Clear Heads Needed for Federated ID

While federated identity has some real potential benefits, great care should be taken before changing the fundamental way people relate to their banks

BY STEPHEN WILSON

One of the more prevalent topics in e-business and security circles is "federated identity". Since the cost, efficiency and convenience of identity management are such hot issues – sometimes they seem to be rated more highly than security – anything with the promise of streamlining can seem compelling.

Yet a clear head is needed when evaluating federated identity. Buzzwords are flying around, and some applications of this new technology may complicate the way banks deal with their customers.

A lot depends on what is meant by "federation", and indeed by "identity" and "authentication". Federated identity advocates say that in the real world we often link together trusted relationships with various parties and so build up a profile that can relied upon by others. Security purists are fond of claiming that identification and authorisation are strictly separate things. There is some truth of course in both these angles (and they're not incompatible) but as is so often the case with new technologies, the whole truth is complex. As much as we yearn for simplification, simple metaphors can be misleading.

So what are we talking about? The Liberty Alliance (www.projectliberty.org) is a big multi-vendor project seeking to establish federated identity standards and methods. They define federated identity as something that "allows users to link identity information between accounts without centrally storing personal information". They add that "in practice, this means that users can be authenticated by one company or website and be recognised and delivered personalised content and services in other locations without having to re-authenticate, or sign on with a separate username and password".

There are two different aspects of authentication at work here. The first has to do with establishing new relationships. How do we come to be known and trusted by an organisation? And when is it useful to parlay one's existing standing to strike up a fresh relationship with someone else? One of the most common metaphors here is the drivers licence. It is said that we "federate" the proof of identity implicit in a drivers licence, when we join for example a video store. This is true in a very restricted sense at the time that we open the account, but thereafter our relationship with the video store is one-on-one. The store gives its members a unique identity card, and the licence is never seen again.

The restriction I mention is that the only attribute of interest to a video store is identity. A drivers licence is useful only because it provides something to go on if the customer absconds with their DVDs. The licence doesn't say anything about the holder's other attributes. Most of our business relationships are rather more complex than DVD rentals.

The second sense of "authentication" has to do with asserting who you are each time you undertake a fresh transaction, usually via some sort of electronic challenge-response. That is, you "knock on the door" of a website, and the server asks "who goes there?". Your response is to present something that proves you are who you say you are, such as a shared secret password, a one-time PIN, a biometric ID, or a smartcard.

A separate problem is authorisation. The requirement here is to assert not only who you are, but what you are; e.g. bank customer number so-and-so, officer of registered business such-and-such, video store member number X-Y-Z. In the real world we act in various capacities depending on what business we're trying to conduct. That is, we make a number of different assertions about ourselves.

It is here that security purists insist on separating authentication (proving who you are, aka your identity) from authorisation (telling which capacity you are asserting) and always requiring that one follows the other. But I don't like to split hairs. In the real world, authorisation is sometimes bound very closely to authentication, so closely that it's unhelpful to tease them apart. We can actually behave according to truly separate identities. Here's an example.

I am an authorised signatory to my company's corporate bank account; I happen to hold my personal bank account at the same institution. Thus I have two different key cards from the same institution. When I bank on behalf of my company, I exercise a different identity. There is no "federation" between my corporate and personal identities; it is not even sensible to think in terms of my personal identity plus my corporate attributes when I am conducting business banking. After all, so much corporate law is all about separating the identity of a company's people and the company itself.

Hence the concepts of authentication and authorisation are not totally disjoint, and it may be more efficient in many cases to allow a single authorisation – in the case above, a corporate bank card – to subsume personal authentication.

Elements of federated identity are of course very useful. There is a lot of merit in the idea of someone passing their 100 point check just once, and being able to refer new service providers back to that original identification.

Authorisation turns out to be difficult to federate. If I have an account with Bank A, what does it matter to Bank B? My relationship with Bank A might help bootstrap a new account with B; for instance, B might be interested in my credit history with A, and of course my 100-point check with A might carry over to B. But once I am up and running with B, then I will have a fresh account, a new key card, different account numbers and so on. In short, I have a brand new identity!

So to a large extent the "federation" concept is an over-simplification. Looking closely at the way we do business, we see that most people actually maintain several different virtual identities. And we should take great care before changing the fundamental way people relate to their banks.

Stephen Wilson is a leading international authority on identity management and information security. In early 2004, Stephen established Lockstep Consulting to provide independent security advice and to develop new smartcard solutions to identity theft.

swilson@lockstep.com.au