PUBLIC

Lockstep Consulting
Suite 1301B, 50 Margaret Street
Sydney NSW 2000

# Submission on the Digital ID Bill 2023 Exposure Draft

Stephen Wilson and George Peabody, Lockstep Consulting

October 10, 2023.

## Summary: Australia's digital ID: creating it first among equals

We are being given a once in a generation opportunity to make Australian consumers and businesses vastly safer against identity crime by creating regulations, processes, and solution patterns to make all data better, not just identification data.

Lockstep believes that the Australian Government Digital ID System (AGDIS) will be useful in a wide range of scenarios. But by itself it won't be sufficient for many critical use cases including open banking, account onboarding, and many payments and financial transactions.

The providers of these services need to know more about the parties they transact with than merely "Who are you?". A single ID value will not satisfy the question of "What do I need to know?". In other words, adding yet another identifying credential won't meet the goals of the legislation.

In this submission, we reframe the concept of "digital ID" within the larger context of today's technical tools, the realities of consumer adoption, and the true needs of relying parties. We explore where the AGDIS is laying the correct technology and governance foundations, and where more work is needed on making digital ID and other credentials acceptable in practice.

A digital ID needs to be adopted quickly or will fail. To be blunt, history already tells us that a digital ID will fail if it comes to market with features we already know to be obsolete:

- Plaintext presentation of an identifier, rather than device-enabled presentation.
- Forced changes to relying parties' existing identification rules.
- A lowest common denominator approach to consumer technology.

A robust commercial ecosystem is needed to manage, switch, and distribute the digital ID along with other verifiable credentials that are already coming onto the market.

## What is digital ID actually for?

Digital identity has been a difficult field for decades, and the very idea has come to mean different things to different people. The language used to describe digital ID is often something like this:

- From the individual's perspective, it's to "prove who you are".
- From a business's perspective, it's to "prove who this person is".

The language isn't quite right. "Prove who you are" can be a confronting proposition for some marginalised people or individuals without full documentation. For others, it's a matter of principle that the question goes too far.

More importantly, it's actually quite uncommon to need to prove *who* you are. In March 2023, NAB convened a digital identity roundtable, and published the following observation:

> *Individuals rarely need to prove their identity. Rather, in most cases, they need to prove they possess an attribute for a particular purpose (i.e. I am over 18 years old and therefore legally allowed to purchase alcohol, or I am a licensed fisherperson and entitled to fish in these waters).* https://news.nab.com.au/news/digital-id

Lockstep contends that this is a critical distinction, not merely a linguistic nicety. Digital ID will affect almost every single individual and business in the country, so let's strive for fresh precision.

## What do we really need to know?

In many scenarios, when trying to work out "who someone is", individuals end up revealing too much information. The plague of data breaches has demonstrated the harm to everyone concerned.

The question should always be: *What do we really need to know about this person?*

Specific attributes are the basis of sound decision-making. The range of attributes is wide:

| | | |
|---|---|---|
| *Trade qualifications* | *Professional memberships* | *Residential address* |
| *University enrolment* | *Driver licence* | *Licence class* |
| *Organ donor registration* | *Purchase order authorisation* | *Health test result* |
| *Vaccination status* | *Medic Alert* | *Residential status* |
| *Voter registration* | *Commercial vehicle licence* | *Health insurance coverage* |
| *Date of birth* | *Over 18 years of age* | *Relationship to another* |
| *Passport number* | *Medicare number* | *Senior Citizen Status* |

Being *precise* about what we need to know is one of the most basic principles of *Privacy by Design*, because from the outset this mindset helps avoid knowing too much.

Lockstep suggests that digital ID is best thought of in terms of:

> *Rules, tools, and solution patterns that help parties prove the things they need to know about each other when working together digitally.*

With this framing we do not seek new or changed definitions. Rather, we suggest that careful use of plain language will help everyone better understand what the AGDIS should come to provide.

