Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

23 August 2016

Mr Rachel Dixon
Head of Digital Identity
Digital Transformation Office

Dear Rachel

Re: The Trusted Digital Identity Framework (TDIF) Project

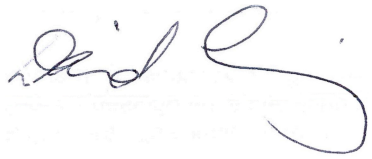
The APF is very concerned about the process being used by DTO in relation to this project, and in relation to many aspects of the product as it is currently envisaged.

We attach a submission identifying those concerns. The APF Board members active on this are David Vaile, Bernard Robertson-Dunn and Roger Clarke.

We request your explicit responses to these important matters, and a specific plan for effective engagement between DTO and civil society. Would you please provide an initial reply this week, including an indication of when we can expect further, more substantive responses.

Thank you for your consideration.

Yours sincerely



Kat Lane
Vice-Chair
0447 620 694
Kat.Lane@privacy.org.au

(Dr) David Lindsay
Vice-Chair
(03) 9905 5547
David.Lindsay@privacy.org.au

David Vaile
Vice-Chair
0414 731 249
David.Vaile@privacy.org.au

Australian Privacy Foundation

DTO Trusted Digital Identity Framework (TDIF)
Comments in Response to Documents Distributed 9 August 2016

23 August 2016

1. Introduction

The federal Digital Transformation Office (DTO) distributed a number of documents on 9 August 2016, outlining a proposal relating to "a DTO Identity program ... [whose intention is] to build ... a service to verify the identity of individuals to a level that means they can access government services [by means of] a federated verification product".

In July 2016, long after an initial approach was made in late 2015, APF's Roger Clarke and David Vaile were invited to participate in a Meeting on 10 August 2016. Over 100 pages of documents were provided mid-afternoon the day before the Meeting was held. Neither person was able to participate, partly because of the amount of effort required to read the material overnight, and partly because of other commitments (including preparations for departure on an 18-day business trip overseas).

Following a brisk review of the documents provided, this paper provides a response, in the following sections:

- **Context**
  This summarises the circumstances within which the project is being undertaken
- **Process**
  This reviews the extent to which advocacy organisations have been engaged during the activities undertaken to date
- **Product**
  This identifies key Principles that need to be embodied in the architecture and design in order to manage the very considerable privacy threats that the project entails

2. Context

This is the latest of many proposals that have come and gone over the last 30 years relating to citizen identifiers, accounts, authenticators and credentials. Apart from express 'national identification schemes', most notably the Australia Card, Medicare Card expansion and Access Card proposals, there has been a series of PKI-based schemes, commencing in 1998, and re-surfacing in varying forms form time to time. These proposals have often been associated with entry-point schemes, most recently MyGov.

The nature of the various proposals, and the processes adopted to developing them, have varied from authoritarian (Australia Card, AML-CTF, Access Card, the DVS expansion) to modestly but unsatisfactorily consultative (GPKA, NTIF). Some projects have sought to ride roughshod over the interests of individuals and society as a whole, whereas others have at least acknowledged the impacts on privacy, and on freedoms more generally.

During the last few years, public trust in corporations and government agencies has been seriously harmed. Examples of recent abuses include:

- the substantial downgrading of the Privacy Act in 2012 in order to advantage the interests of corporations and government agencies over those of individuals
- the assault on the OAIC throughout 2013-15, and the substantial reduction in the resources available to the Privacy Commissioner, associated with the appointment of incumbents since 2004 whose priority is protection of corporations and governments not of individuals
- frequent avoidance by Commonwealth agencies of PIA processes, despite clear government policy that they should be done, and how they should be done
- the expropriation of vast libraries of facial images from existing photographic databases, and the apparently intentional blurring of the distinction between criminal investigation uses and general administrative applications, despite the existence of court judgements that make clear that this is a breach of fundamental human rights
- an eHealth record, nominally 'personally-controlled' and 'my', but in fact designed to advantage public health, public servants and researchers, and not at all oriented towards the needs of individuals
- management of the eHealth record 'engagement' process in such a manner as to prevent interactions between public interest advocates and designers, and to preclude the reflection of their submissions in the design and implementation
- conversion of the eHealth record scheme from consent-based, to opt-out, in breach of the original undertakings and design
- failure to exclude (re-)identifiable personal data from the government's (primarily very positive) open data initiatives
- expansion of the activities of AIHW and ABS well beyond statistics, such that they are now expropriating records from multiple sources, and republishing individual records ('micro-data') in forms that facilitate consolidation both cross-sectionally and longitudinally, and that are readily re-identifiable, in gross breach of the public's expectations about the privacy of the data that they contain
- apparent expansion of the use of the Statistical Linkage Key (SLK) as a means of breaching public expectations and quite possibly the law, and establishing a national identification scheme and consolidated population database by stealth
- unilateral conversion of the Census, without any express consideration by the Parliament, let alone any meaningful public debate, from a purely statistical exercise, to one in which all data is identifiable, all data remains identifiable permanently, data from censuses are linked, and data from censuses are linked to data expropriated from other sources
- declaration of the intention to convert ABS from a survey organisation to a warehouse containing personal data expropriated from any and all government agencies

