KAIMAI
SECURITY
“lead this way”

Digital Identity — New Zealand’s Ecosystem

Building a Digital Trust Economy for the benefit of every New Zealander

GOVIS 2026 · WELLINGTON · 30 JULY 2026

Joerg Micheel

– Software
– Hardware
– Networking
– Infrastructure
– Cloud
– Security and Compliance
– ISO 19011:2018 · ISO 27001:2022 · ISO 42001:2023
– ISACA Wellington, Board Member
– Public Speaking
– Email: contact@kaimai.org
– Web: kaimai.org

01

The Internet is a terrible place these days

We had great aspirations – and we have come a long way –
but we have also created a rod for our own back.

Things that might keep you up at night

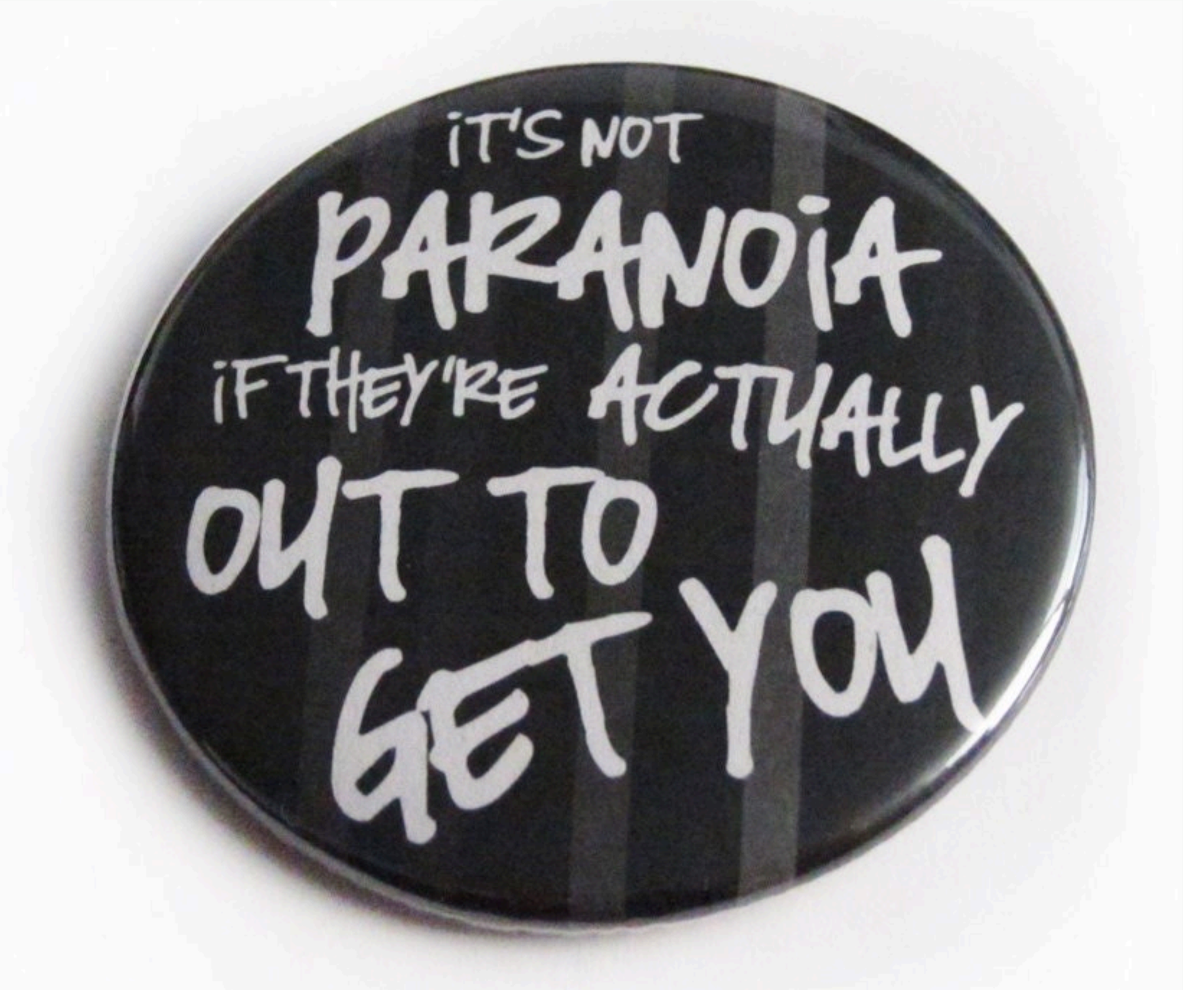
- Multi-nationals and digital sovereignty
- Declining revenue for domestic media
- Election interference
- Social media harm – at scale
- Deep fakes and sexual harassment – at scale
- Scams attacking the elderly and vulnerable – at scale
- Advanced Persistent Threats (APT)
- Identity theft is rampant and causing massive harm (GEM Visa)
- Critical Infrastructure at risk – water, power, electricity, banking, …
- Criminals who are the first and best to know how to use AI

Anonymity is a killer *— the inability to attribute harm and hold individuals to account.*

The scale of the problem

85%

OF CYBER CRIMES INVOLVE LOST OR STOLEN CREDENTIALS



What we have is not working *— existing identity is riddled with problems over problems.*

We used to have laws to protect us.
Without identity the law is toothless.

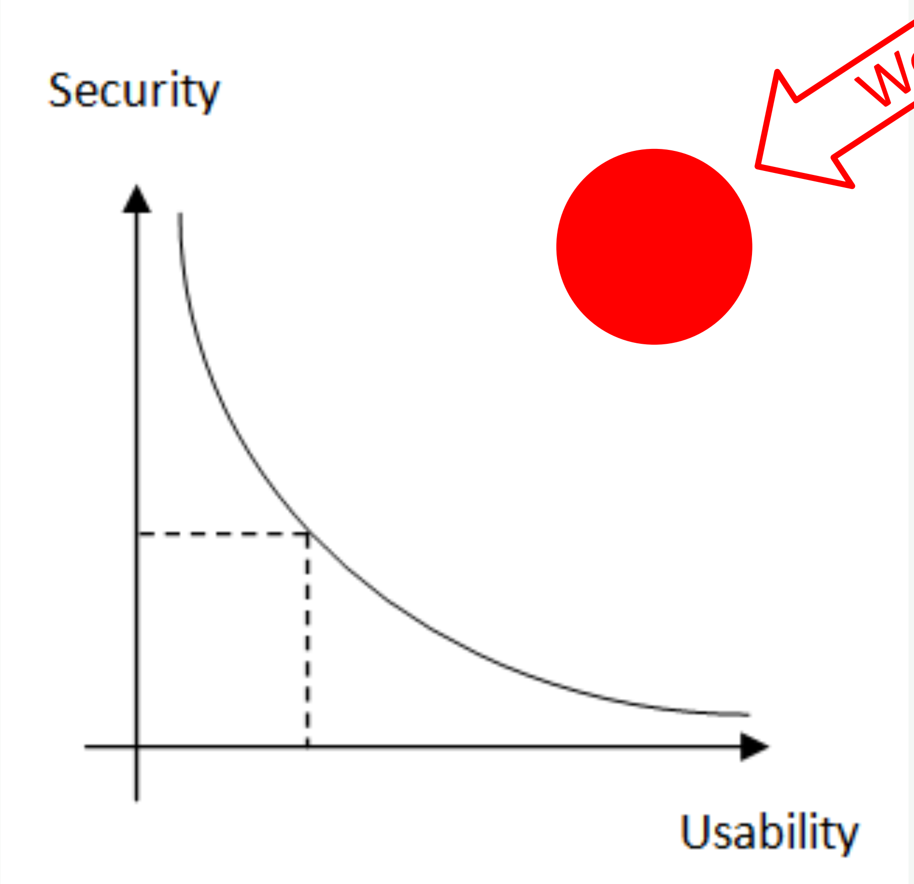
CONSIDER THE INTERNET A “LAWLESS DOMAIN” THAT KEEPS GROWING

02

We have had a problem all along

All transactions on the internet are remote — and we have no remote identity. The Internet offers anonymity and no reliable traceability. It is not possible to definitively identify actors.

