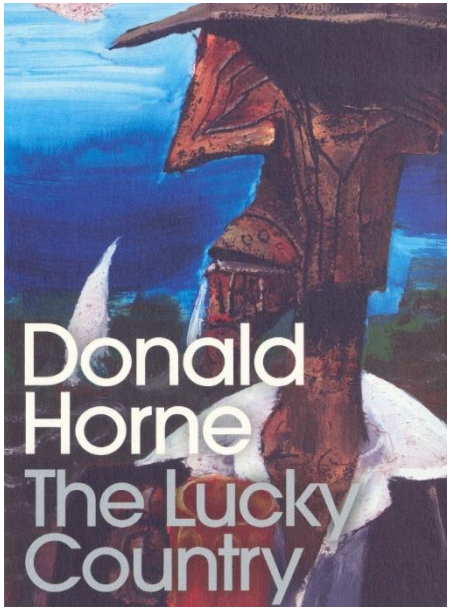
FIDO and the Future of Australian Digital ID

FIDO Alliance Melbourne Seminar

Stephen Wilson
Lockstep Consulting
February 7, 2025

fido™ ALLIANCE | simpler stronger authentication

Digital ID in Australia



- **Federated model by default (2014)**
- **myGov Single Sign On**
- **myGovID mobile app**
- **Trusted Digital Identity Framework (TDIF)**
- **Australian Govt Digital ID System (AGDIS)**
- **Mobile Driver Licensing (mDL)**

The state of Digital ID in Australia has evolved over more than a decade. Federated identity has been the default approach since the Murray Report on the Financial Services sector in 2014. The most prominent example of Digital ID has been *myGov*, designed for accessing Commonwealth government agencies. The aim of extending *myGov* to the states and private sector informed the TDIF hub architecture. AGDIS brought new legislative backing in 2024 and made "Digital ID" synonymous with *myGov* (now *myID*). The ISO 18013-5 based mDL infrastructure, being built by Austroads, remains separate.

Thinking about AGDIS

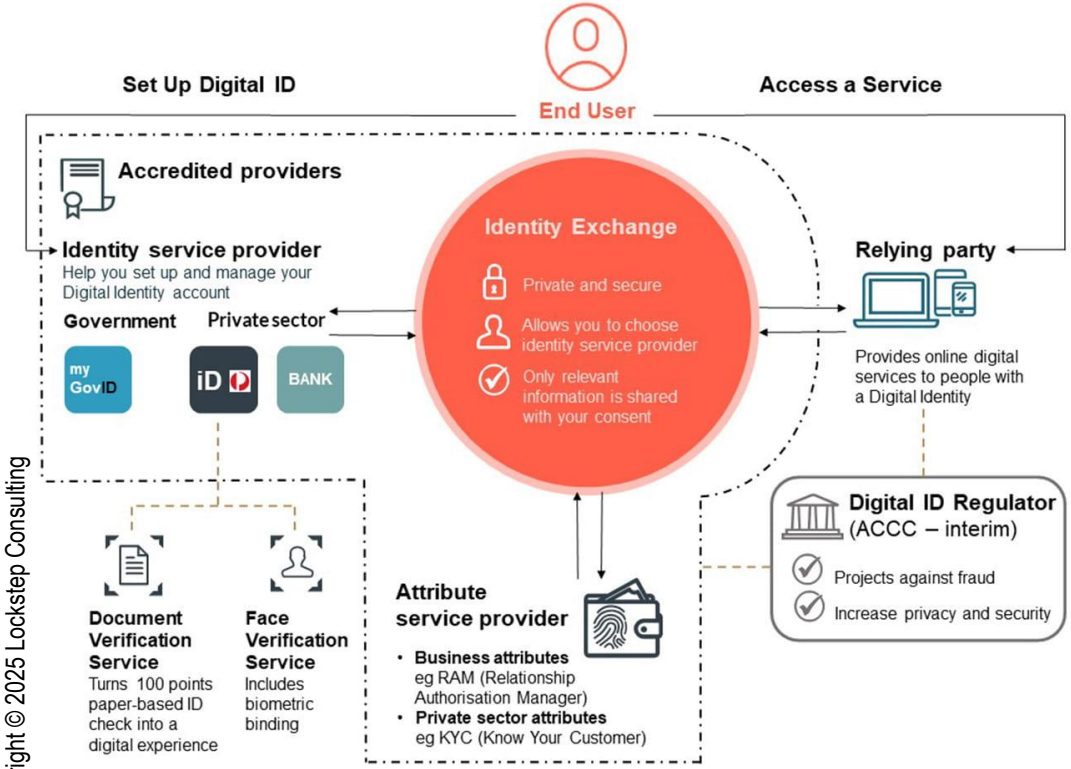
Digital ID: *a distinct electronic representation that enables the individual to be sufficiently distinguished when interacting online.*

"Set it up once, then reuse it to prove who you are."

AGDIS provides a nice broad definition of Digital ID. It *could* encompass digital versions of extant driver licence, Medicare, tax file, provider numbers etc. But what the government really means is a *particular* ID, namely *myGovID* now known as *myID*.