This long series of only the more recent examples makes clear that public distrust of the machinations of federal government agencies is entirely rational, to be expected, and very difficult to overcome. These problems afflict any project undertaken by government, nomatter how well-meaning and how carefully conceived those projects may be.

3. Process

(1) Late Engagement with Advocacy Organisations

The APF has been aware of the TDIF initiative since July 2015, when Roger Clarke was invited to a meeting in Sydney (although in his personal capacity rather than as APF Chair).

Roger drew attention at the time to a directly relevant publication in the area, viz,:
Clarke R. (2010) 'A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation' Xamax Consultancy Pty Ltd, February 2010, at http://www.rogerclarke.com/ID/IdModel-1002.html
Glossary, alpha order: http://www.rogerclarke.com/ID/IdModel-Gloss-1002.html
Glossary, structured: http://www.rogerclarke.com/DV/IdTerm.html

DTO contacted Roger and David Vaile in December 2015 in relation to membership of a 'Privacy Advisory Committee'. Financial support for participation was requested, in the form of both travel and a per diem. However, nothing further was heard.

In addition, APF Board-member and Health Committee Chair, Bernard Robertson-Dunn, made contributions on the DTO blog. The second elicited no response, and his comments do not appear to have been reflected in the project's work.

It was apparent from media reports in March and April 2016 that considerable progress has been made with the project, with the 'Discovery' phase completed in May, an EOI for Capabilities Statements issued in May, the Alpha phase achieved in August. We now understand that a Cabinet Submission may be in train.

The Committee did not eventuate. Instead, a single Meeting was called, at 3 weeks' notice, on 22 July 2016. Little documentation was provided until mid-afternoon the day before the event was held. Neither of the invited APF Board members was able to participate.

APF understands that CLA was represented, and that ACCAN tried to join the Meeting remotely, but DTO's technology was unable to accommodate their participation.

APF further understands that the Meeting was not in any meaningful sense 'consultative', but was almost entirely presentations by DTO, with limited time spent even on questions and clarifications, and feedback not yet possible.

In short, 'engagement' with civil society has not yet even commenced, despite the project having reached Alpha phase, being publicly stated to be inside a year from launch, and being the subject of a current Cabinet Submission.

(2) Lack of Application of Conventional Processes

The APF is not aware of a preliminary Privacy Issues Analysis being performed. This would have provided an informed base of documentation on which the current project's consideration of privacy concerns could have built.

It would also have identified relevant prior processes, and the considerable amount that the APF and others have contributed to them. In particular, we draw attention to the work on the National Trusted Identity Framework (NTIF) in 2011-12, including at:
http://www.privacy.org.au/Papers/PMC-TrustedId-111221.pdf
http://www.privacy.org.au/Papers/PMC-NTIF-121031.pdf

The APF is also not aware of any commitment having been made to the appropriate evaluation mechanism, which is a multi-phase Privacy Impact Assessment process.

Instead, a single Meeting was called, and substantive documentation provided only at the last moment.

The sequence described in the previous section needs to be juxtaposed against the reasonable expectations in relation to consultation processes, which APF documented some years ago: http://www.privacy.org.au/Papers/PS-Cons.html.

(3) Lack of Clarity about Participation

It remains unclear what the philosophy was and is underlying the composition of the group that was invited to the Meeting on 10 August.

The participants:

- included three public interest advocacy organisations (APF, CLA and EFA)
- omitted two particularly relevant public interest advocacy organisations (ACCAN, Internet Australia)
- omitted representatives of user groups (the Choice email-address bounced, and there were no segmental groups such as ACOSS)
- included four well-known specialist consultants in the area, and
- included staff of the State and federal Privacy Commissioners' offices.

However, the list also included a Government Relations executive from a major Internet services provider.

(4) Lack of Clarity about the Intended Uses of the Accounts

There is a generic sense that the framework would reduce friction in online service delivery. However, specific benefits are not as easily visualised.

It would assist the evaluation if a modest set of diverse use-cases were outlined, and the applicable processes and anticipated benefits described.

