What should a secure identity management scheme for the 21st century look like?

Dave Birch of Consult Hyperion, takes some inspiration from TV Science Fiction to explore the concept of a 'Psychic ID' and see if modern technology can help bring his futuristic vision to reality.

The technology needed to create an ID scheme that embodies a vision for the future that works as much for eBay, Barclays and Facebook as it does for border control at Heathrow Airport already exists. Today's technology can deliver far more than politicians, professionals and the public imagine, if they just move away from an 'Orwellian' concept of paper based identity cards. In particular, technology can deliver the apparently paradoxical result of more security and more privacy by exploiting smart cards, biometrics and cryptography, and something we all carry around with us every day... a mobile phone!

This vision for a 21st-century identity scheme is founded on minimising the storage of personal data, alongside a vision that contains some genuine innovation, some excitement and some potential for future development. I would suggest therefore that, as in so many other walks of life, Dr. Who should be our guide.

An idea straight out of Science Fiction?

Many readers will be familiar, of course, with Dr. Who's *psychic paper*. As any devotee of the BBC's wonderful series knows, the psychic paper shows the "inspector" of the paper whatever it is that they need to see. If the border guard is looking for a British passport, the psychic paper looks like a British passport. If the customs officer on Alpha Centuri wants to see a Betelguesian quarantine certificate, the psychic paper looks like a Betelguesian quarantine certificate. The variant I propose is psychic ID. Unlike Dr. Who's psychic paper, psychic ID only shows the inspector what he or she wants to see **if** the holder has the relevant credential. For example, if you are trying to get into a nightclub and you need to prove that you are over 18. The doorman is looking for a credential that proves you are over 18, you show your psychic ID and all it reveals is whether you are over 18 or not. (Your name, age, address, weight and driving convictions are none of the doorman's business.) Your age qualification is all that the doorman is entitled to see, so that is all they do see. Provided you are actually over 18, of course. If you are not, the psychic ID remains blank.

However, since psychic energy does not actually exist, some device or contrivance is needed to act as the interface: the picture would actually be displayed not in the doorman's brain but on the doorman's mobile phone or a turnstile at the nightclub or a small display by the entrance. In other circumstances, someone might be entitled to obtain more information from the psychic ID. Perhaps when I visit the dentist, the receptionist is allowed to know whether I am entitled to free NHS dental care and, and if so, what my health service number is. In that case, provided that my psychic ID recognises the receptionist's authority to ask, the receptionist would see precisely that information. But nothing else.

Security and Privacy risks minimised

The psychic ID will have nothing printed on it except perhaps a photograph of the holder, perhaps some kind of card number for administrative reasons (which is not related to the sector-specific ID numbers that the card stores) and it will divulge nothing except the information that its interrogator is entitled to see. This means that a key feature of the psychic ID must be that it provides only those unique identifying numbers relevant to the questioner. The Dentist's receptionist cannot see my financial services identification numbers, whatever they may be, any more than a bank can see my health service number. If I want to, I can tell the dentist my financial services number, naturally. Similarly, I may wish to tell my bank my health service number. But that is under my control: the dentist cannot obtain the number from my psychic ID and an unscrupulous financial organisation cannot extract my health service number behind my back.

The reason for insisting on this feature is to partition for privacy purposes but also to minimise the impact of data breaches: If hackers break into the dentist's database, all they can obtain is my health service number and they cannot use it to set about looting my bank account.

Virtual 'multiple' identity

It would be crazy, obviously, to design a system for the 21st century that only works in physical, attended environments. In the virtual environment, however, the requirements are more complicated. By connecting my psychic ID to the Internet, remote counterparties can "see" the psychic ID in just same way as the receptionist, cashier and Doorman. I am also assuming here that the psychic ID is being used as a component of some form of user-centric identity management systems, so that each persons' psychic ID card will actually store a handful of different identities, to be used in different circumstances. This is a more sophisticated extension of the psychic ID concept, because in some cases I might be Dave Birch, the UK citizen. In others, I might choose to be Dave Birch the Consult Hyperion employee. In others, Leadbelly Gutbucket, mightiest of the Dwarven heroes of Ravenscrag Pass.

Note that in what I would call a "strongly user-centric" identity management system, I ought to be able to tell my psychic ID who I want to be on a "per transaction" basis, presumably defaulting to the "most" pseudonymous identity because, in the general case, identity is not relevant to a transaction. So, just as the typical wallet contains three or four bank cards, the typical psychic ID will contain three or four identities. While some, perhaps one, of the multiple identities held in the psychic ID will be "underwritten" by the government, in the general case they will be attested to by private organisations: Barclays Bank, perhaps, or Vodafone or the World of Warcraft.

In day-to-day use, in the overwhelming majority of cases where someone will be using their psychic ID, it will not be to show who they are, but rather to prove something about themselves: they are entitled to be in the UK, use the local leisure centre or read a particular e-mail. The psychic ID can disclose the

relevant credentials with no need for access a central database or with the unwarranted disclosure of other credentials.

The smart psychic ID is already available

Of course, the best kind of psychic paper would combine both the smart card and the mutual authentication device, and there is only one realistic candidate for this at present: the mobile phone. They already contain secure SIM cards, have a keyboard, have a display, have communications and with the recent introduction of near-field communication (NFC) in a number of handsets (and if rumours are to be believed, the iPhone 5), able to interact with smart cards (and each other).

One might envisage, to return to the familiar example, that a publican wishing to verify that a patron is of legal drinking age could simply touch his phone to the patron's psychic ID. If the patron's picture is displayed, then they are over 18. If the patron's picture is not displayed, then they are not.

The combination of these tamper-resistant chips, wireless communications, biometric authentication and cryptographic technologies that already exist are more than adequate to deliver psychic ID with all of the desired characteristics. So if we finally couple all this together with the single most important property of the mobile phone being, that everybody already has one - people already take their psychic ID with them wherever they go, we really are a lot closer to my vision of a 21st century ID scheme for the future.