User Experience vs. Identity Security

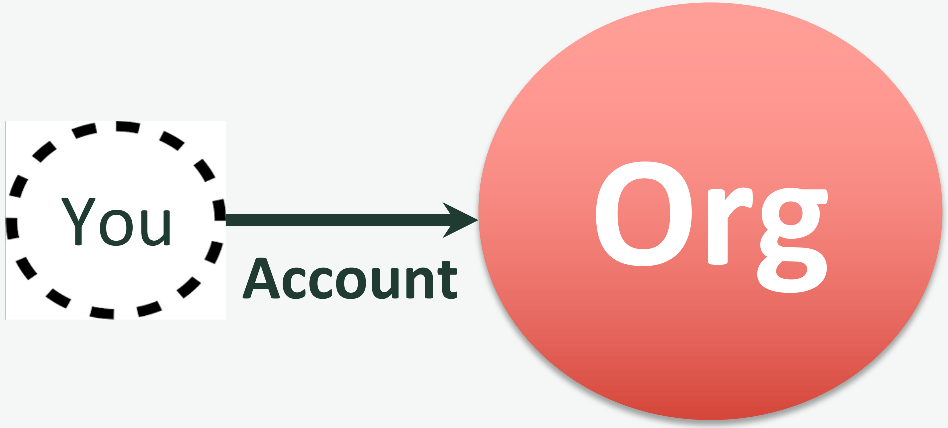


“We Don’t Really Want the Best Security”

- High Security implies Low Usability to the End User – significant friction / inconvenience
- High Usability implies Low Security to the End User
- Between Good Security and Good Usability – “pick one” – the dilemma
- Because End Users ultimately dominate acceptance of a Security Solution – we end up with Low Security
- There have been quite a few attempts in this space – workable solutions are finally available and are being standardized.

Authentication wasn’t really protecting *— high friction forced low security.*

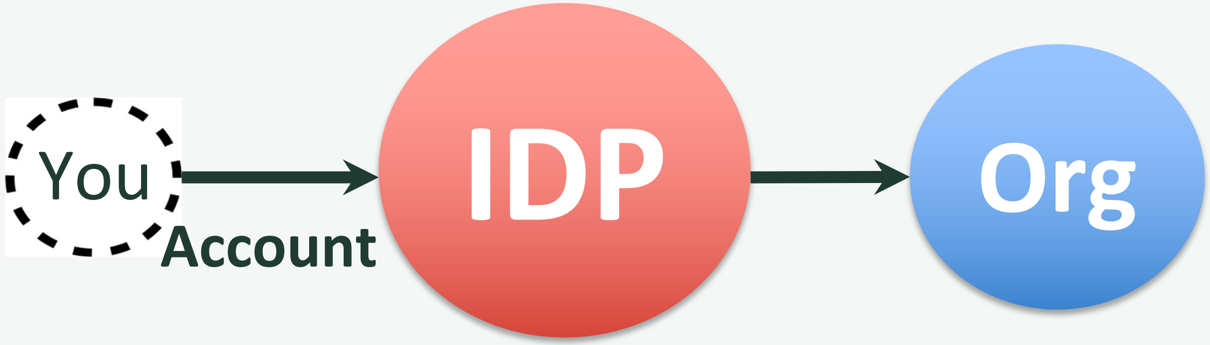
Centralized Identity

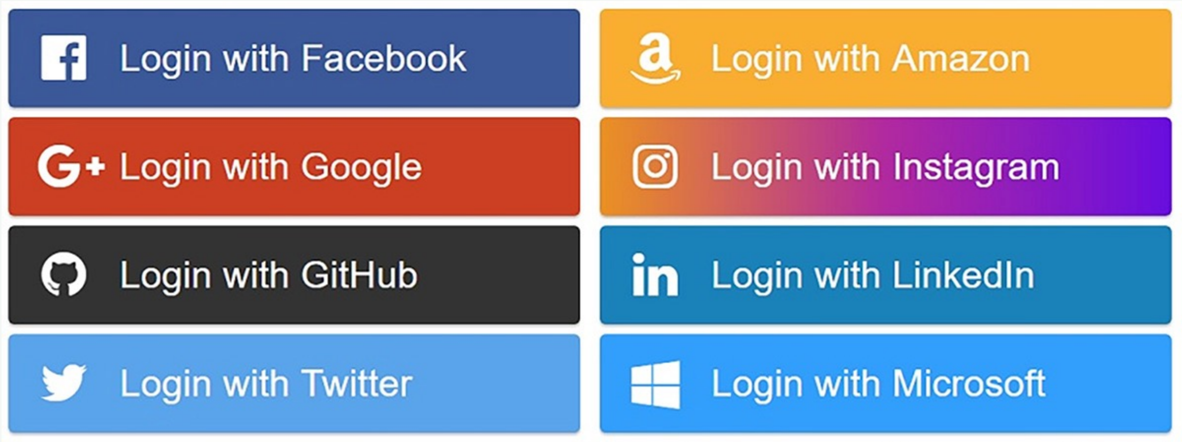


- Identity provided by a central authority
- Could be government or a private company
- Also known as account-based identity
- How we know the Internet to “work”
- Burden to remember all the different logins, passwords and other access credentials
- Each site with its own security and privacy policies, all different and annoying
- No identity data is portable or reusable (in fact that is not permitted)
- Centralized databases are giant honeypots leading to massive data breaches
- May lose your attachment to the organization – losing your identity

Organisations controlling individuals *— individuals forced to play by the rules of the organisation.*

Third Party IDP – Treasure Trove for Multinationals





- Alleviate "the pain"
- Insert an "identity services provider", or IDP, in the middle
- There isn't one IDP that works for everything – previous problems repeat.
- Forces IDP to adopt lowest common denominator for security and policies.
- Large IDPs some of the biggest honeypots for cybercrime.
- Leave the IDP – lose your identity.
- Can't share/store most valuable possessions – passports, drivers license, bank details, health insurance, etc.

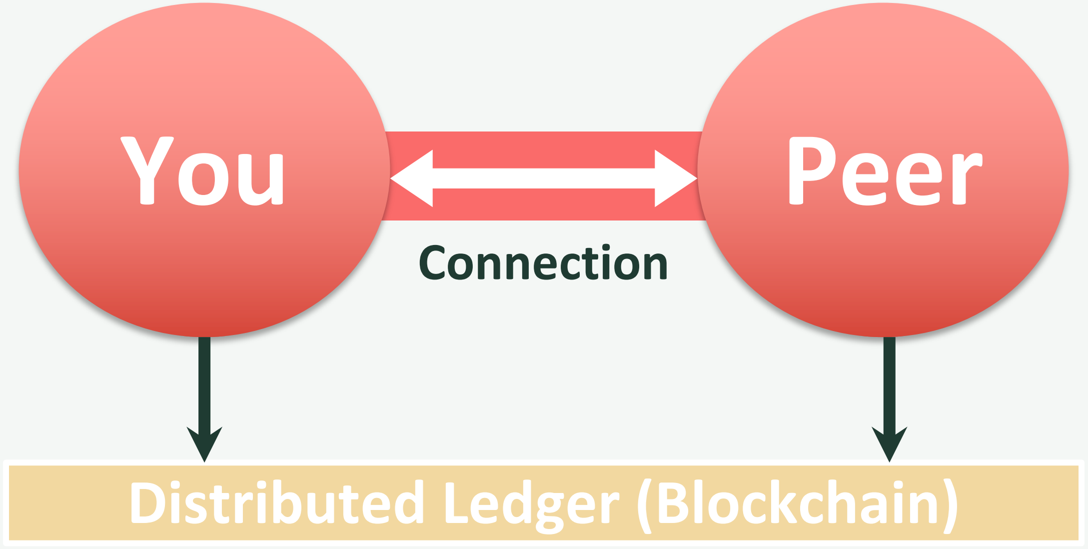
***There is always someone else in charge** — and it is never you – the end user.*

03

Self-Sovereign Identity (SSI)

