



Lockstep Consulting
11 Minnesota Ave
Five Dock NSW 2046
ABN 17 582 844 015

20 October 2017

Stakeholder Engagement and Secretariat
Digital Identity
Digital Transformation Agency

identity@digital.gov.au

By email

Trusted Digital Identity Framework

Lockstep Consulting thanks DTA for the opportunity to provide feedback on the Trusted Digital Identity Framework (TDIF).

About Lockstep

Lockstep Consulting provides independent research, analysis and advice in digital identity and privacy. We have been retained from time to time by DTA to provide guidance on the TDIF and privacy training.

We have consulted on identity and privacy to DTA, Medicare Australia, the National Biometric Matching Capability, the National eHealth Transition Authority, VANguard, the Gatekeeper Competent Authority, Service NSW, Vicroads, the South Australia Health PKI, the Victorian Dept of Innovation citizen authentication strategy, the AusIndustry-sponsored IIA Authentication Hub, the Australian banking industry Trust Centre, the US National Strategy for Trusted Identities in Cyberspace (NSTIC), the Open Identity Foundation (OIX), IBM, Infosys, the FIDO Alliance, and three US digital identity start-ups, Confyrm, Queralt and Evernym.

Sister company Lockstep Technologies conducts breakthrough R&D on personal data protection and identity attributes management. Lockstep Technologies is currently developing a mobile attributes wallet for first responders under a multi-part grant from the US Department of Homeland Security. We are the only Australian company to be awarded a DHS identity and privacy program grant.

I have long been involved in public policy for digital identity. I was a member of the ALRC Developing Technology Advisory Sub-committee (2007-08), the National Electronic Authentication Council (1998-2001), the Federal Privacy Commissioner's PKI Reference Group (2000), and the APEC TEL eSecurity Task Group (1998-2001). I am currently undertaking a PhD within the Australian Centre for Cyber Security (UNSW ADFA) on the evolution of digital identity and its component attributes, with application to the Identity of Things and national scale identity infrastructure.

General remarks on the framework

The whole exercise of Trust Frameworks, from government programs like *GOV.UK Verify*, through the OIX white paper, to the TDIF, seem oblivious to the enormous practical difficulty that federated identity has encountered in governments and banking. Despite years of effort, there are still no examples *absent legislation* of a high-grade identity issued in one domain being relied upon for a high-risk transaction in another domain. There are no LOA 3 or LOA 4 Identity Providers servicing the needs of independent Relying Parties. There is no demonstrated business model for high grade IdPs, much less for even newer concepts like “Identity Exchanges”.

We therefore wonder why DTA would believe that the TDIF will succeed, unless legislation is part of the plan. The framework as presented does not provide any use cases, nor does it discuss Govpass. The framework seems divorced from reality.

Lockstep’s considered position, reached through an incomparable body of work, is that the premise of “trust frameworks” and federated identity itself must be revisited. The best progress in identity management internationally is being seen on multiple fronts of the “attributes push”, where the focus is shifting from abstract identities to concrete claims. We point to the FIDO Alliance, the W3C Verified Claims working group, and the IETF Vectors of Trust draft as exemplars of this trend. In particular, we stress that the FIDO Alliance (clearly the most significant and successful identity management initiative ever seen) deliberately focuses on *authentication*, saying little or nothing about “identity”.

Lockstep suggests in all seriousness that the less said about identity, the better.

On biometrics and the FVS

The TDIF (and recent *Govpass* information releases) has built the new Facial Verification Service into digital identity for Australians. Obviously DTA expects that the FVS will be used by various elements of the framework (including commercial entities only vaguely described), to routinely verify selfies of people applying for identities. This use-case seems a very long way from the FVS applications currently in train, which are restricted to matching images held in established government biometric databases (DIBP, AFP, DFAT and state driver license bureaus). There appears to be no discussion in the TDIF of the obvious image quality challenges with mobile phone cameras and web cams. There has been no PIA as far as we are aware; neither do the entities that would be required to agree to the FVS Access Policy and sign the Interagency Data Sharing Arrangement (IDSA) even exist as yet.

Privacy impact assessments are not even complete for the relatively modest use of the FVS across driver license bureaus, where solid checks and balances (and image quality controls) are in place. The extension of the unproven facial verification service into self-enrolment for digital identities is exactly the sort of function creep which will rile civil society.

On the documentation

The documents are all rather sterile. Each opens with formalities typical of a technical standard before providing any introduction to the topic. It would be helpful to have an Executive Summary to explain the point of the exercise before diving into details. We do not believe it's enough to blandly state on a website that it will "make it easier for everyone to prove who they are when using government services online".

Overall the document suite strikes us as underdeveloped. Some documents are only at version 0.01, i.e. initial draft. Punctuation is generally poor, especially in the glossary. There are many errors, especially in the Core Privacy Requirements.

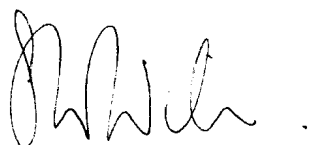
The "conceptual architecture" (TDIF Part 1, Fig 1) is entirely conceptual, and too vague to be analysed. There is no precision in the description of identity providers or identity exchanges. An evidently major part of the architecture – a bus that joins IdPs to the DVS and the FVS – isn't even labelled let alone described. We cannot tell what parameters are passed between these components, or what the rules will be.

The devil in any architecture is in the edges between components, and a precise description of the problem each component is supposed to solve. Identity isn't simply "provided" and consumed. Digital identities are realized through the exchange of attribute data (which help RPs make decisions to accept or reject transactions) and metadata (conferring the provenance and terms of use). Different types of data and metadata apply at different times and in different settings: when enrolling, when attempting real-time access control, when signing or otherwise committing to a transaction, when delegating authority, and when auditing or investigating. We would expect these sorts of matters to be the bread and butter of a "conceptual architecture".

Conclusion

In conclusion, we regrettably feel that DTA has missed a golden opportunity to innovate in digital identity. We have yet to see the high-level notions of "federated-style" identity in the Murray Report reduced to business models for IdPs and RPs, or scheme rules. Meanwhile, major advances around the world in attribute engineering and personal data provenance (which is a more general way to frame authentication) seem to be passing us by.

Yours sincerely,

A handwritten signature in black ink, appearing to read "S. Wilson".

Stephen Wilson
Managing Director
By e-mail.