

User-centric identity management: An oxymoron or the key to getting identity management right?

Malcolm Crompton

E-mail: mcrompton@iispartners.com

Abstract. There are many drivers for strengthening identity management (IdM) in the digital environment. They include: countering identity fraud, identity theft or identity takeover, border control and traveler identification; individual convenience; or better customer service for individuals. A range of approaches are being considered in the public and private sector. Experience is showing that IdM succeeds best where it builds in two way trust and is not perceived by users as yet another policing action. The challenge is even greater if individuals believe that IdM will put all the powers and discretions in the hands of the institution to collect more personal information which is then linked, used, or disclosed. For IdM, the key to success is increasingly to understand and design with individual interests, as well as government or organisation interests, in mind.

This paper looks at the concept of user-centric IdM and suggests some defining features. It will draw on experience and developments in Australia, New Zealand, the United Kingdom and Scandinavia to highlight issues that may help or hinder the delivery of effective user centric IdM. These include choices about centralised versus distributed identity, the impact of each country's culture and history, the approach taken to risk allocation and the importance of keeping agendas simple and transparent. Recognition of the importance of these issues is gathering pace. It has moved from the realm of the advocate, through academia and into mainstream, commercial development, even to the point of creating a unique effort at building interoperable ID management systems that respect user centric principles. User centric IdM is possible with the right mix of individual control, fair risk allocation and accountability.

1. Individuals: the last people to be thought of when their identities are being managed

It is a curious thing that when people in the identity management 'business' talk about and develop solutions for identity management in the digital environment they rarely start by thinking about it from the point of view of the individual person. Given that identity is a very personal concept, in that it relates to the very core of one's being and how one portrays oneself to the outside world, this might seem very surprising. There are probably many reasons for this lack of focus on the individual. It probably starts with the word 'management', where the main impetus for the need to 'manage' identity has come from, and where by and large the power in developing solutions lies.

¹Malcolm Crompton is Managing Director of Information Integrity Solutions P/L. He was Australia's Privacy Commissioner for five years until April 2004.

This paper was first presented at the international conference: "Managing Identity in New Zealand", organised by Victoria University of Wellington with support of the New Zealand State Services Commission, Department of Internal Affairs and Office of the Privacy Commissioner. The conference was held at Te Papa Tongarewa, Museum of New Zealand, Wellington, 29–30 April 2008.

The drivers behind strengthening the approach to identity management in the online environment are many. They include countering identity fraud; identity theft or identity takeover; border control; and traveler identification (particularly in the post 9/11 environment). Although individual convenience or better customer service has been proclaimed as a driver, in some cases this has been a cover for other less customer-centric agendas. This does not mean to say that individuals do not have an interest in the issue. Few of us want money stolen from our bank accounts, but such problems do not always have to be solved by disclosing elements of our identity. At other times, we do want to disclose something about ourselves to other individuals or organisations, but not often in terms of ‘managing’ our ‘identities’ so much as to share ideas or feelings or refine a service offering in an environment we trust.

Let me ask this question: when you think about identity management, whose risks are you thinking about managing? Are you really worried about the individual whose financial affairs or reputation may be at risk? Or is your real focus on your organisation, its bottom line, the loss it may suffer, or especially if you are government, how to better fight crime or gather intelligence? It may seem logical for organisations to focus so much on their own interests and risks when they think about identity management, but they should not be surprised if other stakeholders object.

2. The consequences of such curious thinking

This paper suggests that organisations, including governments, that do not focus on the interests and wishes of the persons whose identity they propose to ‘manage’ are actually exposing themselves to other risks they have not thought about. These include:

- Loss of end user/citizen trust and brand damage;
- Financial loss from solutions that end up on the scrap heap because end users won’t use them;
- Loss of the huge opportunities associated with high level mutual trust;
- Increased vulnerability to the risks they actually are trying to ameliorate.

A key element in the loss of end user trust in identity management systems is often the arrogance and rudeness behind a process which is effectively saying ‘I don’t trust you until you prove yourself to me, but you will just have to trust me without proof.’

