IDIS (2008) 1:189–201
DOI 10.1007/s12394-009-0014-6

Psychic ID: A blueprint for a modern national identity scheme

David G. W. Birch

Received: 17 June 2008 / Accepted: 20 February 2009 / Published online: 28 April 2009

Abstract The issue of identity cards is hotly debated in many countries, but it often seems to be an oddly backward-looking debate that presumes outdated "Orwellian" architectures. In the modern world, surely we should be debating the requirements for national identity management schemes, in which identity cards may or may not be a useful implementation, before we move on to architecture. If so, then, what should a U.K. national identity management scheme for the 21st century look like? Can we assemble a set of requirements understandable to politicians, professionals and the public? We've certainly had some difficulty to date. One reason might be that we lack a compelling, narrative vision. As a result, we're constructing a legacy system that will subvert the rational goals of worthwhile scheme. We're not aiming high enough. The technology, I will argue, can deliver far more than the politicians, professionals and public imagine: In particular, it can deliver the apparently paradoxical result of more security and more privacy by exploiting smart cards, biometrics and cryptography. In this paper, I will set out a high-level vision of what a forward-looking national identity management and identity "card" scheme should look like: Dr. Who's *psychic paper*. Not only is this a simple, clear vision that is familiar to the expert and layperson alike, but it's a very useful artistic representation of the capabilities of the technology. I will further suggest that a utility implementation of identity infrastructure can deliver the on this vision in a practical way, and that all of the technology needed to create an ID scheme for the future already exists.

Keywords Cards · Claims · Identity · Management · Privacy · Pseudonymity · Security

D. G. W. Birch (✉)
Consult Hyperion, Tweed House, 12 The Mount, Guildford, Surrey GU2 4HN, UK
e-mail: dave.birch@chyp.com

1952 calling

The detailed timetable for the introduction of a national identity scheme in the U.K. was announced by the Home Secretary on 6th March 2008 in a speech at the London "think-tank" DEMOS. I was excited to be invited to be present, but to be honest I felt rather let down afterwards. That's because I am (as are many others) a supporter of a national scheme that includes a smart identity card for identity management (Dresner 2008), but I want a modern identity scheme that embodies a vision for the future and works for eBay as well as Barclays, Facebook as well as Heathrow. Unlike many other countries, the U.K. is beginning its transition to the smart identity world with a clean sheet of paper, having no existing identity register or identity card. It therefore had the opportunity to create a modern identity scheme with inspirational properties: using technology to deliver security and privacy in a new way. Yet after all the consultations and consultants, what was announced was a watered-down version of the biometric database originally envisaged, a rather pointless (in my opinion) biographical database and a voluntary card of indeterminate functionality or usefulness.

Especially disappointing is the lack of vision. None of the examples that the Home Secretary gave in her DEMOS speech—opening a bank account, obtaining welfare benefits or checking the status of job applicants—actually require a card (smart or otherwise) or demand any infrastructure beyond a unique identifying number. When you tell the bank your identifying number, they may as well type it into a government web page (after all, there is nothing remotely secret about the identifying number that the government is envisaging) and get back your picture to see if you're telling the truth: no card, no fingerprints, no problem. The government clearly does not envisage the proposed identity card as delivering any more functionality than the cardboard version that was discontinued in 1952.

Yet elsewhere there has been a shift in perspective so that some countries are beginning to look to their national identity schemes to deliver new functionality and new capabilities, not simply to emulate cardboard in a more secure fashion. If we look the around the European Union to see how other schemes are developing, we find that 21 member states either have or are planning to issue smart identity cards and many of these have innovative aspects that are worth studying (Naumann 2008):

- Earlier this year the German government announced that their ID card would use pseudonyms to protect online privacy.
- In Austria, they use sector-specific ID numbers to protect privacy.
- In many Scandinavian countries, the public/private integration is such that people can log on to e-government services using the banking authentication schemes.
- In Belgium, tens of thousands of people every month use their ID cards in PCs to check their own records.
- In Finland, the ID card can now be paired with the OpenID online authentication standard, enabling Finns to use their cards for logging in to any website that accepts OpenID.
- In Estonia, the ID application is being issued in Subscriber Identification Modules (SIMs) by the largest mobile operator, paving the way for citizens to use their mobile phones to access e-government, e-banking, e-commerce and e-everything else securely and easily.