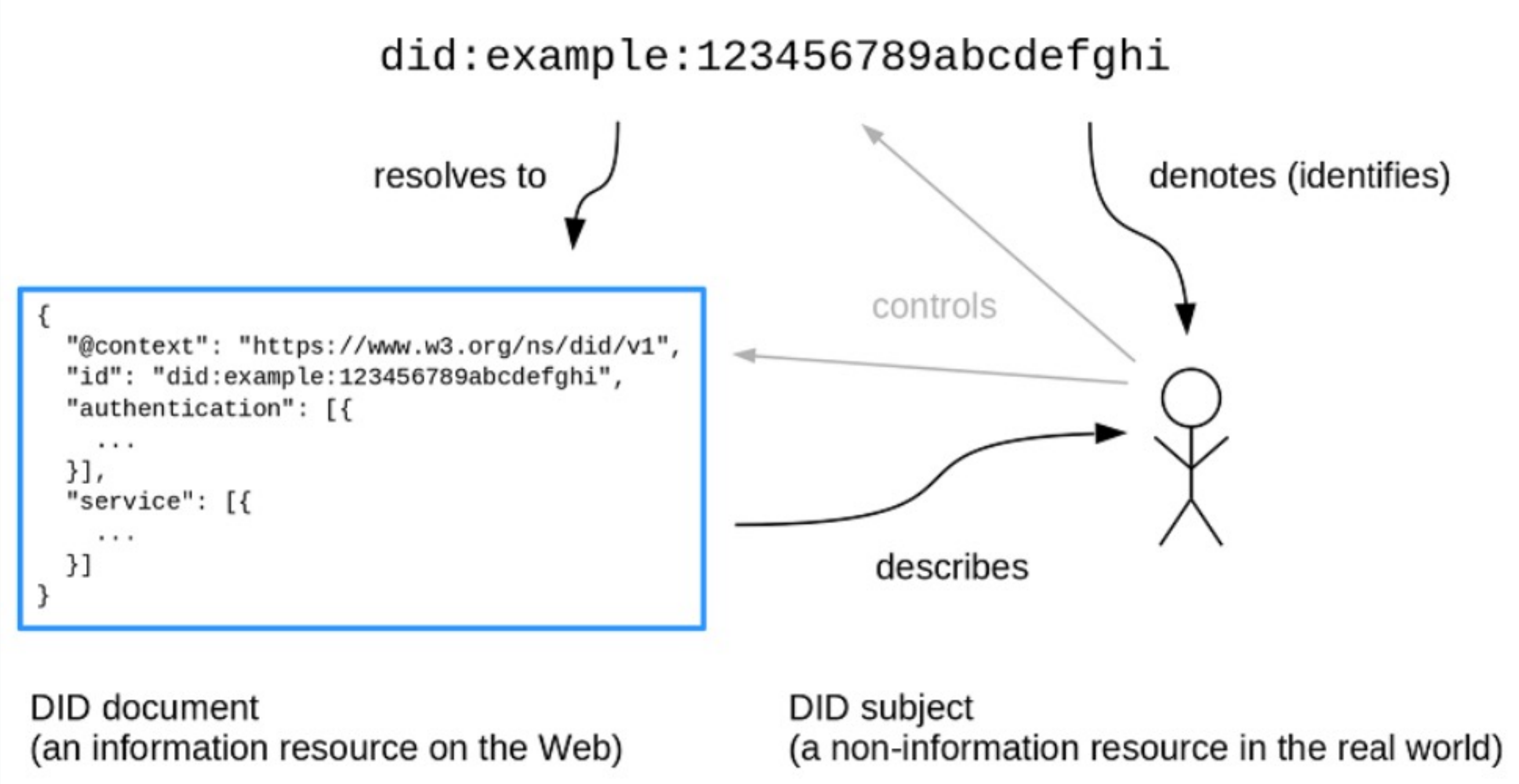
2019. Self-sovereign identity (SSI) is a digital identity model giving individuals full control, ownership, and privacy over their personal data without relying on centralized tech giants or authorities.

Decentralized Identity



- Decentralized model of identity
- Inspired by Blockchain technology
- Also known as Self-Sovereign Identity (SSI)
- Uses Decentralized PKI – DPKI (public/private key pairs)
- No longer account-based, its trust-based
- Direct relationships between you and peer
- No provider relationship between parties
- No control relationship between parties
- No ownership relationship between parties
- General description for identity of different types – humans, animals, innate objects, organizations, tools, etc.
- Quite reflective of how we live ordinary lives today without digital identity
- Ref: DID – Ref: Slab of concrete

DID



The individual is in control *— the DID lives within the Trust Network environment with no expiry.*

DID

- A person will have many hundreds or even thousands of DID (cheap or zero cost).
- Each DID provides for a lifetime encrypted private channel with another person, organization or thing.
- A DID is not just used for authentication, but to exchange verifiable credentials
- There is no central registration – every DID is directly registered on the Trust Network.
- This is genuinely novel technology – no identifier in history has ever presented with these properties.

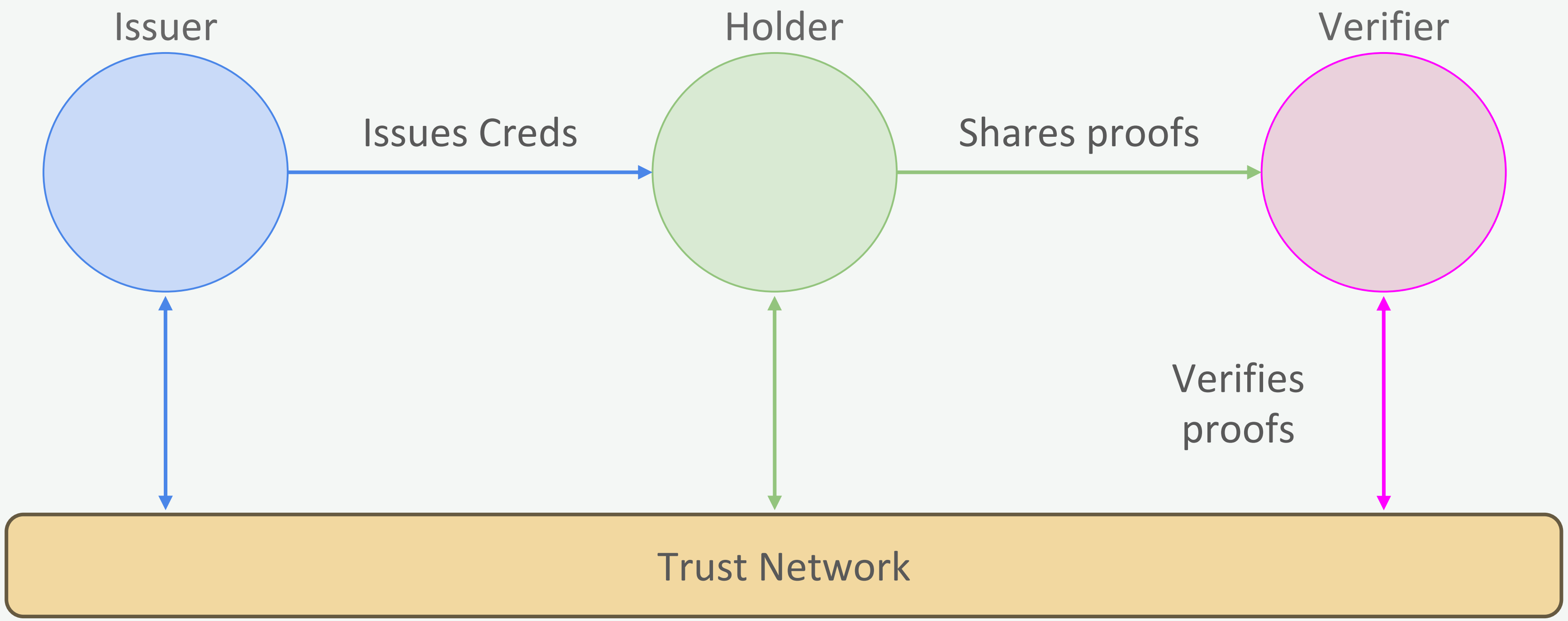
This is novel technology *— no identifier in history has ever presented with these properties.*

DID

- Lifecycle
- Disaster recovery
- Animal
- Newborn
- Guardian
- Power-of-attorney
- Deceased (estate)
- Digital legacy
- Currency
- Property
- Companies and directorship
- Inanimate subjects (things)