3. The internet has shifted the goal posts

A major problem here has been that organisations and identity management solution providers have not thought beyond the technology to the legal, social and other implications for individuals and their identities that are created by moving from a paper based approach to an online based approach. We very often hear the bewilderment of many organisations wanting to provide online or remote services. They say that what is being proposed is simply doing in the online world what was being done in the offline world. But many have not realised that we are moving into a whole new ‘ball game’. As Michael Kirby pointed out so eloquently in his speech to the Australia Internet Industry Association at its gala dinner on February this year when speaking about the ‘use limitation’ privacy principle:

It was effectively a good and moral and ethical principle designed to keep people’s control over the use that was made of their information conundrum and it seemed entirely appropriate, recommended put into law and then along came Google and Yahoo and when the new technology came along with its massive capacity to range through vast amounts of information the notion that you could

control this conundrum of information about yourself, this zone of privacy around yourself, was very quickly overtaken by the technology. Because the technology was so manifestly useful for the users of automated systems that the notion of saying “halt!” was like the notion of Canute who, under the instruction of his officials, went down to the sea to try and stop the waves coming in. Canute, by the way, knew that he could not. The Officials believed this was the kingly power. Canute went to show the limits on kingly power.

What Kirby has so accurately identified is the fact that in the digital environment we are currently asking individuals to make too many decisions, too often, in too much ignorance and then to undertake too much of the enforcement load. His observation is even more remarkable given that he chaired the 1980 OECD Committee that wrote the original OECD privacy guidelines. Another factor, often missed, that transforms the ‘game’ is the digital footprint people leave in the online world that was not a feature of the paper based world. With this foot print, incidental information about online behaviours can be collected and analysed for purposes which may be totally unrelated to, for example, the original purpose of managing identity. The ‘behavioural targeting debate’ that is just beginning in the United States is just that: the beginning. Also missed until recently have been the implications arising from the fact that, just as individuals can easily pretend they are someone else in the digital environment, so can the organisations with which they are interacting.

As with any new technology, after initial enthusiasm and naivety, individuals are starting to understand, with increasing sophistication, the risks of transacting on the internet caused by these changes.

They are also waking up to what we call the great ‘risk shift’. They are starting to realise that when an organisation moves their service to the online environment, organisations manage their own risks by shifting the risks on to the individual. In the context of identity management solutions, this often means:

- Stringent requirements are placed on individuals to identify themselves, but no attention is paid to assuring the individual that the organisation is who it says it is (ie no provision for mutual trust);
- Little attention is paid to the consequences of the huge volume of peripheral data that could be collected through the digital footprint every time individuals electronically identify themselves;
- The security and secondary use risks from the greater ease of aggregating data about an individual through the use of unique identifiers;
- The inconvenience for individuals if the system fails or the individual loses their means of identifying themselves.

A number of attempts to adopt identity management solutions have also run into trouble with the community because they have not been sensitive to the impact the dramatic changes outlined above have had on ability of users to exercise control over their lives and their identities. Also as noted before, much of this challenge has arisen because identity management solutions have mainly focused on addressing weak identity management using technology as the main solution and only from the point of view of the needs of the organisation. As Kirby has indicated, part of the answer lies in the ‘code’ but there are also some other factors that must come into play to create the trust in new identity management solutions.

4. What user centric id management looks like

Having seen the community response to identity management solutions that don’t give users the trust or control they seek, new thinking has had to be done. Mechanisms had to be found to give individuals the same level of trust and control they had in the paper based world. This has become known as the user-centric approach to identity management. It is outlined in work from the London School of

Economics (LSE) in response to the UK Identity Card proposals, in Kim Cameron's [of Microsoft] set of 'Laws of Identity' and in work we have undertaken also.¹

There is little doubt that a user centric approach will be the key to success in getting identity management right. Solutions must ensure:

- that the focus of management is not just on the interests of the organisation, but the interests of the user as well;
- The solution must establish mutual trust. Our analysis suggests that organisations must consider three dynamic factors from the point of view of the individual to ensure mutual trust. These are:
 - * Fair risk allocation – ensuring that individuals understand the risks and are confident that they are fairly allocated to the party most able to bear them;
 - * Control – ensuring that individuals have the control they want over how information is demanded, collected and stored, or if that is not possible or wanted, they understand the organisation and how it will handle the information;
 - * Accountability – ensuring that the organisation is accountable and transparent about how it will handle personal information and take appropriate responsibility for dealing with the impact of failure on the individual including having a good safety net.

These factors are dynamic and interdependent. All components must be addressed from the user's point of view to achieve trust, but some may need more emphasis depending on the circumstances. For example, where people perceive a high level of personal risk, they may demand increased personal control. On the other hand, where an organisation displays high levels of accountability, including transparency, individuals may perceive that there is less risk, and may demand less levels of direct personal control.