The Home Secretary announced no such functionality or applications. I was looking forward to hearing a vision that would be a testament to British design flair, engineering ingenuity and innovation. I was disappointed to hear nothing of the sort, so rather than criticise I would like to suggest a vision of my own: an ID register that improves security and an ID card that improves privacy.

A vision for identity

Let's create a vision for a 21st-century identity card. Let's create a vision that we can communicate effectively. Let's create a vision that is founded on minimising the storage of personal data (Crosby 2008). Let's create a vision that the public and the government can understand. Let's create a vision that contains some genuine innovation, some excitement and some potential for future development. But most of all, let's create a vision that is founded in the mass media, because that's where the British public get their science and technology education (Lacohee 2007). I would suggest therefore that, as in so many other walks of life, *Dr. Who* should be our guide.

British 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" 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*.

To see what I mean, let's begin with the most mundane of the use cases discussed by the Prime Minister in his speech on security and liberty in June 2008 (Brown 2008). You are trying to get into a nightclub and you need to prove to the bouncer that you are over 18. The bouncer is looking for a credential that proves you are over 18. You show your psychic ID to the bouncer and all it reveals to the bouncer is whether you are over 18 or not. (Your name, age, address, weight and driving convictions are none of the bouncer's business.) Your age qualification is all that the bouncer 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, as shown in Fig. 1.

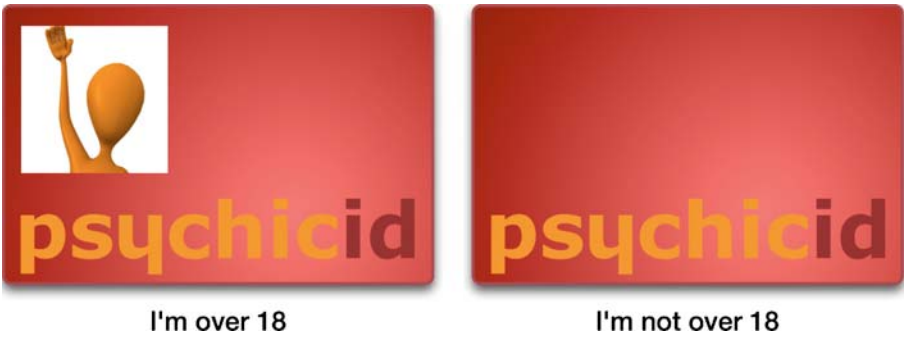

Fig. 1 What the nightclub doorman sees

below. The laws of mathematics, rather than ombudsmen, enforce this mode of operation: no matter how devious, untrustworthy or computer-savvy the bouncer may be, he cannot persuade the psychic ID to divulge anything he does not have the key to.

Practical use cases

It is not possible to envisage every single application of the identity utility infrastructure but we can set out some basic categories by considering two axes: the connection to the NIR (ie, either online or offline) and the transaction locus (ie, either attended, unattended or remote). At high level, the infrastructure would need to be able to support all six categories of use case, each of which would require appropriate authentication to be of practical use. The authentication requirements would naturally vary between these use cases (see Table 1). A PIN might be acceptable for logging in to a chatroom, to point out an obvious case, whereas ordering a new passport might require a higher-integrity "three factor" authentication.

This classification means that we can examine the various possibilities in a structured way, beginning with the most prosaic example: the offline attended situation discussed above, where the ID card holder is trying to prove that they are over 18 in order to get into a nightclub.

Since psychic paper does not, in fact, exist, Fig. 1. is merely a simulation: the picture of my good self or the blank red rectangle cannot be beamed directly into the brain of the nightclub bouncer (yet). Therefore some device or contrivance is needed to act as the interface: the picture would actually be displayed not on the card itself but on the bouncer's mobile phone or a turnstile at the nightclub or a small display next to the door (as shown in Fig. 2), depending on the implementation appropriate to the establishment.

In other circumstances, someone might be entitled to obtain more information from the psychic ID. Perhaps when I visit a polyclinic, the receptionist is allowed to know whether I am entitled to free health care in the U.K. 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, as Fig. 3 illustrates.