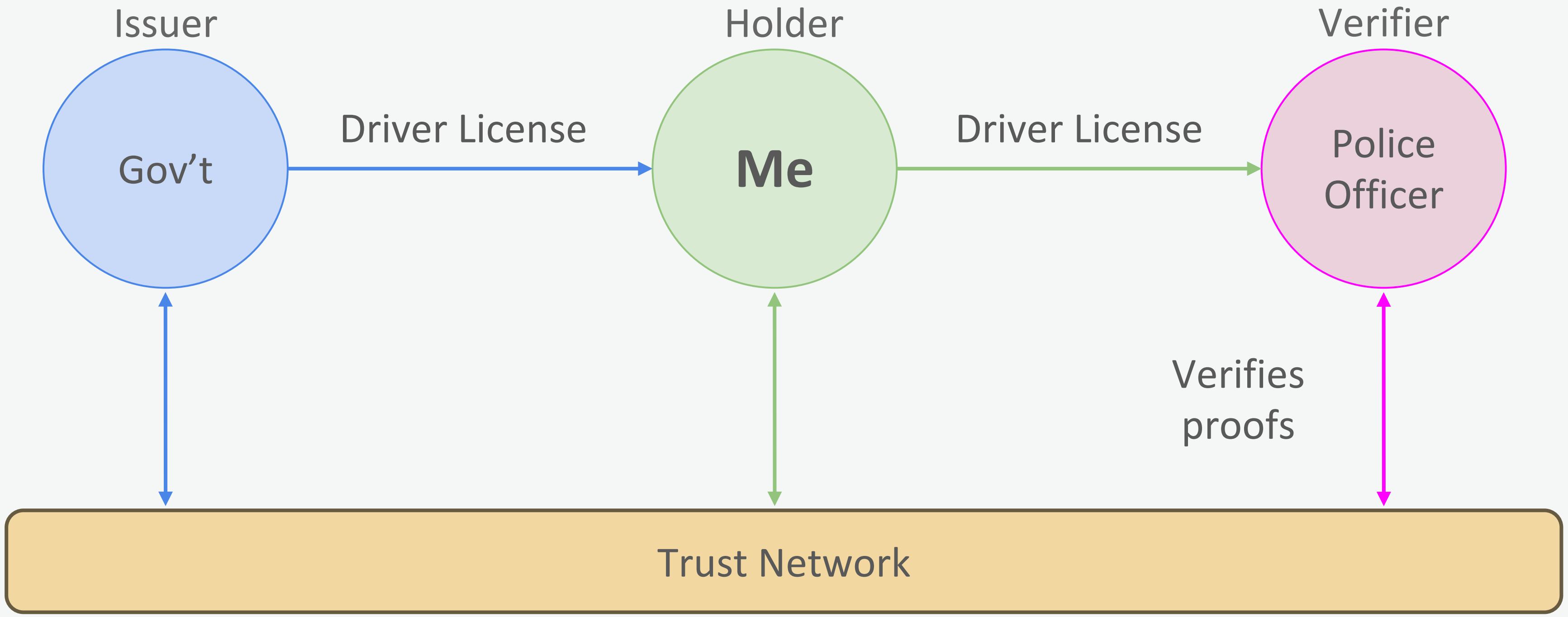
This is novel technology *— no identifier in history has ever presented with these properties.*

Verifiable Credentials – The Works



This is novel technology *— it is privacy preserving and places the control in the hands of the holder.*

Verifiable Credentials – On the Road

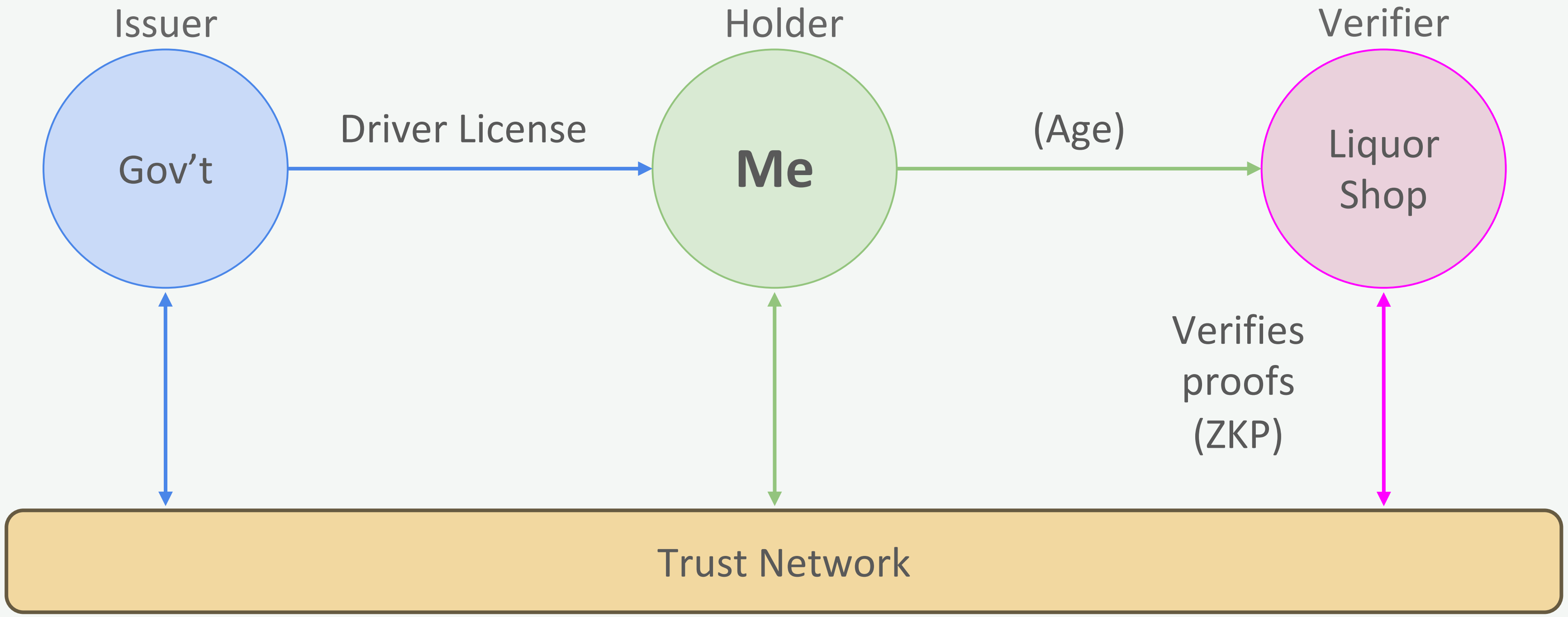


This is novel technology *— it is privacy preserving and places the control in the hands of the holder.*

Verifiable Credentials – On the Road (Whanganui)

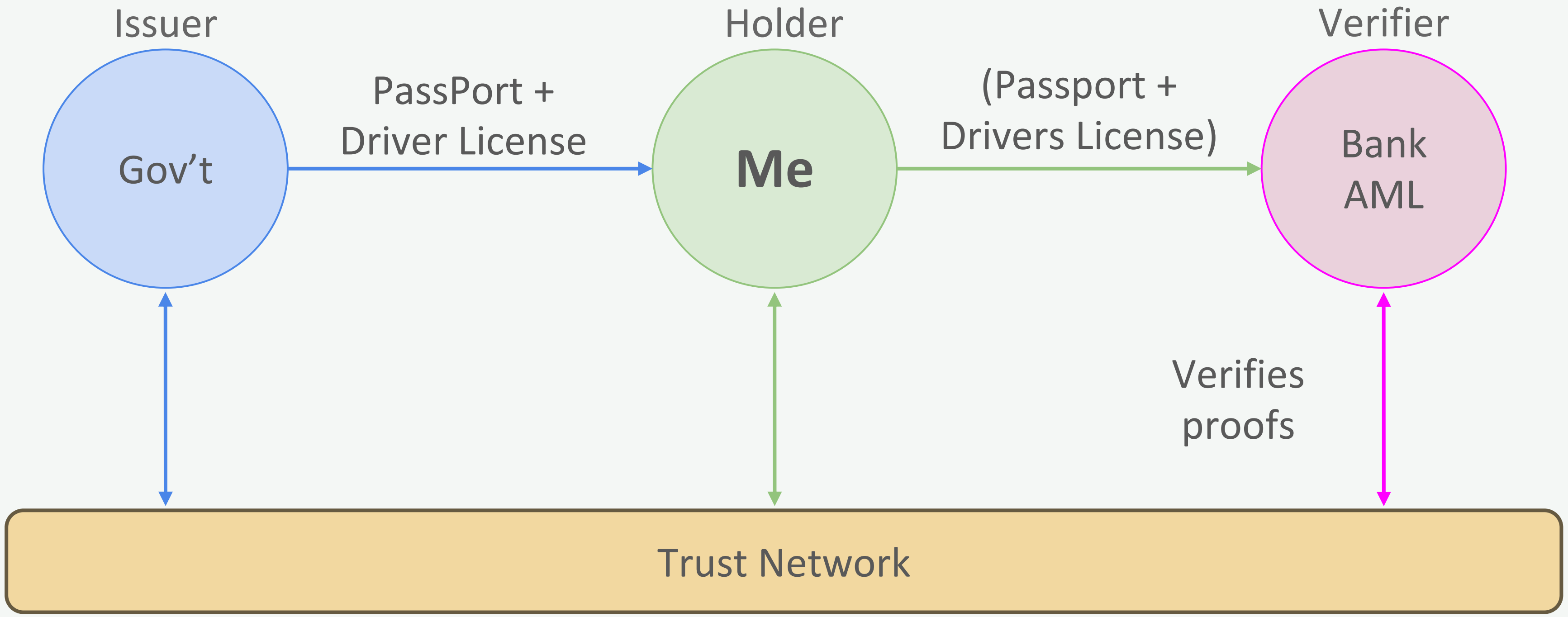
This is novel technology *— it is privacy preserving and places the control in the hands of the holder.*