How these dynamics play out may depend on the legal, historical, cultural environment, including whether the organisation is public or private sector and the purpose for which identity management is being implemented. For further development of this analysis see a white paper called 'Safe to Play' which Information Integrity Solutions wrote with Cisco.²

Governments in the UK, US, Canada, New Zealand, and Australia in particular had significant challenges in implementing new identity management systems compared with other countries. Most of these initiatives have attracted strong public scrutiny, demands for greater citizen control and robust privacy measures.

In contrast, Scandinavian countries have implemented identity management systems with unique identifiers that don't follow strong privacy, user-control-based models without arousing controversy. The level of trust citizens have in their governments may have an impact on this. Centuries of openness in Scandinavian governments, including freedom of information laws, appear to have contributed to citizen trust which has given them higher levels of comfort about how their information will be handled.³

The Australian experience provides a contrast. In April 2006 the former Australian Prime Minister announced that his government would introduce a "Health and social services access card". The primary

¹"The Identity Project, An assessment of the UK Identity Cards Bill and its implications", Chapter 18, 'Design Principles and Options', London School of Economics, June 2005 (<http://is2.lse.ac.uk/idcard/>); "The Laws of Identity", Kim Cameron, May 2005 (<http://msdn2.microsoft.com/en-us/library/ms996456.aspx>); "Proof of ID required". Getting Identity Management Right, Privacy Commissioner Malcolm Crompton, March 2004 (http://www.privacy.gov.au/news/speeches/sp1_04p.html)

²"Safe to Play: A trust framework for the connected republic: a point of view", Global Public Sector Practice, Internet Business Solutions Group, Cisco Systems, as at March 2008 (<http://www.theconnectedrepublic.org/downloads/>).

³See "Identity Management: Use Cases for Identity Management in E-Government", Robin McKenzie, Colin Wallis and Malcolm Crompton, IEEE Security and Privacy, March/April 2008 <http://www.computer.org/portal/web/csdl/doi/10.1109/MSP.2008.51>.

intent of the initiative was stated at the time as preventing fraud and improving the delivery of government health benefits, veterans' and social services. It was to streamline and modernise the delivery of health and welfare payments. However, the Access Card initiative was shelved before the 2007 federal election because it had become an electoral liability for the government. Aware that there was community sensitivity on the issue, the government strongly emphasised that the card would not be a national identity card of the kind that had been rejected by Australians in the late 1980s. This message did not change for the duration of the project despite the strong evidence to the contrary about the way the system would be built and operate. For example:

- Although the government emphasised that it would not be compulsory to have or produce the card – it very rapidly became apparent, that nearly everyone would need one because nearly everyone needs to use the national health scheme 'Medicare'.
- The proposal included a new strong registration process far beyond that needed for the espoused purposes. It required original document production even for citizens with an established existing relationship with government welfare services. It also included a centralised data base holding identity information and scanned copies of original identity documents. With these strong measures for identity management it seemed inevitable that this would become the default identity management process relied on by other government agencies, and even the private sector.
- The card was to have a photograph of the card owner on the front when an encrypted template of the photograph on the card chip would have been sufficient for the stated identity management purposes.
- Although the card was stated to reduce fraud against welfare services, there was no evidence that the fraud was due to identity fraud.

The government attempted to address community concern by appointing the respected former head of the Australian Competition and Consumer Commission to oversee citizen interests in the development of the Access Card initiative through the Consumer Privacy Taskforce. However, confidence in this process was significantly undermined by inadequate consultation processes and the government response to the Consumer and Privacy Taskforce's recommendations which rejected the recommendations about the features of the project that were of most concern to the community. The government's failure to acknowledge the obvious reality that the card would in effect be a national identity card meant that it did not take the steps necessary to reassure citizens that the government could be trusted with the information it was giving them no choice about providing. Instead of being transparent and accountable about the purposes for which the information was to be collected and used, it appeared to be hiding things. The document that outlined the business case for the Access Card, which was released after public outcry, contained a number of large gaps. The Privacy Impact Assessment was never made public. It was only through parliamentary inquiry processes that it became apparent that law enforcement agencies would have access to the information held on the extensive data base of identity information without needing a warrant; although even then officials from different agencies could not agree on which organisations would have what access for which purposes. The draft legislation circulated for consultation failed to provide the strong governance and accountability mechanisms that consultations were asking for. All these factors contributed to rising community concern about the Access Card and were a major reason for the project's failure. Unusually, even though government members held the majority in the Senate committee conducting the inquiry, the committee rejected the legislation as then drafted. In the face of growing community backlash and a looming election, the project was abandoned at significant cost to government, and also to private sector organisations that had spent significant resources on tenders and proposals to build the Access Card. The UK identity card process has had similar features and generated

negative community response. Although the government is still pursuing the project, it has proceeded very slowly and in significantly modified form.

