Submission to the Consultation on Digital ID

Ben Frengley
Independent Security Researcher
ben.frengley@gmail.com

Vanessa Teague
CEO, Thinking Cybersecurity Pty. Ltd.
A/Prof (Adj.), ANU
vanessa@thinkingcybersecurity.com

December 17, 2020

Who we are

Ben Frengley is a recent Master of Science graduate from the University of Melbourne whose thesis (supervised by Vanessa Teague) was an 18-month long investigation of the Trusted Digital Identity Framework, which identified a number of serious security and privacy failings in its design and its existing implementation. The significant findings have already been disclosed to the Digital Transformation Agency and the Australian Tax Office.

This submission contains an extremely brief summary of some of the findings. The full thesis is available at https://bfrengley.github.io/thesis.pdf.

1 Why the TDIF is insecure and what the consequences may be

The Trusted Digital Identity Framework (TDIF) is a high-level design for a federated authentication system. The primary security goal of an authentication mechanism is to prevent malicious parties from logging in fraudulently to others' accounts. A secondary security goal is to maintain the privacy of the identity proof documents and biometric data used to establish identity.

Neither the TDIF's high-level design, nor its implementation by the ATO (myGovID) meet their intended security goals.

- The myGovID system is subject to an easily-implemented code proxying attack, which allows a malicious website to proxy a person's myGovID login and re-use their authentication to log in to the victim's account on any website of their choice. Although detectable by extremely diligent users, the attack is likely to go unnoticed by most victims. A video demonstration is available at https://youtu.be/TgPdVbUbtBM.

  This was disclosed to the ATO in August 2020, but they informed us that they do not intend to fix it.

- The Identity Exchange (IdX) acts as a single point of failure for both privacy and authentication, resulting in an extremely brittle architecture that would allow for large-scale identity fraud if that one component came under the control of a malicious party.[1]

  The Identity Exchange is intended to hide the identity of the Relying Party from the Identity Provider, but fails to do this in the ATO's implementation.

  The implementation of the TDIF in Australia Post's Digital iD does not even appear to use an Identity Exchange at all, which is the fundamental component of the TDIF's design.

- The process for Evanescent Deterministic Identifiers is poorly specified in the TDIF, leaving ample opportunity for insecure implementations that would expose identity information such as Passport and License numbers if the Identity Exchange was compromised. It is not clear that an adequately secure implementation is possible.

More detail on all of these is in Ben Frengley's thesis (Chapters 7, 4 and 5 respectively).[2] The thesis also describes a variety of other errors in the TDIF. Many of the privacy issues described therein, which result from a brokered identity model, were known and published in the early stages of the TDIF's development, so there is little excuse for these issues to still exist in the TDIF. In particular, we recommend a very careful read of the work of **2015:brandao:broker**; the relevance of this work to the TDIF is described in Chapter 4 of Ben Frengley's thesis.

Although we have not examined Australia Post's implementation in detail, it seems to diverge substantially from the TDIF specification, but has apparently been accredited anyway.

2 Recommendations for technical change

The TDIF as currently designed and implemented does not meet its own guiding principles—it is not immediately obvious that a brokered model without technical means to preserve privacy even *can* meet them. We recommend a careful re-evaluation of the priorities of the TDIF, and a consideration of other options which may meet its goals. In particular we recommend the DTA investigates the following alternatives:

Use of a public key infrastructure (PKI)-based system. A PKI-based system, such as those used widely in the European Union, is a promising al-

[1] At the time of writing, a very-large-scale successful compromise of a large fraction of the US government's computers has been reported. It is not plausible that Australia's IT infrastructure is perfectly safe or that the TDIF's systems will be adequately secured, particularly given the value of a successful compromise.

[2] https://bfrengley.github.io/thesis.pdf

ternative to the brokered model.[3] PKI-based digital identity management is widespread and well understood, with published standards for international interoperability. It offers many of the security and privacy benefits that the TDIF aims to have, but with the added advantage that there is no entity who can meaningfully track user activity, as authentication occurs without the direct involvement of a central authority. As such, we believe this to be the most promising candidate to take the place of the TDIF.

Use of a simple, standard, pairwise OpenID Connect protocol instead of a complex brokered model with poor privacy and security properties. We recognise that implementing a PKI-based authentication system on a country-wide scale is a daunting task. As a simpler holdover solution while such a system is developed, vastly reducing the complexity of the TDIF to a two-party OpenID Connect-based system offers better privacy and security than the current version. The main advantage would the the straightforward adoption of an existing, well-understood standard. While the obvious objection to this is the ability of an Identity Provider to track user activity, the TDIF allows the Identity Exchange significantly more power to do the same, and so this is not a compelling argument. Nevertheless, while we believe two-party OpenID Connect to be an easy, quick improvement over the current TDIF, we recommend PKI-based authentication as a much more secure permanent solution.

3 Recommendations for policy change

On p. 32 the consultation paper says,

> The Legislation will include additional mechanisms, including penalties for protecting information used in the system, such as Biometric Information. These mechanisms could include criminal offence provisions and civil penalty provisions.

There are numerous Australian laws that do effectively penalise protecting information, but this is the first time we have seen the objective stated explicitly without invoking terrorists or paedophiles. We hope this is a typo, and strongly suggest penalising the inappropriate sharing or negligent leaking of information instead.

It is important *not* to criminalise security research aimed at improving the system's security by openly examining its (numerous, serious) weaknesses.

The system should be abandoned and redesigned from scratch by people with some understanding of secure protocol design and some concern for protecting their fellow citizens from identity theft. Legislating to make it secure by fiat will not stop organised crime, foreign governments, or ordinary criminals, from taking advantages of its design flaws. A Public Key Infrastructure is much more likely to succeed.

[3] See for example Estonia's https://e-estonia.com/solutions/e-identity/id-card/ or Belgium's https://www.brussels.be/id-card.