The general principle is that if we don't want personal data to leak (as it inevitably will, the more places it is stored (Learning to live with Big Brother 2007)) then we shouldn't give it to people unnecessarily. The government currently plans for the ID card to display a 16 digit national identity registration number, full name,

Table 1 Authentication requirements

	Attended	**Unattended**	**Remote**
Online	At the bank	At the border	At the passport office
	Fingerprint recognition	*Fingerprint & Iris*	*Voice authentication*
Offline	At the nightclub	At the library	At the chatroom
	Face	*Voice authentication*	*PIN verification*

Fig. 2 Psychic ID doesn't actually exist, so we need a device

nationality, date and place of birth, ICAO machine-readable travel document (MRTD) data, and a black and white photo (Hines 2007). I think this is already too much. Let's be ruthless about minimizing the display of personal data: 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 polyclinic 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 clinic my financial services number, naturally. Similarly, I may wish to tell my bank my health service number. But that is under my control: the clinic 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 polyclinic database, all they can obtain is my health service number and they cannot use it to

Fig. 3 What the receptionist at the clinic sees

set about looting my bank account. We cannot assume perfect security and plan on the basis that disgruntled or incompetent employees will never disclose personal data: Consider the recent case of the Chilean government employee who published their national identity register (well, just over half of it) on the web! Partitioning is a simple defence. Thus, when I go to the bank to open an account, the psychic ID shows the bank only the information it is allowed to see (Fig. 4).

I hope it is clear what is being envisaged. In this vision, the national identity card is a special kind psychic paper (without the display) and it is the component of the national identity scheme that makes life ***better*** for citizens because it protects their privacy.

The scheme must improve security as well, and any national identity scheme that is to really deliver more security must be used universally: It must become a kind of utility that both individuals and organisations draw on as and when required. Therefore, organisations would use the same psychic ID system instead of creating their own disconnected, stand-alone versions. By sharing the identity utility infrastructure, the costs are reduced to everyone. The psychic ID works in the same way at the organisational level. If I come along to the Home Office to attend a meeting, then I wave my psychic paper at the guard on the door, who can immediately see (Fig. 5) whether to let me in or not.

Virtual identity

The identity scheme that the psychic ID uses must extend across both real and virtual environments. 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. One of the simplest ways to demonstrate both how non-intuitive some aspects of the problem are, but also how this use of new technology can deliver new solutions, is to consider what I have called before the *Chatroom Paradox*. I can state it very simply in this way: My kids want to go into chatrooms to discuss everything from computer games to saving the planet. I will only allow them into chatrooms if I know that the other people in the chatrooms aren't serial killers, perverts and so forth. In order to make sure of this, I therefore want the name and address of everybody else in the chatroom so that I can validate them against sex-offenders' registers. However, if somebody else in the

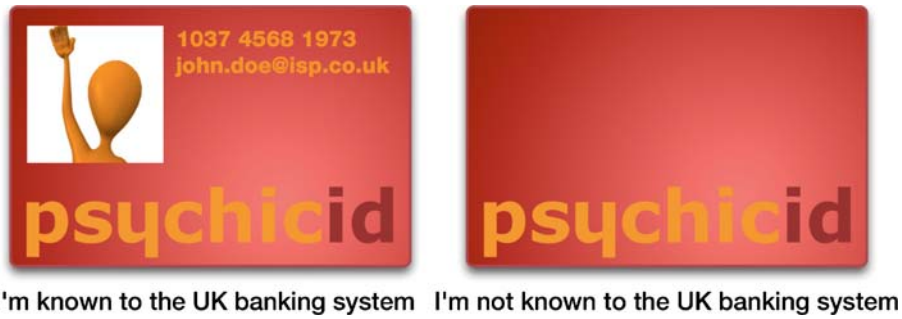

Fig. 4 What the employee of the bank sees

Fig. 5 What the home office security guard sees

chatroom wants my kids' names and address to check them against a register, I don't want to give it to them. What if there's a mistake and they really are a serial killer or pervert? This then is the paradox: In order to harness the power of the Internet, the exponential curve of Reed's Law and the "Here comes everybody" future, I want full disclosure from everybody else who wants to be part of the sub-group but will refuse any kind of disclosure on my side. Stalemate.

Psychic ID to the rescue! By connecting my psychic ID to the Internet, remote counterparties can "see" the psychic ID in just same way as the receptionist, cashier, bouncer and guard. In the chatroom case, however, it is important that the identity is entirely pseudonymous in case there is a breach or a leak. Thus, as shown in Fig. 6, my kids plug the psychic ID into the laptop and punch in the PIN and then their pseudonymous identities are revealed but the actual identities remain concealed (Birch 2003). I am 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. Far from seeing multiple identities as a way for undesirables to hide (Harrison 2007), we should

