National Trusted Identities Framework (NTIF)
Consultation Session
NICTA, Sydney – 10 October 2012

Notes from the Meeting
Roger Clarke, for APF

Summary

PM&C is looking to stimulate the emergence of a 'National Trusted Identities Framework' (NTIF). This reflects the failure of industry to make federated 'identity management' schemes work. One motivation is to reduce the cost to government of many agencies running large numbers of semi-independent identity management schemes, each for specific purposes. Another motivation is of course social control, through the denial of fraud and waste through multiple identities.

The first consultation session in December 2011 was based on a lightweight Discussion Paper, but it was supported by a deeper and much more privacy-aware paper from consultants IIS.

The second consultation session in October 2012 was based on an even more lightweight paper, with no supporting documents.

The attached document provides an Introduction, references to the relevant documents, an outline of the discussions that took place on 10 October at Redfern Technology Park, and comments from the APF perspective.

The tentative conclusions from the APF perspective are as follows.

1. At present the initiative is going nowhere, because:
   - agencies are focussed on their own approaches
   - no agency has the capacity or the motivation to drive a strategic initiative that would develop infrastructure
   - no corporation can take the risk of making a very substantial investment with no clear business model or prospect of paying customers
   - no producer of a document used as 'evidence of identity' is prepared to provide warranties and indemnities to any relying parties at all, let alone to remote parties that have not paid for the privilege
   - most producers of documents used as 'evidence of identity' are government agencies, and government agencies, and governments as a whole, are highly risk-averse, and do everything they can to deny any form of liability to any party
2. If the initiative were to proceed, it would need to be much more specific, at least at the level of an architecture diagram, and some indicative business relationships and business processes.
3. If the initiative were to proceed on the basis of the September 2012 document, it would appear very likely that it would pay at best lip-service to the interests of consumers and citizens, and at worst would ignore them and/or over-ride them with the interests of government agencies and corporations.

   If the initiative were to proceed on the basis of the September 2012 document, consumer and privacy advocates would have no option other than to directly oppose it.
4. The one clear message from private sector participants at the event was that the DVS should be opened up to use by the private sector, and probably operation by the private sector. However, the discussion lacked any meaningful consideration of privacy interests, or even of relevant privacy laws.

National Trusted Identities Framework (NTIF)
Consultation Session
NICTA, Sydney – 10 October 2012

Notes from the Meeting
Roger Clarke, for APF

Introduction

The broad proposition under consideration by PM&C is that it should facilitate or even stimulate a market in identity management. In effect, it sees that:

- the federated id management movement has failed
- many agencies and corporations operate independent identity management schemes for their own purposes
- there are interdependencies among these schemes
- there is scope for rationalisation, which would achieve at least cost savings, but probably also quality improvements

This was the second such event, following one held in December 2011.

Both events were organised by IIS, with Malcolm Crompton facilitating and Robin McKenzie and Chris Cowper supporting, with Christian Hirst from PM&C in attendance.

Little progress has been made in the 10 months since the first consultation session. This is primarily due to inter-agency discussions within federal government transpiring to be lengthy. Many agencies have considerable investment in their own existing identity management schemes. They are naturally concerned about the impact of an NTIF on their own investments and operations.

The Prime Minister recently announced that the Cyber White Paper was being broadened, and re-named the Digital White Paper. This reflects inclusion of the security topic within the scope, which in turn includes the NTIF iniitative.

The current focus is on building a Business Case for government action. However, the government intends putting minimal money on the table. It sees its role as being coordinative and perhaps stimulatory. The likelihood is that the initiative would leverage off existing authenticators and identity management schemes, both within-government and in the private sector.

It is envisaged that in January-February 2013, a Cabinet Submission will be submitted relating to engagement by the federal government in the development of an NTIF.

Malcolm referred to a point I made in December 2011 about the dissonance betweenthe initiative emanating from the 'Cyber-Security' Division on the one hand, and citizen-centricity and privacy sensitivity on the other. (But it's not clear to me whether anything has changed in that regard).

A watch is being kept on developments in the US, the UK (which recently made an announcement in the area), NZ (where IIS has done some consultancy recently), and Canada. All are adopting somewhat different approaches.

Malcolm considered that the event was unlikely to require Chatham House Rules, i.e. 'quote but don't attribute'; but any individual may invoke them, in respect of any comment made. (No-one did).