Verifiable Credentials – Friday night at the Liquor Shop



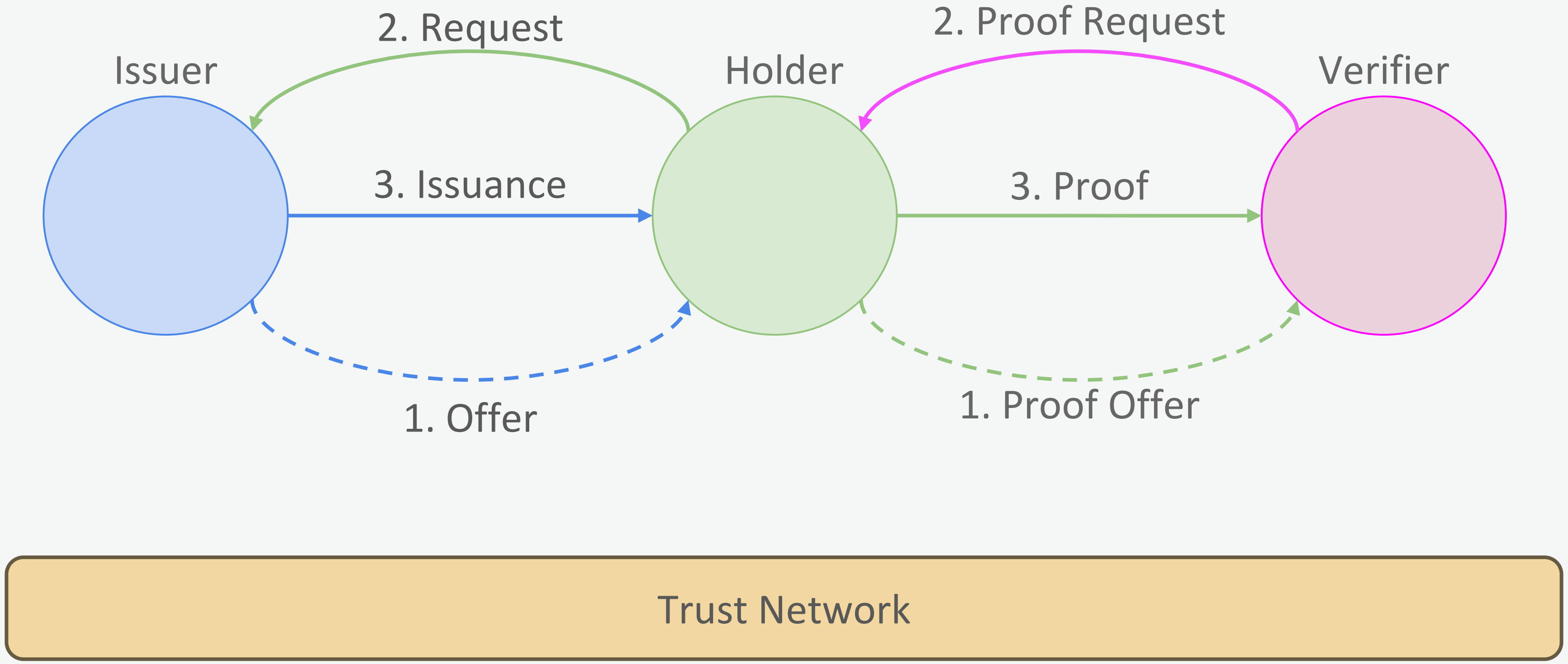
This is novel technology *— it is privacy preserving and places the control in the hands of the holder.*

Verifiable Credentials – Opening a new Bank Account



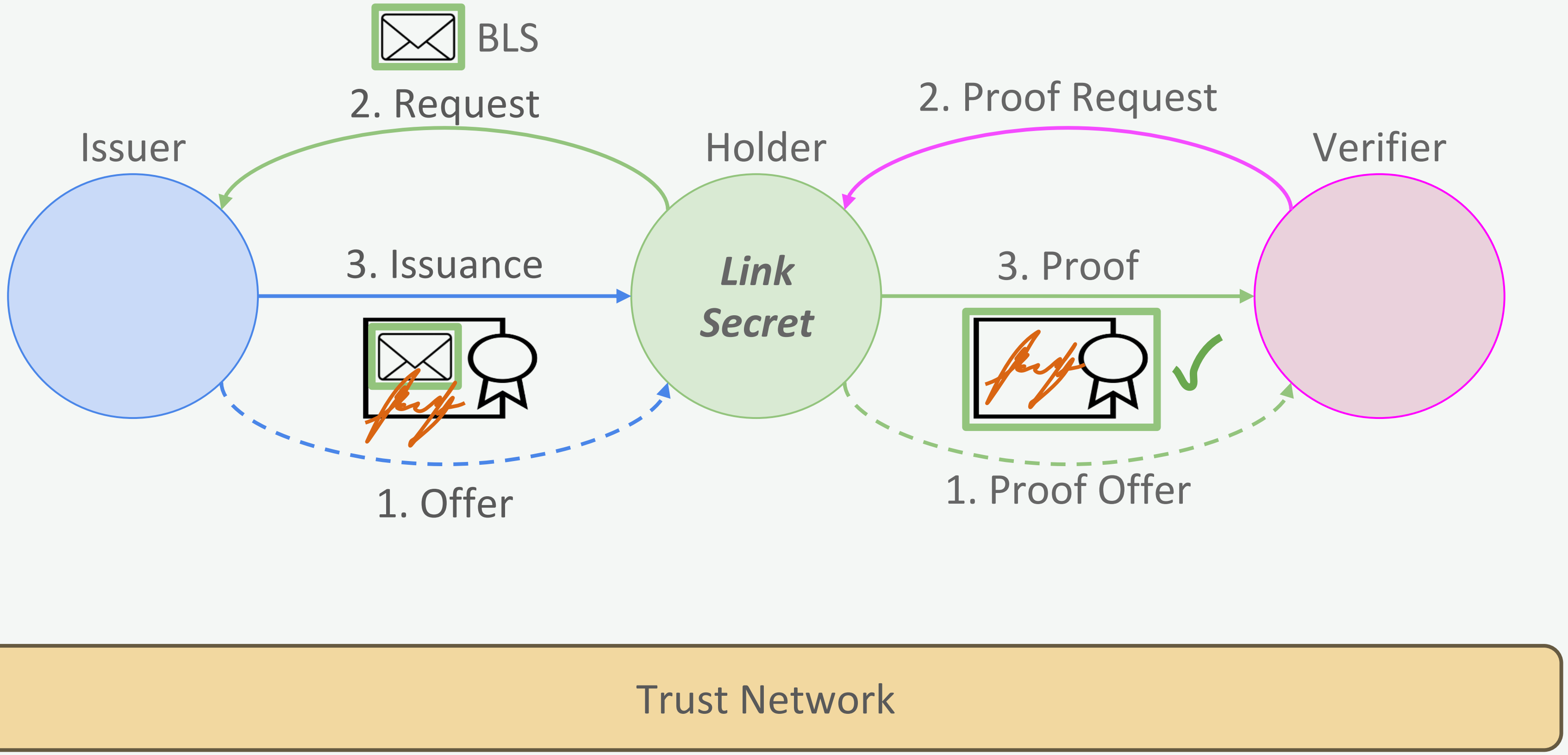
***This is novel technology** — it is privacy preserving and places the control in the hands of the holder.*