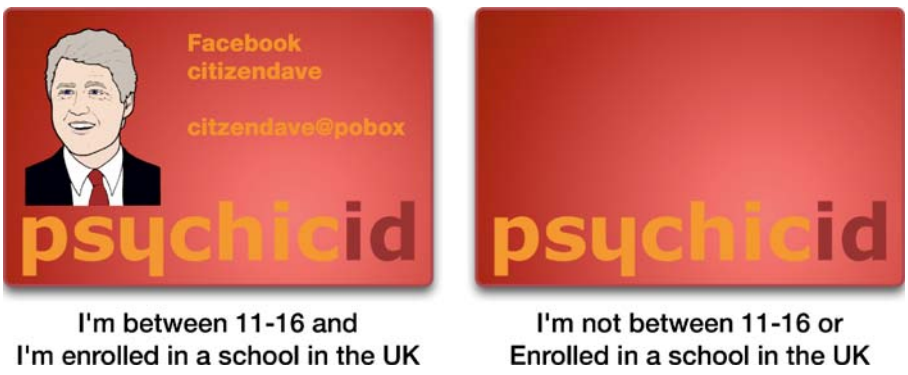

Fig. 6 What the operator of the chat room sees

celebrate them as one of the great benefits of a national identity management scheme. (I've already thought of the tag line for the advertisements: *Who do you want to be today?)*

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[1]. 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*.

These examples serve to illustrate the crucial elements of the identity utility: that it can be used in a variety of circumstances, that it protects personal information to enhance privacy, that it delivers security to where it is needed and that it can be understood by an average member of the public (eg, me).

Building the utility

Now, one might anticipate a certain amount of criticism for basing the vision of a central component of future national infrastructure on a children's science fiction series (although, I have to say, *Star Wars* worked quite well for the Ronald Reagan back in the 1980s). Therefore to demonstrate that this is a practical concept, it's important to explore how the psychic ID would actually work. Is psychic ID like time travel, perpetual motion or Connecting for Health, an appealing vision but something that will never work in the real world, or is it a practical way forward? I claim that not only is it eminently practical but we already have the technology to build it.

Let's begin by picturing the infrastructure that the psychic ID will use. One way to build a practical, useful, successful identity management infrastructure is as an *identity utility* (Hardie 2007). Let us assume that the identity utility will be regulated by the government as a utility, with "OFID" or something like that in charge, but not necessarily provided by the government, and focus on how it would operate rather than who would operate it. The operation of the identity utility would be, from our perspective, founded on five key principles that we can use to guide our thinking on implementation: these are universality, symmetry, speed, practicality and extensibility (McEvoy 2007).

Universality

The process for conducting an identity transaction should be exactly the same, regardless of the status of any individual: nobody (not even the government) should

[1] One might further imagine brokers springing up to manage identity and credentials on behalf of individuals, both in the customer relationship management (CRM) model of the kind envisaged by John Harrison with eDentity and in the vendor relationship management (VRM) model of the kind envisaged by Adrianna Lukas with *The Mine*.

be privileged within the architecture. It must be no less applicable to two people from different continents as to next-door neighbours: everyone should be able to inspect psychic paper. They may not see anything, of course, but they should be able to try. To meet the international requirement, it may be that the involvement of private sector organisations that are used to fielding worldwide, personal, interoperable technology—the payment card schemes and/or the mobile network operators make obvious candidates—is probably desirable.

Symmetry

It is vital that within the same hardware and software identity scheme "package" (available to everyone because of the universality) is the means not only for the holder to assert an identity or credentials, but to verify anyone else's. This is another improvement on Dr. Who's basic scheme: my psychic paper and your psychic paper can validate one another, if needed. In this way, everyone bears the same relation to everyone else; the identity transaction does not in itself place one party in any kind of authority over another. Just as a policeman may have a perfectly valid reason to understand who I am (to a certain level of detail), so it may be important for me to know the same of him: at least that he actually is a policeman (which may be all that his psychic ID is permitted to show me); and that the same policeman is the one who appears in court to give evidence against me. By the same token, a gas board official to whom a leak has been reported may wish to know that my elderly mother is the householder of the property he is visiting; and she will want to know that he is a duly accredited person with a right of entry into her private property.

Note that there is no suggestion that the symmetry is exploited automatically. If the person entering the nightclub is trying to prove that they are a policeman, then the "IS_A_PLOD" credential must be present. On the other hand, if the person trying to enter the nightclub is trying to hide that they are in fact a policeman, then the "IS_A_PLOD" credential must be concealed. This means that counterparties cannot have uncontrolled access to all credentials. ID card holders must have the ability to turn certain credentials on or off (or, more likely I think, display or conceal particular virtual identities). For most people, most of the time, this is not a problem but it must be addressed for the hard cases where it applies.