One of the government's primary objectives in providing digital ID is to replace the presentation of plaintext IDs such as driver licence, passport, and Medicare numbers with a digital token representing the fact that those numbers have been verified.

As Minister Katy Gallagher said to the AIIA forum in Canberra in September, "Importantly, digital ID is not a card, nor a unique number, nor a new form of ID… It's just an easy way of verifying who you are online against existing government-held identity documents without having to hand over any physical information."

So when an individual presents their digital ID from an approved digital wallet — the need for which we'll explain shortly — a relying party can be sure of the person's identifying details without needing to see those details for themselves.

The idea of *proving the things you need to know about* a counterparty covers most important use cases for digital ID.

- *Identification* is performed by an organisation when it onboards a new customer, member, employee, or partner. Identification is performed by banks on new and existing customers, anti-money laundering (AML) reporting entities, employers, and universities on new students. Identification almost always boils down to verifying certain facts about someone.
- Every organisation does identification differently. Even in highly regulated sectors where we might expect identification to be standardised, organisations can find it difficult to accept identification done by others. Know Your Customer (KYC) in banking is notoriously non-portable.
- Proof of age has become an archetypal digital ID scenario, where the subject wishes to prove only that they are at least X years old, without needing to reveal any additional detail.
- Entering into new rental agreements.
- Logon (or Single Sign On) is a special case where a service needs to be sure that the user seeking to access the service is truly a registered user, in possession of an appropriate logon credential.

Being careful and rigorous with *what you need to know* also highlights other important design considerations, such as *proof of possession*. That is, when dealing with someone online, typically remotely, we generally need further cues to be sure that a credential being presented is in the right hands.

When using a credit card or ATM card, for example, proof of possession is provided by the presenter knowing the PIN or possessing a chip card — essentially a smart device — to present the data.

## What you need to know depends on who you are

Trust is not transitive. If Alice trusts Bob, and Bob trusts Carol, it does not necessarily follow that Alice trusts Carol. Everyone has their own interests and risks.

Every entity is subject to risk and conducts risk management. Moreover, every business is supposed to handle risk management on an individualised basis, in line with its own unique context, business goals, processes, leadership, and stakeholders. All these factors shape risk appetite and budget to mitigate risk while maximising returns.

This means that the data which one party considers relevant and reliable may not be adequate for the risk management needs of another.

History bears out this observation. Following the Murray Inquiry into the Australian Financial System of 2014, the Australian Payment Council formed a trust framework working group to develop financial sector digital identity rules. They worked for many years on "reusable KYC" as a use case. The goal was that if a customer passed one bank's KYC review, that test would be sufficient to meet another bank's KYC requirements. And yet the working group, comprising the most capable and most motivated digital banking policy experts, was unable to agree on a suitable mechanism. The published *TrustID* framework was silent on KYC.

Reusable KYC failed precisely because risk management is highly specific to each business.

Therefore, we submit that in the longer term the AGDIS should allow for additional finer-grained or customised attributes about individuals to be digitally verifiable. This would in turn allow for these many variations in what different parties need to know about each other.

## Focussing the legislation's goals

The legislative goal should be to get reliable data into the hands of the relying party, or its agent, so that the relying party can make the appropriate decision based on its own risk assessment parameters.

That reliable data should therefore come from verified credentials and the metadata that describes each of them.

A single credential, regardless of the source, will be insufficient — until proven otherwise — to address the myriad risk management needs of citizens, enterprises, and government itself.

## Verifiable credentials must replace plaintext presentation

All identity-related crime today exploits the weakness of plaintext presentation of personal details, often typed in by end users, which are just copies of pieces of data. There is often no way to validate and verify those credentials against the credential source.

We have built a massive web of databases, each containing copies of government-issued data, mostly self-asserted by the true credential holder as well as fraudsters. The result is redundant, error-prone, and often biased data being used for decision-making and risk assessment.