(5) Lack of Clarity about Overseas Experiences

Mention is made of schemes or projects in the UK, the US, Canada, New Zealand and Estonia (although not those in Denmark, Germany and Malaysia), but no substantive information about them has been provided.

It would assist the evaluation if a supporting document provided brief descriptions of such schemes, the lessons learnt to date, and references to sources.

(6) Lack of Clarity about the Relevant Legal Landscape

Apart from a brief remark to the effect that the scheme could be implemented administratively, i.e. without partliamentary approval or even oversight, no information has been provided about applicable laws, and the impact of laws in such areas as data retention, data breach notification, cybersecurity, disestablishment of the OAIC, and a privacy right of action.

A preliminary legal analysis would greatly assist analysis and discussions.

(7) Shortfalls in Urgent Need of Rectification

At this stage, the project process is well advanced, and yet DTO has failed to effectively engage public interest advocacy organisations.

The APF urges that:

- government policy be respected, and a multi-phase PIA process commenced immediately;
- consultative processes be placed on an appropriate footing as an urgent matter; and
- design factors that have emerged during the Discovery and Alpha phases be regarded as remaining tentative pending effective engagement, feedback and reflection of the feedback in the architecture and design.

4. Product

The intended beneficiaries of the proposal appear to be government agencies, particularly in terms of the cost of achieving authentication of online transaction-partners, primarily (perhaps solely) consumer/citizens.

The proposal offers modest benefits to citizen/consumers, in the form of fewer demands for registration details, because a single 'identity provider' can be used for interactions with multiple organisations. Repetitive authentication process, however, are no less onerous, although the interfaces may be more consistent than they otherwise would be.

On the other hand, consumer/citizens face serious risks in using the scheme. There is the very real possibility of security breaches, both by insiders and outsiders. There is the very real possibility of conversion from voluntary use to opt-out or mandatory use, of correlation among identifiers, and of function creep. If abused, the scheme would represent a convenient stepping-stone to a national identification scheme. That would shift the imbalance of power even further away from individuals, and threaten political freedoms. It is accordingly vital that the privacy protections be very substantial.

This section reflects the APF's long experience reviewing proposals relating to citizen identifiers, accounts, authenticators and credentials. It also takes into account the understanding gleaned to date from the documents provided on 9 August 2016.

However, the details have not been fully assimilated, and some aspects of the comments in this section may require revision or adaptation even in relation to the Alpha version of the proposal, let alone subsequent iterations.

The comments are provided in the form of 'principles' or 'requirements'.

(1) A Clear Problem-Statement is needed

What are the goals, and what are the constraints, from the government's perspective, from the viewpoints of consumer/citizens, and as seen by other participants? Because trust is at the heart of the matter, by all parties of all other parties and their actions, this needs deeper discussion as a foundation for detailed analysis and design.

(2) Voluntariness must be 'baked in'

Previous breaches of public trust have undermined the public's preparedness to accept mere assurances. Hence:

(a) the design must preclude conversion of the scheme from voluntary / consent-based / opt-in to opt-out or mandatory
(b) the design's fulfilment of that feature must be subject to independent review and reporting, and
(c) the implementation must be subject to independent audit and reporting

(3) The Inability to Correlate Identifiers must be 'baked in'

A cross-index among identifiers is no different in effect from a general-purpose national identifier. Hence:

(a) the scheme must be predicated on the use of multiple identifiers per person
(b) the scheme must not create the scope for any organisation to associate identifiers used by any pair of organisations
(c) the design's fulfilment of those features must be subject to independent review and reporting, and
(d) the implementation must be subject to independent audit and reporting(The concept of 'edge-unlinkability' sounds promising, but its meaning is not clear).

(4) The Inability to Correlate Identifiers must also apply to the Hub

If the Hub were to be able to construct a cross-index among any of the identifiers, it would be quite specifically the central registry of a national identification scheme. Hence:

(a) the scheme must not create the scope for the Hub to associate identifiers used by any pair of organisations
(b) the design's fulfilment of that feature must be subject to independent review and reporting, and
(c) the implementation must be subject to independent audit and reporting

(5) The suggestion of biometric authenticators is a very serious concern

The imposition of biometric identifiers may be the measure that completely destroys the social contract between government and the public.

The creation of a massive database of images expropriated from multiple sources has already created a major threat. Its use to support purely administrative processes, which is inherent in this aspect of the TDIF initiative, would take the government a further step along a very slippery slope.

Any discussion of biometrics in government service delivery must commence with an iron-clad commitment that, with the exception of criminal investigation contexts, biometric measures capable of identifying individuals will never be in the possession of a government or a corporation, and that all biometrics will be handled only within the equivalent of a secure PIN-pad.