Verifiable Credentials – Underneath it all



This is novel technology *— it is privacy preserving and places the control in the hands of the holder.*

Verifiable Credentials – A High Level of Digital Trust



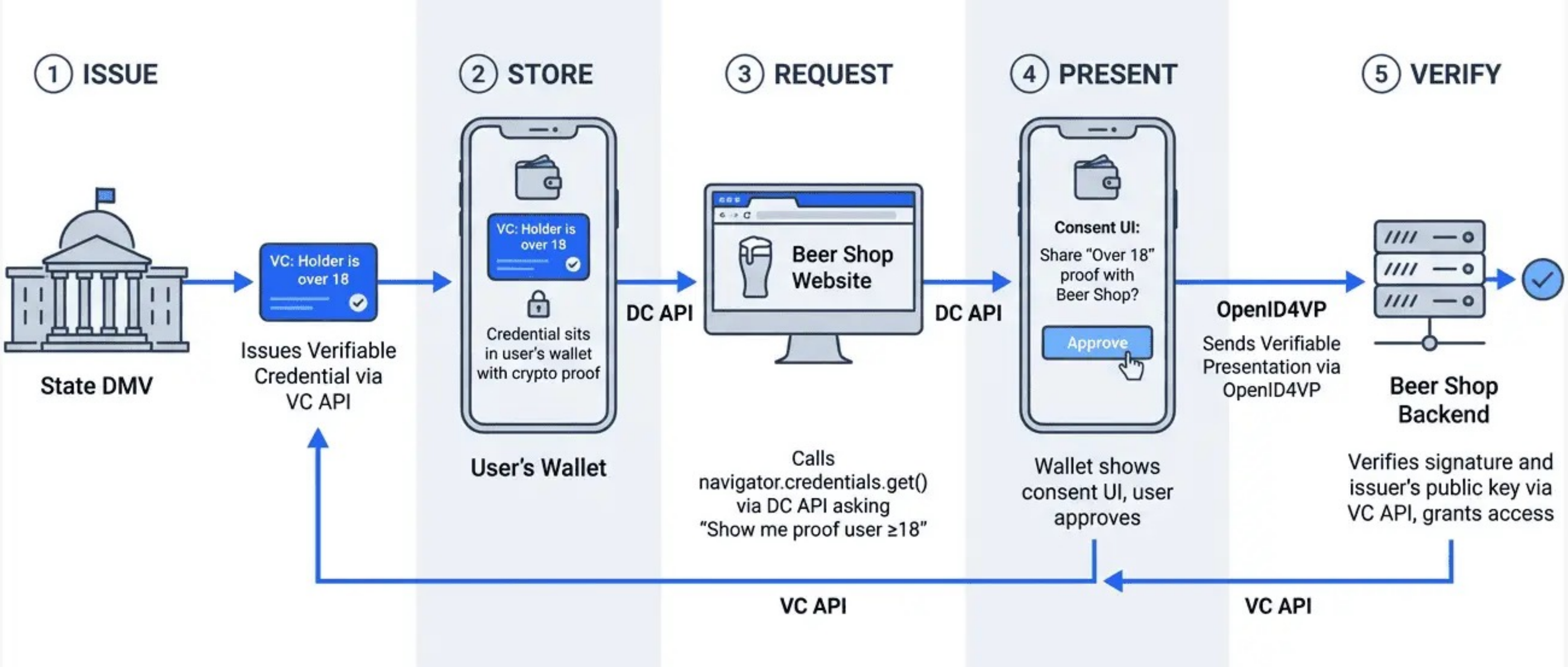
This is novel technology *— it is privacy preserving and places the control in the hands of the holder.*

04

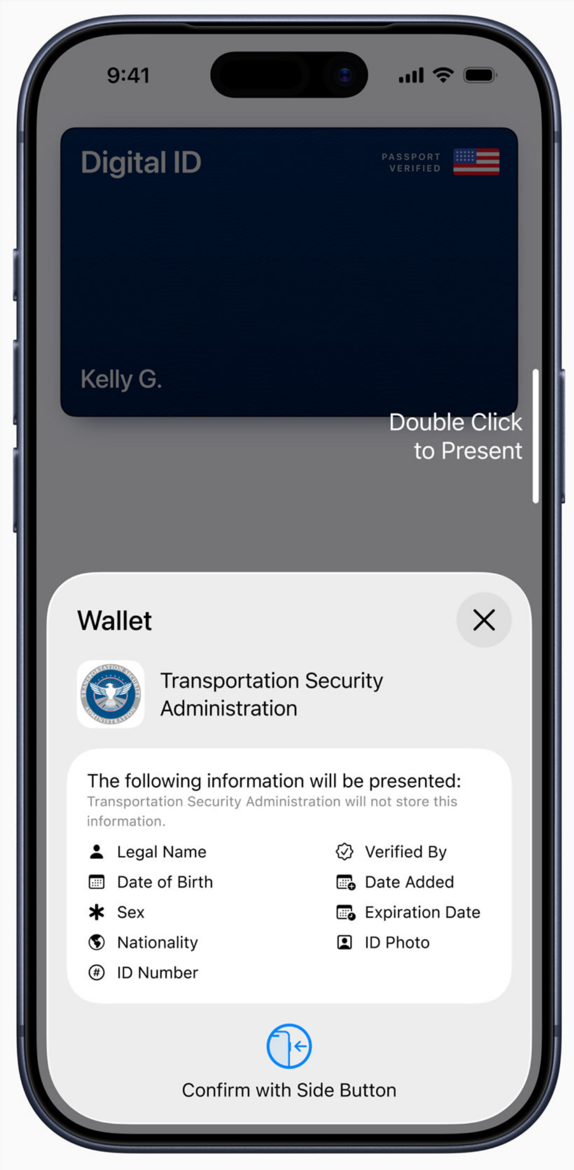
The Industry is Ready

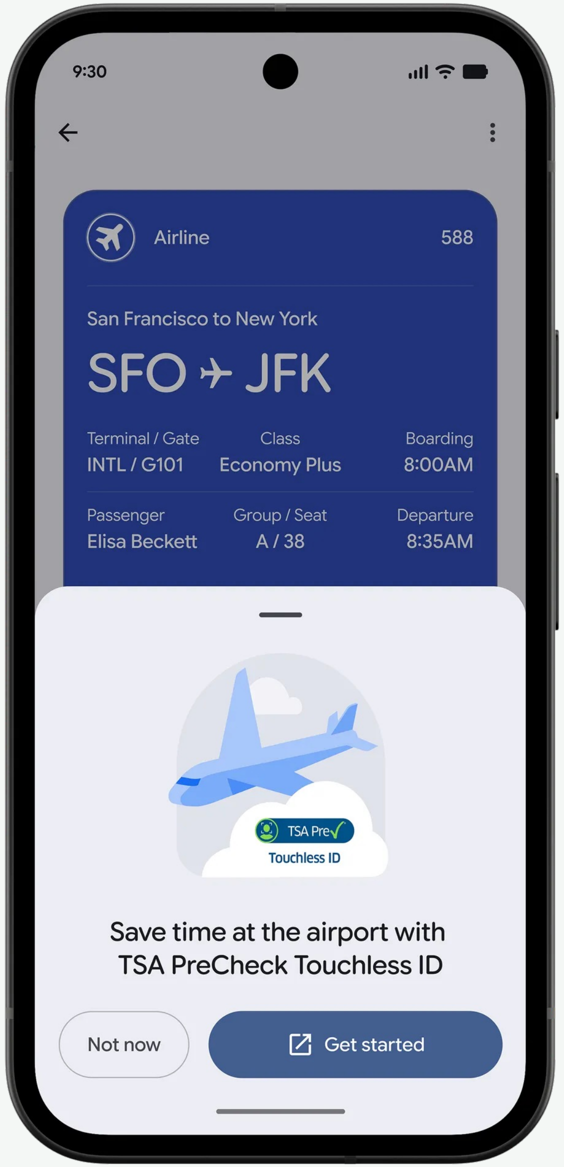
All transactions on the internet are remote — and we have no remote identity. The Internet offers anonymity and no reliable traceability. It is not possible to definitvly identify actors.