A *cryptographically verifiable credential* is essentially a formatted statement about a subject (an individual or an entity) and an attribute about that subject, digitally signed by an issuer that is recognised as authoritative about the attribute.

Special-purpose verifiable credentials have been used since the 1990s in SIM cards for verifying mobile phone subscriber details, and since the early 2000s in EMV (chip-and-PIN) cards for verifying bank account details.

The banking and card industry put together the EMV chip standard a quarter of a century ago to enable the transition from plaintext magstripe cards to the device-assisted presentation of customer details. This technical advance, along with liability guarantees, put a stop to criminal carding and restored trust in card payments.

Now general-purpose verifiable credential standards are becoming available for conveying other attributes for a broader range of use cases.

Bearing in mind how fraudsters can misuse plaintext details about their victims to open new accounts, imagine the power of discernment possible if a relying party could know with certainty that an email address just entered was created 14 months ago, or that a utility account number being presented has been associated with a single physical address for seven years and that it has been paid from the same bank account for as long.

The technology upgrade needed to achieve this can be appreciated as an evolution of data presentation technology, from *plaintext* to *device-assisted*.

Why now? As recent breaches confirm, citizens judge their driver licence, passport, and Medicare numbers to be as important as their payment card numbers. Their everyday bona fides need the same sort of protection provided by EMV chip cards.

There would also need to be an upgrade of credential handling.

Historically, issuers create account numbers, database index values, for legibility purposes, to label and identify their customers and stakeholders. The next, necessary step is to provide those identifiers, accompanied by their metadata descriptors, in digital wallets, to assure relying parties of data provenance.

Since the major credentials today (such as driver licences, birth certificates, and Medicare numbers) are issued by government, government agencies need to reframe and expand

their role as data custodians, and drive a similar shift from plaintext credentials to digital credentials.

This effort will be challenging, but we should be encouraged by the comparable advance made in payments.

## Device-assisted presentation is already state of the art

Digital wallets are now commonplace for device-assisted presentation of critical personal data and credentials. The vast majority of people already have smartphones, and a variety of alternative media is available to serve the needs of those for whom smartphone technology is not an option.

All of these present a user's digitally secured data to a relying party's system, be that another device, a web server hosting a web form, or a merchant terminal.

As we saw through the COVID pandemic, smartphones are the safest option for delivering secure digital credentials and targeted services to the population at large.

Lockstep supports the drafting of the legislation in the usual technology-neutral way. Nevertheless, it is beyond any doubt that the smartphone digital wallet now represents the state of the art, and an essential benchmark for consumer safety in digital transactions.

Smartphones have delivered complex security and safety technology to almost everyone:

- secure element memory (aka enclaves) to protect stored credentials;
- biometric or PIN lock to ensure the device is in the right hands; and
- in-app presentation ("click to pay" by virtual credit card, for example) to smooth the user experience.

The AGDIS could now take consumers from click to pay to "click to present" their digital credentials to any participating relying party.

However not all wallet architectures are equally secure. We expect that the AGDIS rules and standards will consider minimum wallet functionality as part of the trustmark specification.

## Enabling the operator and commercial ecosystem

Lockstep understands the government's desire for a robust commercial ecosystem to provide the solutions and services to support the AGDIS. Yet so far there is little clarity in the legislative environment about fostering commercial participation in digital ID.

Liability shifts and "hold harmless" status are very useful levers, but more direct economic incentives may be necessary.

It has to be said that while many decry compulsory government requirements, it is also true that nothing moves a market like a government mandate.

We mention this because enterprises view their risk-management efforts purely as costs to be managed and minimised. If a verifiable credential can be used to increase enterprise revenues then uptake will be accelerated. Of course, that may run counter to privacy goals and the push to moderate Big Tech.