The 20 participants present were primarily from business, including consultants (e.g. Lockstep), providers (e.g. HP), and potential identity management service-providers (e.g. Telstra, banks), and advocacy organisations (ACCAN, APF, ISOC-AU, with EFA listed but not present).

Documents

Dec 2011: Discussion Paper:
http://www.privacy.org.au/Papers/PMC-TrustedID-Issues-111209.pdf

Supporting IIS paper funded by NICTA:
http://www.privacy.org.au/Papers/PMC-NTIF-IISPaper-1010.pdf

Dec 2011: APF's Comments:
http://www.privacy.org.au/Papers/PMC-TrustedId-111221.pdf

The current document is a 12-page IIS Discussion Paper of 26 September 2012:
http://www.privacy.org.au/Papers/PMC-NTIF-DiscnPaper-1209.pdf

This document comprise notes on the Discussions, followed by Comments and Conclusions from the APF persective.

Schedule

Tue 16 Oct	Civil Society at ACCAN in Sydney
Wed 17 Oct	Financial sector at ABA in Melbourne
Thu 18 Oct	Brisbane
Fri 19 Oct	Melbourne

Tue 30 Oct 3rd Plenary

Discussions

[Meta-Comment:
The Session was hamstrung by a set of Discussion Questions that were largely unanswerable.
This in turn reflected the avoidance of any conceptual design for an NTIF.
Many felt that it was infeasible to develop a Business Case without at least a 'straw man' design.
There appears to be a strong desire by PM&C and/or other agencies to avoid any conflation of the NTIF with a Card. This is the being generalised into avoidance of any specifics.]

A commentator suggested that there are opportunities to leverage off existing corporate identity and authentication, including the ATO and health care providers through the PCEHR / IHI process.

Fraud prevention, detection and investigation were suggested as additions. Malcolm was concerned to avoid over-emphasing fraud, but agreed that it should be included.

There were mentions of DVS by Malcolm and one questioner, including its apparent lack of success, and access by the private sector.

The need for relying parties to be provided with a warranty was mentioned. This was coupled with the conventional avoidance by government of any liability to other parties.

James Kelahar of Smartnet referred to prepaid SIM-cards, and the double-requirement for identification and authentication at both purchase and activation, and the difficulties encountered by both purchasers and issuers in achieving validation. The absence of access to the DVS was mentioned again.

Darren Kane of Telstra has been working with government and ACJIS re data retention for 8 years, and the absence of any agreement is extremely costly to telcos. Telstra is walking away from asking for identity in their shops. [I wasn't entirely clear about the context and scope of that comment.]

Queensland have put the database of individuals licensed to provide service in licenced premises on-line, for checking against the information provided to the employer by the individual (e.g. in relation to training completed). This is administered by the OLGL (Office of Liquor and Gaming Legislation). This was suggested by Philip Joe-Low of Deloittes GreenID / eDentiti as a model. It's being extended within Queensland in relation to dangerous work licences (bulldozers, etc.). It needs inter-operability across State boundaries.

Philip Joe-Low recognises that entitlements are generally linked with an identity.
[More correctly, most entitlements are linked with an attribute, e.g. age and asset-holdings.]
Validation of multiple credentials is frequently involved

Greg Stone – frequently collection of identity is not necessary

Specific use-cases were generally recognised as being valuable. They assist the government to consider whether intervention is needed, and if so then of what kinds.
[And to what extent the individuals' multiple identities need to be correlated or consolidated.]

Additional examples that were mentioned were PCEHR / IHI, and student identifiers at secondary level in various States, at VET in various States, possibly at university-level, and a national initiative in education generally.

Philip Joe-Low commented that the DVS covers only documents issued by government agencies, but the scope could extend to taking data provided by the individual and matching it against a database entry, even though it may not appear on any authoritative 'evidence of identity' document.
(For example, a financial institution may challenge for data that should be known to the cardholder and only to the cardholder, e.g. the credit-limit, or the transaction-code on the last line-item on the last statement).

Several people suggested that the DVS won't be unlocked to private sector use while it is operated by a government agency, and hence the first step is for it to be outsourced or divested.

Malcolm suggested that if the APIs were published, multiple, competitive DVS could be provided by private-sector service-providers, accessing government data.

[At no stage ddid anyone raise the question of what legal authority exists for each re-purposing of the data held by the participating government agencies, whether it is feasible to gain the individual's meaningful consent (i.e. consent that is informed, freely-given and granular), nor what the original purposes were of each data collection.