This is not to say that some governments have not accurately assessed their environments and taken on board the user-centric approach. For example, New Zealand has taken note of its citizen privacy sensitivity and is building a system that is squarely focused on user centricity, privacy and security. A key feature has been separating out the authentication components into logon management and identification. The log on service uses a pseudonymous identity provider.

The Australian Online Government Services Portal has drawn upon some of the concepts present in the New Zealand State Services Commission's model in order to provide a user centric government service online entry point for Australian citizens.

5. Shifting grounds in identity management

Identity management is a very dynamic area. Recognition of the importance of these issues and acting upon them is gathering pace. It has moved from the realm of the advocate, through academia, and is now emerging into mainstream commercial development. New user-centric products are emerging in the private sector aiming to address particular components of user-centric identity management. Open ID for example, through a URL based identity protocol, enables the decentralisation of, and greater user control over, identity brokering. Users can host their identity on any server they choose and they can also choose to have it hosted by one of the growing number of OpenID hosting services. Although it is a low security product best used in low risk environments, it is a start, and work is under way to strengthen the security (starting with a combination OpenID/CardSpace offering).

This development is in line with a general trend towards cooperation in solving the identity management conundrum. Increasingly the big players are setting aside the fierce competition in other areas to recognise that the ultimate key to an identity management system that users trust is interoperability. The User-Centric Identity 'Interop' at the Catalyst Conference in San Francisco in June 2007 is a good example.⁴ The moves in this direction give users the ultimate control of changing identity providers if they are dissatisfied with the one they are using, in the same way that programs are being developed so that individuals can move their information from one social networking site to the other if they wish. As Mike Jones, one of Microsoft's experts in identity management, said to me recently: "Identity isn't a revenue situation. It's an infrastructure situation." This approach recognises that profits will only come once individuals have a system they can trust even if the commercial return is indirect. It will be through greater and deeper levels of engagement in the on-line environment, rather than from identity management itself. They understand that interoperability, and the control it will give users, will provide the platform for such trust.

Another initiative that contributes to end user control is the 'zero knowledge solution'. This allows much greater individual control potentially in a number of ways. For example, it enables authentication of an assertion such as an identity assertion or a proof of age assertion without the party providing the authentication knowing anything about either who is making or who is seeking to rely on the assertion. One solution built around these concepts is Credentica. Credentica removes the privacy risks present in most identity management systems up until now caused by the fact that authentication of an assertion usually requires the authenticator to have some information about the transaction the user is engaging in, or the organisation with which they are transacting.

⁴<http://identityblog.burtongroup.com/bgidps/2007/08/recapping-the-c.html>.

6. Significance of this learning for governments seeking to manage identity

The question that people from the government sector may want answered is how applicable is this user centric approach to identity management in the public sector? Can governments take a truly user centric approach? Sometimes people cannot be given choice about giving information if they wish to receive a service. How can governments address fears people may have that information they have given for a benign service, might be aggregated into a bigger picture about them, or find its way into the hands of law enforcement agencies or the tax man? Increasingly these issues also apply to private sector organisations and the consequences for the approach to identity management are only a matter of degree. Key things that governments must think about are:

- If choice is not an option in a particular identity solution, what other mechanisms can be used to enable people to feel information about themselves will be protected?
- Is our agenda for stronger identity management really about protecting and providing better services to citizens? Or do we have other more government focused agendas?
- Are we willing to be transparent about our agendas?
- If we cannot be fully transparent, what else can we do to gain citizen trust?

Addressing these questions shows why a single identity management arrangement to cover use cases for service provision as well as law enforcement/national security, has the potential to inhibit citizen trust in the services that require its use instead of enhance citizen trust. In particular it can raise doubts over whether government will use information only for the original purpose for which it is collected and not re-use it out of context to the potential detriment of the individual. Separate solutions for the two kinds of use cases may well be the answer.

7. Conclusion

It must be clear that in my view, user-centric identity management is far from being an oxymoron. In fact, it is an inevitability if identity management solutions are to be trusted and taken up by end users and citizens. A further conclusion is that it is a dynamic area and the means for achieving user-centric identity management are many faceted. A government, or any organisation, seeking to develop a comprehensive, centralised stand-alone approach is almost certain to fail. Cooperation and interoperability will be key. Nonetheless, governments, by virtue of their unique position, do have a significant role in guiding the online world towards solutions that meet everyone's needs. This will involve taking off our business or government hats, even if it is for just a moment and looking at it all from a personal point of view.