Only government should influence, or direct, the overall development of a sustainable economic model to encourage commercial participation. There is no need to mandate citizen use of the AGDIS. We can be confident that consumers will continue the move to mobile and digital experiences. But there may be a need to incentivise business adoption of digital ID, and thereby cultivate the desired commercial ecosystem.

## The need for an acceptance and distribution network

A missing facet of all discussions to date around digital identity, wallets, and verifiable credentials is *acceptance*. How do relying parties (RPs) come to be ready to accept an identity or credential? How do RPs know what to expect? How can they tell which credentials are fit for purpose in the particular context?

Verifiable credentials don't verify themselves. New digital wallet technology is necessary, but not sufficient. RPs must also have rules in place.

In plain language, *What will it take for a relying party to declare "Digital ID Accepted Here"?*

(Note that not all digital IDs are going to be accepted by all relying parties. The AGDIS is not going to be compulsory for citizens. RPs will insist on retaining the autonomy to determine which IDs are necessary for its specific risk management needs.)

The greatest challenge for digital identity systems in Australia for the past 20 years, and internationally, has been acceptance. Even with in-principle agreement that digital ID is a good thing, even with legislation, digital IDs are not accepted automatically.

It is worth remembering that a digital ID acts as a special type of electronic message. As with any electronic message, digital IDs must interoperate at both the "technical level" (computer systems must be capable of reading the message) and at the "semantic level" (the meaning of the message must be interpretable). Standards and rules are necessary but not sufficient for messages to be interpretable. Endpoints (relying parties) must have the right software and the right configuration data with which to check incoming digital IDs for fitness for purpose.

Many of these interoperability factors can be rolled up and regarded as *branding*.

*What is it that distinguishes digital IDs which are acceptable to a relying party from those which are not?*

The AGDIS trustmark will be a crucial indication. It must be indelible and it must be machine-readable, legible to relying parties and their software systems. The trustmark should be regarded as metadata that tells a story about the digital ID in question.

The ability to automatically ingest and verify the trustmark boils down to end points being equipped with metadata including cryptographic root keys (and probably APIs) with which to process incoming digital IDs.

This capability is analogous to the way that merchants in a card payment system are equipped to accept certain types of cards. The preparations are made on the merchant's behalf by intermediaries which also provide technical support and contractual support in the form of standardised participation agreements.

## Conclusion

AGDIS has the potential to lead a national transition from reliance on plaintext data presentation to device-assisted credential and data sharing for more than just simple identification.

The current proposal already includes many of the elements needed to make this possible, and the technical components are already commonplace.

Australia's digital ID would roll out as the first credential delivered under this model. Given that, citizens and the private sector would then be able to apply the model to an ever-widening range of credentials.

## About the authors

Stephen Wilson is a researcher, innovator and analyst in data protection. He has been a lead adviser on digital identity to the governments of Australia, Hong Kong, Indonesia, Kazakhstan, Macau, New Zealand, and Singapore, and has been awarded 10 patents. He was a member of the NSW Digital Identity Ministerial Advisory Council over 2021-23. Wilson's consulting clients and projects have included the NSW Digital Driver Licence, the U.S. ID Ecosystem Steering Group, the U.S. Department of Homeland Security, the National eHealth Transition Authority national health PKI, Medicare Australia's healthcare provider PKI, and the W.H.O. digital vaccine certificate. Lockstep is the only Australian company to be awarded a commercialisation contract by the U.S. Dept of Homeland Security (for a mobile digital credential wallet).

George Peabody is a payments adviser, writer and entrepreneur, based in Boston. He consults across a range of business and technology areas with emphasis on mobility, merchant risk, online and offline data security, and digital identity. An accomplished communicator, Peabody was the producer and host of Glenbrook Partner's 100+ episode podcast series, *Payments on Fire®*.

In 2013, Peabody and Wilson published *Fractional Identity: An Alternative to NSTIC and Federated Identity*, which made the case to shift focus from centralised identity providers to contestable attribute providers, foreshadowing today's verifiable credential movement.