[DVS currently encompasses:

- passports (involving access to DFAT's database)
- visas (DIAC's database); and
- drivers licences (presumably against the NEVDIS copy of motor registries' databases).]

[DVS has long intended encompassing:

- birth certificates (involving access to the Registry of BDM records of all States and Territories, or some consolidation of it);
- death certificates (or perhaps a register of birth certificates against which a death has been recorded);
- possibly all marriage certificates ; and
- possibly all evidence relating to change of name.]

However, DVS is predicated on providing no data, and only providing Ack or NegAck (i.e. 'the data you provided matches our database', or it does not). Several members of the audience mentioned this, and Malcolm confirmed that this was his presumption as well.

Philip Joe-Low noted that there is very little infrastructure to support authentication of individuals and organisations that provide 'evidence of identity' documents. (He was referring not so much to government agencies, but to the school-teachers, bank managers and JPs who vouch for individuals, and certify photographs and document copies).

Steve Wilson queried whether the term 'identity management' was appropriate. Several responded that they were focussing on 'verifying information', rather than on 'identity authentication'.
[The conversation reflected the notion of 'attribute authentication', without using it.]

Darren Kane of Telstra had declared himself as a strong supporter of law enforcement access to data. He asserted that new legislation did or would impose tighter constraints on airlines, requiring identity authentication of ticket-purchasers and flyers, and creating [?] a criminal offence of 'using a false identity' [?]. He suggested that this would be a good case study for the NTIF initiative. [I queried such things as what the legislation was, what the obligation was on airlines, and how the inter-operability with other governments would be achieved, e.g. Salman Rushdie's State-facilitated 'false identity'.]

General Comment by Roger (i.e. not an APF Comment)

This investment is in multi-purpose infrastructure.

Multi-purpose infrastructure, by its nature, cannot be cost-justified, because:

- the benefits will arise as a result of applications running over the infrastructure
- the benefits will be attributed to the applications not the infrastructure

A Business Case for infrastructure therefore cannot be based on cost-benefit analysis, and has to specifically recognise the iniitative's strategic nature.

Comments from the APF Perspective

1. Scope of Entities

The scope appears to be nominally all entities. However, the language is phrased almost entirely in terms of individuals, and no provision is made for the significant differences between individuals and imaginary entities such as corporations, government agencies and associations.

A great many of the threats in the digital world arise from misrepresentations by corporations (e.g. email-spoofing, phishing, web-site spoofing). In the absence of any focus on entities, there is limited contribution to trust by individuals.

Malcolm, confirmed by Christian, agreed that:

- this is within-scope
- the current paper has lost those nuances, and needs them re-inserted

2. Scope of Authentication

The scope appears to be focussed solely on identity authentication, without reference to the authentication of other forms of assertion. Of particular importance is attribute authentication, which includes authentication of a person's authority to represent an entity.

Malcolm, confirmed by Christian, may have agreed that:

- the scope is broader than identity authentication
- the current paper has lost those nuances, and needs them re-inserted

3. Indicative Architecture

The supporting document to the 2011 discussions included a useful graphical representation of the players involved.
At least APF and ISOC-AU provided constructive feedback, to enable it to be improved.
Neither the original nor an improved version is included in the 2012 paper, even by reference.

The absence of an architectural framework appears to be a serious backward step.

(It is acknowledged that this derives from the strong desire in government circles to avoid any details; but that makes it very difficult to make meaningful comments – and to anticipate any real progress being made).

4. List of Power Imbalances

The supporting document to the 2011 discussions included a valuable discussion of power imbalances in s.3 on p.4.
This is not included in the 2012 paper, even by reference. That appears to be a serious backward step.

5. Guiding Principles

The supporting document to the 2011 discussions included a valuable discussion of power imbalances in s.4 on pp.4-5.
At least APF provided important feedback, to enable them to be improved.
This is not included in the 2012 paper, even by reference.

The absence of fundamental principles appears to be a serious backward step.

6. The Business Case Discussions

With only limited exceptions, the discussions focussed on the authentication of human identity, and excluded organisations.

In addition, the notions of citizen-centricity, citizen-control and citizen trust were entirely missing from the conversation.

Nothing was said about the untenability of the proposition that DVS do anything more than confirm or deny that the data provided matches the data in their records.