Understanding Digital Identity and Privacy

Consultancy Offering

Robin Wilton
Director
Future Identity Ltd

mail@futureidentity.eu
+44 (0)705 005 2931

February 2009

Purpose

Digital privacy is a topic of increasing importance to citizens, governments, enterprises and regulators; it is also a notoriously difficult topic to address. Privacy means different things to different people, and frequently means different things to the same person, depending on when and why you ask them about it.

Over the past two years, I have moderated a world-wide programme of Privacy Summits, bringing diverse stakeholders together to address high-level issues such as trust, privacy, 'ownership' of personal data, and the intersection between policy and technology in these areas. The Summit participants were selected to include policy-makers, technologists, lawyers, academics, industrialists, analysts and privacy advocates. The Summits crossed national and cultural boundaries, reaching Washington DC, Yokohama, Tokyo and five European cities. However, one consistent theme ran through all of them: that the digital identity and privacy issues confronting us cannot be solved by the actions of any one stakeholder group.

This raises a problem: the diverse participants all have a perspective, a vocabulary and a conceptual view of the problem... and these are at best different, and at worst conflicting and incompatible. All of us have sat in meetings where discussions of trust, privacy and digital identity go round and round the same circles and achieve nothing. For the Privacy Summits to work, we had to solve this problem. As a result, we defined a number of simple models to address basic questions of terminology and conceptual framework.

- What is 'digital identity', and how is it related to identity data?
- How is identity data related, in turn, to privacy?
- If identity and privacy problems can be fixed by technology, policy or a combination of the two, how does one balance that choice?

We tested these models through the Summit programme, and found that they can quickly be used to bring participants to a common understanding of the basic concepts and vocabulary. It was then possible to have a meaningful and productive discussion of the 'high-order' topics such as trust, privacy, and data ownership.

This briefing is based on the findings and models developed through that two-year programme.

Outcomes

- By the end of the session, the participants will have a set of clear, simple conceptual models for identity, personal data and credentials, and will understand how these relate to personal privacy.

- They will have examples of systems where identity data is protected predominantly by policy means, predominantly by technical means, or by a combination of the two, and will understand how the technical and non-technical measures must interact.

- They will understand the broader context of how these principles relate to the disciplines of identity management, privacy good practice and data protection.

- They will understand some of the issues which remain currently unresolved in this field.

Deliverables

- Two-hour interactive briefing on Digital Identity and Privacy
- Hand-outs (per attendee): copy of presentation materials, copy of Privacy Summit report from the Liberty Alliance Public Policy Expert Group.
- One soft copy of the hand-outs on CD
- Write-up of key points from each briefing session.

Pre-requisites

None. The briefing is designed on the assumption that participants are not specialists in privacy, identity management or the related technology.

Summary

What you get is a well-tested workshop, conducted by an experienced industry practitioner, which distils the findings of several years of work on these issues. The workshops will help your staff understand the different perspectives their colleagues and counterparts may have on digital identity and privacy, and give them simple models they can continue to use as they work collaboratively in this area.

These sessions are ideal for establishing common ground amongst different departments or organisations who all need to contribute if they are to meet a common privacy objective. They are also useful for training staff who need an understanding of the principles of digital identity and privacy (such as compliance, audit and HR personnel), and for helping IT staff understand the wider organisational implications of identity technology.

The briefing can be repeated as many times as needed, depending on the number of stakeholders you want to reach. Each session should be assumed to take half a day.

The guiding principle is this: your stakeholders need to embody these principles as a team long after the session is finished – so the sessions are structured to create interaction amongst the participants as a group, and make that lasting effect as strong as possible. With that in mind, there is a distinct benefit in keeping numbers to around 15 per session, so that everyone has an opportunity to contribute.