The mental model of "Digital ID" is more about UX than technology; AGDIS is constructed around a particular way of conducting yourself online. AGDIS explicitly expects that citizens will be comfortable with (and will seek out) a new general purpose Digital ID. *MyID* is a discrete product, to be available from a small number of approved providers, with which the customer will have a new account. There will be a choice of *myID* providers, though the basis for making a selection is not clear.

“Identity Exchange”



Picture credit: Ashurst, https://www.ashurst.com/en/insights/australias-digital-id-act-and-a-new-trusted-exchange-tex-an-update-and-a-deep-dive

Digital ID proponents are quick to stress that there will be more than one ID but they really do envisage one uniform type of ID. Borne out of the *myGov* Single Sign On, the identity exchange was architected to allow users who might start with an ID from say Centrelink to use that same ID to access Medicare (or vice versa). There is a tacit assumption that each Relying Party wants to know the same things about every user.

From there the idea naturally emerges that your ID might just as well be issued by a bank or commercial “Identity Provider”. And equally, private sector organisations could recognise the ID for their own logon purposes.

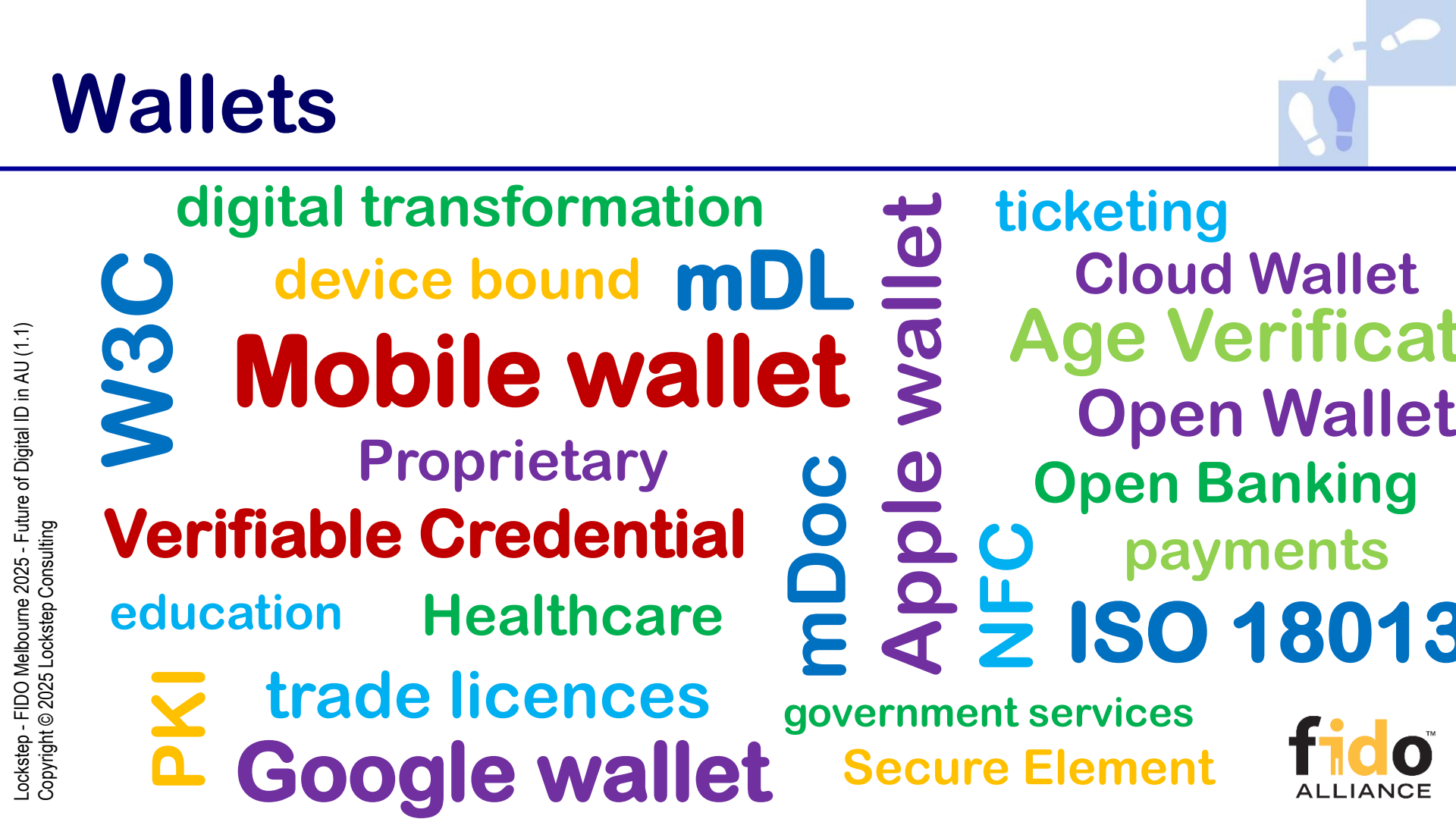
The exchange is premised on the equivalence of all IDs issued within a sort of monoculture. This is what some people call “interoperability”.

