A la carte identity

by
Dave Birch <mailto:dave@consult.hyperion.co.uk>
Consult Hyperion <http://www.consult.hyperion.co.uk>

The use of online identity certificates (digital IDs) is growing. There are now two international bank–owned consortia (Identrus and Global Trust Authority) who want to issue digital IDs to bank customers, as do BT, the Post Office and many others. Soon it will become natural to use your digital ID (almost certainly carried in a smart card) to pick up your e–mail or surf the web. Frankly, I'd much rather go to the Guardian Online web site and present the same digital ID that I use at other web sites than have to remember yet another not–very–secure username/password combination. Big Brother's triumph? Actually, it's probably not.

The assumption behind ventures such as Barclays' Endorse or BT's Trustwise is that an individual will have a digital ID that is linked (by a body known as a Registration Authority, or RA) to their real identity. Thus, when you go into cyberspace you can prove who you are. There is a direct mapping between my real identity and one of my e–mail addresses, dgwb@pobox.com, and people can send e–mail to that address in the reasonable assumption that it will reach me. For added security, they might encrypt the message using the public key associated with that address, or for even more security they might demand a certificate containing that public key and signed by some third–party that they trust (*eg,* my bank). The technicalities might be different, but the concept is familiar. I have a true identity, and a Net identity that matches it.

Until the industrial revolution, true identity was the only identity there was. The advent of postal services, cities and payphones (amongst other things) allowed people to exist anonymously. The Net offers new ways to communicate anonymously. Buy a pre–paid mobile phone for cash, for example, and you can make calls without anyone knowing who they're from. Next time you're passing a cybercafé, stop in and get a few anonymous e–mail accounts: Microsoft's Hotmail is one of many such free services. Hotmail have no idea who I am, so even under duress they couldn't tell you. It might be useful to have a couple of anonymous mail accounts hanging around: suppose you want to report some insider dealing to the SFO but don't want the tip to be traced back to you? Hushmail (at www.hushmail.com) is even better, because it's encrypted so if hackers (or your boss) access your e–mail account they can't read it[1].

There is a third way between anonymity and absonymity. Imagine walking into a shop to buy something with your bank card. The bank card has a computer chip on it (as many already do) and, when you are asked to put your finger on a pad at the checkout, the chip tells the merchant's till that the fingerprint is correct. Therefore the merchant's till is happy to accept the bank card, you take your goods and walk out. Where did your name come in to this? The bank knows who you are and guarantees the payment, so why should your name even appear on the front of the card? This is a pseudonymous transaction: the first party (you) knows your identity, the second party (the shop) doesn't know but trusts the third party (the bank).

[1] Please note: the author is a member of the advisory board of Hush Communications plc, the operators of the Hushmail service.

What makes the widespread use of pseudonymous digital IDs a practical solution is that, as the think–tank DEMOS pointed out in their *Future of Privacy* report, there are a great many commercial transactions that do not depend on true identity. If I order pencils online from our stationer, they are not interested in my identity (am I Dave Birch?) but my credentials (am I an authorised purchaser on behalf of my company?). There might be a number of third–parties capable of providing cryptographically unforgeable credentials attached to a pseudonym.British Airways might know that customer 72084392 is me, but no–one else does. Thus if British Airways were to give me an e–mail address (72084392@baexec.co.uk) and a certificate containing that address, signed by them, I could go to other web sites and prove to them that I am a British Airways Executive Club member without letting them know my true identity. If I feel that my privacy is being protected (indeed enhanced) by British Airways in this way, I might feel more inclined to browse around online. If I was caught e–mailing nazi drug–dealing bomb–making material to someone else (perhaps someone from the FBI masquerading as a member of a bomb–making book reading circle) then British Airways (as a law abiding organisation) would, of course, disclose my true identity to the police. One might expect such a condition to be part of their terms and conditions.

Far from being a triumph for Big Brother, the emergence of "identity brokers" offers a way to partition identities in cyberspace and leave privacy decisions in the hands of individuals. It's unlikely that the average person will have hundreds of digital identities, but it's equally unlikely that they'll have only one. They'll have at least two or three. I might have one from the bank that proves I'm Dave Birch the trusted Barclays account holder. I might have one from Tesco that proves I'm Marco Polo the Clubcard holder. I might have one from Disney that says I'm Donald Duck. When I go to a web site, and it asks who I am, I'll have a menu to choose from.

Please note that an edited version of this article first appeared in *The Guardian* (London) in the *Online* supplement (14th October 1999).