PUBLIC

Lockstep Consulting
11 Minnesota Ave
Five Dock NSW 2046
AUSTRALIA

14 July 2021

Digital Transformation Agency

By web submission.

Phase 2 Consultation on Digital Identity legislation

Lockstep Consulting thanks the DTA for the opportunity to make this response to Phase 2 of the Digital Identity legislation consultation, and the Position Paper (*digital-identity-legislation-position-paper-2021-06-10.pdf*).

Is the need for Digital Identity legislation going to last?

After many years in the making, the TDIF is unfortunately at risk of being overtaken by events. The most important topics in the digital identity industry for some time now have been *decentralised verifiable credentials* and cryptographic *wallets* (to hold end users' private keys and digital credentials). Major global standards are rolling out for these ecosystem elements. And yet TDIF and the Position Paper are silent on the megatrends. Lockstep does understand technology neutrality in legislation, but the DTA's role must span technology leadership as well as regulation.

Meanwhile Australia's state governments are well advanced on digital driver licences and mobile apps. The Service NSW app for one will soon carry driver licences, trade licences, work permits, proof of age, Working with Children checks and so on. State ministers have flagged extensions for digitised COVID vaccination status and test results.

A *de facto* standard for digital wallets will probably emerge amongst the states, independent of the Digital Identity legislation. An interoperable state government wallet standard could perhaps be aligned with the W3C *Verifiable Credentials* draft and would almost certainly migrate in the medium term to the ISO 18013-5 mobile driver licence (mDL) standard. The user experience of presenting everyday digital credentials will be *exactly as easy as waving a credit card or mobile phone*. Will Australians then need *MyGov* for Medicare and TFNs, alongside their broader purpose data wallets which will service everything else? We must ask: What need would the Digital Identity Legislation meet?

If DTA's goal is to "enable Australians to prove who they are online" then it would be truly transformative if we could simply prove verified facts and figures about ourselves—licenses, IDs, medical certificates, Medicare and other social security numbers, student numbers, work permits, trade qualifications and so on—in a safe, fast, peer-to-peer mode. Why doesn't Services Australia lead in the first instance by making the Medicare Card and similar credentials available in Apple and Android mobile wallets?

Imagine an ecosystem where digital twins of driver licences and government IDs are widely available in standard mobile phone wallets. The ability to "tap" and prove any verifiable credential to a Relying Party is just around the corner. Banks and AML reporting entities would naturally look for simple regulatory approval to perform KYC from mobile wallets credentials. That sort of regulatory reform would be more straightforward and more attractive than a novel new Digital Identity paradigm.

The market failure of digital identity

The elephant in the room for the DTA's vision is the market failure in comparable economies of digital identity, or more precisely, what could be called the *Standard Model of Digital Identity*.

For many years—following the introduction of Kim Cameron's *Laws of Identity* in 2005—digital identity has been imagined to be some sort of good or service able to be traded amongst three archetypal participants: the Subject, the Relying Party and the Identity Provider. These three main actors make up the Standard Model, sometimes augmented by Identity Exchanges and Attribute Providers.

IdPs have been enshrined in Trust Frameworks such as TDIF, and the public-private partnerships of NSTIC in the U.S. and Verify GOV.UK in Britain. And yet not one commercially sustainable IdP was delivered by these programs. With so much demand for digital identity, it is deeply significant that identity provision has not turned out to be a viable business in any free market.

If the Standard Model is indeed a market failure, then this is critical to TDIF because of the explicit assumption that consumers will have a free choice of IdPs and that multiple Identity Exchanges too will come online (to help prevent Digital Identities becoming national identities).

We hope the DTA can reframe its work so it doesn't end up on the wrong side of history.

Sincerely,

Stephen Wilson
Managing Director

By e-mail.

About Lockstep and the author

Lockstep (est. 2003) is an independent research and advisory group dedicated to digital identity, privacy and data protection. Lockstep Consulting has been engaged to provide digital identity advice and analysis on (among others) the Consumer Data Right for the ACCC, the U.S. National Strategy for Trusted Identities in Cyberspace (NSTIC), Australia's TDIF, the Australian Payment Council's *TrustID* framework, the NSW Digital Driver Licence, Australia Post's ID project, Project Gatekeeper, the FIDO Alliance, Service NSW, Service Victoria, SA Health, the AGD's National Facial Biometric Matching Capability, Medicare Australia, the National Authentication Service for Health (NeHTA), the Open Identity Foundation, IBM's blockchain identity product team, and Evernym.

Sister company Lockstep Technologies conducts breakthrough R&D on personal data protection and verifiable credentials. We were contracted over 2016-19 by the U.S. Department of Homeland Security (DHS) through the Kantara Initiative to develop a mobile credentials wallet for first responders. Lockstep is the only Australian company to be awarded a DHS commercialisation contract.

I have long been involved in public policy for digital identity, with deep involvement in numerous trust frameworks, cross-sectoral federations and governance including:

- Trusted Digital Identity Framework (occasional adviser)
- Australian Payment Council TrustID (occasional adviser)
- National Facial Biometric Matching Capability (undertook the first four PIAs)
- Internet Industry Association authentication hub (architect)
- NIST Privacy Engineering Framework (first industry partner roadtest)
- New Zealand govt PKI (accreditation framework for offshore CAs)
- eASEAN (harmonising SE Asian e-signature laws)
- Hong Kong CA Recognition Office (technical lead in the new governance regime)
- The Biometrics Institute Trust Mark (research, feasibility study and pilot design)
- Australian banking sector *Trust Centre* (smartcard technology analysis)
- Webtrust for CAs program (Australian accounting industry representative)
- NATA IT testing Accreditation Advisory Council
- NeHTA–NATA health software accreditation program
- numerous Gatekeeper PKI accreditations (Certificates Australia Pty Ltd, Medicare Australia *HeSA*, the ATO and the National Authentication Service for Health).

I was a member of the National Blockchain Roadmap Cyber Security Working Group (2021), the Australian Law Reform Commission Developing Technology Advisory Sub-committee (2007-08), the U.S. NSTIC Privacy Committee (2012-14), the National Electronic Authentication Council (1998-2001), the Federal Privacy Commissioner's PKI Reference Group (2000), the APEC eSecurity Task Group (1998-2001) and the Gatekeeper Policy Committee (2004-14), and chair of Smartcards & Information Security Australia (2005-07).

More information is available at http://lockstep.com.au/about/identity.html and a broad selection of our research is collected at http://lockstep.com.au/library.html.