Verifiable Credentials

- Provenance
- Proof of Possession
  - i.e. Verifiable Presentation
- Presented peer-to-peer, verifiable on their face
  - i.e. “decentralised”
- New standards

Despite the fresh interest and new standards, verifiable credentials have been in use for decades. SIM cards and chipped credit cards provide digitally signed proofs of a user’s account details. I don’t make this point as a historical curio but to stress the profound change brought about by smart payment cards especially. They replaced plaintext account details with cryptographic proofs of origin and customer control and thus put an end to almost all skimming and card present fraud. We could do the same again to combat all identity crime.

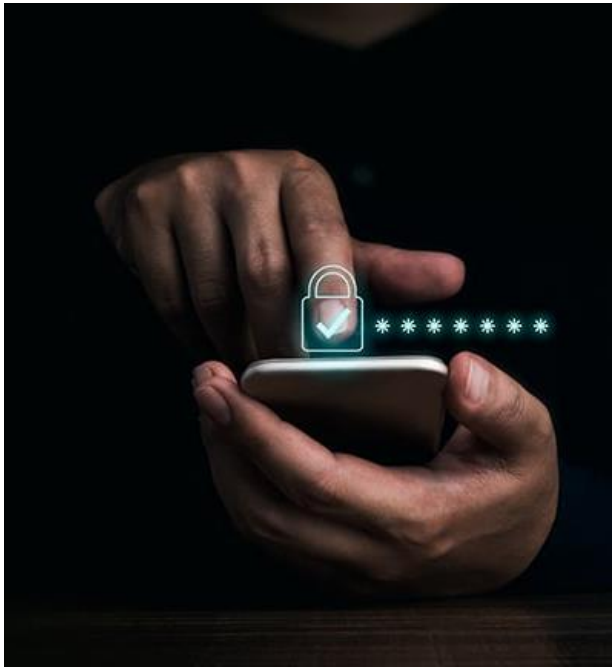
Wallets



The FIDO Alliance

- Leveraging personal cryptography to eliminate passwords
  - pivot from plaintext authentication to digitally signed proofs
- Not about identity but *authentication*.

The FIDO Alliance



The FIDO Alliance is the most impactful digital identity initiative of all time—except it has very little to do with identity. It was founded in 2013 by a set of companies that saw the security potential in the spread of strong cryptography and security features in smartphones. It's often said that a smartphone today has more computing power than the entire NASA space program of the 1960s; more's the point, a smartphone has more cryptographic power than the whole NSA in the 1990s. FIDO leverages that power. Most users now possess a device that can:

- generate key pairs and securely hold the private keys locally
- lock those keys with a biometric or PIN, and
- exercise the private key to digitally sign authentication signals.

FIDO protocols memorialise a user's registration with a service. Each FIDO registration creates a new key pair unique to the user's device. Next time they come back to a server where they have previously registered, the server can ping the device, check that it's unlocked, do a challenge response against the specific registered key, and thus be sure it is connected to the registered user.

FIDO leaves all registration rules untouched; it doesn't care how a business decides to authenticate its users. FIDO simply sets minimum cryptographic and biometric benchmarks. Further, FIDO metadata provides signals for the server to confirm the device type, authentication strength , and even the state of the device.

Thinking more clearly

- **Identification is not the same as identity**
- **We don't need a new identity but more resilient identification**
- **Feed identification with better data**
- **Harden the IDs we're familiar with.**

Identification and identity are not the same thing. This is not splitting hairs. Identification procedures are almost always local and hardly ever lead to a reusable identity. "Identification" is a loose term for the way one party establishes enough information about another party in order to carry out some sort of transaction.

Every business does it differently, because identification is deeply connected to risk management. And you can't outsource risk management; that's why KYC does not commute.

Every identification is just a *sample* of your identity. It's only an approximation of who you are — and that is by design.

"Identity theft" is a crude emotive term for digital impersonation, where plaintext data about you is obtained and replayed on unsuspecting RPs. We cannot solve "identity theft" with more identity; rather, we need better quality data. KYC would work fine online if we just gave it better data.

Learning from FIDO

- **Eliminate plaintext**
- **Put authentication (WHAT) ahead of identity (WHO)**
- **Make all important data verifiable**
- **Conserve relationships; leave RPs free to identify as they see fit.**

FIDO recognises that each user has a number of accounts because they access range of digital goods and services, and each service is unique. Different services need to know different things about their customers. So, they do on-boarding and identification differently, each according to their business needs and risk appetites. FIDO changes none of that.

In fact, FIDO has nothing to do with "identity"! FIDO protocols were devised on the assumption that every customer service relationship is distinct, with a specific registration procedure.

The authentication problem is simply this: Each time you come back to one of your registered services, how do you securely prove your registration status?

The FIDO solution enables every service to put a strong unique cryptographic key into the hands of each of their users, as a by-product of the registration.

So, FIDO conserves all customer service relationships and avoids the fatal mistake of most federated identity programs, namely the enormous business process reengineering that follows from trying to reuse identifiers across domains, i.e. outsourcing identification.

Thank you

E: swilson@lockstep.com.au
W: https://lockstep.com.au