(6) Credentials must be Attribute-Specific

Credentials must not lump multiple attributes together, except to the extent that they are relevant to the specific purpose for which the transaction is being conducted.

(7) The scheme must be oriented to the needs of natural persons

The design must not be polluted or compromised by features intended for legal persons

(8) The scheme must reflect the practical needs of natural persons

For example:

- natural persons have multiple roles, which means that each individual may have multiple identifiers. Examples include passport-owner, home-owner, investment-property owner, company director, club treasurer
- some roles are fulfilled by multiple people, over time, and at the same time. Examples include company chair, association spokesperson, club treasurer
- most people use multiple devices (own desktop, own portable, own handheld(s), airport or library desktop), and use them in contexts that have varying security profiles (family home, shared flat, workplace, 'Internet cafe')

(9) The scheme must authenticate organisations' identities to individuals

Individuals are at risk of communicating with imposters. Hence the scheme must embody means whereby individuals are assured that each of the multiple parties they are dealing with is the party they purport to be, and the scheme must provide warranties and indemnities to that effect.

(10) All dimensions of privacy must be considered

This includes not only data privacy, but also the privacy of personal communications, of personal behaviour, of personal experiences, and of the physical person

(11) Risk must be considered from the perspectives of individuals

Risk assessment must be performed, and risk management plans must be developed and implemented, from the perspective of the consumer/citizen

(12) The scheme must not be risky or onerous for individuals

The scheme's primary benefits are for organisations, and individuals have very little ability to influence the scheme's design. Hence risks must be borne by the organisations concerned, and processes must be no more privacy-intrusive than current, equivalent processes, and no more onerous or expensive.

(13) Security Safeguards must be comprehensive

The scheme is subject to accidental and intentional breach by participating organisations and their staff, by the Hub and its staff, by individuals, and by third parties. Hence:

(a) the design must incorporate a comprehensive suite of safeguards against all parties

(b) the design's fulfilment of that feature must be subject to independent review and reporting, and

(c) the implementation must be subject to independent audit and reporting

(14) Nymity must be supported

Many interactions that individuals have with organisations do not functionally require that an identifier be provided, e.g. enquiries and whistleblowing. Hence The scheme must not in any way constrain service-providers from conducting transactions with individuals who retain their anonymity or utilise persistent pseudonyms which are weakly authenticated.

(15) Authentication choices must reflect the specific need

There is a strong tendency for government systems to demand identifiers and authenticate them. In all cases, a risk assessment needs to be conducted, in order to identify the

nature of the assertion that needs to be authenticated in order to manage the risk. This will frequently be an assertion of fact, value, attribute, or agency, rather than an assertion of identity.

(16) Authentication strength must reflect the specific need

There is a strong tendency for government systems to ratchet-up authentication requirements to high levels. For example, the AML-CTF standards are referred to with approval in the documents received. Hence:

(a) the design must reflect risk-based definition of the strength of authentication needed, in each particular instance
(b) the design's fulfilment of that feature must be subject to independent review and reporting, and
(c) the implementation must be subject to independent audit and reporting

(17) Sanctions must exist and be enforced

The notion of 'a privacy policy' is completely inadequate as a basis for privacy protections. Hence:

(a) the privacy safeguards must give rise to formal rights, as is the case with terms of contract
(b) sanctions must be specified
(c) sanctions must be proportionate to the harm, including liquidated damages and access to suits for specific performance
(d) practical enforcement mechanisms must exist, including simple complaints mechanisms and a suitably empowered and resourced enforcement agency

(18) Consents must be revocable

Individuals must be able to withdraw from the scheme, and have their data deleted.

(19) A Privacy Management Plan must be promulgated and implemented

It is essential that the accumulated knowledge about privacy management be applied. Hence:

(a) A multi-phase Privacy Impact Assessment (PIA) must be conducted
(b) Relevant public interest advocacy organisations must be effectively engaged throughout the project life-cycle
(c) The PIA must produce a Privacy Issues List cross-referenced to a Design Features List
(d) the design's fulfilment of those Features must be subject to independent review and reporting, and
(e) the implementation must be subject to independent audit and reporting

(20) Effective and Representative Governance is essential

Governance must be invested in by DTO, in accordance with Australian and international Standards, and must apply throughout the project life-cycle. Hence:

(a) Institutions and processes must exist, be empowered and resourced, continue for the life of the service, and exercise authority over the service
(b) The members of the governance body must include sufficient, appropriate and effective representation of public interest advocacy organisations