Lockstep Consulting
11 Minnesota Ave
Five Dock NSW 2046
AUSTRALIA

27 October 2021

Digital Transformation Agency

By web submission.

Trusted Digital Identity Bill package (Phase 3)

Lockstep Consulting thanks the DTA for the opportunity to make this submission on the proposed Trusted Digital Identity legislation.

I am happy for the submission to be made public.

Lockstep has previously submitted detailed analyses of the proposed Trusted Digital Identity (TDI) regime [1][2], and noted shortcomings and concerns including the risk of general purpose digital identity being superseded by state-based digital wallets, the market failure of commercial Identity Providers here and overseas, the fragility and ambiguity of the term "identity", and the conspicuous industry-wide trend away from general purpose identity towards specific digital credentials. We will not traverse these issues yet again, except to observe that we still see no sign of tangible steps to support a choice of Identity Providers and Identity Exchanges. Instead, this submission will focus on the question of digital credentials which we find that TDI has not yet properly embraced.

Executive Summary

The Trusted Digital Identity Framework, system designs and draft legislation seem oblivious to the international trend towards (and indeed formal standardisation of) Verifiable Credentials, and decentralised architectures. Instead, the TDI seeks to institutionalise a particular Single Sign On system for Commonwealth government services (namely myGov) and extend it to state governments and business.

Embedded within the TDIF is a particular authentication architecture featuring a central identity exchange. There is an express assumption that Australians will come to have a choice of identity providers and that the system will have more than one identity exchange. This assumption is central to privacy, and has been called out as critical to "the entire model" by at least one PIA.

The centralised identity exchange could potentially see all identity usage, rendering the TDI as effectively an Australia Card. There is mention in passing of "technical blinding" in the bill package, but this architectural pattern is not substantiated. Lockstep in fact contends that technical blinding is still an unproven technique with novel legal implications and therefore substantial risks to business acceptance and take-up.

The need to embrace Verifiable Credentials

The TDIF has not kept up with the Verifiable Credentials movement. Within TDI, "credential" in fact has a special technical meaning, namely "technology used to authenticate a user's digital identity" (that is, for example, static passwords and OTPs). This is not the sort of credential that most of the industry is working on or recognises as such.

This special meaning of "credential" creates compatibility problems. Further, the Regulatory Impact Statement describes the Identity Service Provider as "a conduit for the verification of additional information". That appears to make all credentials in the TDI regime *systemically secondary* to "digital identity" which in turn would affect the business processes of real-world credentialling authorities and the very meaning of credentials. Lockstep urges a treatment of digitised credentials as meaning nothing more and nothing less than the fact of holding the corresponding real-world credentials. Hanging digital credentials off digital identity would forces credential providers to adopt arbitrary digital identification protocols, at untold cost.

The market failure of the Standard Model

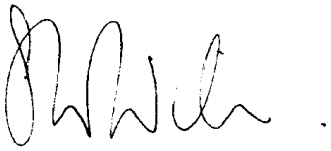
The TDI is based on the Standard Model of Digital Identity—handed down by the "Laws of Identity" in 2005—centred on *Subjects* (aka End Users), *Relying Parties* and *Identity Providers*. Australia—as with in the other Five Eyes jurisdictions—some decades ago decided to let the market sort out digital identity. Since the early noughties, several attempts at identity services, shared infrastructures and authentication hubs have come and gone. We still see no commercially sustainable Identity Providers (as envisaged by the Standard Model) and no significant uptake of independent "digital identities" as such in Australian business. So the Standard Model has proven to be a market failure. Yet the government persists.

Strangely, the digital identity legislative initiatives of Australia and the U.K. do seem to acknowledge something is amiss, and have adopted the broader term "Identity Service Provider" in place of Identity Provider. The language has been hollowed out to mean potentially anything now connected with digital identity provision and management.

Conclusion

Thank you once again for this opportunity to comment on the Digital Identity Legislation. As always, I stand by ready and willing to discuss any of these matters further.

Sincerely,



Stephen Wilson
Managing Director

References

[1]. *Phase 2 Consultation on Digital Identity legislation* Lockstep Consulting, 14 July 2021 https://www.digitalidentity.gov.au/sites/default/files/2021-08/32_lockstep.pdf

[2]. *Proposed Digital Identity Legislation v2* Lockstep Consulting, 29 December 2020 https://www.digitalidentity.gov.au/sites/default/files/2021-01/consultation01-lockstep.pdf

About Lockstep and the author

Lockstep (est. 2003) is an independent research and advisory group dedicated to digital identity, data privacy and data protection. Lockstep Consulting has been engaged to provide digital identity advice and analysis to (among others) the U.S. National Strategy for Trusted Identities in Cyberspace (NSTIC), DTA in the early stages of TDIF, the Australian Payment Council, Project Gatekeeper, the FIDO Alliance, the NSW Digital Driver Licence, Service NSW, Service Victoria, the ACCC CDR program, the AGD's National Facial Biometric Matching Capability, Medicare Australia, the National Authentication Service for Health, the Open Identity Foundation, IBM's blockchain identity service, Evernym and the Sovrin Foundation.

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

Lockstep founder and principal Stephen Wilson is currently a member of the NSW Digital Identity Ministerial Advisory Council, Standards Australia Technical Committee for identification cards IT-017, and the Turing Institute Trusted Identity Interest Group. He was a member of the Australian National Blockchain Roadmap Cybersecurity Working Group (2020-21), the Australian Law Reform Commission Developing Technology Advisory Sub-committee (2007-08), 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).