It is a matter for further consideration as to whether this ability should be universal or whether there should be one or more "reserved" virtual identities that cannot be disabled. Note also that while it may seem tedious to have to find terminals to change data on the card, if the ID card is implemented in a phone these issues (setting default identities, enabling and disabling identities and so forth) become trivial.

Speed

There is no greater barrier to adoption at the consumer level than inconvenience and speed is fundamental to overcoming that barrier. For such a scheme to be become a part of the fabric of life, psychic paper must be usable in the widest possible range of circumstances and, in particular, in ordinary circumstances, such as a face-to-face meetings. When it is thus familiar, it can move into other territory, for example

remote transactions, for which there is no very good existing means of identity verification—certainly not one that has achieved anything close to ubiquity. In fact, as the escalating figures for "card not present" payment fraud in the U.K. demonstrate, such means have proved elusive even in face of significant financial incentive, let alone government policy.

In order to displace familiar mechanisms (as a first step to achieving still wider utility), an identity utility must be better than them. We imagine that the benchmark should be the swapping of business cards, so that the transaction should take no more than a second or two. Of course, by digital means, other aspects of the transaction can be improved within this transaction timescale: in particular, by the use of cryptography, the privacy and integrity of the transaction can be improved by several orders of magnitude.

Practicality

We must understand that the security demands of an identity infrastructure are such that software solutions are not, by themselves, adequate to implement psychic ID. There has to be some "token", some item of tamper-resistant hardware (such as a smart card) in addition to whatever device is being used for mutual authentication. Of course, the best kind of psychic paper would combine both the smart card and the mutual authentication device. 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 will soon, with the introduction of near-field communication (NFC) be able to interact with smart cards (and each other) in high-speed zero-configuration exchanges (Birch 2004). Thus, the swapping of business cards will be accomplished by "kissing" phones[2]. In an instant, verified contact details will be swapped, will appear on screen, and can be filed automatically in the phone's address book. The same identity transaction might be achieved by other means according to convenience: by Bluetooth across a room; by SMS or data connection to the next county; via USB cable and an internet-connected PC across the world. As has been clear for some time, mobile operators will have a critical role to play in the future of identity management (Edwards and Fieschi 2008), and the introduction of NFC will further emphasis their key position.

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, as illustrated in Fig. 7. If the patron's picture is displayed, then they are over 18. If the patron's picture is not displayed, then they are not. Please note that the phone in Fig. 7 is not an artist's impression: it is a Nokia 6131NFC, as used by Barclays Bank, mobile operator O2 and Transport for London in a London pilot scheme that allowed customers to get on the bus and buy a coffee simply by waving the phone over a suitable reader (eg, the same technology as the yellow buttons used with *Oyster* contactless cards in London's mass transit system). Such phones are already in use for mass transit in Vienna and Frankfurt and tens of

[2] "Kissing" is not a technical term: it just what we at Consult Hyperion have taken to calling zero-configuration NFC peer-to-peer connections.

Fig. 7 The "real" psychic paper

millions of similar phones are in use in Japan, where consumers seem very happy to use their mobile phone instead of plastic cards (Ohashi 2007).

Incidentally, while we haven't focused on authentication (I've simply assumed that the psychic ID will have a PIN and a local biometric for the verification of the holder) mobile phones can also capture and transmit the most natural and convenient biometric: voice. Challenge/response mechanisms, whereby the parties may ask each other to repeat a random phrase, make remote and secure biometric authentication more practical than other methods, and avoid the negative connotations of fingerprints and iris scans.

Finally, the single most important property of the mobile phone is that everybody already has one. People already take their psychic ID with them wherever they go.

Extensibility

An infrastructure is something that can be built on and anyone should be able to do this: much as the government builds roads and lets private companies design and build cars, so anyone should be able to access the identity infrastructure. This has some obvious implications around standards and interfaces: psychic ID needs to be founded on the right standards, of course, but there are plenty to choose from. The government should choose a profile through existing standards to define the U.K.'s psychic paper implementation and the standards within that profile should be where possible open. The security of the implementation should rest on secret keys, not secret implementations: The recent tribulations of the Dutch national transit implementation bear witness to this straightforward principle.

