Dept of Prime Minister & Cabinet
Workshop on 'Trusted Identity'

Facilitated by Malcolm Crompton of IIS
20 December 2011

Comments Made on Behalf of the Australian Privacy Foundation

Roger Clarke
21 December 2011

The Scope of Entities

Which categories of entities are within-scope?

- Individuals
- Incorporated Organisations, incl. corporations whether under the corporations law or their own statutes, coops, associations
- Unincorporated Government Entities
  incl. agencies and appointees who are merely parts of the Crowns
- Unincorporated Organisations
  - economic, incl. trusts, sole traders, partnerships
  - social, incl. 'committees'
- Computing and Communications Devices

Priorities

A great deal of the material is written as though individuals were the sole, or at least the primary, focus of the undertaking.

So which of the following are in focus:

- citizens cheating government?
- corporations cheating consumers?
- criminals cheating everyone?

Focus on individuals would be likely to cause considerable disquiet among consumers and citizens, because the common perception is that the big issue in cybertrust is the prevalance of scams designed to extract information and/or money out of people.

The concern is exacerbated by the organisational location of the current initiative. From the consumer and privacy perspective, an agency such as NOIE or DBCDE has the advantage of having broad scope and the ability to reflect multiple interests. AG's Security Division and DSD, on the other hand, are imbued with a narrow social control perspective, and dominated by national security extremism. PM&C's remit might seem broad, but the Group within which the cybersecurity initiatives are being developed is expressly part of a 'national security' community that is highly focussed on social control and not at all with human rights.

Credibility of the initiative is critical to its acceptance, and advocates can be expected to be sceptical about the purposes and the priorities.

The Scope of Authentication

It is essential that this initiative always make very clear that authentication should be performed on those assertions or claims that are relevant to the business need, and that the strength of

authentication required must always be subject to risk assessment, and from the perspectives of all parties to the process.

In particular, the documents need to make clear that data authentication, value authentication or attribute authentication will commonly be easier and less expensive and onerous than identity authentication, and much easier and less expensive and onerous than entity authentication. And hence (id)entity authentication should not be conducted if it is not justified, and not conducted in a manner that is disproportionate to the need.

A brief summary of the concepts is here:
http://www.rogerclarke.com/DV/IdAuthFundas.html

Note that key aspects of the work that I did on the original Aust Govt Authentication Framework (AGAF) in 2004-05 were gutted in the National eAuthentication Framework (NeAF) in 2009. AGAF could be quoted as an authority for the above, but unfortunately NeAF can't be.

The Indicative Architecture

The diagram is a useful framework for people to think about.

However it omits several vital elements.

(1) Identities need to be distinguished from Entities, by interposing 'My Identities' Between 'Me" and 'Digital Me'.

(2) 'Digital Me' then needs to be amended to 'Digital Mes', or 'My Digital Personae' or similar. (Identities exist in the real world, so there are benefits in avoiding the term 'digital identity').

(3) I support Narelle Clark's point that the diagram should also contain a diagram-element signifying the (many kinds of) devices used to achieve representation of 'My Identities' in the digital world. This would naturally come between 'My Identities' and 'Digital Mes'.

(4) Some of 'My Identities' are shared by other Entities, e.g.:

- 'Signatory on the bank account of XYZ Ltd'
- imposters conducting masquerade

So the m:n relationship between 'Mes' and 'My Identities' needs to be indicated in some way, e.g. by showing multiple Mes down at the bottom (maybe shaded dark grey rather than black, to indicate that the others are secondary, at least from the perspectiive of 'Me').

The most recent (and tightest) version of my model is at:
http://www.rogerclarke.com/ID/IdModel-1002.html
supported by:
http://www.rogerclarke.com/ID/IdModel-App-1002.html#AO

Viability

Large numbers of schemes have been devised to address (some aspects of) 'trust' through 'identity management'. Almost all have failed.