Apple Safari and Google Chrome integration



__This is novel technology__ — no identifier in history has ever presented with these properties.





Wallets

This is novel technology *— no identifier in history has ever presented with these properties.*

12th International Interoperability Test Event & Showcase

- Hosted by NZTA and DIA
- 16th to 21st November 2025
- 20 organizations
- 8 countries
- 53 ISO compliant implementations
- 19 different holders
- 16 proximity readers
- 17 remote readers

New Zealand is moving at pace*— we are integrated into technology progress around the globe.*

05

New Zealand’s Journey with Digital Identity

New Zealand is actually roughly in lock-step with its overseas partners – Australia, United Kingdom, Canada, United States and the European Union.

New Zealand’s Journey

From Cabinet decision to a mobile driving licence — six years, one gap

Foundations
2020 – 2024

Aug 2020

Cabinet backs a legislated Trust Framework — RealMe can only serve government

Apr 2023

Digital Identity Services Trust Framework Act passes

Jul 2024

Act commences, Authority stands up — accreditation is voluntary

Rules and reach
2024 – 2025

Nov 2024

Rules name W3C VC, ISO 18013-5 and ISO 23220 — all “latest published version”

May 2025

NZ Verify reads US and Queensland mDLs — not NSW or Victoria

Jul 2025

Issuer tracking banned — NZ outlaws “phone home” before ISO deletes it

Build
2025 – 2026

Jul–Nov 2025

Dave Clark NZ and MATTR appointed; MATTR wins the issuance platform

Nov 2025

Wellington hosts the 12th International Interoperability Test Event

Dec – Mar

govt.nz app, wallet and issuance platform go live

Now
2026

Jan 2026

First accreditation: NEC — still the only one

Apr 2026

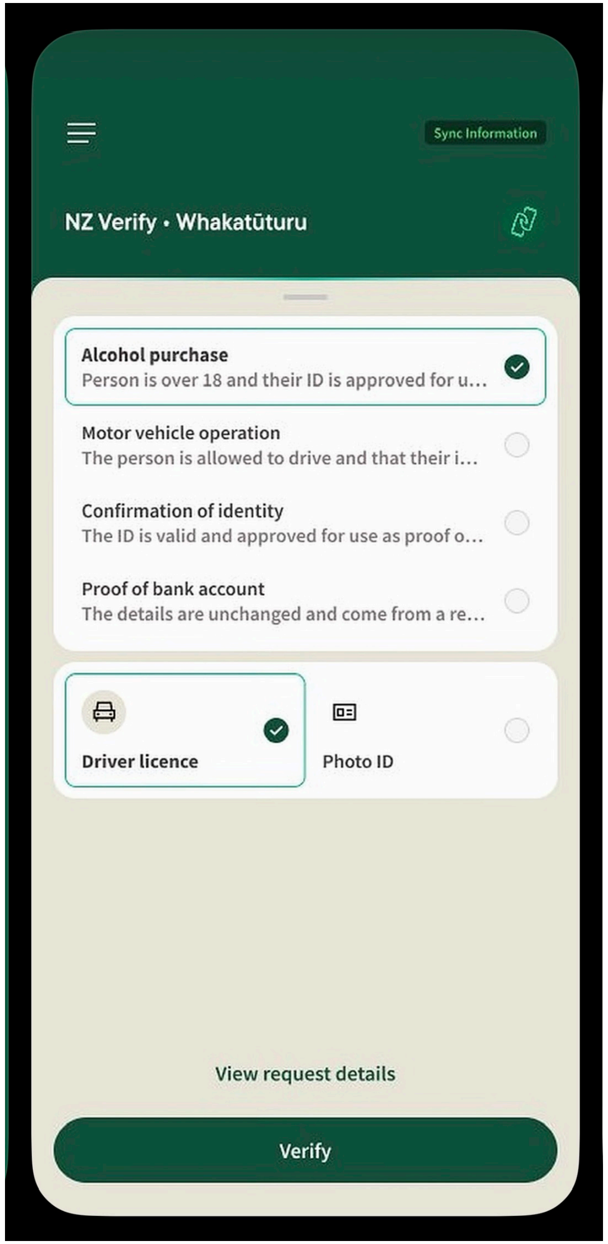
GDDA established; digital identity moves to the Public Service Commission

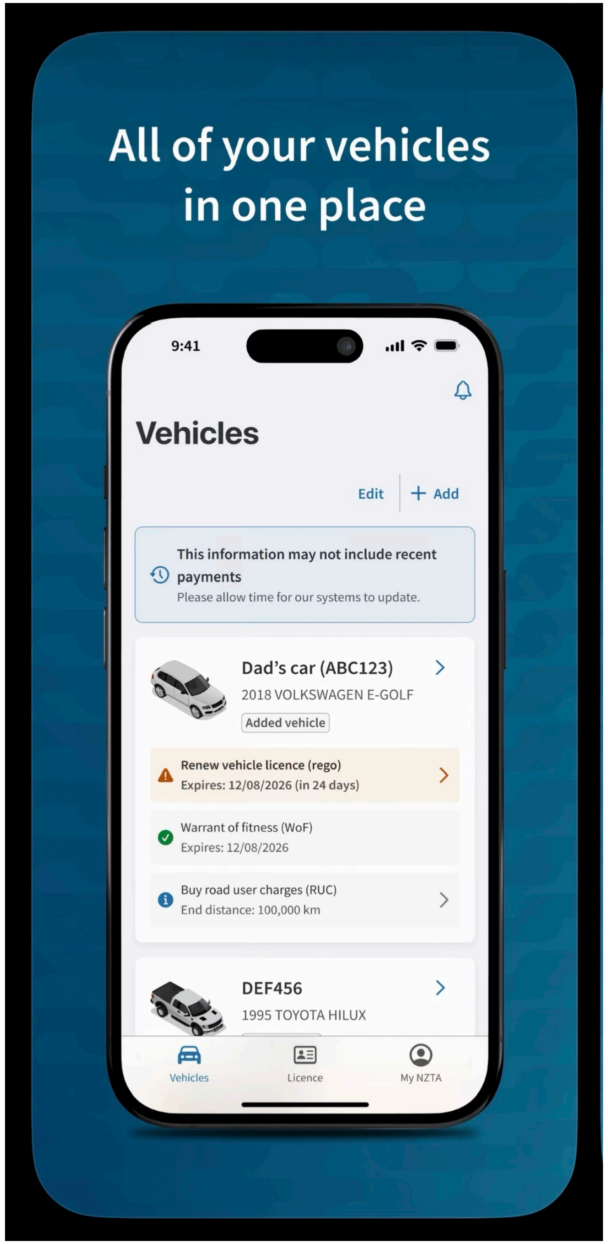
May–Aug

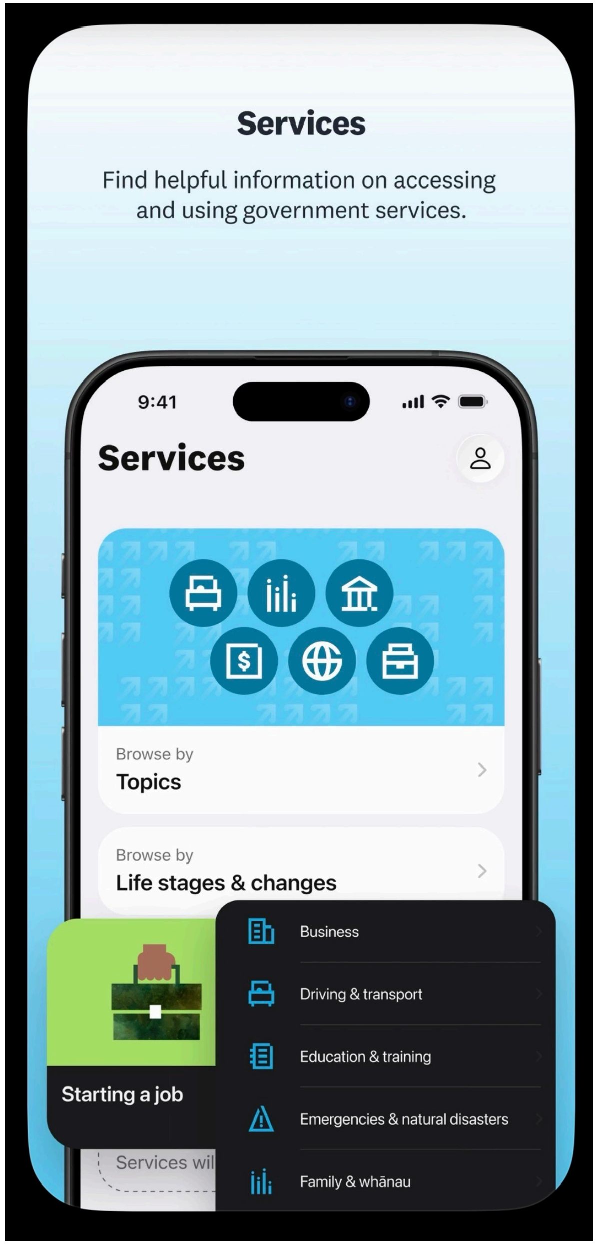
Licence made lawful; NZTA consults to 12 Aug; delivery targeted end 2026

***We are ready for Digital Identity and Digital Trust** — all that is missing is – you.*

New Zealand’s Journey







06

This is where you come in – at Government.