Note the critical architectural assumption underlying these requirements, which is that none of the service providers can obtain the sector-specific identity number to which they are entitled without going via the centralised identity broker that sits in front of the NIR or the decentralised identity broker built in to the NIC.

Magic

We can implement an identity utility that meets all of these requirements through the magic of cryptography. Take the example cited repeatedly in this paper, the use of psychic ID at the nightclub. What is happening "under the hood"? In this example, the steps might be as follows. The identity card reader at the door of the nightclub sends a challenge to the customer's psychic ID: let's assume that it is a simple card rather than a mobile phone. The challenge is, as previously noted, not really sent via psychic brainwaves but via a very short-range radio-frequency communication at 13.56MHz (ISO standards 14443 and 18000). The challenge is signed using the private key of the nightclub and is transmitted to the card together with a digital certificate (digitally-signed by the Home Office) containing the nightclub's public key. This certificate tells the card that the nightclub is licensed to request age verification. The card sends back the picture of the cardholder if the cardholder is over 18 or a picture of a red "X" if the cardholder is under 18, digitally encrypted using the nightclub's public key that was contained in the certificate. This ensures that only that specific nightclub can decode the message: Eavesdroppers cannot. The nightclub reader decodes the message and displays the cardholder picture: The nightclub doorman can easily see that the picture is, say, me and then let me in. All of this takes place in a few hundred milliseconds, using tried and tested contactless technology.

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. None of these technologies have to be perfect in order to function together in a properly-designed system that can tolerate imperfection: so, if the tamper-resistant chip is counterfeited that should not mean that a biometric database entry can be duplicated (in other words, counterfeit cards should not mean counterfeit identities) and, similarly, if the database is compromised so that the biometric record can be altered that should not mean that the on-card biometrics are changed.

Practical solution

Smart cards can do things that cardboard cards cannot (Birch 1996): This, fundamentally, is why we need a new vision for national identity management that is beyond the scheme abandoned by the U.K. in 1952 (Birch 2005). The *psychic ID* vision for identity leads to an eminently practical solution that delivers the apparently contradictory result of more security and more privacy, using existing technology in an open and extensible way, allowing a new identity ecosystem to grow and flourish. Essential to this practical implementation is the smart identity device (which may be a card, mobile phone or something else in the future) that uses the principles discussed in this paper. 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 card can disclose the relevant credentials with no need for access a central database or with the unwarranted disclosure of other credentials—using well-known

and well-understood cryptographic techniques—and this is what make will make it a 21st century card (Birch 2007).

Acknowledgements Many thanks are due to my colleague Neil McEvoy for his concise statement of the central principles of the identity utility concept, to Piotr Cofta of BT for his detailed and constructive criticism of the psychic ID concept, to Caspar Bowden of Microsoft for his helpful comments on an early draft of this paper and to Sara Marshall of the U.K. Identity & Passport Service for challenging me to find new and better ways to explain identity concepts rooted in technology.

References

Birch D. Smart cards and pseudonymity. London, IBC: Smart Card Technologies; 1996.
Birch D. Who do you want to be today? Public Service Magazine**:** 7; 2003.
Birch D. The identity management market—who could the future players be?. London, IIR: Identity Management Summit; 2004.
Birch D. A better class of ID card. Prospect. 2005; 44-47.
Birch D. Making national identity work. London: Prospect; 2007.
Brown G. Security and Liberty. Retrieved 17th Jun., 2008, from http://www.number-10.gov.uk/output/Page15785.asp. 2008.
Crosby J. Challenges and opportunities in identity assurance. London: H.M. Treasury; 2008.
Dresner D. So, what are ID cards for?. NCC: IT Advisor; 2008.
Edwards C, Fieschi C. UK confidential. London: DEMOS; 2008.
Hardie A. Chips or mash?. London, BCS: ISSG Information Privacy Day; 2007.
Harrison S. The view from government. London, Westminster eForum: Big Brother Britain; 2007.
Hines D. A view from the identity and passport service. Ensuring privacy and consent in identity management infrastructures. London: Kable; 2007.
Lacohee H. Trustguide. Ensuring privacy and consent in identity management infrastructures. London: Kable; 2007.
Learning to live with Big Brother. The economist; 2007
McEvoy N. e-ID as a public utility. European e-Identity. Paris: EEMA; 2007.
Naumann I. Privacy features of European eID card specifications. The European e-Identity conference. The Hague: EEMA; 2008.
Ohashi I. NTT DoCoMo case study. NFC technology & applications forum. Barcelona: Marcus Evans; 2007.