One major reason for this has been the inadequate models of entity, identity, (id)entification and authentication on which the schemes have been built. I've been trying for over a decade to get the message through, with only modest success. (The paper above is merely the most recent of many).

Another major reason for the schemes going nowhere has been that they fail to deliver trust. Trust depends on post-controls as well as pre-controls. Verisign and other certificates are valueless, because they are not the subject of meaningful and actionable warranties and indemnities. Until certificate-issuers stand by their certificates, and do so for all relying parties, whether or not a contract exists between them, identity assurance will remain low-grade.

(From a privacy perspective, it may well be better for schemes to keep failing. A high-grade scheme involves strong pre-authentication, which is highly onerous and expensive for individuals, and is almost inevitably highly privacy-invasive and insecure as well. But if a high-grade scheme were to be developed for some limited, critical functions, it would be pointless unless an insurer of last resort stood behind the assurances given. Among other things, this means that issuers of 'breeder documents' such as birth certificates and immigration papers have to pay CAs money when they get it wrong).

The 'Guiding Principles'

The idea is attractive, but the current set of eight requires work on the following aspects if it is to satisfy consumers' needs:

- one needs more careful expression
- each of the items needs articulation
- one or more additional principles may be needed

(1) The second ("strengthen participants' privacy") needs to be amended to refer specifically to individuals. Privacy is a human right. It has no applicability to any category of entities other than humans. (That wouldn't of course preclude some additional principle that addresses interests of other entities, but any such principle should be kept separate from the principle(s) relating to privacy).

(2) The principles need to very clearly invoke data privacy rights, but also the other dimensions of privacy - privacy of the person, privacy of personal behaviour, and privacy of personal communications. I suggested the following wording for an additional principle:

> "do not impose unjustified or disproportionate privacy intrusions on individuals, nor processes that are unduly onerous or unduly expensive"

(3) Another important need not covered in the principles as they stand is:

> "do not create new risks to individuals, or exacerbate existing risks, as may arise from additional collection of sensitive data, consolidation of sensitive data from multiple sources into 'honey-pots' that attract crackers, and the creation of high-value credentials that attract attention from forgers"

(4) It is essential that recognition of and support for multiple, unrelated identities per person be enshrined in the principles.

DVS

The Document Verification Scheme (DVS) has some real potential benefits. For example, it can aid in the detection of fraudulent documents by providing facsimiles of what, for example, Ukrainian birth certificates looked like in 1945.

DVS also harbours serious threats to privacy and freedoms more generally, because of the ease with which it can lead to a de facto national id scheme, through multiple-use of identities, and the consolidation of data-trails.

It is vital that use of DVS be limited to circumstances in which it is demonstrably justifiable, proportionate, expressly authorised by the Parliament (not through delegated legislation), and subject to governance including effective controls and protections. In addition, the government must back its express or implied statements about quality by providing warranties and indemnities to relying parties.

Engagement of Civil Society

NGOs were absent from early discussions (fn. on p.2 of the Proposal), but APF, EFA and ISOC-AU were present on 20 Dec 2011, and ACCAN, ACS and Choice had also been invited.

The Access Card and the impending PCEHR fiasco are just two recent examples of the folly of excluding or marginalising consumer and privacy advocacy organisations. From a corporate risk management perspective, it's vital to achieve early and ongoing engagement of relevant NGOs deep in the processes whereby initiatives are initiated, articulated and developed.

APF's expectations of meaningful consultation processes are here:
http://www.privacy.org.au/Papers/PS-Cons-101106.html

Corporate memory is important, on all sides, to ensure cumulative commitment rather than stop-start communications. Unlike the representatives of business and government interests, many consumer and privacy advocates do not have an employer able and willing to fund their participation. Travel support and at least per diem / sitting fees are therefore an essential element of consistent engagement and corporate memory. This is all the more necessary where the advocate brings deep expertise to the table and is foregoing time and in effect performing charity consultancy.