With digital identity we suddenly have a mechanism to create accountability on the Internet and reenable lawful behaviour – if necessary – enforce it. It needs you – we need appropriate laws, regulation, adaptation, technology support.

Reframing the status quo – Scams

- With a universal Digital Identity system scams become a non-issue.
- The opportunity vanishes. The end to this class of crime.

- Email based scams.
- TXT based scams.
- Phone based scams.
- Call centre scams.
- SIM swapping scams.
- Video Conferencing Identity

Reframing the status quo – Protecting our Media

- Digital Identity and Digital Signatures can provide a proof-of-origin.
- Posts on Social Media become traceable.
- Social Media companies can be charged for and be held accountable for content that they replicate.
- The entire discussion about how to fund our media – vanishes.

Reframing the status quo – Deep Fakes and Evidence

- Digital Identity and Digital Signatures can provide a proof-of-origin.
- We can enforce signatures on all photos that are posted.
- It will become trivial to tell a genuine photo from rendered one.
- It will be obvious who conducted fraud.
- We can hold criminals to account.
- With automation.

Reframing the status quo – Social Media Ban

- With a universal Digital Identity system age verification would be come “the new normal”.
- We wouldn’t need “new laws” or a debate about a “ban”.
- We would be in a position to regulate what different age cohorts are permitted to be exposed to.
- We would be in a position to radically enforce it.
- It would become a natural part of the framework that we deploy.

Reframing the status quo - NetSafe

- With age verification in place and working automatically across media, the role of NetSafe would fundamentally change.
- They would be much much more effective in what they can actually achieve with the resources they have – protect the vulnerable youth.
- The opportunity for criminals fades.

Reframing the status quo – Know Your Customer (KYC)

- Financial services and Insurance industry are required to have this process.
- With a universal Digital Identity system KYC becomes almost trivial.
- The opportunity for fraud vanishes.

Reframing the status quo – Anti-Money Laundering (AML)

- With a universal Digital Identity system AML becomes straightforward.
- Real estate sales/purchase is much much easier and cheaper.
- There is a High Trust in each transaction.
- There is no need to store photocopies of all your identities (passport, drivers license)
- There is no opportunity any more for criminals to break into systems.
- An important threat to our society simply vanishes.

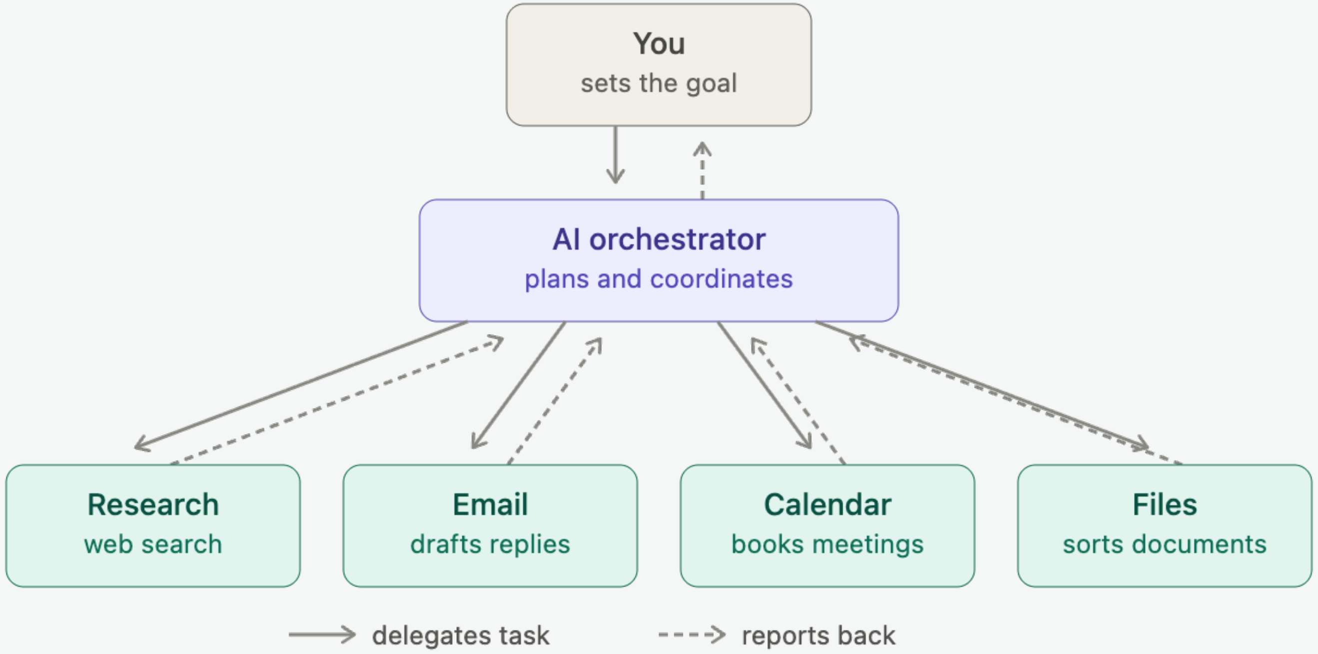
Reframing the status quo – MBIE NZBN + IRD TAX

- Accountability becomes straightforward.
- Nobody can highjack your identity on the NZBN.
- Directors and Shareholders are clearly identified.
- Running a Trust is significantly simplified.

- (relationships with your professional trustee significantly simplified)
- (relationships with the IRD are significantly simplified).
- (relationships via XERO are significantly simplified)
- (relationships with the accountant are significantly simplified)

- Impossible for criminals to break into these systems/relationships.

Reframing the status quo – AI and AI agents



- We cannot have good deployment of AI – and AI Agents – without Digital Identity
- Consider these:
  - Booking flights
  - Entering a contract
  - Getting married

***Digital Identity recreates the rule of law** — it enables to hold people accountable for their actions.*

Digital Identity reestablishes the rule of law.
Digital Identity creates protections for everyone.

FIRST KEY POINT OF THIS TALK

Reframing the status quo – Digital Contracts

– The European Union is making a big push into this direction.

– The eUDI wallet is targeting contracting as the next phase after 2026.

– The European Union is of the strong believe that European "Trust" will fuel Europe wide business transactions as you don't need to spend an excessive amount of time "flying around" and "building trust" with partners in other parts of the European Union – you can simply sign a contract and rely on it.

– New Zealand is well advised to follow in the footsteps of this development if we want to participate in this upswing of trading based on Digital Trust.

Reframing the status quo – Digital Currency

- European Union has already foreshadow their next steps.
- They are going to continue the work beyond the eUDI wallet.
- Digital Euro is squarely on the cards before 2030.
- Announcement by Christine Lagarde, President of the European Central Bank.

- Removes even more opportunities for criminals and state sponsored actors.

Reframing the status quo – The Economy

Research and publications reveal:

High Trust creates High Speed.

High Speed creates a Vibrant Economy.

(think about all the online shopping you do).

High trust is the key to a modern digital society.
High trust means high economic benefit.

SECOND KEY POINT OF THIS TALK

KAIMAI

SECURITY

“lead this way”

Questions?

Joerg Micheel
contact@kaimai.org
kaimai.org