluate their fit for purpose. These will include:

Features	<ul style="list-style-type: none">- Issuing credentials in real time- Verifying issued credentials dynamically- Verifying credentials created by a template in a wallet- Creation of DIDs for each verifiable credential- DID revocation via the DID Book (Developer only app)- TANZ Pallet- Deployment infrastructure
Outcomes	<ul style="list-style-type: none">- SDK to create verifiable credentials- SDK to create decentralised identifiers / DID Documents- SDK/Service to create cryptographic keys- SDK/Service to create digital signatures- Connector to the decentralised infrastructure- Service to store DID Documents in a distribute storage (IPFS)- Verifier module- MVP Demo Wallet- DID Resolver

Appendix 1

- [White Paper: “Request for Comments for Decentralised Identifier at TANZ infrastructure”](#)
- [Demonstration video: Technical proof of concept DID creation and verification](#)
- [Demonstration video: Digital Identity for non-technical audience](#)
- White paper Trust over IP as a reference

Disclaimer

Please note that in the demonstration video and the related communication material TrackBack Ltd. is mentioned, they were the partner to develop the Proof of Concept on behalf of the Trust Alliance NZ.

At this stage TANZ has forked the tools, protocols and MVK’s on their own development stack, continues improvement and future developments is happening under Trust Alliance NZ.

The technical proof of concept video is for internal use only. The licencing and IP for the tools, protocols and MVK’s are documented and publicly declared in the Github portal.

Extract of Glossary of Terms by DIA¹¹

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.
Authentic ation 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 of 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.

¹¹ Digital Identity Services -Trust Framework DIA Jan 22 - NOT GOVERNMENT POLICY – WORKING DRAFT – IN CONFIDENCE

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: <ul style="list-style-type: none"> 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.
Digital Identity Credential Service(s), or credential service(s)		A digital identity service that: <ul style="list-style-type: none"> 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: <ol style="list-style-type: none"> Trust framework providers; Users; and 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 management		For record keeping and format of personal and organisational information, to ensure a common understanding of what is shared.
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.
Security risk assessment		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.