

Chips or Mash? Composite Identity in Context.

Andrew Hardie

V1.1, 2006-07-26

Discussions about personal ID management often get sidetracked by the question of context, such as “are you talking about identity in a personal or corporate context?” Instead of speaking about identity in context it may be helpful to turn this around and look on context as being part of the identity in any given instance. For example, this might include you, your normal job, the job you are doing today (e.g. covering for someone on leave), your office, your branch and your company. Your identity for a particular task, transaction or need, at a particular time and, maybe, in a particular place is therefore a combination of personal ID data and the data about these contexts.

The contexts can be regarded as a set of pointers (or indexes, or XRI's if you prefer) that can reference a series of federated identity management systems. So, it's less a case of multiple identities but more a case of multiple contexts, adding to the basic identity information. Indeed, many of the multiple identities people now have are more likely to be multiple contexts in which users have chosen how much of their identity to reveal. Think of it as a composite identity, with each aspect of the context being additional metadata, which can be from a variety of sources, added to the fundamental data of who you are. In fashionable Web 2.0 parlance, it's a 'mashup'. (A mashup, according to Wikipedia, is “*a website or web application that uses content from more than one source to create a completely new service.*”)

This way of looking at identity changes the perspective of authentication from being a set of complex rules applied to a simple query based only on identity into a complex query consisting of the identity plus all the context metadata. Instead of one pointer, there are several, combined in a composite record which is split apart for each aspect of the context to be checked. Imagining this being stored as a composite identity record, along with the information or transaction that resulted from the query or task being authenticated has interesting implications for audit and compliance requirements.

With the next generation of smart identification devices around the corner, composite identity and context will take on new meanings. The ID card debate, by its very name, seems to assume a card. Chip and PIN is already obsolescent. NFC, Near Field Communication, will result in identity information of all kinds converging into that most ubiquitous of smart devices, the mobile phone. Why carry cards as well when the data can be wirelessly transferred into the phone almost instantly? The card becomes merely the backup device from which to reload the smart device, which can then be used in multiple contexts at home, at work or at play. Don't think cards with chips, think smart devices with mashups.